Framework for Minimizing Critical Information Infrastructure Threats from Insiders

إطار لتقليل تهديدات بنية التحتية المعلوماتية الهامة من قبل العاملين

by

AHMED OMAR AL KATHEERI

A thesis submitted in fulfillment

of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN COMPUTER SCEINCE

at

The British University in Dubai

October 2017

Framework for Minimizing Critical Information Infrastructure Threats from Insiders

إطار لتقليل تهديدات بنية التحتية المعلوماتية الهامة من قبل العاملين

By

Ahmed Omar Abdulla Al Katheeri

A thesis submitted to Faculty of Engineering and Information Technology in fulfillment of the requirements for the degree of

Doctor of Philosophy in the Computer Science

at

The British University in Dubai
Oct, 2017

Dr. Cornelius Ncube

Approved for award:

____

Name

Designation

____

Name

Designation

____

Name

Designation

____

Name

Designation

DECLARATION

The research presented in this thesis has never been previously presented or submitted as part of the process for completing diploma, higher diploma, bachelor, master or any other higher education qualification degrees. The thesis does not contain any previously published work or material written by other researchers except the referenced works.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder maybe copied and distributed by The British University in Dubai for the purpose of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution , where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that U may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Signed : Ahmed Alkatheeri

Date : 30-10-2017

COPYRIGHT AND INFORMATION TO USERS

Abstract

Malicious insiders are posing unique security challenges to organizations due to their knowledge, capabilities, and authorized access to information systems. Data theft and IT sabotage are two of the most recurring themes among crimes committed by malicious insiders. This research aims at investigating the scale and the scope of the risks from malicious insider's activities and exploring the impact of such threats on business operations. The developed framework targets minimization of the insider threats through profiling the user activities using information from the log files of several components participating in these activities, like IDS, IPS, firewalls, network devices, sever hosts and workstations.

Malicious activities potentially leave suspicious patterns and references to users which can be used to infer the main actor or actors and mitigate the threat before they actually occur. The analytical backbone of the framework can be build upon Actor Network Theory. Organizations need to implement a multi layered defensive approaches to combat insider risks; safeguarding sensitive business information from malicious insiders requires an effective security framework that can identify the malicious group members involved and predict their offensive intentions something like a black box. To open this black box and explore the intention of the insiders, the framework developed here relies on two different security technologies: Security Information Event Management (SIEM) and User Behavior Analytics (UBA). They allow extracting the data from different entity logs, analyzing and separating the malicious activities from non-malicious ones on the base of the User Security Profile (USP). On the other hand, the security engine must allow formulating different hypothesis, which have varying degree of flexibility to address the security requirements and have the ability to identify the main actor and the other participants using analyzed information.

Organizations need to implement multi layered defensive approaches to combat insider risks; safeguarding sensitive business information from malicious insiders requires an effective security policy that communicates widely the consequences of stealing or leaking confidential information in an unauthorized manner. Secondly, logging and monitoring employee activity is essential in detecting and controlling system vulnerabilities. Thirdly, conducting periodic and consistent vulnerability assessments is critical to identify any gaps in security controls and to prevent insiders from exploiting them. And last, but certainly not least, taking extra caution when dealing with privileged users is important to proactively protect the information infrastructure from insider risks.

نبذة مختصرة عن البحث:

يعتبر العاملين ضمن المؤسسة أحد تحديات الأمنية و الفريدة من نوعها على المؤسسات و المنظمات سواءا حكومية و خاصة بسبب معرفتهم وقدراتهم وإمكانية الوصول المصرح بها إلى أنظمة معلومات الهامة . سرقة البيانات و تخريب بنية التحتية المعلوماتية هما من أكثر المواضيع المتكررة بين الجرائم التي يرتكبها المتخصوصون من الموظفين ضمن المؤسسات. يهدف هذا البحث إلى التحقق من مدى و نطاق المخاطر من الأنشطة الخبيثة ضمن المؤسسة واستكشاف تأثير هذه التهديدات على عملية استمرارية أعمال اليومية الحيوية. يهدف هذا الإطار المطور إلى تقليل التهديدات الداخلية من خلال تصنيف أنشطة الالكترونية للموظفين و ذلك من خلال استخدام معلومات من ملفات السجل الخاصة (Logs) و التي يتم إصدارها من قبل أجهزة شبكية مختلفة مثل IDS و IPS وجدران الحماية وأجهزة الشبكة والمضيفات الثابتة وأجهزة كمبيوتر الشخصية.

من المحتمل أن تترك الأنشطة الضارة أنماطًا وإشارات مشبوهة للمستخدمين يمكن استخدامها لاستنتاج شخص المحرض أو الممثل الرئيسيين والتخفيف من التهديد قبل حدوثه فعليًا. يمكن بناء العمود الفقري التحليلي للإطار على نظرية فاعلية الشبكة (Actor Network Theory). تحتاج المنظمات إلى تطبيق مناهج دفاعية متعددة الطبقات او المستويات لمكافحة المخاطر الداخلية ؛ تتطلب حماية معلومات الأعمال الحساسة من المطلعين الداخليين الخبيثين إطارًا أمنيًا فعالًا يمكنه تحديد أعضاء المجموعة الخبيثة المتورطين والتنبؤ بنواياهم الهجومية مثل الصندوق الأسود. لفتح هذا الصندوق الأسود واستكشاف نية المجموعة ، يعتمد الإطار الذي تم تطويره هنا على تقنيتي أمان مختلفتين: إدارة أحداث معلومات الأمان (SIEM) وتحليلات سلوك المستخدم (UBA). فهي تسمح باستخلاص البيانات من سجلات الكيانات المختلفة ، وتحليل الأنشطة الخبيثة وفصلها عن الأنشطة غير الضارة الموجودة في قاعدة بيانات انشطة المستخدين الشخصية (USP). من ناحية أخرى ، يجب أن يسمح محرك الأمان بصياغة فرضيات مختلفة ، تتسم بدرجات متفاوتة من المرونة للتعامل مع متطلبات الأمان ولديها القدرة على تحديد الجهة الفاعلة الرئيسية والمشاركين الآخرين باستخدام المعلومات التي تم تحليلها.

تحتاج المنظمات إلى تطبيق أساليب دفاعية متعددة الطبقات لمكافحة المخاطر الداخلية ؛ إن حماية معلومات و البيانات الحساسة من المطلعين الداخليين ذو نوايا خبيثة تتطلب سياسات أمنية فعّالة تتحدث على نطاق واسع عن عواقب سرقة أو تسريب معلومات سرية بطريقة غير مصرح بها. ثانيًا ، يعد تسجيل ومراقبة نشاط الموظفين أمرًا أساسيًا في اكتشاف الثغرات الأمنية للنظام والسيطرة عليها. ثالثًا ، يعد إجراء تقييم دوري ومتسقة للضعف أمرًا بالغ الأهمية لتحديد وجود أية فجوات في عناصر التحكم الأمنية ومنع الجهات الداخلية من استغلالها. وأخيرًا ، ولكن بالتأكيد ليس آخراً ، من المهم اتخاذ المزيد من الحذر عند التعامل مع المستخدمين خاصة الذين لديهم خبرة كافية عن تكنولوجيا المعلومات لحماية البنية التحتية للمعلومات بشكل استباقي من المخاطر الداخلية.

Acknowledgement

Thanks to God Almighty, who guided us throughout the whole PhD programme. This study has been completed thanks to the support and cooperation with different authorities, staff, organizations, companies and persons to which I owe my sincere gratitude.

I extend my heartfelt thanks and gratitude to my instructor and supervisor **Dr. Cornelius Ncube,** lecturer at the School of Engineering and Information Technology, British University in Dubai for his supervision and guidance at most stages of this research study. The competition of this thesis could be very difficult to achieve without his valuable guidance and encouragement.

Also, I extend my thanks and appreciation to my family who suffered from the lack of the attention and consideration they deserve during the period of research.

Table Of Contents – Volume 1

Chapter 4: Research Methodology.

Chapter 5: Implementation, Results and Discussions.

Chapter 6: Conclusions and Recommendation for Future Work.

List of Tables

Table Content **Page**

-List of Figures.

Figures **Page**

List of Abbreviations

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ANT	Actor Network Theory
SIEM	Security Information Event Management
UBA	User Behavior Analytic
SE	Security Engine
CI	Critical Infrastructures
CII	Critical information infrastructures
CIIP	Critical information infrastructures Protection
ICT	Information and Communication Technology
ISP	Internet Service Provider
LAN	Local Area Network
WAN	Wide Area Network
NIAC	National Infrastructure Advisory Council
CISAC	International Security and Cooperation
POC	Prove of Concept
CERT	Centre of Excellence for Applied Research & Training
ECI	European Critical Infrastructure
DHS	Department of Homeland Security
SCADA	Supervisory Control And Data Acquisition
UNE-G	United Nation E-government
WEF	World Economic Forum
GITR	Global Information Technology Report
CICPA	Critical Infrastructure and Coastal Protection Authority
CNIA	Critical National Infrastructure Authority
GIS	Geographical Information System
ADSIC	Abu Dhabi Systems & Information Center
NESA	The National Electronic Security Authority
DDoS	Distributed Denial-of-Service
VPN	Virtual Private Network
PAAS	Platform As A Service
RAM	Read Only Memory
VoIP	Voice Over IP
ECB	The European Council of Barcelona
INCIIPC	The Indian National Critical Information Infrastructure

	Protection Centre
NAERC	North American Electric Reliability Council
FIA	Freedom of Information Act
ORCON	Originator Controlled dissemination
FISMA	Federal Information Security Management Act
ISAC	Information Sharing and Analysis Center
CI - KR	Critical Infrastructure Key Resource
UIT	Unintentional Insider Threat
APT	Advanced Persistent Threat
ITSR	Insider Threats Spotlight Report
CIA	Central Intelligence Agency
NSA	National Security Agency
USSS	United States Secret Service
IT	Information Technology
OPP	The Obligatory Passage Point
IAPP	International Association of Privacy Professionals
LIDS	Log based Intrusion Detection System
KPIs	Key Performance Indicators

Chapter 1: Introduction

1.1 Introduction

Malicious insiders are posing substantial security challenges to the organizations due to their inside knowledge, professional capabilities and authorized access to information systems containing sensitive and valuable business information. Data theft and IT sabotage are two of the most recurring themes among the crimes committed by malicious insiders. This research aims to investigate the scale and the scope of risks of insider malicious activities and to explore the impact of such threats on business operations.

The framework developed here targets minimizing the insider threats through profiling the users and controlling user activities using the information from log files of key infrastructural components, such as IDS, IPS, firewalls, network devices, sever hosts, workstations, etc. Through the use of the information about user activities stored in log files one can reveal suspicious patterns of behavior and can expose hidden links between different users which can help identifying the main and collaborating actors and can help in mitigating the threats before the actual damage occurs. A framework which allows applying this method can be built upon Actor Network Theory. To analysis the logs based activities two different approaches are being used: Security Information Event Management system (SIEM - Data analysis) and User Behavior Analytic System (UBA - Data Mining). The main result of using the framework will be the creation of a custom-built Security Engine (SE) which will analyze the user activates based on the user profiles created by SIEM and UBA in order to identify the main and collaborating malicious actors.

The organizations need to implement a multi layered defensive approach to combat insider risks. Firstly, safeguarding sensitive business information from malicious insiders requires an effective security policy that communicates the consequences of stealing or leaking confidential information in an unauthorized manner. Secondly, logging and monitoring the employee activity is essential in detecting and controlling the system vulnerabilities and their potential exploitation by malicious insiders. Thirdly, conducting periodic and consistent vulnerability assessments is critical for identifying any gaps in security controls and preventing insiders from exploiting them. And last but not least, taking extra caution when dealing with privileged users is important to proactively protect the information infrastructure from insider risks.

This thesis is concerned with the frameworks - theoretical and software framework for developing of software engines capable of profiling the user behavior, recognizing the malicious activities and identifying the key actors through security logs analysis. The research investigated the frameworks in the context of ‘research intelligence’ applications which involve data analytics to distinguish malicious from non-malicious insider actors within the organization.

Our work brings together the otherwise disparate research traditions of higher-order computational logic and workflow systems; as such, this thesis constitutes a bridge between the Critical Information Infrastructures protection which includes both ICT components and different type of insider users within the organizations.
In this first chapter a range of research intelligence use cases that motivate the work will be introduced, the software architecture will be outlined and the theoretical foundations on which the proposed frameworks are based will emerge. The research question will be also formulated and the potential contribution to knowledge will be coined.

1.2 Motivation

Critical Infrastructures (CI) provide services that support our society and economy, while Critical Information Infrastructures (CII) contain ICT components used by interconnected computers to support the information flows between them. This includes databases and other data repositories, networks and communication infrastructure. Critical information infrastructures (CII) are vulnerable to cyber-attacks and breaches. It is widely accepted by most of the specialist that protecting them is very difficult due to the characteristics of critical information infrastructures (“CII” or “CIIs”) which are deeply interconnected and complex by design as well as geographically dispersed.

Critical Information Infrastructures (CIIs) are one of the most crucial technical and economic systems that have an impact on organizational facilities, utilities and services of importance for the organizations and companies. In the case of improper operation of the CII, this would lead to disruption of other dependent services.

The Emirate of Abu Dhabi is currently implementing a complex program through which it aims to build public services using computer, communication and software technologies. In this program the Government of Abu Dhabi has adopted the vision of an E-Government which aims at "building a high performance government that delivers world-class services to all its customers." E-Government has several definitions with close objectives; the 2002 United Nations definition of E-Government is “the use of the Internet to provide information and services to citizens". The vision of The Emirate of Abu Dhabi has been translated into an E-Government strategy that focuses on customer care and efficacy. In this understanding the efficacy of a service means maximizing the satisfaction of service recipients by achieving operational efficiency and accuracy, by shortening the time, reducing the cost for completion of the transactions and maximizing the information. In this understanding one should not forget the coordination between different government agencies which complement each other's work to achieve efficiency and transparency.

As Abu Dhabi Police General Headquarters (AD GHQ) is an integral part of this government it also aims similar achievements in accordance with the vision of the Government of Abu Dhabi 2030. AD GHQ is keen to apply the best international practices through smart applications and systems to provide digital services to the public by all ways and means available. The most prominent of them are available in the Internet and are mirrored in the local intranets. Such systems are available to the public through the technologies developed for the Internet, and the user can use them to access different available public electronic services after local registration on site. This would enable the users to access a lot of services in a safe and easy way and especially services related to the control of file traffic.

The availability of smart services to the general public at all time (24/7) depends entirely on the Critical Information infrastructure (CII) and its Information and Communication Technology (ICT) components. They include three main components: computing equipment (hosts, databases and application software) as well as networks (LAN, WAN technology) and communications (ISP and connection lines).

Due to its importance for the uninterruptable business operations, which is one of the most fundamental and strategic objectives of any sector, the Information infrastructure needs to be protected and secured from all forms of threat - whether traditional, such as physical targeting, or non-traditional, such as electronic break through or accidents. Such threats can cause large losses as a result of the damage to the infrastructures, the reputation of the organization and the confidence of its customers.

The organization in which the researcher is working provides most of the services to the society and has become increasingly dependent upon the information and communication technologies. So protection of Critical information infrastructure (CIIP) is a key priority for this organization.

According to (Marwan, 2015) about 70 percent of the threats to an organization's network infrastructure originate in insider users, while most of the business organizations invest in their computational resources to protect their assets from malicious activities coming from outside. Moreover, many organizations ignore the rising threats from malicious inside users (*insiders*) who can use their authorized and privileged authenticity to access information systems and steal or modify sensitive data that could affect the reputation of the organization due to the loss of integrity.

According to Vormetric Insider Threat Report which has been produced by Vormetric Data Security Center (Poll, 2015) more than 89 percent of organizations globally felt they are at risk from an insider attack, while above 34 percent felt they are extremely vulnerable. In the same report they found that the biggest internal threat to an organization posed from privileged users with 55 percent; the contractors and service providers came second with 46 percent and then the business partners with access to the organization assets with 43 percent.

The insider malicious activities can be hidden by distributing among different devices and spreading them over different time frames so that even if the malicious behavior is identified, it doesn’t help much to be linked to a specific user - i. e., " the lack of contextual information from security tools" is considered the biggest barrier to determine if insiders poses a threat (Ponemon Institute LLC, 2014).

On the other hand, the main factor that supported the decision to initiate this research was the availability of two different security tools: the User Behavior Analytics (UBA) and the Security Information Events Management (SIEM). These two security tools are typically working separately in different fields while the proposed solution combines them together to works as one entity to get the maximal advantage from each of the two security technologies behind them.

1.3 Statement of the problem.

The National Electronic Security Authority (NESA) is a government body involved with protecting the UAE’s critical information infrastructure and improving national cyber security that support organizations. It is dedicating time, efforts and money to identify and protect the CII services within the United Arab Emirates and for this purpose it has released a set of standards and guidance for government entities in critical sectors. These regulations are different depending on the type of organization, the geographical location, the services, responsibilities and priorities.

The problem of protecting the Critical Information Infrastructures (CIIs) of organizations and institutions which are providing e-services lies in its focus on protecting the vital infrastructure for serving beneficiaries from outside. They are typically benefiting from very high value services and are not focusing adequately on the employees within the organization in different positions.

Different levels of protection are built for infrastructure devices to ensure their efficiency, continuous operation and non-penetration by hackers. On the other hand, the best international practices applied to employees for ensuring that they do not exceed the privileges granted to them are typically controlled by application of strict security policies, which are supported by different methods for monitoring the electronic activities of the employees within the organization. But all these precautions do not prevent all possible breakthroughs or excessive uses of privileges by the staff who can use their own extensive experience and competence in the area of specialization and their own knowledge of the organizational weaknesses and gaps that may be missed by the eyes of the censorship.

In addition, in some cases the staff may work in small groups that are rationalized or given instructions by a person who serves his own interests and goals, whether criminal or not. He might be exploiting their psychological, family, or health status to let them work in an unnoticed manner as shown in the figure 1.1 below (the black box).

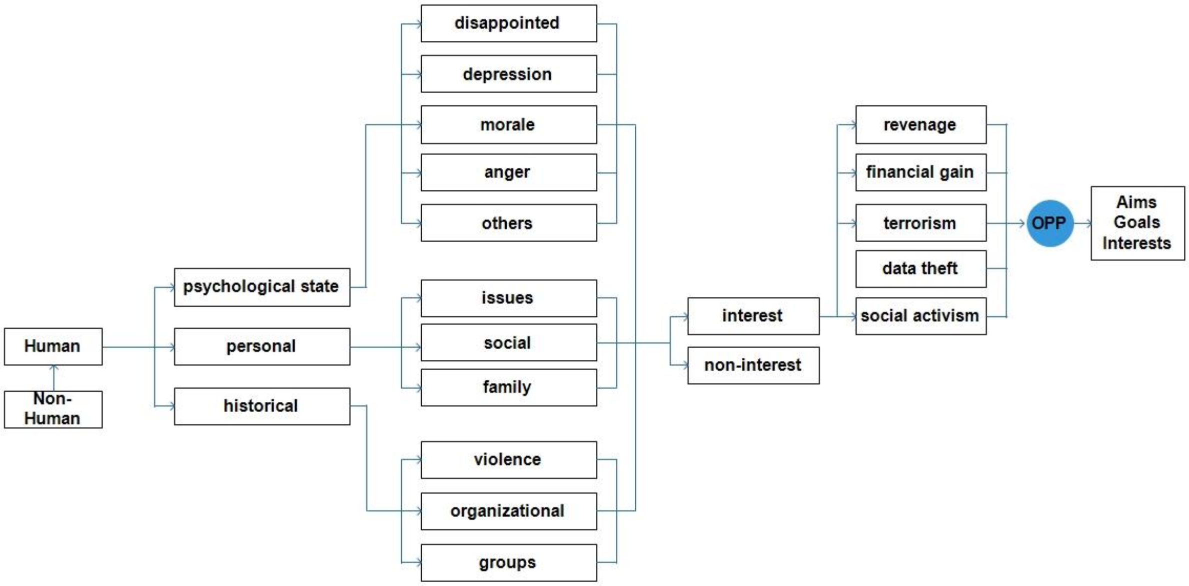


Figure 1-1: Insiders status

The biggest issue with this type of insiders is that they act secretly and it is very difficult to distinguish between malicious and non-malicious behavior. The behavioral drivers are very difficult to analyze through normal observations which makes impossible to predict the attitude or intention of the employees who are preparing different types of attacks. In most cases the individual user's decision to become involved in malicious activities is related to the benefits which these individuals expect to get as a result of engaging in such activities, but often this behavior is also influenced by internalization of the interests, goals, targets or beliefs of other people.

In order to identify the main influences, the different collaborating actors as well to detect the malicious behavior patterns, the analysis can be customized and/or automated. This can be done through a software engine which tracks the activities, creates hypothesis and identifies the keys that indicate malicious activities and suspicious. Such an engine would register various events:

1. General Authentication Failed.
2. Remote Login Failure.
3. Remote Login Success – Odd hour.
4. User Login Failure.
5. Excessive Firewall Denials between Hosts.
6. New Account Use Detection (UBA).

7. Malicious Exploits.
8. User Access at Unusual Times (UBA).
9. Multiple login failure.
10. Successful Admin Login at odd hours.
11. Successful General Authentication at odd hours.
12. Brute Force.

The hypothesis about the possibility of occurrence of insider threat activities in the case of observation of specific events can result in the formulation of additional heuristics which guide the process:

- The higher the number of brute force successful logins in odd hours from a user, the higher the chance for involvement in suspicious activity by that user.
- Users with high number of brute force logins along with high number of login failures have higher chance of involvement in malicious activity.
- The higher the count of successful logins at odd hours, the higher the chance of malicious activity.
- Users with high count of login failures have higher chance of involvement in malicious activity.
- Users with high count of login failures in odd hours have higher chance of involvement in malicious activity.
- Users having high number of malicious exploits have higher chance of being involved in malicious activity.
- Users having high number of malicious exploits at odd hours have higher chance of being involved in malicious activity.
- The higher the count of account privilege changes in odd hours, the higher the probability of malicious activity.
- Users with account added to Admin group in odd hours have higher chance for involvement in suspicious activity.

1.4 Aims and objectives of the study.

Malicious insiders, especially the formal employees of organizations, are posing unusual security challenge to the organizations because of their skills, experience and privileged access to information resources. Insider threat is an issue that causes nightmares to most of the organizations. The main reason for this is the fact that employee’s unnoticed behavior and activities and any type of unawareness or neglect can lead to heavy incidents which the organizations cannot overcome for a long time. So the main aim of this study is to construct a framework which minimizes the Critical Information Infrastructure threats from insiders, as well as proposes preventive and protective measures for the insider threats to be identified before they actually manifest themselves.

Furthermore, the solution will be sought by analyzing the behavior of different users in order to recognize the factors that could influence their decision to join the Actor Network. This approach will be used also to identify the influence of the main actor over other users to accept his plans or to pursue his own interests, goals and targets. The same approach will be used to identify the members of the groups with malicious intentions in order to mitigate the insider threat.

On the other hand, the main objectives of this study are to find the main actor, to fill the gaps in the security policies and to reduce the investments needed to protect the critical infrastructures from known threats while ignoring unknown threats like insider employee threats.

The first objective of this study is to find out the main actor who exploits the physical, psychological, personal, financial and historical state of some insiders to form a malicious network, forcing them to adopt his own interest, to achieve his goals and to execute his plans. This objective can be achieved only through balanced and systematic planning framework with a model that covers all aspect of the process.

Secondly, most of the organizations depend mainly on security policies and guidelines which prescribe log monitoring and auditing applications to protect their assets from insider threats. Unfortunately, most of these approaches can't stop insider threats which are becoming more and more sophisticated and continue searching for ways to exploit any gaps in security policies and hide their footprints after committing attacks from inside. The study fills this gap by introducing a new theoretical model for maintaining user security profile which incorporates all initiatives that may be needed to improve the technical guidelines and organizational security policies in affective manner. This proactive approach is likely to protect any organizational information infrastructures also from dissatisfied employees or employees who are facing physical, social, financial or mental problems (Omar, 2015).

Thirdly, in the field of insider threats to the Critical Information Infrastructure (CII) the National Infrastructure Advisory Council (NIAC) found a gap in insider threat awareness in many organizations. These organization need to improved their security information sharing method to help them in the process of making security investment decisions.

The Figure 1-2 below shows the dependence between the cost of investment and the level of security vulnerability. We can observe that most of the security investments are spent for protection against known threats from outside users, while the investments in protection from insider threats are not a match to it since they are lower than that needed for combating against unknown threats like insiders. This difference creates a Critical Information Infrastructure Protection (CIIP) investment gap, which is considered as a very high level of security risk with a negative effects caused by the huge financial waste in the case of breaches by insiders.

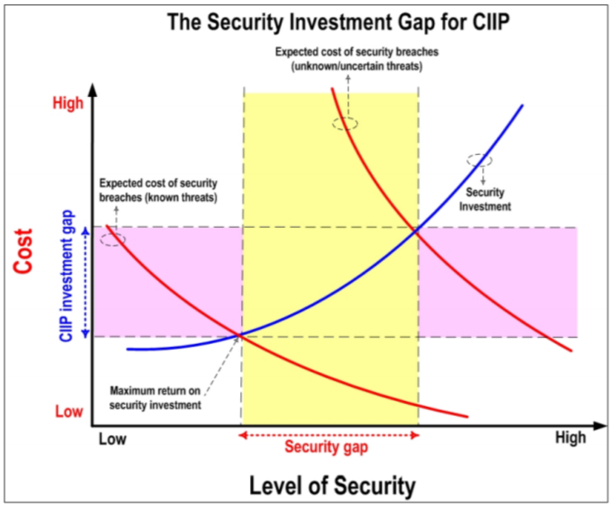


Figure 1-2: (CIIP) investment gap

Nowadays most of the organizations which depend entirely on ICT component in their business, like E-Government service providers and private business organizations like Amazon and EBay spend a majority of their security budget on defending from external attacks.

However, "***one of the toughest and most insidious problems in information security, and indeed in security in general, is that of protecting against attacks from an insider”*** (Dimitrakos, 2007). The spending gap in information security is due to following the traditional security paradigm which is focused on external threats as a result of fearing cybercriminals, while many businesses neglect insider threats.

The proposed framework fills this gap through identifying different malicious activities from different internal and external threat sources. The conceptual security framework gives the security specialist holistic view of different attackers whether insiders our outsiders, which helps them to take decision of who and where to spend budged.

1.5 Research Questions.

The study of this research is trying to give a proper answer to the question,

Can the lens of ANT concept be employed to achieve the main objectives of this research?

In this study the Actor Network Theory (ANT) was used as a analytical tool to answer the question. The translation of the concepts in Actor Network Theory (ANT) supports the answer to the ‘can’ question in different stages through the process that is defined in ANT translation. In this process a user who originates some objects intends to use them in a certain way, which is inscribed in the tool next to help achieving the planned goals. The ANT process also identifies the behavior negotiation, the association of users in actor-network and the alignment of interests.

1.6 Thesis Focus and Key Contributions.

The study expects to contribute to the field of Cyber Security in several areas by adding a new conceptual framework for protecting CII and its ICT components from insiders by using data from security log files and applying the Actor Network Theory (ANT).

Defining and mitigating the insider threats is complex due to the dynamics of processes which utilize CII, in some cases characterized with fast technology growing, globalization, and outsourcing. Due to this complexity insider threats required an integral approach with multiple separate solutions to mitigate fully the impact of malicious attack.

It must involve combination of three different activities - detection, response and prevention against several attacks. These activities fall within the scope of two different types of measures - purely ***technical*** (Access Control, Event Monitoring, Integrated Detection Systems, Trust Systems, System Hardening and Data Analytics) as well as ***organizational*** (Policies, Profiling and User Monitoring, Detection and Forensics).

According to (Hunker and Probst, 2008) *"**In practice to date no single approach has proved dominant as a solution**"*, This is a result of the careless use of information systems which do not incorporate proper protection of company information as well as of the ignorance of the need of security policy, security control and appropriate practice by both the standard users and the administrators.

The major areas of contribution to the body of knowledge in security field of this research are:

1. From the theoretical perspective the study uses one of the famous socio-technical theories which is rooted in science and technology studies and considers research method with a focus on the connections between both human and non-human entities.

2. The study is focusing on how to find out the main actor who is involving other users or insiders within the organization in his malicious activities to attack the target based on his own plan.

3. The proposed conceptual framework depends entirely on the use of security log files extracted from several ICT components like IDS, network devices, servers and workstations.

4. The main purpose of the log analysis is to monitor the event flow and create a profile for each user based on the logs containing record of activities so that malicious and non-malicious activities can be distinguished.

5. The most active users with highest percentage of potentially malicious activities will be considered as main actors and thus will need to be monitored.

6. The study contributes to the literature by developing a new method for minimization of the threats to Critical Information Infrastructures from insiders by isolating the malicious users before the attack ever occurs, which is considered as a protective solution.

7. The main issue for most of security research projects is the availability of representative datasets as both SIEM and UBA security tools need large quantity of data to detect, recognize, classify or generate security information. Due to this the relative costs of datasets cost can be very high, while the dataset used in this study exceeds 65000 event records and will be released for research purposes in the public domain.

1.7 Proposed solution.

Globally the international community and organizations whose services heavily rely on Critical Information Infrastructure (CII) must be aware that uninterruptable continuous business operations and their ability to gain user confidence totally depend on secure systems and software.

In order to protect the Critical Information Infrastructure (CII) and Information and Communication Technology components (ICT) against different type of threats from both internal and external sources security measures should be deployed across the organizations. They must be based on an integrated security framework which incorporates suitable models, methods and policies. These security measures should have the ability to support different security features to protect from outsider's attacks like data encryption, network monitoring, user authentication, etc. and should enforce security policies supported by the Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS). The main issue with such a solution is that most of the features are not applied and most of the security warnings are ignored due to unawareness.

The attacks from insiders should be taken into considerations more seriously due to the type of the employees and the nature of their work within the organization. The potential insiders among them have privileged access to most of the CII resources. Scott Sagan, an eminent security specialist in the Center of International Security and Cooperation (CISAC) claims that organizations tend to ignore many security warnings about potential malicious activities and behavior within the organization. Insiders malicious behavior and users attitude toward attacks is largely influenced by different personal issues like physical, financial, psychological, social and family problems, which can be used as an advantage to involved these user in malicious activities by someone with malicious intent.

The proposed solution is built up of two different parts, which are the conceptual (theoretical) part and the proof of concept (practical) part which complement each other in one integrated framework to minimize the critical information infrastructure threats from insiders.

By reviewing the literature for a suitable theory that can support the study the Actor Network (ANT) theory was selected. This theory states the principles for analyzing the behavior of different employees (Actors) as well the malicious activities that allow categorizing and classifying the users in different security groups in order to apply restriction policies to them. It will be the organizational backbone of the framework.

The second part of the study (POC) will be based on experimental validation of the framework using active component like workstations, servers, applications, databases and any other sources of log data. The record of user activities will be extracted from the log files of active components of the CII or ICT and will be analyzed to classify them as malicious or non-malicious. This will be the base for finding out the users who are involved in a malicious actor network and the relationships among them.

1.8 Outline of the Thesis Content.

The thesis is structured in seven chapters, which can be summarized as following:

Chapter one is introducing the research about minimizing threats to CII from insiders. The problem statement is explained as a motivation for the research study. The research questions, the aims and the objectives of the study are specified. The proposed solution with the key expected contributions is briefly stated and an outline of the study is provided.

Chapter two reviews the state of the art in security field, dividing it into three parts: background information about Critical Infrastructure (CI) and Critical Information infrastructure (CII), analysis of the insider threats and discussion of the relevant publications. The first part introduces detailed information about Critical Infrastructure (CI) and Critical Information infrastructure (CII) from the point of view of potential threats, observed effects and possible protections, while part two introduced details about the insider threats defining malicious and non-malicious insiders and analyzing the scope and motivation for malicious activities. The last part discusses the relevant works.

Chapter three provides details of the key theory used in this study, Actor Network Theory (ANT). The chapter starts with ANT background information followed by the process of ANT translation. It ends with motivation for using ANT and its limitations.

Chapter four presents the theoretical perspectives of the study. It is divided into five sections that give brief idea about the theoretical part of framework for minimizing critical information infrastructure threats from insiders. These sections explain the basic knowledge of the theoretical framework, such as the actor-network perspective, the factors which motivate the actors to enroll in actor networks, and propose several processes within the framework.

Chapter five introduces the methodological part of the study. It contains four different sections and starts with explanation of the new CIIP research approach. Then it explains the methodology behind the proposed framework, the problems that appeared while trying to test the framework models, and the role of actor network theory within the framework. Finally the chapter discusses the technology, the tools and the methods used to collect data in the multidisciplinary study of critical information infrastructure protection.

Chapter six present the results of data analysis as performed according to the methodology described in chapter five. Two basic targets helm the collection of the data and then followed data analysis: to find out the main actor who has malicious intentions and to align these intentions with other actors involved with the network. For this purpose it is also determined who are the members of the closed actor network acting in hidden manner by analyzing the security behavior patterns and discovering malicious behavior.

Chapter seven concludes the study with a summary of the main results of the study and provides directions for future research.

Chapter 2: Overview of the Research Literature.

2.1 Introduction.

Critical Information Infrastructure Protection (CIIP) is very complicated but it is extremely important for all nations globally because they depend on services such as water and energy supply, telecommunications, financial and governmental services.

During the recent decades people's lives have become increasingly dependent on various different infrastructural assets, ranging from physical roads and national grids to the global network-based services such as financial services or the internet. People can perform many activities and can satisfy many of their essential needs using these infrastructures. On the other hand, modern society has become more and more dependent on the availability, reliability, safety and security of different technological infrastructures due to the social and economic benefits they provide and because of the critical effect of their potential malfunctioning.

Infrastructures considered critical (CI) are those physical and information-based facilities; networks and assets, which if damaged would have a serious impact on the well-being of citizens, on the proper functioning of the governments and industries, or can lead to other adverse effects. The people's economic well-being, health, safety and security as well as the functioning of the governments depends on the possibility to perform successfully the daily operations. A society could experience extensive disruption and even loss of human life due to such systems becoming inoperable. The whole industrialized world depends upon the interconnected CI systems. The availability, reliability, integrity, stability and safety of the CI have become key to the operation of the modern society. The disruption of CI can be caused by manmade errors, technical failures and natural disasters.

Critical Information Infrastructures (CII) form a vital part of CI, since they provide the interconnection between and within CI, which are becoming globally interconnected. Unfortunately, the possibility for malfunctioning of CII are not always balanced with countermeasures such as increasing the maintenance cost, enhancing the connectivity, adding remote monitoring, improving the scalability and reliability. CII are globally a fertile ground for cyber-attacks and can be targeted by malware, hackers, hacktivists and adverse organizations. Their malfunctioning can seriously affect other organizations CI as well the national security and stability, the economic growth, the citizen prosperity and may have a far-reaching impact on other nations due to the global interconnectedness of CII. The issue of information security is becoming increasingly important for homeland security.

Computer networking and information technologies occupy a pivotal position in CII, but they are also constantly changing due to the rapid technological developments and innovations. This dynamics becomes a negative factor for cybersecurity, but the greatest threat to information Systems, such as national defense and CI, is often an insider threat. The 2011 Cyber Security Watch Survey concludes that even with multiple attacks occurring on a larger scale the insiders remain the most costly threat.

Unfriendly insiders can be a threat to an organization. Insider threats occur when legitimate users abuse their privileges, causing damages or losses. Cybercrimes committed by insiders are often more costly and damaging than attacks from the outside according to 67% of the respondents of the survey. Given the limited ability of existing systems to counter abnormal insider behavior as many of the security technologies only prevent threats from outsider attacks the insider threat is becoming a real issue. CERT has been working with government and industry leaders to develop recommendations for new solutions to this problem using commercial and open source tools, and has invited organizations to share their achievements and insights in order to participate in the process of counter fighting insider threats. This research uses the Actor Network Theory dynamic model to simulate and analyze insider's behavior.

Insiders do not need a great deal of knowledge about computer intrusions, because their knowledge of victim's system often allows them to gain unrestricted access to cause damage to the system or to steal system data. When this happens you do not know if it is an insider, an organized crime group, a terrorist, a foreign intelligence agency or a rogue nation state planting seeds for future destructive attacks. But the most common case is the disgruntled insider as a principal source of computer crime.

There are many cases in the public domain involving disgruntled insiders. For example, Shakuntla Devi Singla used her insider knowledge and another employee's credentials to delete data from the U.S. Coast Guard personnel database system. It took 115 agency employees over 1,800 hours to recover the lost data. Ms. Singla was convicted and sentenced to five months in prison and five months home detention and was ordered to pay $35,000 in restitution. In another case, a former Forbes employee named George Parente hacked Forbes systems using another employee’s credentials and crashed over half of the Forbes’ computer network servers, erasing all data on the crashed services. The data in that case could not be restored. The losses to Forbes were reportedly over $100,000.

The motive of the insiders is often revenge or blackmail. The insider threats have historically been linked to disgruntled employees exploiting their knowledge of the company to gain unauthorized access into sensitive corporate systems. However, industry analysts note that their definition of an insider must expand to include employees of a business partner of the company who is not under their immediate control, such as a subcontractor, a supplier, or a customer.

Insider theft can only be prevented through a multi-layered defense strategy consisting of policies, procedures, and technical controls. Therefore, the organizations must look beyond information technology to their overall business processes and the interplay between those processes and the technologies used. The management must pay close attention to many aspects of its organization, including its business policies and procedures, organizational culture, and technical environment.

2.1.1 Critical Infrastructures.

In the recent decade, for most of the fast developed, growing and modern societies CI are considered essential for productivity. The enhancement and development of CI is considered as performance indicator for the country's economic competitiveness, which is vital for the wealth. So the CI should be fully protected to guarantee continuing progress in the globalized world (Lysenko, 2013).

The meaning of Critical Infrastructure was described in the American Heritage Dictionary as

*“**The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons**”(* Robles et al 2008).

According to the European Union CI is described as "*an* ***asset, system or part thereof located in member states which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of***

people, and the disruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions" whereas European Critical Infrastructure (ECI) is defined as "***critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross sector dependencies on other types of infrastructure***" (European Union Directive 2008/114/ec, 2008).

The USA PATRIOT Act of 2001 (P.L. 107-56) describes the CI as "***systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*** " This understanding was later endorsed by the Homeland Security Act of 2002 (P.L. 107-296, Sec. 2.4) which lead to create the Department of Homeland Security(Lewis, 2006). The Department of Homeland Security of US (DHS) is now responsible for protecting and ensuring the continuity of the CI of the United States which are essential to the nation's security, public health and safety, economic vitality, and way of life.

According to the Australian State and Territory governments the definition of critical infrastructure refers to " ***those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defense and ensure national security*** " (CIR Strategy 2015).

Despite the many attempts made so far to define CI, there is still no universally endorsed proper definition, or at least a definition which meets the characteristics of all nations (Baldoni, 2014). The definition of CI differs slightly in the criteria used to define the criticality of the country's infrastructure, because each of them has its on specifics and socio-cultural characteristics, which are also changing over the time due to the progress in the world and the evolution of the society. Because of this some countries are using crosscutting criteria (assessed in terms of the potential number of individual fatalities or personal injuries, economic losses and political effects, which take into account the infrastructures of all public and private sectors). In other countries the definition depends on the purpose of the infrastructure (its function performance vital to the society), whereas in some other countries the definition relays on the effects of destruction of the critical infrastructures on the society as a whole (Novotný and Rostek, 2014). There are also some further differences between the United States (US), the European Union (EU) and other developed countries like Japan, Australia, Canada, South Korea and others in technical terms.

The systems and assets which were used in the above definitions can be classified into three categories:

Physical assets: they include both material entities (like buildings, components, real estates, government properties and products) and non-material content (data, information and knowledge). Physical assets protection is very difficult considering the fact that multiple studies show that 85 percent of the global CI is not state-owned. The strong protection of physical assets needs cooperation between the government and private sector.

Human assets: this type of assets consists of organization's employees with legitimate privileged access to information systems, operations and sensitive information. They need to be protected, despite the fact that the staff may also be considered an insider threat.

Cyber assets: all types of the information infrastructure components like hardware, software, computer networks and data that are important for the operation and functioning of the other assets. Damage to such assets can cause further damage on the physical assets, disruption and even casualties amongst the human assets.

Most of the Critical Infrastructures (CI) totally depend on the Critical Information Infrastructures (CII) and Information and Communication Technology (ICT). They need to be functioning at least at a minimal level for the public and private sectors to be able to survive.

According to the Kosciuszko Institute which conducted a research of the critical infrastructures one of the main factors to decide whether an infrastructure is considered as a critical element of a critical system is for it to be classified as a basic element responsible for providing services that fulfill the requirements of the country and its society). According to (Panek, 2014) who reviewed the literature on this subject there are only a limited number of critical asset identification methodologies in existence today. On the other hand, there are several taxonomies of human needs available. Abraham Maslow’s abstract hierarchy of human needs divides them into five different levels: physiological, safety, love or belonging, respects, and self-actualization). Erik Allardt groups them into three different fields, related to having, loving and being. Andrzej Luszniewicz creates seven groups of human needs: food, shelters (like housing, clothes and shoes), health care, education, recreation, social protection and material security.

By analyzing the above taxonomies we can conclude that the services provided by the infrastructure which meet critical needs of living human beings justify their role as Critical Infrastructure (CI). There are six different basic ways which endanger human well-being (6WTD model) and three sets of vital services which protect:

1- Sheltering to save them from heat and cold.
2- Supplying to save them from hunger and thirst.
3- Protecting from illness and injuries.

One possible approach to determine CI is to consider their role to protect the public from life and health threats as defined by the 6WTD model. Following this model, infrastructure can be divided into three different groups (Bennett and Gupta, 2010).

s	Type of CI	Example
1-	Infrastructure that supports sheltering and protection of the living environment	power plants, refineries and water purification plants
2-	Infrastructure that accompanies and secures the life supply chain.	road network, power and gas grids and waterways systems
3-	Infrastructure that ensures access to basic safety services	Telephone switchboards, helpdesks and information databases.

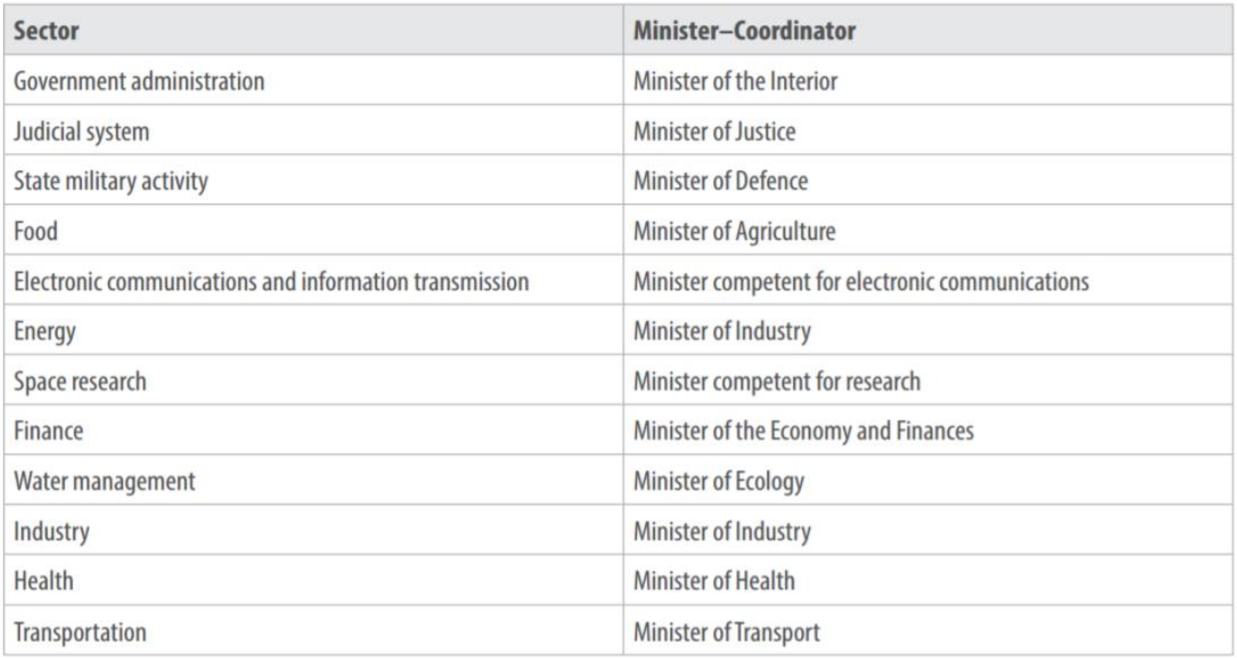
Table 2-1: Critical Infrastructures grouped by their role in meeting human needs.

There are two alternative approaches which can be applied to identify Critical Infrastructures as follows:

1- Bottom-up approach: to look at the sets of sectors and services defined as critical by other nations; those sectors and entities primarily depend on the physical assets

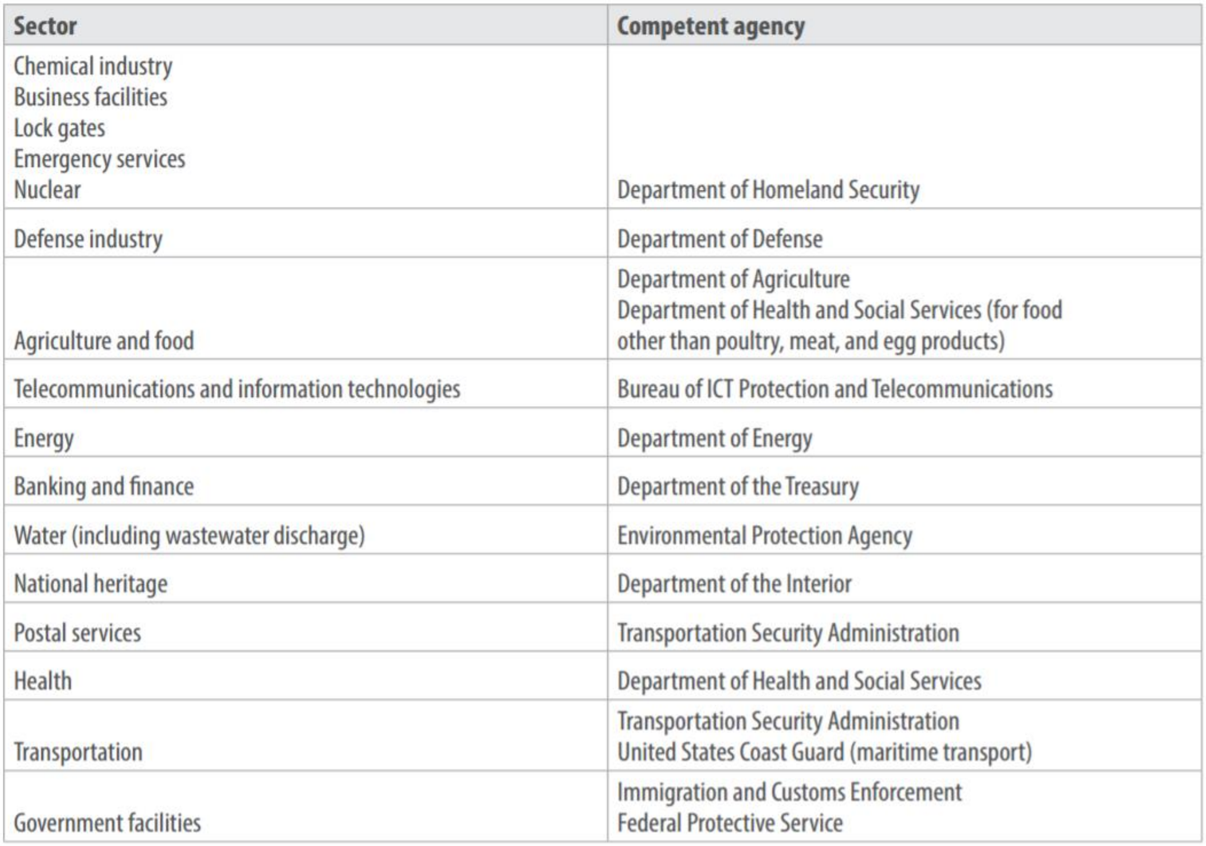
2- Top-down approach: this approach concentrates on identifying and assessing the functions of the critical infrastructure rather than on the physical assets which support it. It is function-centric and assesses the risks associated with the network and system interdependencies, which is more effective for highly distributed infrastructures such as Communication, IT, Food and Agricultural systems (Abgarowicz et al, 2014).

The classification and assessment of critical factors is directly linked to the successful establishment of reciprocal relationships between Critical Infrastructures (CI), the society and the state. The analysis of available examples leads to the conclusion that the critical sectors (systems or services) in different countries looks very similar as shown in tables 2-2, 2-3, 2-4 and 2-5.



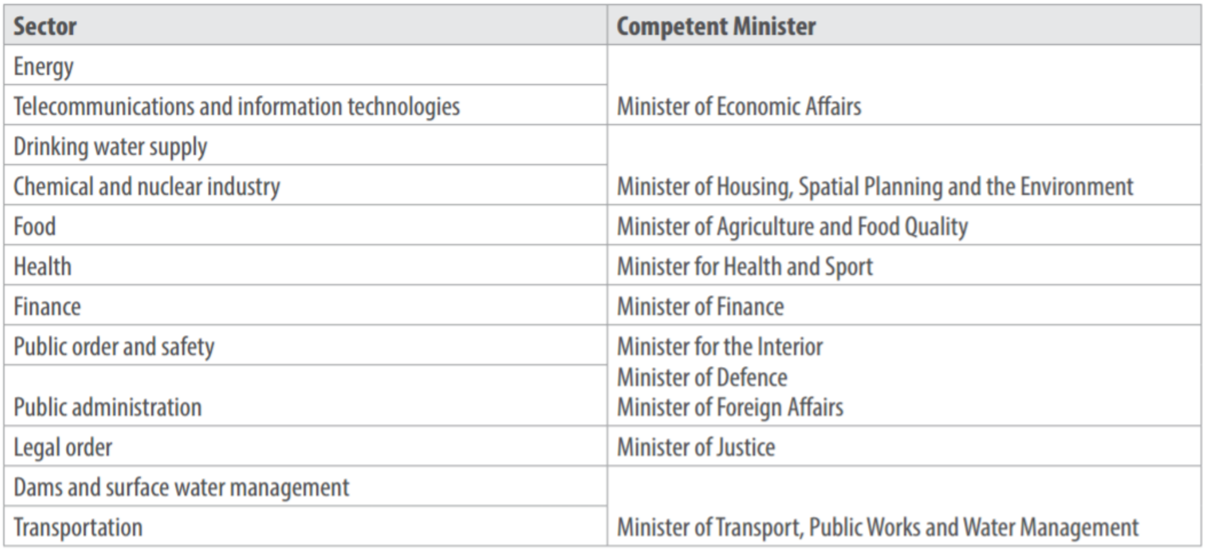
Sector	Minister–Coordinator
Government administration	Minister of the Interior
Judicial system	Minister of Justice
State military activity	Minister of Defence
Food	Minister of Agriculture
Electronic communications and information transmission	Minister competent for electronic communications
Energy	Minister of Industry
Space research	Minister competent for research
Finance	Minister of the Economy and Finances
Water management	Minister of Ecology
Industry	Minister of Industry
Health	Minister of Health
Transportation	Minister of Transport

Table 2-2: List of critical sectors (systems or services) in individual countries (i)



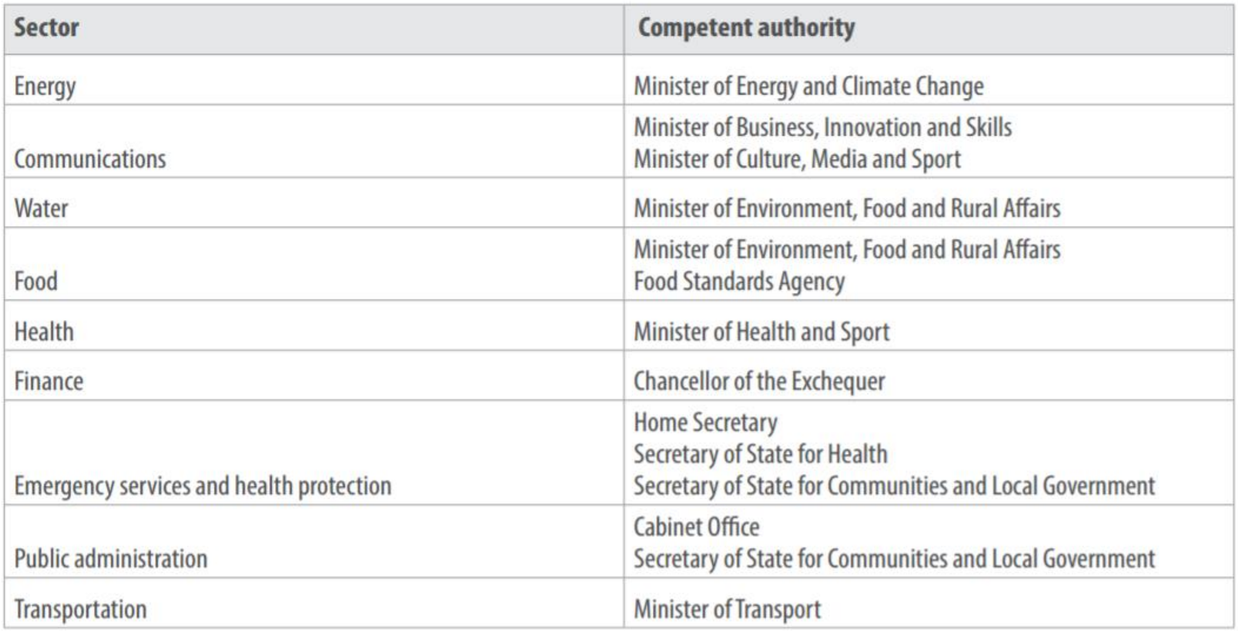
Sector	Competent agency
Chemical industry Business facilities Lock gates Emergency services Nuclear	Department of Homeland Security
Defense industry	Department of Defense
Agriculture and food	Department of Agriculture Department of Health and Social Services (for food other than poultry, meat, and egg products)
Telecommunications and information technologies	Bureau of ICT Protection and Telecommunications
Energy	Department of Energy
Banking and finance	Department of the Treasury
Water (including wastewater discharge)	Environmental Protection Agency
National heritage	Department of the Interior
Postal services	Transportation Security Administration
Health	Department of Health and Social Services
Transportation	Transportation Security Administration United States Coast Guard (maritime transport)
Government facilities	Immigration and Customs Enforcement Federal Protective Service

Table 2-3: List of critical sectors (systems or services) in individual countries (ii).



Sector	Competent Minister
Energy	Minister of Economic Affairs
Telecommunications and information technologies	
Drinking water supply	Minister of Housing, Spatial Planning and the Environment
Chemical and nuclear industry	
Food	Minister of Agriculture and Food Quality
Health	Minister for Health and Sport
Finance	Minister of Finance
Public order and safety	Minister for the Interior Minister of Defence Minister of Foreign Affairs
Public administration	
Legal order	Minister of Justice
Dams and surface water management	Minister of Transport, Public Works and Water Management
Transportation	

Table 2-4: List of critical sectors (systems or services) in individual countries (iii).



Sector	Competent authority
Energy	Minister of Energy and Climate Change
Communications	Minister of Business, Innovation and Skills Minister of Culture, Media and Sport
Water	Minister of Environment, Food and Rural Affairs
Food	Minister of Environment, Food and Rural Affairs Food Standards Agency
Health	Minister of Health and Sport
Finance	Chancellor of the Exchequer
Emergency services and health protection	Home Secretary Secretary of State for Health Secretary of State for Communities and Local Government
Public administration	Cabinet Office Secretary of State for Communities and Local Government
Transportation	Minister of Transport

Table 2-5: List of critical sectors (systems or services) in individual countries (iv).

In order to increase the flexibility in any type of business process or operation on certain level, such as remote access for operation, maintenance or monitoring, and to maximize the benefits the CI should be integrated with CII and must include the ICT (Luiijf and Kernkamp, 2015).

2.1.2 Critical Information Infrastructures.

Nowadays, the most important factor that contributes to the well-being of human life is the information. There are many different infrastructures which provide services to the cultural, political, social and economic processes by processing, storing and transmitting information. They are collectively called Information Infrastructures (II).

The disruption or destroying of Information Infrastructures could lead to tremendous human and financial losses. In addition, many traditional critical infrastructure systems such as power plant or gas grid, water supply or transport network, food distribution system, public health services, emergency services, government services, military, financial and banking systems are also build upon information infrastructures.

The meaning of Critical Information Infrastructure (CII) is unclear as it has no internationally agreed definition, and its meaning is defined differently by different countries and bodies based on their own essential requirements, security considerations, and environment situation. CII maintain many key sectors of developed countries and the modern society, including those essential to the national security. Because of this CII are vital for functioning of security processes which typically rely on a chain of linked and inter-dependent national and international information systems.

CII belong to the Information and Communication Technology (ICT) sector. They contain multiple electronic, hardware and software components and systems so it is very important to understand the relation and mutual dependence between CII and CI (Luiijf and Kernkamp, 2015).

The European Green Paper defines the Critical Information Infrastructures as: "***ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.***")(László, 2009). According to (Cukier 2005) the Critical Information Infrastructure is " ***the communications or information service whose availability, reliability and resilience are essential to the functioning of a modern economy, security, and other essential social values have grown significantly in importance*** ". In summary, CII interconnect different digital system elements like computers and network devices that allow easy flows of critical information within or between Organizations.

According to a study of Hungarian researchers (László, 2009) CII can be considered from two points of view:

- **Computer-based Network Systems:**
    - Communication systems (wired, mobile, satellite, wireless).
    - Transport command and control systems.
    - Finance and banking systems.
    - Disaster warning, defense and security systems.
    - Healthcare systems.
    - Power grid systems.
    - Governmental service systems.

- **Computerized Network Services:**
    - Computer networking services.
    - Supervisory Control And Data Acquisition (SCADA).

- Internet and internet infrastructure maintenance services.
- Mobile communication services.
- Radio telecommunication services.
- Wired communication services
- Satellite telecommunication services.
- Administrative information communication services.
- Broadcasting services.

CII are considered a top priority for most of the governments, public and private organizations and a vital element of national security because of their role for interconnectivity of the distributed services, the likelihood of disruptions and the increased need for alignment in order to reduce the vulnerability of all Critical Infrastructure (CI) sectors, both public and private.

2.1.3 UAE Critical Information Infrastructure.

Over the last several years The United Arab Emirates has progressed significantly in the field of E- Government. According to the report of the United Nations E-Government (UNE-G), considered one of the most trusted resources for monitoring the progress on the level of E-government, Year 2012 was the worldwide progress year. From being placed on number ninety nine according to the quality of its E-government services in 2010 The United Arab Emirates jumped to number seven in 2012.

The report also shows significant progress in the e-participation. In a very short period of time the UAE jumped from being ranked globally number 86 in 2010 to number 6 in 2012. This reflects the overall progress of the UAE e-government which rose from being ranked number 49 in 2010 to being ranked number 28 in 2012. Moreover, according to World Economic Forum (WEF) which issued Global Information Technology Report (GITR) between 2010 and 2011 the UAE is ranked number 24 globally and number one among all Arab counties in the use of information and communication technology.

The contribution of the telecommunications sector in the UAE economy jumped from 4.1 percent in 2007 to 5.3 percent in 2007. The Department of Economic Development in Abu Dhabi prepared a report which state that the spending on information and communications technology in different UAE public and private sectors exceeded 18.4 billion dirhams in 2011, an increase by 15 percent compared to 2010 with 16.1 billion Dirham.

To make the UAE one of the best countries in the world by 2021, which would coincide with the country’s celebration of the 50th anniversary of its founding, the Council of Ministers issued Vision 2021. It gives priority to four different objectives - national identity, economy, education, and health, planned to be achieved by relying on knowledge-based technologies. The knowledge-based technologies can be led by qualified, experienced and skilled Emirati nationals with high expertise, looking forward in long term for even greater UAE prosperity.

The main responsibilities which are assigned to ICT in Vision 2021 is: **" *It enables advanced information infrastructure and communications to connect companies with each other and give them a competitive advantage in dealing and interacting with the world*** "(UAEPedia, 2015).

His Highness Sheikh Mohammed bin Rashid Al Maktoum, The UAE Vice President and Prime Minister and Ruler of Dubai launched an initiative on 22th May 2013 for creating a smart city in Dubai. This initiative is a step beyond the E-government targeting to provide various services and facilities on mobile and smartphones platforms anywhere and anytime for all customers.

The Dubai smart city strategy counts on more than 100 different initiatives aiming to convert nearly 1000 services owned by the government into smart services. These initiatives focus on smart society, smart economy, smart life, smart transportation, smart government and smart environment and are all based on three enablers: communication, integration and cooperation.

To achieve success in all these UAE initiatives, and to fulfil the vision of the government of UAE there should be a secure, available, scalable and highly integrated national information infrastructure that the user can trust and use with confidence in the services, provided by the government.

The UAE Critical Infrastructures (CIS) are divided into two different parts based on the geographical location and the responsibilities which are controlled by two different entities, the federal government and the local government.

The physical assets of the CIs (Power grids and plants, Hospitals, National defense, Petroleum fields and companies, Government buildings, Telecommunication systems and ISPs, Airports , Nuclear energy fields , Diplomatic entities and any other critical buildings) are protected by the local governments through a government body called ***Critical Infrastructure and Coastal Protection Authority (CICPA)***, which was established in May 2007 under the Presidential decree issued by HH to protect Abu Dhabi's infrastructure and promote economic stability as show in figure 2.1 below.

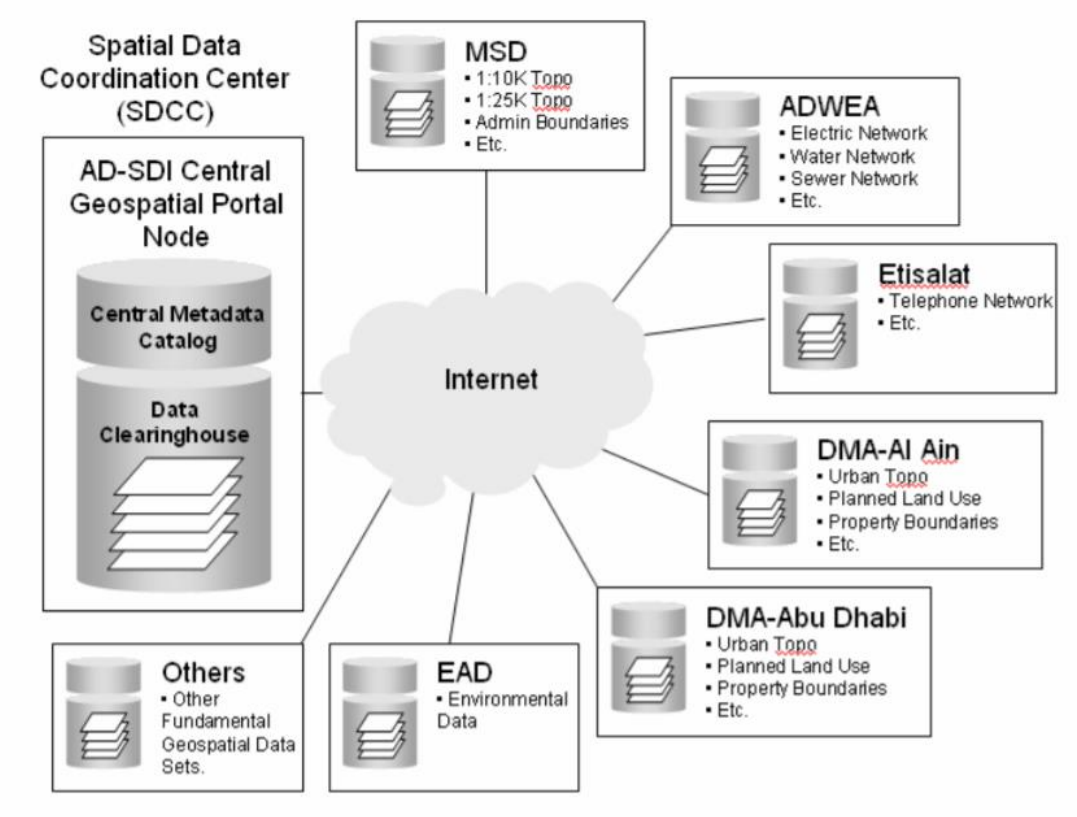


Figure 2.1: SDCC

The Critical National Infrastructure Authority (CNIA) *is* one of the national organizations *which is part of the* Critical Infrastructure and Coastal Protection Authority (CICPA) *operating under the General Directorate of Armed Forces*. *It is* committed to provide the necessary security and safety for all CIs, *vital assets* and public or private establishments spread across emirates of Abu Dhabi just to strengthen the security system of the authority for the continued economic and social prosperity of the Emirate. The Authority works to ensure that critical facilities are secure from potential threats, possible disruption and imminent destruction.

CNIA is cooperating with other government security entities. The authority applied all important precautions to stop and respond to any type of destructive acts of hostile forces, which could lead to a harmful effect on the well-being of Abu Dhabi.

The CNIA has taken steps towards building a database for its Geographical Information System (GIS). Currently CNIA uses GPS technology for mapping all facilities and incidents to allow monitoring of the locations and distribution of the critical facilities, as well as for providing quick response to critical incidents and emergency services in multiple locations. It supports health service centers and other critical services linked to ADSIC and AD-SDI for data and system collaboration.

In 2009 CNIA became a member of Abu Dhabi Spatial Data Infrastructure (AD-SDI), which is initiated by Abu Dhabi Systems & Information Center (ADSIC) in collaboration with nine government stakeholder entities to allow sharing different government and semi-government organizations infrastructures geospatial data information in emirates of Abu Dhabi. This allows CNIA to use AD-SDI data for mapping critical facilities and for providing a reliable source of accurate updates to the spatial data it uses. This is an important factor for developing of a relationship with different governments and semipublic bodies in the AD-SDI community, since it allows to assess their needs of geo-spatial information, including critical data such as maps of utilities, planning and distribution of the telecommunications, monitoring sensitive areas, etc.

On the other hand, the federal government is responsible for protecting Critical information Infrastructures (CII) through the governmental body called National Electronic Security Authority (NESA). This is a federal authority directly responsible for developing, supervising and monitoring of the implementation of strategies, policies and standards related to cyber security protection in the UAE's critical information infrastructure. It ensures that the environment supporting the life in the country is electronically secured by standards aligned with ISO 27001 and NIST and must provide guidance to government entities in critical sectors. The NESA information set includes documents such as the Critical Information Infrastructure Protection Policy, the Information Assurance Standards and other which work towards improving UAE national security by improving the protection of national information and communications infrastructure (ICT) as shown in figure 2.2 below.

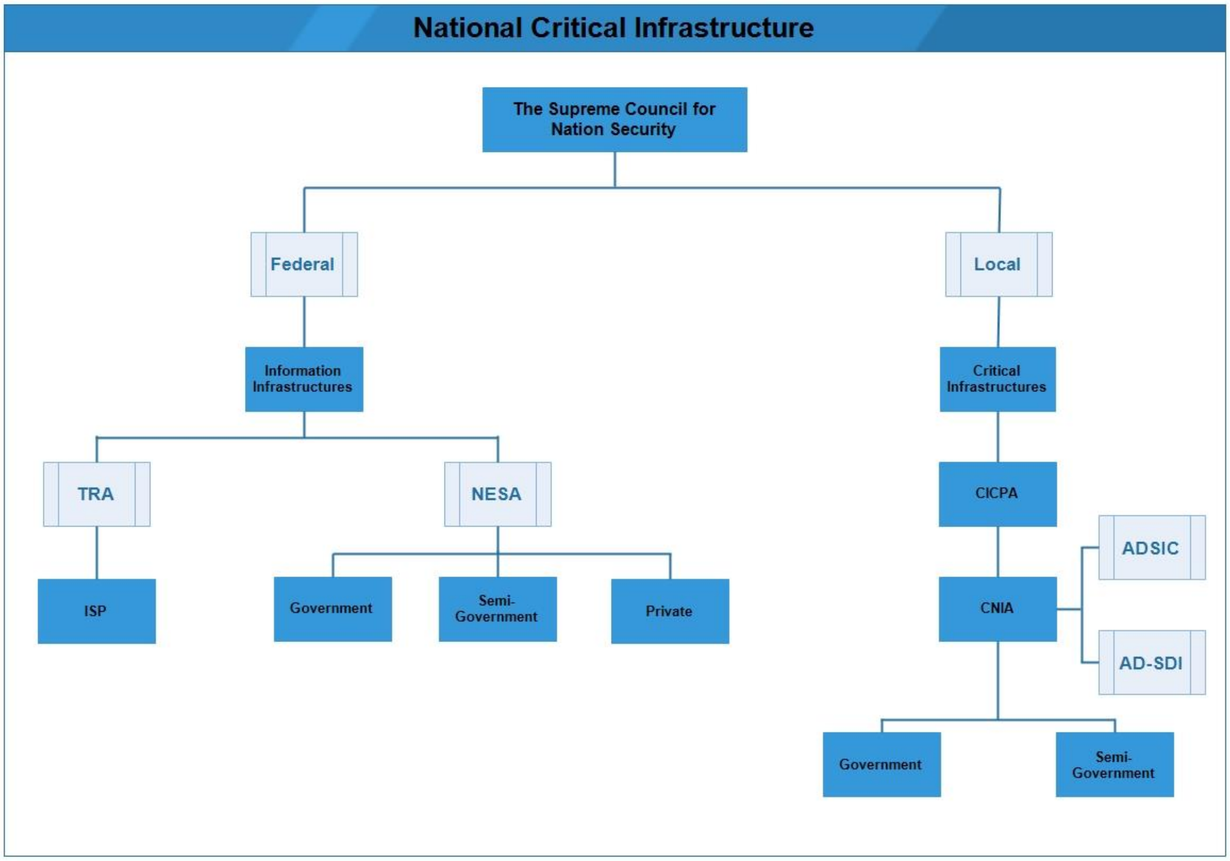


Figure 2.2: UAE National Critical Infrastructure.

2.1.4 Threats to Critical Information Infrastructure.

At the beginning of the cyber revolution Internet was created to distribute and share unclassified research between scientists who did have enough knowledge to abuse the network but had no interest in this. But nowadays the Internet links millions of different computer networks (local, regional, national and trans-border), allowing national services and critical infrastructures to function on a higher level, controlling essential physical elements like power plants and grids, transportation, water supply system, nuclear plants , road systems, and stock markets that exist beyond the cyberspace. A big diversity of malicious activities by users, rogue actors and criminals can perform attacks against critical information infrastructures, which could lead to serious disruption of critical infrastructures, the economy or the national security of whole countries.

In January 2015 CNBC released an article, which contains significant evidence about possible cyber-attacks which the critical infrastructures of many countries can face at any time. The Chairman and CEO of Kaspersky Eugene Kaspersky states that there is a lot of evidence about terrorist attacks targeting critical infrastructures like transport networks, power grids, banks and other vital services worldwide which could strike a very visible damage. He also commented that every country should be auditing its critical infrastructures periodically and should be allocating appropriate budget in order to secure the critical infrastructures over the years (Brocklehurst, 2015).

According to (Robles et al, 2008) the threats to CI that indirectly affect CII can be divided into the following 3 categories:

Natural threats: These types of threats affect the critical infrastructures in vast geographic areas and disrupt, destroy or displace their services. They can be caused by environmental factors triggered by meteorological events such as floods, hurricanes, tropical storms and ice storms, earthquakes and tsunamis but some of them can affect directly the people, like the infectious diseases and epidemics.

Human-caused threats: These types of threats are usually indication for terrorism and include bombing, cyber-attacks, and product and service tampering, which affect directly the ICT, but may also include rioting, which affect both physical and non-physical assets.

Accidental and technological threats: most threats of this type are considered internal security threats caused by accidents like transportation accidents and failures, infrastructure failures, and hazardous material accidents.

Nowadays the CII has become especially vulnerable due to the proliferation of malicious activities and the involvement of new categories of people - from entertainment seeking, hackers and criminals to insiders and terrorists. The fast development of the digital technologies and the growing demands for digital services have reduced the system administrators and operators ability to integrate the necessary safety features with the cyber services, which requires clear standards, working practices, quick mitigation, immediate detection and reliable and lasting protection.. The large variety of vulnerabilities in CII creates big gaps between different security levels which affects seriously the utility services, databases and systems that can protect sensitive and confidential information.

In the criminal world, especially in the world of cyber-crime, the threats can be generated from three different sources. Firstly, the computer network hackers who are snooping for known vulnerabilities in order to generate financial profits or to make political statements. Secondly, the hackers who are forced by conflicts between companies either individually or as part of an organized group. Thirdly, attackers motivated by foreign enemies or intelligence agencies and non-government actors targeting the businesses as part of an industrial spying targeting to achieve competitive advantages or to collect intelligence information (Pradhan, 2016).

There are several types of tools being used to attack CIIs: tools for eavesdropping of information exchange in computer systems and networks, malicious tools for changing and modifying the daily functions of the system which block the user access to its services, and harmful malware (computer viruses, logical bombs, worms and Trojans) which erases, destroys or modifies sensitive information or force computer systems to be inaccessible; further tools include network tools for remote access control and various settings. PCs based tools typically target unauthorized data access via unnecessary system services, but many vulnerabilities can be exploited within the network environment through account management, directory and registry security settings and unnecessary e-services.

In most of CIIs attacks the breach is easy to perform due to the numerous vulnerabilities as well as the wide availability of instructions on the Internet how to attack. In addition, the background knowledge necessary to perform many types of attacks is steadily low so that all what is needed to perform an intrusion is a personal computer connected to the network or the Internet with some malicious tools and software, while most of the organizations trying to prevent attacks are usually suffering from shortage of both experienced staff and suitable tools to countermeasure effectively to the attacks. According to S D Pradhan who was the chairman of India's Joint Intelligence Committee (IJIC) and country's deputy national security adviser between 2008 and 2010 the recent classification of threats falls into one of the three groups, with each group divided into two categories depending on the attacker’s skills and capabilities. Tier one and two attackers exploit the known vulnerabilities. Tier three and four have higher level of experience and some ability to discover new vulnerabilities in the system. Tier five and six attackers have sufficient funds and time to create new vulnerabilities using full spectrum of tools. Many countries are reported to have this capability, like US, Russia, China and North Korea. The threats to CIIs can be divided into three different categories based on their origin - natural threats, accidental or technical threats, and man-made threats. Natural threats mainly refer to natural hazards phenomena such as weather problems (hot, cold or windy). Geological events such as land sliding, volcanic eruption, earthquakes, fires and tsunamis can also cause natural threats. Accidental or technical threats include hardware or computer system failures, which can occur due to poor manufacturing, defective materials or wrong exploitation. The manmade or human threats are typically caused by authorized or not authorized users which can cause internal threats (insiders) or external threats (outsiders). All these groups are divided into two categories based on Intent, namely non-intentional and intentional as shown in figure 2.3 (Gregory et al, 2012).

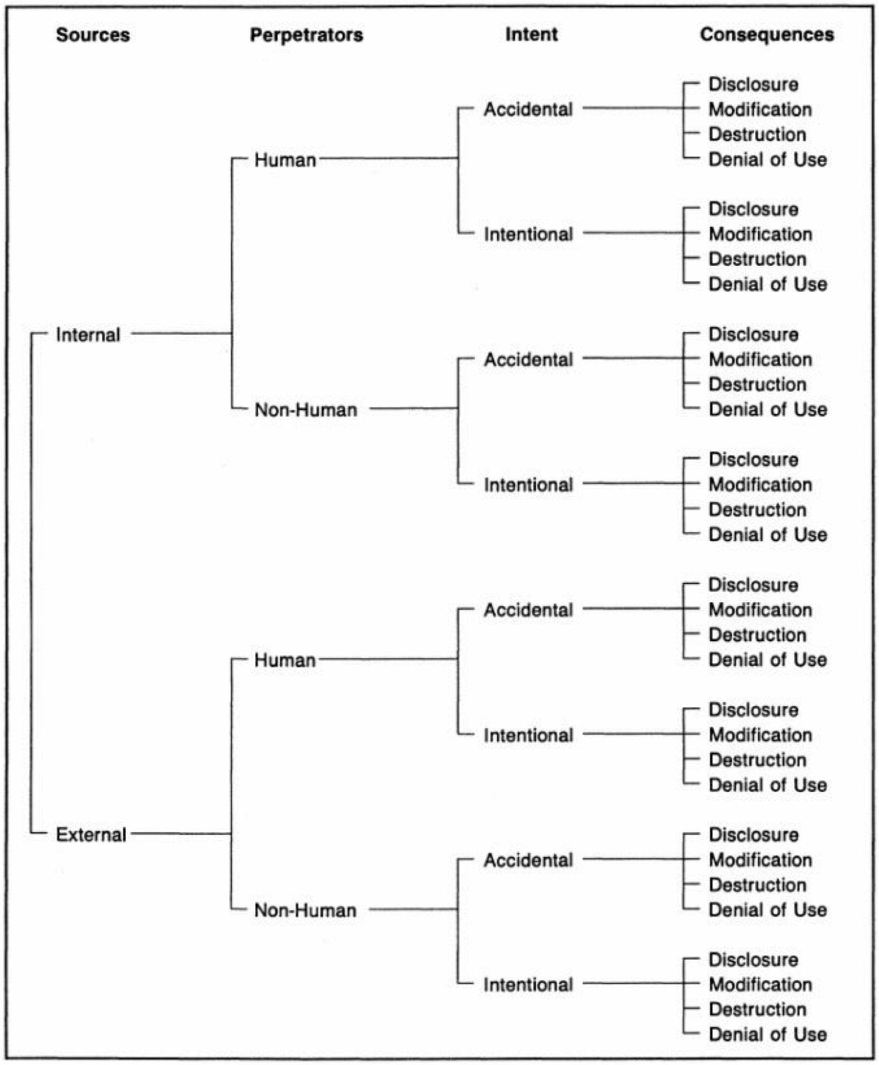


Figure 2.3: Category of Intentional Threats.

Cyber-based threats are developing rapidly, from very simple to more complex forms. They are also initiated from a wide range of sources. The unintentional threats can be created by defective equipment or software upgrades that accidentally as well as without intention disrupt the systems. The intentional threats, which contain both targeted and untargeted attacks, may come from a vast range of sources, including groups of hackers, criminal and disgruntled employees, foreign intelligence agencies involved in spying and information warfare, and terrorists.

Unintentional threats to the Critical Information Infrastructure (CII) are performed without any malicious intent by trusted actors or employees who have legal access to the organizational information but accidentally expose, or make vulnerable to exploitation or loss sensitive or privileged information, technical secrets, essential technological information, assets or premises, spear phishing, or stolen identity. Some employees can also become attack vectors and victims due to social engineering fraud, which affects the organization's business activities.

Unintentional threats exist where an insider is deceived into harming the organization without knowledge, or because of not understanding the value of the information. Examples include social engineering fraud, when an individual is deceived into providing information relating to personnel, ICT systems, or security processes. It can be also based on phishing scams which attempt to obtain confidential information or access to protected systems typically using an email that appears to be from a legitimate and trusted source. Regardless of the motivation, the insider threat can cause damage to your organization and fixing it can be expensive, time consuming, detrimental to the reputation and disruptive to the operations.

An employee can be unaware that they are exposing information, or that the information they are disclosing is priceless or sensitive. Leaving a personal PC or laptop unlocked, not securing authentication with strong password or not following security policy procedures are examples of unintentional threats that can drive to much more serious compromising of the security. Additionally, misplaced or stolen personal security passwords, using laptops and mobile devices without any type of encryption can also lead to unintentional exposure of sensitive or valuable information (Hon George Brandis, 2014).

McAfee labs threats report from 2016 states that the top three causes are result of user misconceptions and deficiency of awareness, the use of untrusted or unofficial online services during working hours and the use of social media applications and web sites at work.

On the other hand, intentional threats are the type of threats that are performed by legal or authorized employees or contractors who intentionally use authorized or privileged level of access to systems, networks or data, with the intent to steal confidential, sensitive or secret information from the organization by using different attack techniques that can negatively affect nation's information, networks, software, computers, functions, process or operation and result in destruction or disruption of critical systems and serious damage to the economy and the national security.

Intentional threats differ from the other two threat categories as it is the only type of threat which includes a specific type of information security events such as cyber-attacks, and each attack is performed with a different probability of occurrence and therefore can lead to different levels of risk and loss. These threats can be both targeted and untargeted attacks and can be performed from a variety of sources, including hackers, virus writers, criminals, disgruntled employees and contractors working within an organization or foreign nationals involved in espionage and information warfare, as well as terrorists (Wilshusen, 2015).

Behind the intentional threats there is a whole variety of actors with very different intentions, motivations and capabilities. They can be motivated by different factors, some of them external, such as foreign terrorist organizations, criminal organizations and foreign forces, other entirely personal. The personal motivation factors can be related to disgruntlement in work place, revenge due to feeling of injustice, criminal financial gain, curiosity or even fun (Nurse et al, 2014).

2.1.5 Effects of Critical information Infrastructure Attacks.

Critical information infrastructures (CII) are especially vulnerable to various different types of attacks. For example, large-scale attack using distributed denial-of-service (DDoS) can be launched quickly using bot-nets and can stop organizational systems from functioning at full capacity. Some cyber-attacks may also affect the information infrastructures with significant physical impact on the countries. Sometimes attacks on the information infrastructures within one country can have indirect effects on linked infrastructure in another country, while a large scale cyber-attack can have even global effects due to the globally interconnected critical infrastructures.

On the other hand the impact of the threats on CIIs can scale up from a simple inconvenience, like shutting down an email or academic network temporarily, to a physical destruction like in the case of hammering incident in oil pipelines which causes them to burst, to deaths due to shutting down the power if a hospital or other critical buildings with no back-up generators. The negative scope can affect everything from a single individual to entire communities.

According to (Robles et al 2008) the effects of the attacks on CIIs can be categorized into direct and indirect, caused by the effects of other attacks.

- **Direct effects:** such effects take place internally and disrupt or completely stop the main functions of the CIIs or vital assets by causing malfunctioning of sensitive part, system or functions, for example the attack which held on 9/11 on WTC affected directly the assets of banking and finance infrastructure.

- **Indirect effects:** some effects are inflicted indirectly by other critical infrastructures experiencing attacks themselves, for example the sabotage of the transport infrastructure will affect indirectly the logistic infrastructure running on the due to the system dependencies (see figure 2.4).

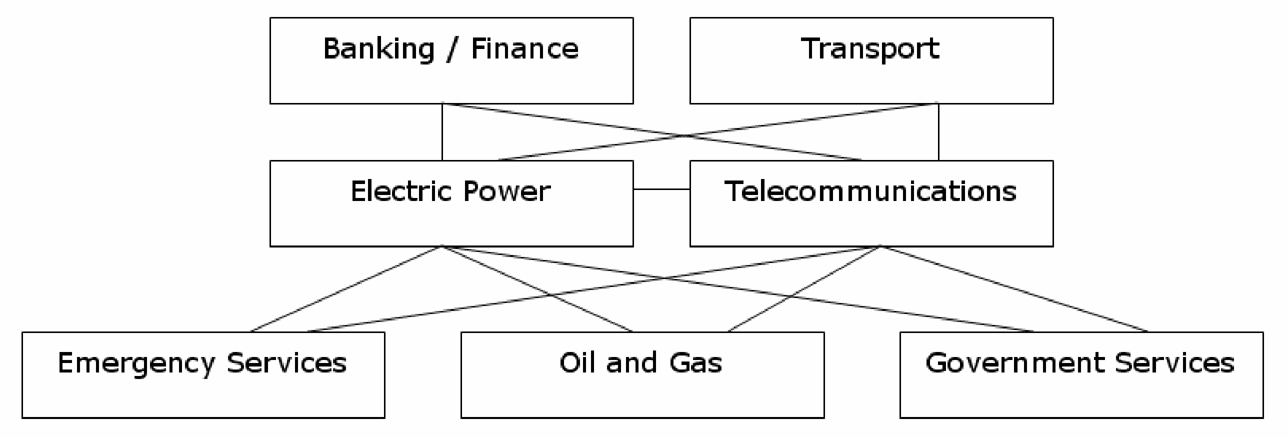


Figure 2.4: Indirect Attack Effects.

As the above diagram shows most of the systems are based of electric power and telecommunication systems so any attack on one of these sectors will directly or indirectly impact many other critical infrastructures. According to the Insurance Business America magazine who quotes DHS during the period 2012-2013 more than 50% of the attacks occurred within the energy sector.

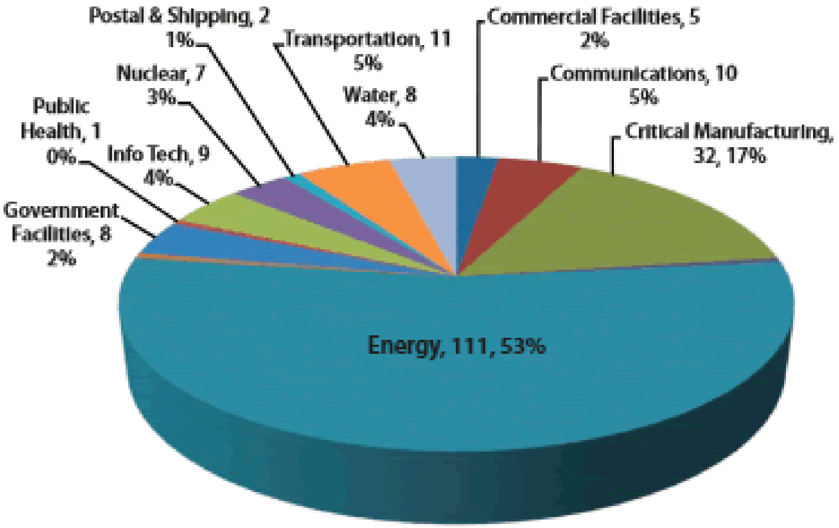


Figure 2.5: Attacked Sectors.

Any type of a system which processes critical information (CI) , and the services it provides, will be a main target for third parties more often than other systems, because exploiting such type of infrastructure has considerable negative impact on all services and activities of the organization, the security, safety and stability of the societies as a whole. According to the Industrial Control Systems - Cyber Emergency Response Team (ICS-CERT) which works for reducing the risks within critical infrastructures, the most common attack against CIIs during the period 2012-2013, SQL injections and spear phishing, were targeting the energy field in 53 percent of the attacks, while the manufacturing sectors were targeted in only 17 percent of the attacks (Storm 2013).

Critical Information Infrastructures (CIIs) are used to process, transfer and store critical and sensitive information between different systems or infrastructures, so it is characterized by very stringent security requirements. All components of CII like networks, data, services and systems should be protected from any type of malicious activities and attacks which could affect the availability, integrity and confidentiality of the CII systems as a whole.

The Critical Information Infrastructure (CII) and the Information and Communication Technology (ICT) security rely on three orthogonal dimensions, namely Confidentiality, Integrity and Availability, known as the CIA triad and considered to be the heart of Information Security. These features should be ensured in any secured and protected information system, from privacy of the user information to encryption of the communicated data. The same dimensions are used to determine the risk management priorities by classifying the information and identifying the security requirements. Bellow we will describe them in some more details and will discuss their importance for the (CIIs).

2.1.5.1 Confidentiality.

Confidentiality of an information asset requires the asset to be accessible only by those authorized by the asset owner. For example confidentiality prevents unauthorized access to private information, customer data and employee data. The security mechanisms must guarantee that some specific information and data should be protected from being accessible by unprivileged users.

One additional role of confidentiality in information infrastructures is to ensure that the information shared within the organizations is intelligible only to authorized users on both ends. In Critical Information Infrastructure (CII), for example, there are many elements of the infrastructure that are required to remain confidential especially when they include configuration information of assets and the protocols for interaction between them.

Breaches of confidentiality can occur in different forms. Allowing someone to have a look at your computer screen, while you have very confidential and secret data displayed on it is one such breach of confidentiality. Stealing laptop computer containing very sensitive information about an organization could lead to breach of confidentiality on a large scale. The breaches of confidentiality increase the risk of fraud; they can damage the organization's reputation, may violate customer’s privacy and legitimate rights, and can potentially lead to breaking the laws or regulations.

To preserve the confidentiality the preventive measures should address several areas like the access to file system, the security of backup data, the protection of confidential data from natural hazards, the encryption or password protection of confidential data, the security of exchanging data over Virtual Private Network (VPN) as well as the physical and logical access control mechanisms.

2.1.5.2 Integrity.

The integrity relies on the methods used to identify and prevent data modifications, alteration or removal without proper authorization during transportation from point to point within the communication media. At the same time it must ensure that the authorized changes by users cannot provoke damages and can be tracked to recover the data if necessary. Integrity is violated when a user accidentally or with malicious intent erases important files, when computer viruses infect the system, an employee modifies his own information in the payroll database or an unauthorized user deliberately destroys or damages the Web site of the organization.

Traditionally the accent in information security has been put on the requirements for availability and confidentiality rather than on the integrity. However, in CIIs the integrity is more important.

Aligning information security with integrity is a requirements for the information that is transmitted both from and to the citizens, government, private sector, political parties, financial institutions, the media, the military and security services. The information gathered from the world is interpreted in such a way as to enable the learning and to help individuals and communities prepare for potential events, while the information sent out drives the vital infrastructure, directing industrial control systems to perform their tasks. Whether transport networks, nuclear power plants, industrial control systems, or public and private electronic service systems, the end result is that the confidentiality and availability of such information are secondary to their safety.

According to Mike Gault, the co-founder and CEO of Guard Time there are several types of integrity in CIIs - System Integrity (Execution), Network Integrity (Supply Chain) and Operational Integrity (Governance). So the integral definition of integrity can be formulated as "***the absence of compromisation across systems, networks and operations (and humans in its traditional sense)*** ".

System Integrity often defined as “**Anti-Tampering**” in the military sector is about ensuring your systems are free of compromises. But what does that mean in order to ensure it is there and what assumptions are necessary to verify this? If you think about viruses or malware – they compromise the integrity of the systems they infect. If you think about the breaches that have occurred over the last years almost all of them have been driven by some form of malware infiltrating customer records (e.g., Target) or disabling control systems (e.g., Stuxnet) to cause physical damage.

These are integrity attacks but we just haven’t use this language to recognize them as such. Currently the language used to describe such attacks is misleading – “we have procedures in place operated by trusted insiders to ensure our systems are in the correct state”. Malware like Stuxnet is able to deliver the deadliest attacks on the critical information infrastructure integrity. We just haven't had the tools to address the problem.

Process or Supply Chain Integrity is ensuring that every step in the process is correct, is verifiable and can be replicated. Factories easily understand the role of supply chain and as Jason Hoffman of Ericsson recently pointed out Cloud Computing represents the "new digital factories of our age". Take in inputs from the network, manipulate them and pass the results on to the next node, return the results back to the user or store them locally for future use. The challenge is that there is not a single Enterprise CIO who is willing to rely on an outsourced supply chain for mission critical processes. They have no visibility, no way to verify that the processes are correct, and only a limited legal recourse when things go wrong. The procedures they have relied on in the past are no longer theirs and the insiders have become outsiders. “Dynamic Attestation” or the ability to verify that the outsourced supply chain is correct and compliant in real-time is often unachievable goal, although it is often formulated as a requirement in order to move mission-critical processes to the cloud.

Operational Integrity, or Governance, is to ensure that the prescribed rules are being carried out correctly (e.g., “don’t let the machines operate beyond their limits” in factory environment). In cloud computing environment governance rules are often specified in the PAAS (Platform as a Service) layer. The question which comes next is how to ensure that they are being enforced without trust. It’s ok to specify rules but as we all know not everyone feels obliged to follow them. Take, for example, Edward Snowden’s case – he broke the rules of operation and it was not possible to detect his actions on time. Big Data also poses a serious governance integrity problem. As many leaders like Sandy Pentland have pointed out it is impossible to legislate around how data is collected and retained – there is simply too much of it being collected from a myriad of connected devices. The only thing that is possible is to legislate how data is used. However, how then to enforce, verify and audit those rules is the real problem, which is namely a governance problem.

2.1.5.3 Availability.

The meaning of the term “availability” varies in Computer Science, Information Technology and Engineering. According to (Khazanchi et al, 2008) the availability as “***the ability to make information and related physical and logical resources accessible as needed, when they are needed, and where they are needed***”.

Most of the CIIs interconnect and therefore depend on the continuing availability of other technical systems and their functions. For example, most of e-government services depend on information which requires alignment with the communications and the information supply. Any disruption to ICT systems therefore affects the availability of e-government services as a whole.

On the other hand, computer networks allow unauthorized people with minimal experience to gain access to private information and critical resources. The computer networks, whether public or private, are considered one of the main communication systems that face considerable security challenges. For example attacks such as Denial of Service (DoS) on communication network could lead social and military communications to become unavailable and could potentially prevent legal users from accessing vital services in moments of emergency.

As we mentioned before most of the organizations in today’s world are dependent on the use of ICT. But they are connected to Information Systems via computer networks, which are build upon CII resources. On the other hand, CII availability depends on the availability of their components, which can be divided into Software, Hardware and Network.

2.1.5.4 Software.

The software component is considered one of the most important components of CCI because while the hardware and network components run their own operations the software code is what malicious users exploit during attacks. Most of the security attacks target the application software or the operating systems, so to keep the CII secure it is very important to secure the application programs code and the operating systems code.

The program code is usually spread across three different levels based on the application software architecture as follows:

Service Level: it is the most critical level in the application software architecture where the malicious actors trying to exploit the vulnerabilities. At this level the hackers are mostly searching for open services ports to get into the system in order to sabotage it by intercepting the interaction between application components like clients and servers. The user (client-side program) typically interact with different services (server-side programs) in order to get the task done, which means a number of services ports need to be open by an application program. This increases the level of systems vulnerability to threats from other calling programs because holding the services for legitimate access can be exploited for malicious purposes.

Component Level: this is the second level of software code which provides access to the services via interfaces as needed by client programs. These interfaces need very strong access control and authentication mechanisms. Only authorized client programs should be able to gain access to their respective services. The components and their interfaces use technique known as proxying, which can affect the performance of the whole system.

Object or Class Level: this level exploits the concepts of Object Oriented Paradigm (OOP) which uses information hiding, encapsulation and other techniques for efficiency, performance and secure functioning of the software. Due to the dependency between the levels and potential design flaws the lowest level would be exploited last so the security of software system should be propagated from the lowest level up across all layers of the software.

2.1.5.5 Hardware.

When the application is exploited the goal of attackers is achieved by sabotaging the information system and forcing the system to be unavailable for its normal functioning. In the case of hardware, though, it is totally controlled by software which runs on it and wherever the software process goes the hardware will follow. The main goal of the attacker in the case of hardware target is to consume the resources of the system through exhausting the information processing capabilities by sending unnecessary traffic above the normal quantities so that the processor and the RAM cannot handle. Such a behavior can be achieved by installing malicious software on the target CII component, or via live network attack such as Denial of Service (DOS) attack using a piece of software called Sockstress, which utilize resources to crash the services of a whole machine.

2.1.5.6 Network.

When the attacker fails to access the target hardware system to make the services of the target machine unavailable he could direct the attack on the network to which the target system is connected instead. Most famous type of network attacks is to flood the network using Distributed Denial of Service (DDoS) attack which multiplies the compromised computer systems and can generate data of the magnitude of 400 Gbps. Also worth mentioning is the Logic DoS attack which exploits the vulnerability of the Internet Protocol (IP) packets, where the attacker modifies the payload data size which can potentially lead to crashing the target OS due to a fault in the OS software handling it (Qadir and Quadri, 2016).

2.2 Critical Information Infrastructure Protection.

The Critical information infrastructure (CII) is the set of computing systems (computers, servers, databases and applications) and communications systems (network components and communication links) that distribute different types of digital services to organizations, companies, industries, and the society as a whole. The problem of providing appropriate protection of CII (CIIP) is similar to the general problems faced by most government authorities in need to be reformed by the government through legal interference in the private sector.

A number of governments worldwide are clear about the need of CIIP and already face the complexity of pursuing it, while the governments in developing countries are at a late stage of their CIIP programs and are still struggling with the alignment of their strategy for CIIP. The main problem with Critical Information Infrastructures (CII) is that this type of infrastructures comprises a single point of failure. They can be disabled, possibly interrupted, by exploiting the very foundation of the information infrastructure. The interconnected nature of CII systems through public network or the Internet gives the attackers ability to perform malicious activities from anywhere in the world. The fast and rapid progress in the technology field as well the growth of countries critical infrastructures in modern societies attracts attackers to launch similar attacks in new places. This problem is exacerbated by the inefficiency or the lack of cyber security policies and proper information infrastructure for preventative solutions.

The development of critical information infrastructure protection (CIIP) in different countries is very essential to protect the new information infrastructures and to support other vital systems which are interconnected with them. Likewise, increasing the level of CIIP would improve the conditions for doing business in developing countries. Indeed, with regard to the needs of the business community, "the long term neglect of vital infrastructure and development needs" ranks number fourth among the main concerns of emerging markets and developing economies to prompt business and economic collaboration and to guarantee trade performance.

The global needs for infrastructure investment are up and estimated at about US$ 3.7 trillion annually. This means that the difference between infrastructural requirements and infrastructure expenditures which considers investment is a big concern in many countries and especially in the developing countries as show in figure 2.6 below (Zaballos and Jeun, 2016).

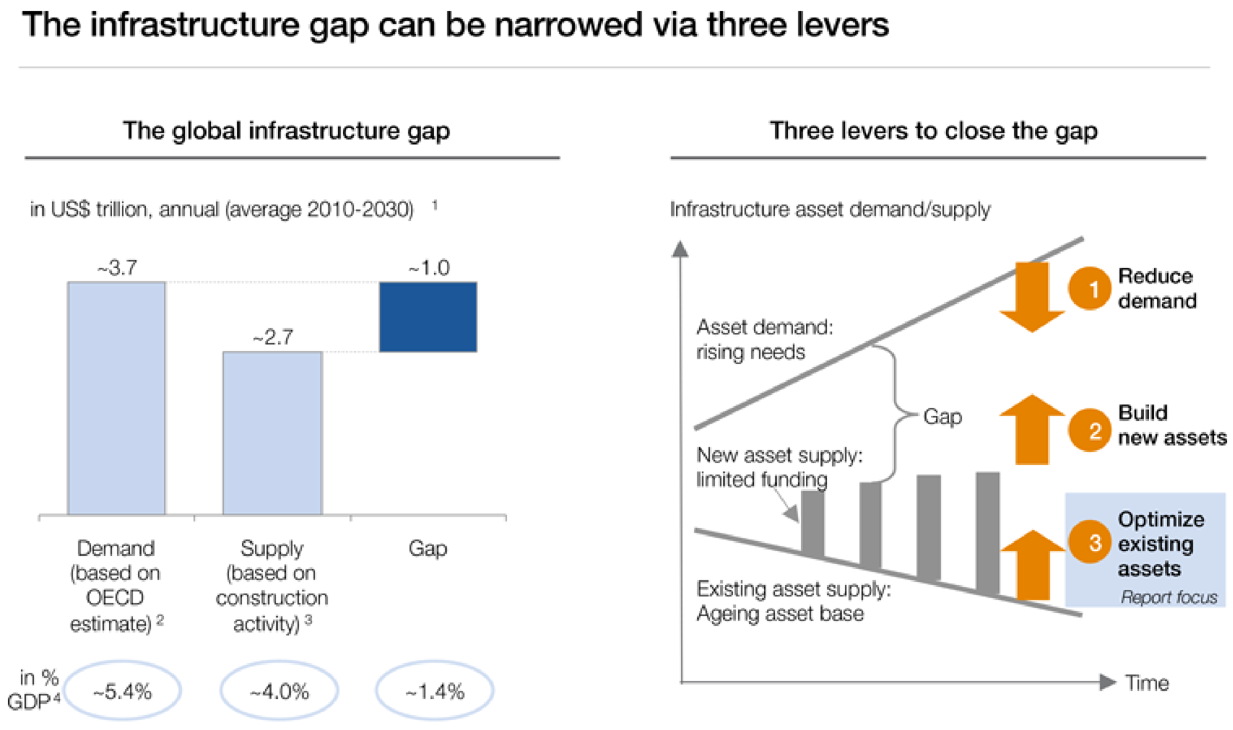


Figure 2.6: Infrastructure Investment Gap.

2.2.1 Critical Information Infrastructure Protection.

In the past the traditional concept of Critical Information Infrastructure Protection (CIIP) was focused only on governmental sectors and large companies with a major share in the country economy. The invention of the Internet has changed the scope and the nature of small and medium organizations by giving them the ability to interact directly with the government or with larger organizations globally and this led to amplitude of cyber threats which were previously only the concern of large economic organizations.

CIIP can be considered as action of providing support to keep normal operations of vital systems or to assist in the process of recovery in the events which could disable the normal operation of such systems. The definition of CIIP according to CERT as follows: " ***Protecting communications or information service[s] whose availability, reliability and resilience are essential to the functioning of a modern [national] economy, security, and other essential social values***".

Most large organizations like government agencies and companies usually have experienced security groups that fulfill all type of support services needed in the event of security incidents. However, as the complexity of CI systems increases, there is an increase in the level of interdependence required to operate them even in smaller organizations. The Information systems that are basically interconnected through the CII are becoming extremely critical because of their role in operating other important systems. CIIs like organization ICT network (LAN) as well as the wide area network (WAN) are designed to continue operating properly even in the event of computer security breaches, but they can be easily affected by events outside the organizations, whether locally or globally.

There are several different types of communication services within CII which are vital for the effective operations of the organizations: Virtual Private Network services (VPN), Emailing services, SCADA services, Web services, Wi-Fi access services, Application and database services, Voice over IP services, Firewall services, etc. All these services are under constant threat from self-motivated insiders or outside malicious activities. The security breaches usually begin in CIIs due to the inherited system vulnerabilities from the hardware and software resources that can be exploited easier to make unplanned changes in the services or to disrupt their normal behavior.

These security breaches can be divided into two different groups: internal and external. An internal breach corresponds to the abnormal changes that occur within the system without external intervention. External breaches are related to interactions that originate outside the system, such as natural disasters, malicious activities, or accidents. Regardless of the cause, any exploits of the systems can lead to internal effect which can collapse the services and the overall control of the systems.

The internal and external threat events can lead to serious deterioration in the services and can cause main function failure. The rapid technical development and the competition between organizations to reduce the expenses have decreased the level of security. The lack of essential security features like monitoring, detection, analyzing and prevention lead to vulnerabilities which not only affect the infrastructure services but also corrupt digital assets such as communication links, application databases and system repositories.

The restoration of disrupted CII services could be a very uneasy task and the effect of such a failure can affect the public and business confidence in e-commerce and e-government services for a while. The costs of recovery or putting mitigation strategies in action are enormous. In terms of both productivity and income it could easily exceed billions of dollars. In the example of Amazon.com, whose business heavily relies on e-services, any type disruption could cost millions in just minutes.

The CIIP has three main strategic goals which can be summarized as follows:

1. To protect critical infrastructures from both internal and external cyber-attacks.
2. To decrease the level of vulnerability to cyber-attacks on a national scale.
3. To reduce the level of damage and to minimize the time for recovery from cyber-attacks.

In order to achieve these goals, a new strategy is required that combines not only technical measures but also accounts the following principles:

- The preventative measures should be considered at all levels.
- In order to control the damage, an early detection and rapid response capabilities should be improved.
- The level of disruption of government and businesses should be limited to a minimum.
- The affected systems should be able to continue operating at a minimum level and must recover within the shortest period of time.

The measures on national level can be divided into five different priority groups:

- Operating a national cyberspace security response system.
- Establishing of a national cyber security vulnerability and threats reduction program.
- Initiating national cyber security training and awareness program.
- Protecting government information systems from cyber security threats
- Increasing the level of national and international collaboration in cyber security.

The framework for protection of critical information infrastructures on national level should be considered in the wider commercial, social and technical context. CIIP needs a multidisciplinary approach which combines technical, business and educational measures. Partners, traders and consumers need to give higher priority to security of the products and should accept and share best practices.

In order to establish good understanding of the security issues within academic and educational institutions and to increase the awareness of the whole society of security threats it must adopt a kind of security ethics. It requires a strong communication and commitment on three different levels: inside the organizations, between the organizations and the government sector, and within the government bodies themselves.

The CIIP threats cross the borders and reach out the international political scene. The cyber terrorism is often referenced in relation to such threats, but the threats in fact come from a much wider scope, ranging from literal crimes to human errors and even natural disasters. Protection against the full range of threats and risks at all times is practically impossible due to technical, economic and human reasons. What is possible, however, is to focus the measures on preventative strategy in order to exclude significant impact. Alternative strategy would require focusing of the protecting measures which minimize the impact of the attacks when they actually take place (Alcaraz, Zeadally, 2015).

- US CIIP framework model and practices:

The US is one of the pioneer countries in the field of CII and CIIP and it has made significant developments on strategic level. They has helped enormously enhancing the information sharing between infrastructure owners and operators, on one side, and the government, on the other side.

The Department of Homeland Security (DHS) coordinates most of the US government’s CIIP initiatives at all governmental levels and within other agencies.

Canada has also integrated its ICT protection in a “Total Defense" framework which aims to protect all infrastructure components from any type of hazards. The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is responsible for the national strategy and acts as a co-ordinating body there.

- European CIIP framework model and practices:

The European Council of Barcelona (ECB) requested the City Commission to create an action plan that help improving the security of ICT infrastructures and encourage the user services such as e-government, e-learning, e-business and e-health as defined in "eEurope Action Plan 2002".

The CIIP in UK was not considered as a highest level until 1990 but the National Infrastructure Security Co-ordination Centre (NISCC) and the Information Assurance Advisory Council (IAAC) which are in charge of taking care of state side, public as well private sectors work now in alignment with the US standards and initiatives.

- International CIIP framework models and practices:

There are several countries which are making huge efforts to improve and enhance their frameworks to protect CII that parallel the developed countries such as USA and UK. Amongst them are the following:

India: under the framework of an Information Technology Action Plan the Ministry for Information Technology of the Indian Government has created a number of relevant initiatives and frameworks, such as the Information Technology Act of 1999.

Malaysia: the Malaysian Communications and Multimedia Commission Act was created by the Malaysian Communications and Multimedia Commission owned by the Malaysian central agency aiming to protect the critical infrastructures on national level and most the initiatives and frameworks are following its instructions.

Japan: in January 2000 The Action Plan on Building Infrastructure to Counter Hackers and Other Cyber Threats was published by the Cabinet Secretariat and later on the Special Plan on Fighting Cyber Terrorism against Critical Infrastructure was launched as an original Japanese initiative (Brömmelhörster, 2002).

2.2.2 Critical infrastructure interdependency.

Critical infrastructures are heavily linked at multiple positions through different mechanisms. Every pair of linked infrastructures are mutually benefiting because they are heavily dependent on common physical assets and information. These interdependencies lead to an abnormal increase of the overall complexity of some CII systems and ICT components responsible for monitoring and controlling their operations. Most CII sectors and their services have extensive dependencies on other CII sectors and services.

According to (Luiijf et al, 2016) the dependencies can be identified as follows. Firstly, the dependency is "***the relationship between two products or services in which one product or service is required for the generation of the other product or service*".** Secondly**,** the interdependency is **"*the mutual dependency of products or services*"**.

The US Department of Energy Argonne laboratory defined both dependency and interdependency as follows. A dependency is a "***linkage or connection between two infrastructures, by which the state of one infrastructure influences or is reliant upon the state of the other***." An interdependency is a ***"bidirectional relationship between two infrastructures in which the state of each infrastructure influences or is reliant upon the state of the other"***. They are illustrated on figure 2.7 below.

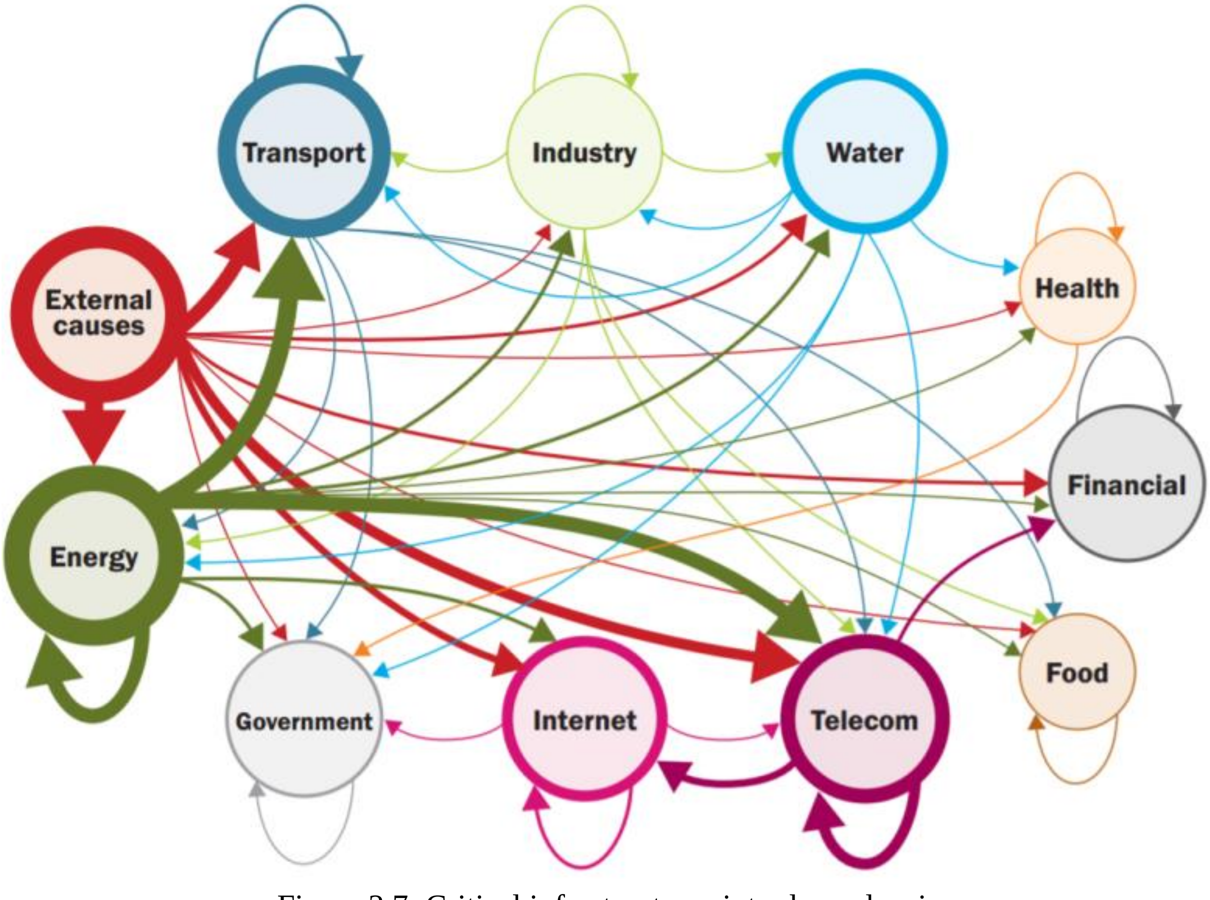


Figure 2.7: Critical infrastructures interdependencies.

Dependency as defined above is a connection or link between two different infrastructures through which one infrastructure influences or correlates to another so that the failures could directly or indirectly affect the function of the system, while the interdependency is a bidirectional relationship between two or more infrastructures in which each infrastructure involved influences the others in a way so that if any of them experiences failure this will affect the whole group. Infrastructure systems interactions have a number of characteristics. Traditionally, the dependencies are analyzed along two different dimensions: physical dependencies and functional dependencies, like in the case when communication system needs electricity from power supply to function normally.

The Indian National Critical Information Infrastructure Protection Centre (INCIIPC) issued in 2013 guidelines on critical information infrastructure containing a complex relationship between various vital components sitting in between and within the organizations. The critical information infrastructure should not be considered an isolated element, and vertical and horizontal connectivity with other critical information infrastructures should be taken into account.

The vertical interdependency is defined as a symbiotic relation between different organizational layers like sectors, departments, divisions and groups as shown in figure 2.8 below. The dependencies between the layers are shown using directed flows of control from top to bottom and directed flows of information gathering from bottom to top.

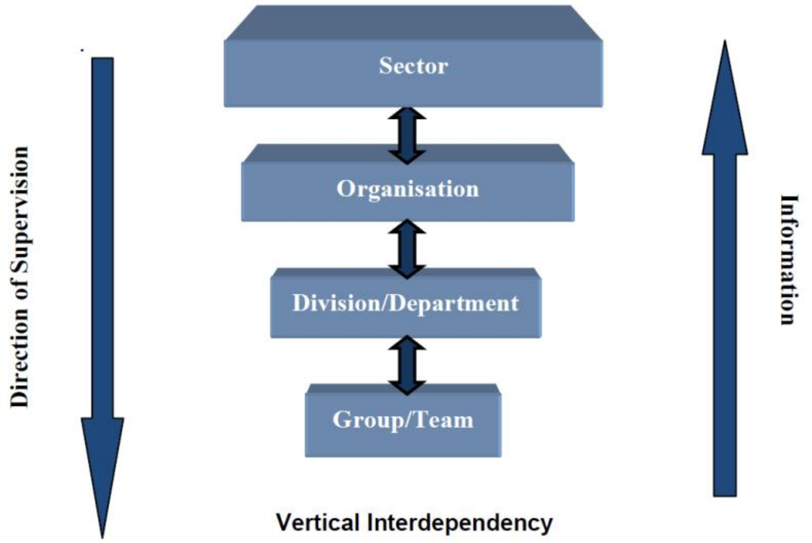


Figure 2.8: Type interdependency

The horizontal interdependency is based on two complementary dependencies which are in-bound and out-bound. In-bound dependency indicates that the target organization's role and services depend on the source organization, while out-bound dependency indicates that the source organization role or service depends on the target.

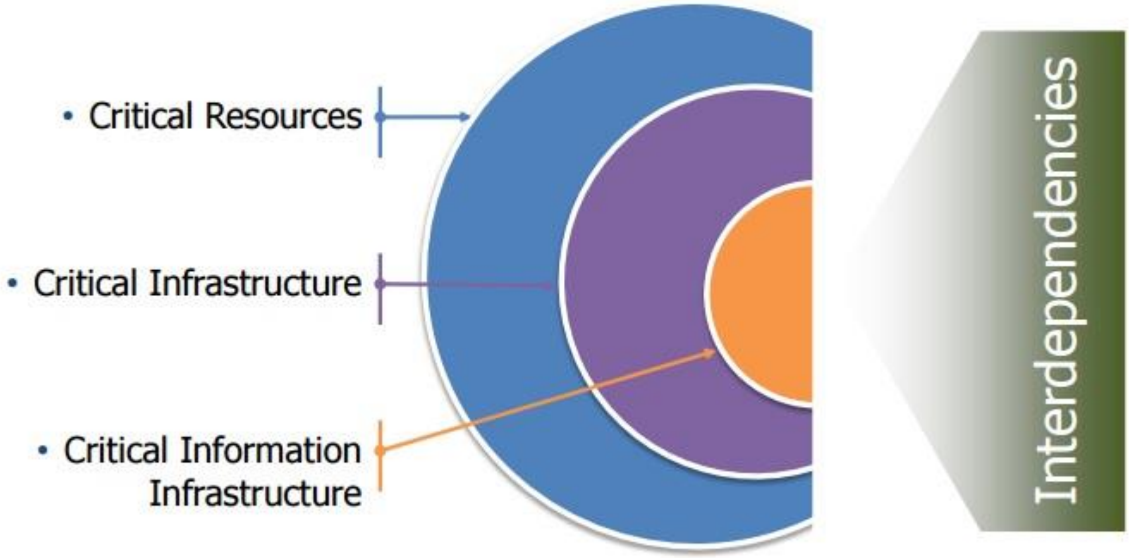
(Pederson et al, 2006) classified CII interdependencies into several groups:

- **Physical interdependency:** direct interaction between infrastructures and engineering reliance between components as from a consumption, supply and production relationship.
- **Geospatial interdependency:** this type of interdependency exists within the organization because of components proximity, like in the case of a fire the local destruction could affect all assets located in the same building or in the neighboring area.
- **Policy or Procedural Interdependency:** this type of dependency is a result of a policy or an action that involves changing the states or leads to events which can subsequently affect other CI.
- **Informational Interdependency:** this is a requirement for the information which controls the operation and the functions of CII components, like the interruptions in SCADA systems used to control the power grid which can affect all components of the power stations and hence must be independent.

The same research also introduced a topology of interdependencies based on the following two concepts:

- **Spatial Interdependencies:** where two organizational infrastructures are located nearby physically for economic reasons, and component failure in one infrastructure lead to possible disruption and failure in the other facility.
- **Functional Interdependencies:** in this type of interdependencies the infrastructure rely on each other's function, For example, ICT needs electrical power to function, while electricity needs ICT communications to control the power generator systems, so they must be mutually interdependent.

It is well known that the complexity and interdependency of CI and CII as shown in figure 2.9 are very hard to manage or protect. Most of the researchers in the field focuses on the system of systems (SoS) or the interlinks to be protected, which classifies the interdependencies into four different types: physical interdependency, cyber interdependency, geographic independency and logical independency.



• Critical Resources
• Critical Infrastructure
• Critical Information Infrastructure
Interdependencies

Figure 2.9: Interdependence Complexity

The interactions between critical infrastructure and its environment can be divided into three groups:

- **Upward dependencies:** The services and products distributed to one organization by external organizational infrastructure are essential to survive its operations and functions.
- **Internal dependencies:** This type of interactions takes place within the organization processes, operations and functions of the infrastructure. Internal dependencies are typically the internal connection between different subsectors of a critical infrastructure. For example the communication system depends primarily on its own power generator for energy supply.
- **Downward dependencies:** The interactions have consequences which could affect the users or the consumers of a critical infrastructure due to degradation of their resources.

The interdependencies as defined above can be also divided into four different types as described by (Rinaldi et al, 2001):

- **Physical interdependency:** occurring between two different critical infrastructures when exchanging resources for critical operational processes, for examples in order to function the communication system require electricity and any failure directly or indirectly will affect the functioning of the entire communication system.
- **Cyber interdependency:** occurring when information is transferred between different critical infrastructures and any state change in one of them should not affect the operation or the daily monitoring of the other CI.
- **Geographic interdependency:** this type of interdependency is related to the geographic proximity of the CSs and means that any failure of a system in a CI in one geographical area should not affect the CIs laying within the same areas, for example the environment disasters like floods lead to damage of the roads and the transport systems which can affect indirectly the water plants due to the water pipelines being laid under the roads.
- **Logical interdependency:** this type of interdependency is very different from the previous because it is relates mostly to economic characteristics, for example the events of 9/11 in 2001 which led to the attack of the World Trade Centre forced most of the organization worldwide to enhance their security systems to protect more effectively the businesses.

On another dimension the interdependencies can be classified based on the type of failures the CIIs experience concurrently.

- **Cascading interdependency:** any type of failure to one infrastructure affects the other infrastructure at a later stage (also called the “domino” effect).

- **Escalating interdependency**: the disruption of one infrastructure exacerbates the disruption of the second infrastructure.

The intensive growth of Information Technology resulted in an increase of the interest of many researchers and research centers in the study of interdependencies and especially in the cascading effects of operation of CIIs. The cascading failures occur when a failure of one specific component in a system leads to a failure of another component within the same or inside another system. It can occur in a single system, for example a power grid, when one energy node leads to subsequent failure of other nodes from the grid, or in connected systems.

The interdependencies are normal in nature, but the cascading failures can make the critical infrastructures more exposed to attacks. The analysis of cascading failures is an essential issue in CIIP due to the fact that a relatively small events can result in devastating effects in different critical infrastructures.

The cascading effect was introduced by (CascEff, 2016) where it was described as follows:

"***Cascading effect are the effects of the start-up event where the dependencies of the system lead to effects spread over other systems, and the combined effects of the spread event have greater consequences than the root effects and involve multiple stakeholders or respondents***".

More specifically, cascading failures happen when a disruption in a specific organization infrastructure leads to the failure of an element in another internal or external infrastructure, which later may lead to further disruption of the second infrastructure. For example, the disruption of the power grid due to an unintentional act like natural disaster may result in a failure of the power utilities within the communication service providers (ISP) which may affect directly or indirectly the normal activities. The incident results in shortage of power distributed in a specific area but the issue cascaded from the power grid to other organizations, in this case Internet Service Provider (ISP).

Interdependencies are influential factor to understand system weaknesses and the potential impact on their users. Interdependencies nowadays are considered to be a source of vulnerability in critical infrastructure. Here are some examples of vulnerabilities where failure in infrastructure component cascaded the issue to other infrastructures:

- The Slammer worm infected the security monitoring system of Davis-Besse nuclear power plant in US in a city of Ohio which replicated very fast and led to stopping the system for five hours. A statement released by the North American Electric Reliability Council (NAERC) stated that the plant was not disabled but the failure caused disruption to other power utilities.
- The signaling failure of the entire CSX transportation *system* in 2003 (due to a virus which infected the computer system) disrupted the rail system in 23 states, where the monitoring and controlling train movements and signals failed (Stergiopoulos et al., 2016).

2.2.3 Information sharing in Critical Infrastructure.

The information sharing and protection are very important parts of the cooperative efforts to enhance the resilience of critical infrastructures. The secure information sharing based on organizational policies and legislation will allow to exchange valuable information on the risks and the overall condition of critical assets. This gives to both public and private organizations the ability to assess the risks in an appropriate way.

These days interconnecting the critical infrastructures can make a huge difference in preventing any type of incident, or in fast responding to any regular or irregular event which could directly affect the critical national infrastructure. On the other hand, the accurate sharing of the information among different partners like national, regional, local and even private and public sectors is essential for the critical information infrastructure security and resilience. There are many different benefits of sharing information between critical information infrastructures that we can summarize as follows:

- It allows coordination between different levels of government departments, such as federal, state and local government bodies for better estimation of the critical infrastructure vulnerabilities as well as for repairing and responding to threats and attacks.
- The amount of information from private entities provides ground for technical expertise for improving the security that allow better control and better protection of critical infrastructure assets.
- Sharing information allows faster recovery and more efficient response to any type of insider threats or cyber-attacks.

Recently, there are huge demands for CII information sharing which leads to an increase of the level of its risks. Indirectly the more information are shared among national critical infrastructures the probability of malicious activities and the chance for exploiting the system by both insiders and outsiders increases. So there should be very strong security measures applied during sharing crucial information especially in the private sectors due to potential incidents, Such accidents can take place at any time and the leakage of sensitive business information to competitors could damage the private sector reputation and increase the liability substantially.

In addition, to create effective information sharing some additional factors should be taken in consideration, for example:

- Government organizations should have the ability to ensure that the information which is released to private sectors is not sensitive, while many private sectors limit the information they are sharing due to the application of the Freedom of Information Act (FIA).

- The CII should limit the release of information to meet the restrictions of the Originator Controlled dissemination (ORCON), which requires that the creator of the information must have the ability to track all possessors of the information.

- The conflict with the Federal Information Security Management Act (FISMA) should be resolved to prevent critical information infrastructure sharing. Common federal information security procedure can be more than enough to increase the level of critical information sharing with private sectors.

Although there are several benefits of CII information sharing, there is also a level of alignment with threats that makes the information sharing problematic. These threats increase the vulnerability of CI due to the possible unauthorized information sharing within CI or with other CIIs by insiders. The interdependency and interconnectivity of communication systems with other critical infrastructures may result in an increased risk of attacks. The streaming of shared information among several CIs can increase the probability of malicious activities and the exposure of that information (Luiijf et al, 2016).

2.2.4 Role of ICT in Critical Infrastructure.

Information and Communications Technologies are considered the most essential tools in fields, where the information and knowledge systems are building on critical information infrastructures (CIIs). Nowadays many developed and technologically advanced countries which are driven by new technologies prefer to use ICT platforms for providing enhanced, efficient and effective electronic service to the public and private enterprises.

The increase in using ICT worldwide leads to improving the alignment with faster network-based communication systems. On the other hand, the performance of such advanced communication system forces the majority of e-governments and businesses organizations to convert most of their operations from traditional manual system to ICT, increasingly relying on CII which raises the cyber threats as a result (KANG 2008).

Nowadays ICT is considered a pillar for most National Critical Infrastructures (NCIs) due to its essential role in monitoring, controlling and functioning of their daily operations. The security threats are one of the most concerning issue in the field of ICT systems which inherit multiple potential breaches, like design errors done by engineers, human made or system failures, or vulnerabilities that can be exploited by harmful software and patches.

In most critical infrastructures ICT falls under one of the two categories: Information Technology (IT) and Operation Technology (OT). The CI offers to different beneficial party's services like finances, communication, emergency services and others resources, while ICT links all these services together and supports business processes (Abgarowicz et al 2014).

The dependency on ICT and CII in modern society is increasing day by day which as results increases the availability, reliability, integrity and security of these infrastructures to ensure continuity of their essential services. Therefore, protecting CII concerns most organizations which consider an alarming feature the fact that it takes huge amounts from organizations budgets to support security projects.

Potential malfunctioning of ICT assets of CII like networks, servers, software applications and databases may have direct impact on social and economic services. It also has an indirect effect on human wellbeing and governmental or organizational business and information processes, which in most cases are based on electronic facilities.

According to (Tiirmaa-Klaar, 2011) almost 98 percent of the banking sectors depend on internet and communication technology (ICT) and the corresponding Information Infrastructures, while more than 90 percent of the citizens are paying their tax online and the government sectors are using specific e-government information system for daily essential core business services.

According to (Cavelty,2005) most of the ICT systems based Critical Information Infrastructures (CII) have vulnerabilities which are considered as central point of CIIP standards, policies and frameworks. Also they state that CII are considered one of the easiest and most vulnerable access point for cyber-attacks since 1990 till nowadays, while mitigating the threats and attacks against CII remains difficult.

The type and nature of communication networks allow attacks to be launched from anywhere in the world and finding the origin of the attack remains one of the major issues due to complexity of the attacks. The attacking techniques are getting more and more complicated and as a consequence the gap between the action of intruder and the ability of the intrusion detection system to react is widening. In a second place, the methods and tools used in the attacks are becoming more and more sophisticated, which can result in a wide spreading of the crisis caused by a single point of attack.

2.2.5 Protecting the ICT elements of the CII.

The protection of various types of CII can be achieved through   preserving the integrity, availability and continuity of all infrastructures and processes in coordination with external structures. This can be achieved be applying security frameworks and models which are entirely based on ICT.

Any type of attacks on ICT components of CII can lead to serious damage of the public and business confidence, especially in e-commerce and e-government services initiatives. The recovery or mitigation of ICT after cyber-attacks caused by viruses or malicious human actions are enormously costly to the people and the economy and this forces the private and public sectors to spend significant budgets estimated in billions of dollars to protect CII.

The protection of CII, including ICT pursues three different strategic objectives:

- Preventing cyber-attacks on CII.
- Eliminating well know vulnerabilities of CII to cyber-attacks.
- Reducing the non-operational time as a result of a damage caused by cyber-attacks.

On the other hand, an enhanced and integral strategy can achieve highest level of protection through different security measures including the following elements:

- Improve early detection and immediate reaction capabilities of potentially exploited control systems.

- Eliminate the impact of attacks which effect the government, private services and indirectly society to a minimal level.

- Provide level of endurance that the disrupted systems can continue to function at a minimum level of processing capacity or that it can easily restore it within the shortest time (Roberto Baldoni, 2014).

2.2.6 The challenge of protecting critical information infrastructure.

Many researchers point at the significant consequences of complex cyber-attacks on CII and ICT worldwide. They have been introduced as a result of long-term development which cannot be undertaken by public and private organizations or individual due to the complex nature of CII and ICT. Several challenges can be mentioned regarding this:

- **The role of public and private sectors**: in many countries most CIIs are controlled by private sectors, for example in USA only it was estimated that more than 85 percent of critical infrastructures are owned by private sectors and the authorities are no longer sure about security of sharing information between public and private sectors.
- **Unrestricted distribution:** Most CIIs do not have any type of physical barriers or policy restrictions. Identifying the responsibility of different member in both public and private sectors with respect to security and monitoring and controlling of malicious activities is one of the biggest challenges that concern many organizations.
- **Dynamic internetworking:** CIIs are connected to each other through ICT components which cover large area creating an open networked environment which is time sensitive and dynamically evolving. The size of this interconnected network varies based on the demands and the timing also fluctuates depending on the different actors' response time.
- **Extreme complexity:** CIIs are very complex due to number and type of connected component. Simplifying the architecture of the infrastructure is essential for identifying the security breaches and system reactions in order to avoid wide impact of the damage and to guarantee fast service recovery. In the large networks the incidents which could be created due to a failure easily spread to other interconnected networks and the impact could affect whole countries.
- **Human made failure:** Critical infrastructures depend on human and expert decisions that are informed scientifically justified; ordinary knowledge may be insufficient to face emergency cases on a large scale

- **Vulnerability:** the inherited vulnerabilities can be propagated by the information infrastructures, which can lead to exposure of confidential information. Furthermore, they can be exploited by attackers who are unconscious about them thus causing even bigger damage to the business (HÄMMERLI, 2010).

2.3 Insider (User) threats.

Recent studies by security research centers have found that insider threats are becoming a main security risk to most organizations information infrastructure assets. For example, (Sugata, 2010) states that about 70 percent of the threats to an organization's computing and network-based information infrastructure originate from inside, while most of the business organizations invest valuable computational and financial resources to protect their network from outside malicious attacks, completely ignoring insider attacks. Both public and private organizations fail to recognize clearly the intensive threats coming from insiders who can dramatically rise and even exceed the level of their authorization to access confidential information and to modify or steal important business information for malicious purposes and financial gains.

Moreover; Insider threats have become famous in information security community because they are targeting both the private sector organizations and the government sectors for reasons that range from IT sabotage and industrial espionage to financial gains. The main reason for the problem of insider threats comes from the fact that the government and business organizations do not have acceptable security defenses to detect and prevent insider attacks (Barrios, 2013).

According to the Verizon 2016 DBIR Report about 77 percent of the internal breaches were counted on insider employees, while only about 11 percent are attributed to external users, around 3 percent are attributed to business partners and the remaining 8 percent are divided between internal and external collusions, which makes them difficult to categorize.

2.3.1 Insider definition.

Recently many organizations have analyzed in their research the insider threat problem, government organizations like the Homeland Security, federally-funded organizations such as Secret Services, as well as private research organizations such as RAND Corporation, The Centre of Excellence for Applied Research &

Training, different university researchers as well as industry members especially in the financial sector. Unfortunately, no common definition of an insider has emerged.

The absence of an agreed definition of insiders globally creates difficulties for the research on detection of threats from insiders. In fact, the definition of an insider is the first step towards ensuring that the proposed research for detecting threats of a specific user type will help in using different detection methods just to determine the best methods for detecting and preventing particular types of threats from insiders.

The definition of an insider should be formulated differently within different domains, based on both cyber and physical security issues experienced there. Most of the researchers consider insider an attacker if he is inside the organization within certain perimeter determined by the role. For example the inside user who is within the access control domain can be considered as potentially causing higher level of damage, which assigns to him higher level of threat. This definition can be more accurate if it accounts various risk factors because the level of insider threat depends on the intensity of the impact. Some key attributes which can be used to distinguish between the insiders and outsiders are:

- **Access to the system**, whether the authorization is legitimate and legitimated by whom, also what to access and not. It is necessary to distinguish between legitimate and authorized access since some users have legitimate access to physical assets but are not authorized to even glance through secret materials, either digital or printed.
- **Capability to present the organization to outsiders**, especially when the policies apply to inside users which are not known by outsiders.
- **Knowledge and skills** of the person who designed the system or worked on such type of systems. The biggest advantage of insiders is that they have good knowledge of the information system, its operation and functions and the organization has been dependent on these users for a period of time. This knowledge is considered tacit because it is stored in their minds. The security procedures should take into consideration the experience and the level of knowledge they have.
- **Organizational trust and empowering the inside users** (dependability and assurance). These trusted users are most often employees but can be also contractors, consultant, temporary skilled people or third party partners with whom there is an informal or formal business relationship. The difference

with outsiders is that these insiders are trusted due to the nature of the relationship with the organization according to the business agreement.

Nowadays the following external users who have privileged access are considered as insiders:

- The recently dismissed employees whose system privileges have not been canceled yet.
- The software developers who have written the code of the systems and have privileged access to the system.
- Curious guests who have logged in and used someone’s computer without informing them.
- The janitors of the employees who have physical access.

Oliver Brdiczka, who is the Chief Data Scientist at Vectra Networks and who leads their insider threat research reports that more than 70 present of critical information infrastructure organizations have security breaches, including Oil, Water, Gas, Transport and Electrical grids (Brdiczka, 2014).

The malicious insider is defined by the CERT Program which is managed by Carnegie Mellon University on behalf of the Software Engineering Institute as " ***any current or former employee, business partner or contractor who has the following norm: has authorized organizations network, data and system access that used this access in negative manner that affected badly on the integrity, availability and confidentiality of the organization's information or system***". The CERT programs have mentioned some criteria which should be met by the users to be counted insiders:

- Have an authorized access to an organization’s system, data or network.
- Intentionally use authorization to affect the confidentiality, integrity and availability of the organization’s information or information systems (Silowash et al, 2012).

The difference of the insiders’ threats with traditional threats posed by current employees is the conspiracy with outsiders: many insiders involved in crimes fulfill the requirements of outsiders, including foreign organizations and organized crime groups, or unfriendly governments.

The National Infrastructure Advisor Council (NIAC) defined the insider threats to Critical Infrastructure (CI) as " ***one or more individuals with the access and/or insider knowledge of a company, organization and enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products or facilities with the intent to cause harm***" (Gücüyener, 2015).

Recently, threats from insiders have been growing fast and are currently considered as a serious problem due to the economic growth in the world. In most cases the insiders take advantage of their legitimate privileges, supported by their authority, experience and knowledge of the organization infrastructure. This allows them to breach critical physical protected components or other elements of the business processes such as safety control system and operating procedures as show in figure 2.10 below.

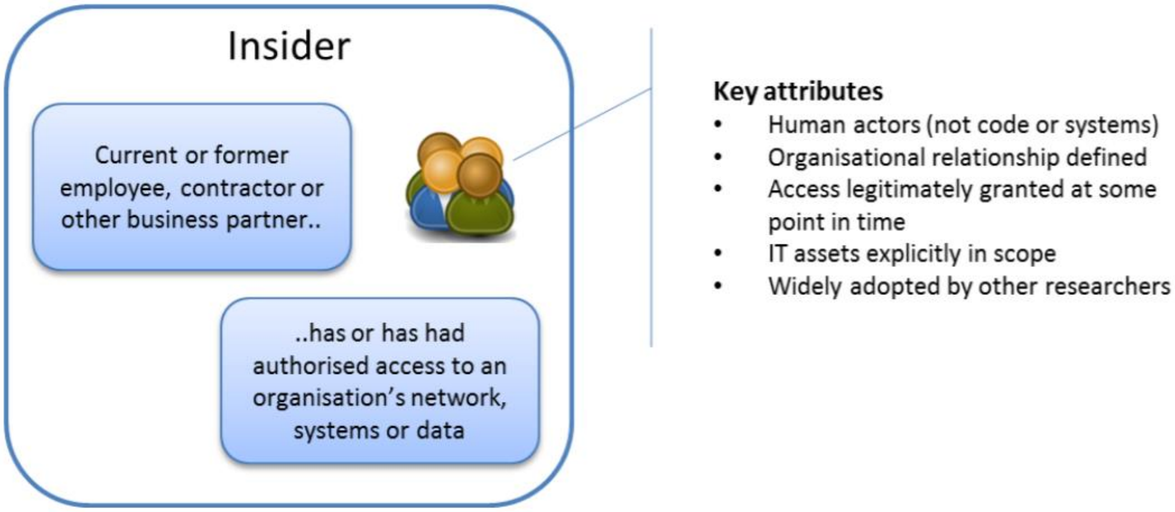

Insider
Current or former employee, contractor or other business partner..
..has or has had authorised access to an organisation's network, systems or data
Key attributes
• Human actors (not code or systems)
• Organisational relationship defined
• Access legitimately granted at some point in time
• IT assets explicitly in scope
• Widely adopted by other researchers

Figure 2.10: Key Attributes of Insiders

2.3.2 Who Are The Insiders?

This question sounds simple and easy to answer. But as with other fundamental concepts in information security mentioned before, such as security triad (confidentiality, integrity and availability), the concept of insider is not well defined. There are three different possibilities for defining it:

- An employee, student, guest or members of an organization that accesses computer system to which he/she has legal access.

- Contractor, supplier, business partner, computer technician, guest or anyone who has a formal or informal business relationship with the organization.
- Users authorized to access specific resources, like online customers who use the organization's system to access their account.
- Users who are authenticated by the system and act as legitimate users, or users who have been given legitimate guest access via shared username and password.
- Users who are forced by an outsider to perform malicious activities.
- A former users using previously granted access which has not been revoked when resigning and continue using their privilege secretly.

The differences between users may depend on their physical presence and logical existence, for example some inside users are logically (operationally) inside but they are physically outside, while some inside users are physically inside but are logically outside; both logical and physical users are considered as insiders. In addition, there are different levels of logical insiders depending on the nature of the system and networks involved, the authentication or authorization mechanisms which have been put in place, and the environment which the user is operating.

Insider is not all time the same during security breaches. There are several different types of insider threats depending on the type of activities that they involved:

- **Malicious insiders** (Intentional): who have intent to cause a worthy damage or to impact the confidentiality, integrity or availability of the organization’s information or infrastructure, relaying on their legitimate access as insiders. Administrators with full privileged identities are especially more dangerous.

- **Exploited insiders** (Compromised): insiders who have credentials to access, or security devices that have been compromised (tricked) by an outside actor. This type of insiders is more difficult to identify due to the fact that the attack in such a case originates from outside.

- **Careless insiders** (Unintentional): Insiders who expose confidential or sensitive data accidentally, for example an employee who unwittingly accesses organization data over insecure or unprotected public network. A large numbers of incidents of this kind come from users who do not follow the security policies and practice negligence.

- **Vengeful actors:** Insiders who steal secret data or damage organization networks intentionally, such as former employees who trigger malware or logic bombs in the information system on their last day at work.

- **Tech savvy actors**: Insiders who act to challenge the organization. They totally depend on their knowledge of vulnerabilities and weaknesses and their ability to access confidential information. They can provide for free or sell confidential information to enemies or black marketing bidders (Nurse et al, 2014).

The most dangerous insiders are the users who have privileged access to the entire information system, like system administrators and software developers, as well as the ones who have accounts with minimum controls on the rights to enter or access. The damage that a user with admin rights could cause is unaccounted, because such users are not monitored and controlled properly. Privileged access for user's who are gained by outsiders are not less dangerous than the access for insiders, as it happened with Sony and Orchestrated when a hacker stole the credentials of the system administrator and this crime was considered a very high-profile data breach by US investigators.

According to Vormetric Insider Threat Report from 2015, almost 55 percentage of insider threats were created by privileged users, among which the contractors and service providers account for 46 percent, while the third place is occupied by users who have access to company networks with 43% percentage (See Figure 2.11).

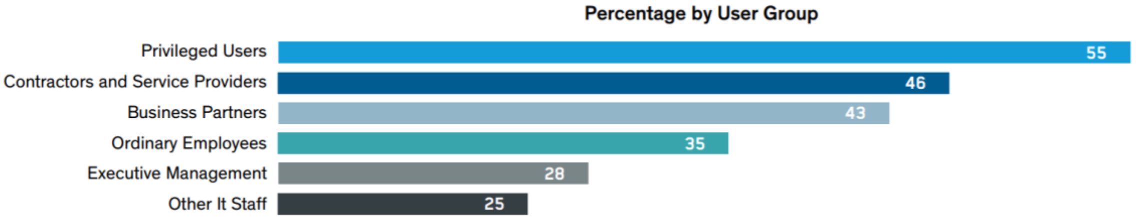


Figure 2.11: Insider Threats By User Group

On the other hand, only 58 percent of the organizations have technology which allows them to control privileged users and only 56 percent monitor and audit privileged users' activities (Vormetric, 2015).

The analysis done by U.S Secret Service and CERT Coordination Center in 2004 found some common characteristics of the insiders attackers in many organizations:

- Most of the insiders were former employees or contractor at the time of incident with 59 percent while 41 percent were current employees or contractors of the affected organizations. On the other hand, 48 percent of the former employee (insiders) left their job due to fired, 38 percent resigning and 7 percent only lay off.

- More than 77 percent the of insiders were full-time employed, either previously or currently working in technical position within the affected organization, while only 8 percent of the insiders have been working part time, 8 percent have been hired as contractors, 4 percent as temporary employee and only 2 percent working as subcontractors.

  - According to the study 86 percent of the insiders have been working as technicians as:

    - System administrators (38%).
    - Programmers (22%).
    - Engineers (15%).
    - IT specialists (15%).
    - Other professional positions (10%).

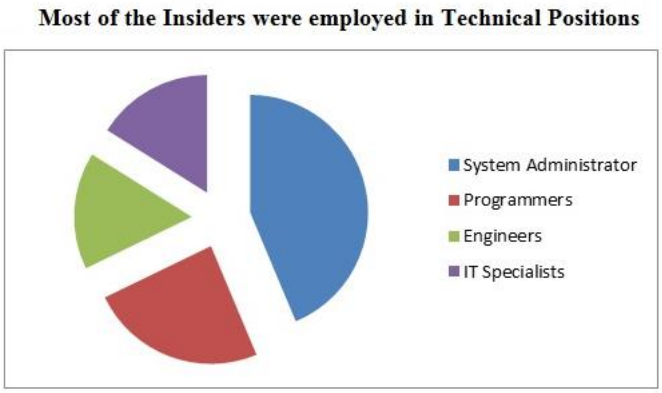


Figure 2.12: Insider Technicians Types.

The insiders age have been ranging from 17 to 60 years, with 96 percent of them being male and 49 percent being married, while 45 percent have been single and only 4 percent divorced at the time of the incident. 30% of the insiders have been previously arrested for various crimes such as:

- Violent offenses (18%).

- Alcohol and drug offenses (11%).
- Nonfinancial fraud and theft offenses (11%).

2.3.3 Malicious and Non-Malicious Insiders.

There are a large number of users (insiders) who never act dangerously. According to (Hayden, 2014) the insiders can be divided into categories based on their intent: malicious insiders and traitors who are motivated by malevolence or profit, enthusiast who are motivated by strong belief or ideology, and non-malicious insiders who are just browsing from curiosity, or users with positive intent who could cause incidents accidentally. Malicious and non-malicious insiders will be analyzed in more detail in the following.

2.3.3.1 Non-malicious insiders (Unintentional):

Non-malicious insiders are users who can cause damage to an organization unintentionally by their behavior or action. From large collection of security incidents the data breach investigations report by Verizon from 2013 mentioned that 14 percent of the incidents were caused by unintentional insiders, while much higher percentage were malicious and deliberate in nature. Still there is a perception that they are intentional, from low-skilled technical events such as sending sensitive documents to the wrong recipient, to the less-frequent mistakes which require special skills such as system administrators and programmers errors.

Incidentally the unintentional insiders may expose information which can be compromising the security due to the accepted organization work processes because poor training or low quality tools at work. For example some users send work containing sensitive information to themselves, use personal emails like Hotmail or Gmail, or share information on cloud storage beyond the organization control. All these actions can put the organization at risk of compromising the confidentiality and the privacy of the information.

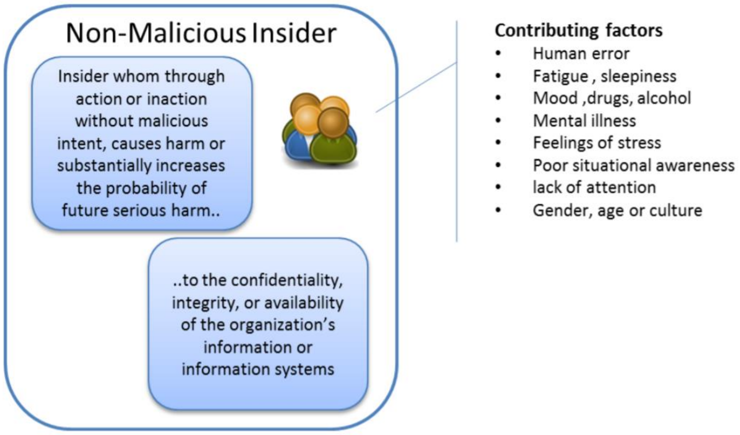
According to CERT non-malicious insiders cause security accidents unintentionally for many reasons, which include stress, poor situational awareness, human error, overwork or exhaustion, bad mood, lack of attention, drugs and other psychological, health of cultural factors like age, gender and education. The CERT defined the Unintentional Insider Threat (UIT) as *caused by* non-malicious insider when *"**a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or***

substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems".

For example accidental or unintentional security exposure can happen by giving undue rights to the wrong people, writing configuration errors, disabling security features, ignoring vulnerabilities during software development and forgetting unencrypted USB or portable storage device containing sensitive data unattended in a public place.

Some external organization or groups are attacked by worms and viruses, which are generated with no specific target but are propagated as far as possible after revealing the existing vulnerabilities, compromising the systems and exploiting them without targeting them specifically. Insiders can unintentionally help spreading out such non-targeted malware through participation in social engineering, distributing infected removable media, visiting infected web-sites or opening unprotected attachments to emails.

The incidents could be more risky when the attack is specifically targeting the organization. Such attacks are called Advanced Persistent Threat (APT) and they are originally designed to improve the likelihood of success. For example, the insider user receives an email message from an outsider, which looks like sent from a friend with normal information, written in a conversational style used by him. These trusted messages may contain hidden scripts of programming code, created by an attacker and the unaware recipient may be tricked to perform an act which unintentionally leads to a security breach.



Insider whom through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm..

..to the confidentiality, integrity, or availability of the organization's information or information systems

Contributing factors

- Human error
- Fatigue , sleepiness
- Mood ,drugs, alcohol
- Mental illness
- Feelings of stress
- Poor situational awareness
- lack of attention
- Gender, age or culture

Figure 2.13: Non-Malicious Insider Contributing Factors

2.3.3.2 Malicious insiders (intentional):

The main issue with the insider threats is that this type of users are considered trusted employees, while they could betray their commitment and loyalty to their employer. This changes the problem itself, because the users are given legitimate access to the organization's systems and information with the hope that they will definitely act in proper way all times.

According to (Cappelli et all, 2012), a malicious insider is *"**a current or former employee, contractor, or other business partner who has or has had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems**"* where 'other organization or business partner are employees at the Internet Service Provider (ISP) , outsourced bodies or remote partner companies.

Another definition which is essentially similar but is formulated in a more military-language as opposite to the usual commercial language sounds like the following: "***anyone who is or has been authorized access to a DoD information system whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector and exceeds or abuses their authorized access to exploit, attack or otherwise misuse DoD information systems***" *(*Smith,2015).

With reference to the above definition, an insider isn't considered as malicious until he abused his access to commit a breach, while before this incident he was just a normal insider, However it is worth considering at least the opportunity that a person may change and from an insider may become malicious insider.

Most employees join the public or private organizations without any malicious intent or wish to abuse their position, but after a while due to various reasons they may decide to become malicious. Such employees are called "Self-initiated insiders". On the other hand, exploited insiders typically join the organizations without any intent to cause harm but are forced to do this at a later time. And finally, malicious insiders are those users or employee that join the organizations with a deliberate intent to use their legitimate privilege for exploiting the information systems and abuse their privileged position (Smith, 2015).

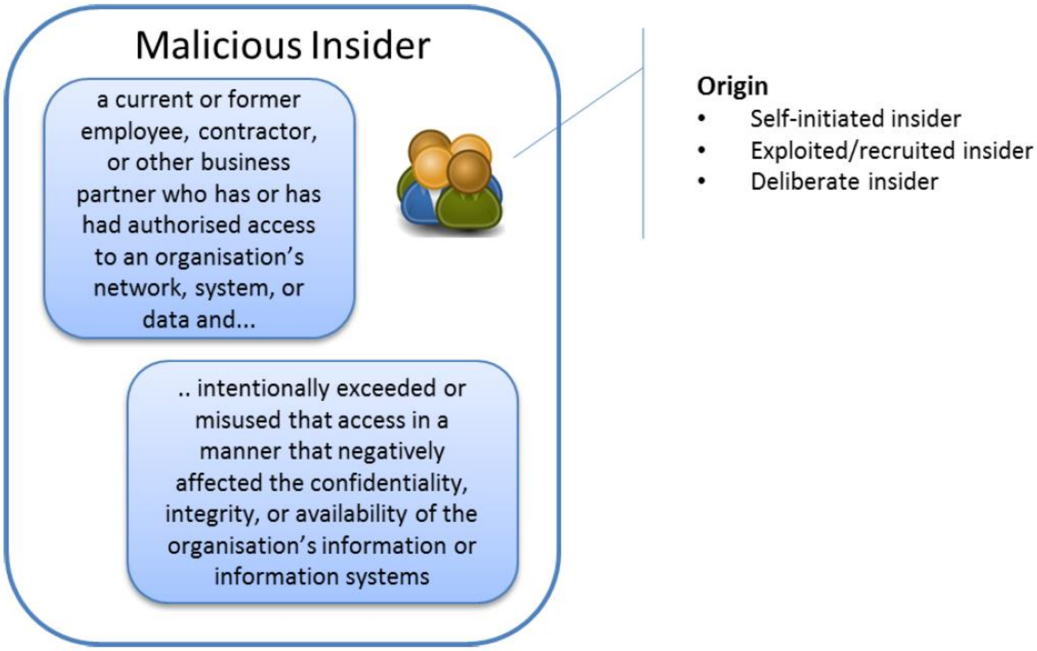

Malicious Insider
a current or former employee, contractor, or other business partner who has or has had authorised access to an organisation's network, system, or data and...
.. intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems
Origin
• Self-initiated insider
• Exploited/recruited insider
• Deliberate insider

Figure 2.14: Malicious Insider Origins.

Any individual insider who shows these characteristics may reach the point where he engages in harmful activities against the organization. One of the best prevention solutions is to observe and document the behavior indicators of inside employees or authorized users. There are many behavioral indicators which indicate potential malicious activities:

- Remote access the organization resources while on holyday, vocation, at odd times, or on a sick leave.
- Attending and working at odd hours without permission or authorization.
- Demonstrating enthusiasm for working during weekends or overtime.
- Coping confident data or information, especially proprietary or classified in nature.
- Paying attention to matters beyond their scope of duties.
- Personal vulnerability indicators like drug addiction or alcohol abuse, gambling, financial problems, mental health swings or violence tendencies, illegal activities, etc.
- Warning signs such as unexpected acquisition of unforeseen wealth, unusual overseas travels, irregular working hours or unexpected absences (Smith, 2015).

2.3.4 Insider Threats.

Michael Chertoff who was Homeland Security Secretary asked The National Infrastructure Advisory Council (NIAC) to initiate Insider Threat to Critical Infrastructures Study in 2007, including the definition of “Insider Threats" for physical and cyber security. He also requested from the NIAC to produce analysis of all negative economic consequences of insider threats. The following is the conclusion of the NIAC's study:

"***The insider threat to critical infrastructure is one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity’s security, systems, services, products, or facilities with the intent to cause harm***" .

The NIAC's definition of the insider threat is strictly focused on the access to the systems, network, database or information systems, where most of the infrastructure’s vulnerabilities exist.

A review of the literature produced by NIAC in their Insider Threat to Critical Infrastructures Study report shows three factors which permanently produce internal threats:

- **Terrorism,** involving deliberate and politically motivated violence against non-combatant targets by secret groups or agents.
- **Spying,** the practice of espionage or the use of spies to obtain confidential or sensitive technical information about the plans, studies, developments and activities of organizations, which can be foreign private or public (organisations), governments or rival companies.
- **Corruption,** where illegal behavior from powerful people such as government employees or police staff that abuses the given power in favor of private interests.

(Munshi et all, 2012) define insider threats as " ***the potential harm posed by any trusted entity with inside access to the organization, each trusted entity will have a different level of trust assigned, appropriate to their position and role and each trusted person will be influenced by different factors, thus resulting in different behavior*** ".

Insider threats are caused by a wide range of criminals who maliciously or mistakenly do things that expose the organization and its information to risks. The insider threat phenomena is becoming more and more complex to deal with as the offenders are no longer the typical insiders and often go beyond legitimate users and privileged IT staff.

The traditional concept of cyber security focuses on protection against attacks that arise from external sources, while much greater threats to an organization's information system exist inside, as is proved in many recent surveys like "Insider Threats Spotlight Report 2016", "SANS 2015 Survey on Insider Threats" and "2016 Internet Security Threat Report - Symantec".

The statistics from the Vormetric Insider Threat Report 2015 shows that the level of awareness of insider threat has increased. Only 11 percent of the respondents felt that the organization which is they working for were not vulnerable to insider threats. On the other hand, almost 93 percent of IT based organizations were looking forward to increase the budget in order to improve the security and to protect the information in the following years.

While globally nearly 89 percent of the respondents accepted that their organizations were more at risk from an insider attack, with 34 percent feeling that they are extremely vulnerable. However, when asked about who represents the largest internal threat to organization data, 55 percent pointed at the legitimate privileged users.

To emphasize this point, a recent research by "Clearswift", which is an information security company situated in the UK which provides security solutions to protect organizations data from internal and external threats, reports that almost 58 percent of the reported security cases were due to insider threats. The insider threats issue is reported by a number of recently published and high profile incidents of data leakage and exposure.

In last decade, many high-profile incidents involving trusted insider employee or user inflicted damage to the organization. Some examples:

- A Stuxnet attack is a computer worm targeting industrial computer systems (programmable logic controllers, PLCs). Stuxnet is a U.S. and Israel cooperation project which was responsible for causing damage to almost a fifth of Iran's nuclear centrifuges by causing them to spin out of control. Such functionality uses private networks with no uplink to the public network which has very strict access policies so that the malware infiltration can be done only by an insider. The initial infection happened outside the nuclear plant, but the technicians who were responsible for maintenance of the targeted PLCs unknowingly connected an infected USB drive into the secure plant, and the payload was activated on the PLC maintenance computer.

- Edward Snowden was a contractor responsible for developing or maintaining critical systems. He was a system administrator within the Central Intelligence Agency (CIA), but jointly worked as a contractor for Dell and Booz Allen Hamilton. He was responsible for designing and managing of systems for the National Security Agency (NSA), one of their largest customers, and had access to highly classified data for several years. He copying sensitive classified information from the National Security Agency (NSA) without authorization and exposed all documents in his possession to journalists in 2013 who in turn published them in The Der Spiegel, Guardian, The New York Times and The Washington Post.

- In 2010, Bradley Edward Manning was an intelligence analyst in the US forces. He was convicted of several crimes under the US Espionage Act and several other after leaking the largest number of classified documents in US history. He released also Iraq and Afghan war logs to Wikileaks. Among the documents he leaked to the press was the controversial *'Collateral Murder'* video, documenting a friendly fire incident where an Apache attack helicopter attacked journalists in Baghdad.

- Former product engineer for Ford Motors Company from 1997 to 2007, Xiang Dong Yu, a 49 years old Chinese was sentenced to 70 months in federal jail and ordered to pay a fine of $12,500 as a result of accessing Ford trade secrets and copying more than 4,000 Ford documents onto an external USB, including sensitive design documentation on which Ford spent millions of dollars and decades on development, research, and testing.

These reports cover perhaps only a small percent of the cases of insider threat worldwide. It is widely accepted that there is an abundance of insider cases which have never been reported due to many reasons, for example as a result of fear of damaging the organization's reputation or missing unnoticed attacks due to the lack of proper threat detection tools (Noonan and Archuleta, 2008).

2.3.5 Scope and scale of the insider threats.

The main issue with insider threats is that such type of threats exposes very high risk to an organization's security information infrastructure, which cannot be ignored. Malicious insiders are not the same as hackers in many aspects. They are very hard to identify and control so it is easy for them to hide their malicious or deliberate behavior within organization's information infrastructure. The employees, customers, vendors or contractors who have legitimate privileged access to the information and the network system will deliberately be tempted to compromise the confidentiality, integrity and availability of those information resources.

The power of today's emerging technologies, the wide spread use of portable and removable drives, as well as the increased use of cloud storage allows the insiders to transfer large amounts of data in just seconds, which means more damaging information, higher vulnerability and bigger exposure to attacks. This gives an idea about the scope of the problem of insider threats, potentially more damaging than any other types of threats in the world of the Critical Information Infrastructures (CIIs).

Although it is unquestionable that the interconnected information system have clear advantage since they help sharing the information, speeding up the decision making and increasing the accuracy, they also have some disadvantages. The information system today is more vulnerable to insider security threats, because even if the insider works only in a certain position, he has the capability and the ability to compromise the entire organization's system. The effect of this could be easily cascaded geographically from purely local to regional and even global.

Many insiders have big experience and knowledge about the specific security measures the organizations apply to physical and virtual assets and they can use it to make the threat harder to detect or prevent. Without suitable and well-designed procedures, the organization security systems are threatened by insiders who have admin passwords and can access secret information which can cause serious damage to the organization reputation.

The study conducted by NIAC found that the insiders' threats on critical infrastructure-level may lead to the following possible consequences:

- The interruption of critical information infrastructure services directly affect many other services which are depend on the information system

- They could affect indirectly other geographic areas or sectors of the economy.

- They may lead to physical damage and financial losses - material loss of critical intellectual assets, financial failure of a service provider, loss of economic competitiveness with other countries on regional or global level, affecting the ability to deliver vital infrastructural services as a result of large-scale economic losses.

- They can have psychological effect which leads to loss of public integrity and confidence in services which damages the reputation of both private and public organizations.

- Potentially, they can also cause loss of life or expose of public health to dangers through damage to the critical health infrastructure or public transport system like corrupting traffic signals or airports systems.

The effects of insider threats can be cascaded to larger geographic areas and other infrastructures, even beyond the borders to other countries and economies as it happened as a result of 9/11 attack on the World Trade Center, which affected the national economies worldwide (Noonan and Archuleta, 2008).

2.3.6 Potential Actors and Motivations.

Insider threats mitigation should be aligned with precise understanding of the potential insider threats. The full understanding of potential insider threats must account the potential malicious behavior, all types of potential insiders, insiders' abilities and capabilities to attack critical infrastructure services, and the real motivations behinds the attacks. Each employee who demonstrates disloyalty by being an insider can be classified into three different types:

- Psychologically motivated insiders - disgruntled or alienated employees.
- Ideologically motivated insiders – motivated by ideology, religious beliefs and radicals ideas.
- Criminals.

The above mentioned types are distinguished on the basis of the insider motivation, which is not necessarily correlated with the characteristics of the insider.

Over the last decade, the insiders have demonstrated variety of motivations: they can be active or passive, directly involved in criminal activities or not violent at all. The word "motivation" is usually used to describe the driving forces that leads to insiders' intention and attempts to perform malicious activities.

There are multiple factors which motivate the insiders to perform malicious activities. Among them are personal threats, manners of thinking or ideological reasoning, financial gains, psychological aspects and other factors such as coercion. On the other hand, insiders could work independently or in cooperation with other malicious groups. They could convert from a normal insider to a malicious one influenced by a single stimulus which triggers their desires, or act in a willful and well managed act, based upon their motivation.

Further, the passive insiders limit their participation to providing information to adversaries that help performing malicious act. Active insiders, on the other hand, are considered key actors that take effective part in an inside attack and are intentionally willing to provide information or assist in performing act.

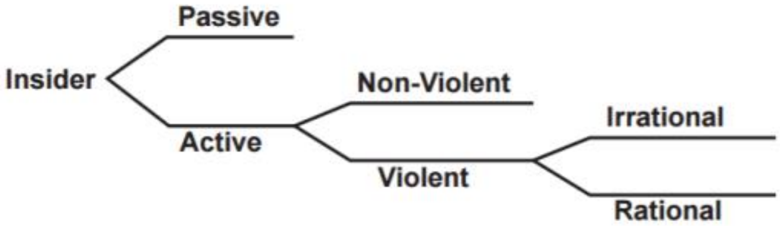


Figure 2.15: Malicious Insider Participation Type 1.

Limited or temporary Insider - this type of insider participates in an attack on a one time basis, or participates in some process of malicious act only once.

Expanded or permanent Insider- an insider who is participating most of the time and is acting as well as continuously participating n a malicious attack over an extended period of time.

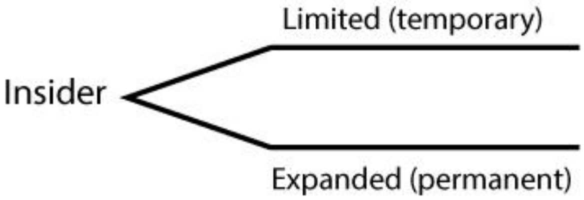


Figure 2.16: Malicious Insider Participation Type 2.

The motivation for insider threat falls into one of the three broad categories, each of which requires specific measures to mitigate the threat.

1) The threat can come from idealists like Snowden.
2) The threat can also come from employees motivated by monetary benefit.
3) A broad threat exists from non-malicious behavior that results from carelessness or lack of competence.

Motivation to attack gives a clear idea about the reason why an insider might desire to attack the organization. The concept of attack motivation is well addressed in the information security and threat-assessment field where the motivation in general is categorized into different reasons and can summarized as follows: political, revenge, financial, power, fun or curiosity, peer recognition, or competitive advantage

According to research reported in (Nurse et al, 2014) it is found that the insider's current psychological state is the most significant motivating factor which lead them to intentionally attack. For example, the contractor's inconvenience caused by the lack of respect might increase the desire for revenge, unlike the fear of being dismissed from the organization.

According to the research the reasons why an employee would engage in an insider act are complicated and have many facets. Insiders in many cases have more than one motivation for their malicious act, as found in almost third of the investigated cases. The percentage of different motivation factors is as follows:

- Financial gain (47% of cases)
- Ideology (20% of cases)
- Desire for recognition (14% of cases)
- Loyalty to friends/family/country (14% of cases)
- Revenge (6% of cases)

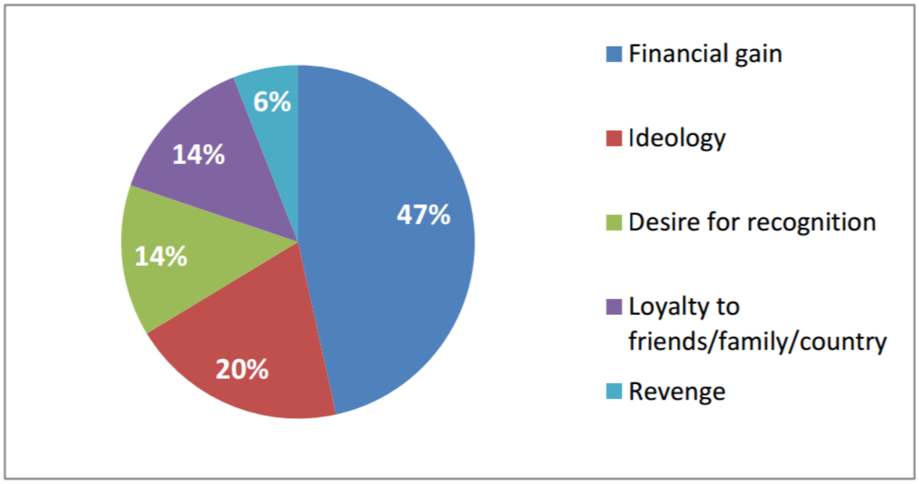


Figure 2.17: Percentage Motivation Factors.

Monetary Motivations: an outside party lures a trusted employee from public or private sector with an offer of financial gain in order to get insider information. The employee accesses confidential information source and copy it on a storage device, preparing it for exchange with specific party, while as an insider he thinks his malicious behavior is justified. In reality, the organizations tolerate damaging the integrity, confidentiality and lose of reputation due to the sensitivity of the information, and some organizations and parties have long term engagement with some specific insiders to obtain leaked information. In 2013 Colton Millay, an US information system specialist received a jail sentence for spying and trying to sell secrets US military information to Russia for financial gain (Cappelli et al, 2012).

2.3.7 Contributing Factors.

Insiders using legitimate and authorized access to their organizations information infrastructures and system pose a serious risk to the employers. Employees with financial problems could easily use the systems they use every day to commit fraud. Other employees have been motivated due to financial problems, revenge, greed, a desire to gain business advantage, or a desire to persuade a new employer to steal confidential data, private information or intellectual property from the other employers. In addition, technical staff could use their technical capabilities to sabotage employers' systems or networks in retaliation for negative workplace events.

A survey conducted by (Munshi et al, 2012) states that the Major factors contributing to insider threat behavior can be summarized in the following:

- **Access and level of trust:** giving possibility to avoid physical and logical controls because detecting and preventing can rely on their own knowledge of protecting methods, policies and countermeasures. The research claims that the level of trust the insiders are holding is one of the critical factor which motivates them to perform successful insider attacks. The academic literature reports that 67 percent of the insiders had authorized access to the information they stole (Moore et al, 2008). According to the same source 75 percent of the insiders with authorized access performed theft (Cappelli et al, 2012).

- **The insider technical position or technical skills:** usually insiders have familiarity with the systems and they use their skills in malicious activities, such as downloading and installing hacker tools, gaining remote access, setting up and using backdoor accounts after termination. Nearly 70 percent of the suspected insiders were holding technical positions like system administrators, engineers and programmers.

- **Motivation to perform malicious act:** insiders attack motivation can be classified into three main different types: IT financial gain, sabotage and business advantage. The motivating factors increase the ability of insiders to abuse their organizational information system and its assets. Most insiders in the financial fields, such as banks and stock markets, are motivated by financial gain but they comprise less that 50 percent of all cases, while revenge occupied almost 84 percent of the cases of insider threat against their organization due to negative event such as termination or transfers, dissatisfaction, strict managers, and demotions (Moore et al, 2008). Finally, insiders motivated by business advantages count for nearly 32 percent of the cases of stealing information for getting a positive advantage at a new job or for initializing a new competitive business (Cappelli et al, 2012).

- **Outsourcing increases the possibility of attack:** many recent researches undertaken by specialist determine that there is a fast increase in the number of third party users who have sufficiently long period of access to organizations' systems and the critical information in them. In some organizations third party workers and partners have the same type of authorized access as an employee to both physical and logical assets, and this legitimate access increases the possibility to have an attack. On the other hand, most of the studied show that the contractors were linked to less than 20 percent of the insider incidents (Moore et al, 2008).

- **Cultural factors**: include manner of thinking, religious beliefs, ethical values, psychology, experience and attitudes toward their organization. Most of the data sabotages reported by UK government and the HRMC cases indicate that only 5 percent is caused by technical factors while 95 percent is due to cultural factors.

- **Lack of organizational security policies:** poor and inappropriate organization security and technical policies are caused by human factors. According to (Cappelli et al, 2012) and (Moore et al, 2008) in 62 percent of the incidents they studied the insiders exploited the vulnerabilities of processes, policies, procedures or applications and in most of these cases the attacks were committed due to the lack of physical and technical access control policies.

- **Psychological factors:** the main issue with this factor is the complexity in identifying the serious criminal intent or behavior toward their coworkers or organizations, because most of the time they conceal themselves and their behavior from observation, monitoring and detection. It is very difficult to predict the malicious intent of insiders but there are some characteristic can be observed which can be increase the probability of predicting harmful behavior. Such indications are: a history of personal and social discouragement, lack of empathy, ethical lapses, a sense of entitlement and computer dependency. According to a joint study by United States Secret Service (USSS) and CERT 80 percent of the insiders who committed attacks on their organizations were motivated by negative psychological factors before the incident, and 92 percent were affected by negative job events like transfer, demotion, termination or warning.

- **Remote access:** there are small a number of academic researchers considering remote access as a factor in insider threat behavior. The reports published in (Cappelli et al, 2012) and (Moore et al, 2008) conclude that 64 percent of the insiders used remote access to perform attacks, and 43 percent of them were outside the workplace when they attacked.

- **Gender:** most of the study done by researchers and specialist show that male was the predominant gender involved in criminal activities. According to (Moore et al, 2008) in 82 percent of all CERT studies the insider was male and 91 percent of the insiders who stole intellectual assets were male gender.

(Moore et al, 2008) published a (big picture) report about insider threats, and reported a number of important observations supporting the factors that could contribute to an insider attack. Their study focused on analysis of every elements of the insider incidents, such as characteristics of the insider, technical skills, designing and preparing before the attacks, identification and detection of the insider, and outcome of the attack. In the (big picture) analysis of insider Information Technology (IT) exploit they mention seven different observations which could identify factors contributing to the betrayal inside employee as follows:

Factor (1): Personal predispositions give clear idea why specific insiders perform malicious activities. Personal predispositions include different factors that influence insider to perform malicious behavior which are:

- Mental health problems: drug addiction and alcohol habit, seizure disorders, physical abuse by spouse and panic attacks.
- Social and decision making skills: being horrified and intimidated by other insiders, detecting unprofessional job skills, schizophrenia or personal conflicts, personal cleanliness problems, and inability to comply with the rules.
- Rules violations history: some insiders have a previous history of government or security law violations, hackings, arrests due to law violation, and complaints about harassment.

Factor (2): Disgruntled due to unmet expectations: The study found that 57 percent of the insiders were disgruntled due to some negative expectations, 84 percent planned to take revenge after negative work related incident like termination, conflict with an existing or former employer, demotion or transfer and almost 92 percent of insiders attacked their organization.

Unmet expectations include lack of promotion, unsatisfactory salary or bonus, shortage of the available organization resources, violations of the privacy in the workplace, reduced responsibilities or authority, perceived unequal work requirements and poor relationship within the organization employee.

Factor (3): stressful events; according to the study in several incidents potentially stressful events, like organizational sanctions, were effective factor which contribute to the willingness of the employee to sabotage. Almost 97 percent of the insiders security breaches were related to one or more stressful events like sanctions exposure and different potential job related events, while most of these attacks took place after suspension or termination from organization or job due to poor performance, excessive absence without acceptable reason, unacceptable acts during the duty time and various other reasons.

Factor (4): The ignoring behavioral of the organization which was clearly able to observe the potential damage but for different reasons simply ignored it. The research reports that 97 percent of the insiders malicious behavior was observed or known by the managers, supervisors or staff but was ignored due to some reasons. The observed behavior in many insiders' malicious incidents was in conflict with the managers or other staff, drug abuse, aggressive or violent behavior, uncontrollable change of mood, frequent absence, sexual harassment and others.

Factor (5): In many incidents by insiders sabotage the organization failed to detect individuals who by involving computer or storage media were able to perform malicious insider attacks. In 87 percent of the cases the IT sabotage remained undetected due to the organization failure to document system error warnings, unauthorized access logs, inappropriate Internet access, downloading and using of hacker tools and setup or use of backdoor accounts.

Factor (6): Insiders (employees, contractors and partners) create access paths that remain invisible to the organization management just to hide their identity and set up a base for an attack in the following days. In the above report 75 percent of the insiders created access paths unknown to the organization, 59 percent of the samples were former employees, 57 percent were without authorized or legitimate access to system at the time of the attack, and 64 percent of the insiders used remote access. In many cases insiders use privileged access to create a malicious code or triggers to perform an attack before termination using backdoor accounts, installed remote access tools, patches for password crack, connect private network with internet uplink to access organization systems.

Factor (7): Poor access control to the physical and IT facilities contribute to encouraging the insiders to perform security breaches or to cause damage. The study found that 93 percent of the insiders exploited imperfect access controls which include employee PCs left logged, The insiders can create access accounts unknown to organization with legitimate privileges, and are able to install malicious code and patches to production systems without knowledge of the organization and without ability to disable the system or with purely physical access control (Moore et al, 2008).

2.4 Related Work.

Nowadays the ICT security of critical information infrastructures is a prominent problem. In many cases risk assessment methodologies must be applied in order to have effective solution. The necessary data must be provided to check the functions and the behavior of the system being analyzed to reveal its vulnerabilities.

A number of papers have been published in this area. The more interesting contributions are summarized below.

(Suter et al, 2007) proposed a framework for protecting critical information infrastructure which they modeled after the Swiss Reporting and Analysis Center for Information Assurance (MELANI). The aim was to build confidence in securing the ICT infrastructure framework. They defined a generic framework which can be used in different countries to determine the actions against the challenges of critical information infrastructure protection and specifically the ICT infrastructure. The framework is designed according to the four pillars of CIIP: Prevention and Early Warning, Detection, Reaction and Crisis Management.

According to (Chaturvedi et al, 2007) the ICT infrastructure is the main interconnecting line between critical national infrastructure components and the existence of a cyber security framework is a prerequisite for all e-governments and the e-commerce worldwide. They reveal that the three main functions of any Critical National Infrastructure are business continuity, government operation, and national defense and all they depend on the network of critical information infrastructures. They produced an overview of different initiatives at international level starting from NATO, EU as well the USA and UK approaches for data protection and privacy. They developed a framework, called the 4-E framework based on four main elements (Engage, Educate, Enact and Enforce) and proposed it to the National Association of Software Service Companies of India (NASSCOM) and it was adapted by the Data Security Council of India.

(Bruce et al, 2010) published an article about ICT and critical information infrastructure secure communication model for risk management that can be applied on both national and international level in both public and private sectors. This article is referred to as International Policy Framework for Protecting Critical Information Infrastructures since it outlines various problems in national and international polices worldwide. They agreed that the network model should reflect on how different users in the public and private sectors cooperate to manage future cyber risks rather than on focusing on function, information flows, processes and procedures within the sectors. Furthermore, this model contains three groups of stakeholders - policy makers, policy implementers and operational personnel and they can exchange three different types of information within the cyber security area: response, policy and assessments.

Information Sharing and Analysis Center (ISAC) is one of the trusted organizations created by Critical Infrastructure Key Resource (CI - KR) which prepares information analysis shared with both private and public sectors. The ISAC proposed a framework for exchanging information between different organizations which allow communicating securely within the same or different sectors and between different private and public sectors. Recently the model has been adopted by the US Department of Homeland Security which established ISAC's secure communications to allow sharing information within their critical infrastructure for maintaining of continuous work and for protection of the economy. In other countries the ISAC framework is considered a trusted information sharing network. The United Kingdom authorities adapted ISAC framework after it was approved by Assurance Report Program (Bruce et al, 2010).

(Goodman et al, 2010) state that the main problem with Critical Infrastructures is the dependence on ICT and CIIs which are complicated and include vulnerabilities due to complexity, accidents, and hostile intents. Most of the ICT is designed and applied with very low level of security assurance or primary security considerations which can be easily exploited over the networks or through vulnerable components. According to their approach the security is a process, not a product and should be defended through options like Preventing an attack, Thwarting an attack, Limiting the damage during successful attack, Reconstituting after an attack and Improving defender's performance. Based on the survey of national and international security initiatives and standards focused on critical information infrastructure protection they conclude that ideally, an international network framework should be introduced to deal with the problem of preventing, thwarting and punishing attackers on cyber systems. To overcome the worldwide misunderstanding and unawareness of the cyber threats it is of paramount importance that internationally cooperative actions are taken against those who threaten the network critical information infrastructures.

(MacDermott et al, 2012) presented a research paper related to the protection of critical infrastructures and the intrusion detection. They also proposed a framework for critical infrastructure protection based on SCADA security review. They found through the research some critical weaknesses in the creation of critical infrastructures. The main focus of their research was to develop a framework for protection of critical infrastructures based on network intrusion detection. The framework is connected to an external component from the SCADA network that works as middleware between two different networks. Through such a separation they aim at using network sensors to collect and analyze the traffic which passes through the network for real time monitoring. Secondly, this would allow adding a security layer that can run over the SCADA network without disturbing the other networks.

(D'Antonio et al, 2006) introduced in the first international conference on Critical Information Infrastructures Security their framework for protecting critical information infrastructures. According to the article the most effective way to address the network security is through strong intrusion detection and tracing the path of the attack back to the source. They developed a security framework based on two different approaches just to detect an intrusion: precise classification that classifies the behavior of each user by the means of a specific model and approximate classification relying on generalization of the behavior. The behavior of each separate users is generalized from base properties within the classification model. This type of generalization approach uses data mining methods.

(AMICI et al, 2004) state that the group of critical infrastructure specialist in Italy cooperate with various public institutions who are the main operators of critical infrastructure. They are operating companies and are engaged in the security of telecommunications networks as described in a book under the name "Network security in Critical infrastructures". The group worked on analyzing the continuity of operations and the security of critical infrastructures. This book is the best reference for an initial proposal since it has a complete information about network security in critical infrastructures. The book shows that the daily increase in the level of interdependence between different infrastructures leads to an increase of the threats that exploit the infrastructures thanks to the spread of ICT. This book is published by the Istituto Superiore delle Comunicazioni e delle Telecomunicazioni, the Observatory for Communication Network Protection and Security.

2.5 Actor Network Theory, a New Approach.

2.5.1 Introduction.

In recent years cyber security related events like Duqu, Flame, Stuxnet or Gauss have led to the understanding that cyber incidents have become more frequent, sophisticated, organized and dangerous and this increased the awareness of cyber-security threats and raised the priority of the issue to the top of security agenda worldwide

Infrastructure security research can be classified into two main categories: technical research, which is focused primarily on the network design and on securing the ICT components that help protecting the information resources, and socio-technical research mostly focused on the organizations management and employment issues related to the information security. Actor-Network Theory is one of the most famous socio-technical theory today and it has being in the focus of many researchers (Hedstrom et al, 2010).

Actor-Network Theory was introduced in the 1980s at the Centre de Sociologie de L'Innovation (CSI) by Callon, Latour and Law, French philosophers, supporting the processes of innovation and knowledge transfer by explaining the science and technology development from the perspective of semiotics. Actor Network Theory (AN)T is difficult to define in exact terms due to two different reasons:

- ANT has different names formulated using different terms like Agent Network, Sociology of Translation and Social Network Theory.

- ANT is the crossing point between a confusing set of theoretical genealogies.

About the Actor Network Theory among social experts is well known fact that it has totally flat social topology which rather than having small structures includes large ones. On the other hand, the ANT concentrate on the connecting elements, like connectors of actors to networks and connectors of networks to actors. Information security requires change in the model to remove the deviation and avoid the problems in containment-based modeling.

ANT describes how different actors form alliances in order to influence other actors to use non-human actors like technology for joining the alliances as well to strengthen their interests (Huang and Hsieh, 2011) . On the other hand, Actor Network Theory does not specifically explain why the network is build up in such a manner, focusing on how the actor networks gets created, retains its integrity, or crumble. Actor network theory (ANT) "**examines *the motivations and actions of actors who form elements, linked by associations, of heterogeneous networks of aligned interests***" (Walsham and Sahay, 1999).

ANT considers all elements within the network, human and non-human, as one and the same, or at least described in the same term, called "generalized symmetry". According to the theory the relationships between them arises in the network, it hasn't existed before. Also according to the theory any type of behavior can't be performed by only a single actor, usually it is a combination of related existences and without it, the procedure would be different. In more details, when actor interacts with other actors, these interactions are connected through external networks of non-human artifacts.

ANT is useful in the examination of the actors' behavior and motivation since they form elements, connected by entities of heterogeneous networks aligned with interests. Also, the theory helps to understand the transformation and construction of different (heterogeneous) networks, including the social and technical networks, which means that the theory links both the technical and non-technical elements, The theory is significant, but still potentially discord in its way to understand human or non-human behavior and its impact on inanimate objects (Hedstrom et al, 2010).

The ANT in general deals with symmetric and material heterogeneous networks, in which the actors are both humanoid, like people or robots, and non-human phenomena, such as technologies, machines and organizations. So ANT can be classified as a semiotic model which links the material items with semiotic concepts. The non-human elements and the people together are analytically treated the same way by ANT. In their daily live the people are influenced by several factors, both social and technical, like for example when someone is driving a car he is surrounded by traffic roles, driving skills, road conditions and the car's performance.

According to (Elbanna, 2009) ANT is mainly concerned with finding how different actors define and spread out the roles and motivate or convince other actors to follow these roles, which can be political, technical, social or routine, while the target objects that are aimed to fill the roles are heterogeneous and include people, organizations, machines, or scientific findings.

ANT makes possible an objective view of the daily behavior or activities, giving the opportunity to access inside the black boxes and to understand how they had been created and what they actually are. On the other hand, ATN can be used by information systems researches to investigate different malicious network formations by analyzing the human and non-human actors activities involved, the alliances and the networks they build up. ANT allows any type of differences among human and nonhuman actors, but rejects dealing with them separately.

ANT also dive deeply into the networks to interpret how relations are arranged, how they emerge and develop into a network, how they are build and preserved, how they cooperate with other networks and how they became stronger over the time. On the other hand, the interactions between humans are mediated through different non-human artifacts, and these interactions could be mediated through other networks of human and non-human objects or artifacts. ANT also explains how actors join up other actors into their group and how they explain their desires, visions and motivations to these actors (Silic, 2015).

To meet the need to treat both human and non-human actors equally and in a similar manner, ANT is based on three principles: agnosticism, generalized symmetry and free association.

Agnosticism: means that analytical integrity is required by all the actors who are engaged in a project under consideration, regardless whether the actors are human or non-human.

Generalized symmetry: it helps interpreting conflicting viewpoints among different actors by using indifferent terms which work the same way for both human and non-human actors, so both the social and technical objects in the heterogeneous networks can be analyzed from the point of view of their explanatory value.

Free Association: needed to remove all a priori distinctions between social and the technological.

Actor Network Theory is not a theory in the ordinary sense according to Latour himself, because ANT does not explain "why" a network takes a specific form or "how" this take place. But ANT is a method that helps to find and describe relationships between different actors, as Latour mentioned it in his researches in one word, "how-to-book". The main concept of ANT is that the actions usually happen in interaction between actors within the network, when one actor is trying to influence another actor and fight for authority. Most people usually visualize the social interactions between only human actors, but ANT is different than traditional social theories by assuming that the actors are not only humans but also non-human, objects as well. (Jessen et al, 2017).

2.5.2 Key concepts in ANT.

Actor Network theory (ANT) is a flexible form of knowledge that scientists and researchers can rely on as a reliable method. It is sufficient to understand ANT concepts as capable and flexible research tools that support experimental investigations.

The way that the ANT concepts reflect the meanings and how they are applied in different research differs from many other approaches in technical and social sciences. The Actor Network Theory (ANT) concepts are unclear, mysterious and overlapping, which does not explain the issues but helps to identify and characterize them. They focus on experimental problems and issues without providing solutions how to solve them, while the main role left for ANT is the awareness (Bueger and Stockbruegger, 2015).

ANT contains a number of theoretical concepts that can be used to illustrate and to support the analysis. Maybe all of them are not necessary for our analysis, but they can help us to understand how different actors reveal their interests and behave within the network.

The Actor Network Theory main concepts are as follows:

Actor: the concept assumes that everything usually has an active potential, and there is no any difference in the capability of humans, non-humans, material or abstract objects such as technologies to act. Agency can't be only for humans or objects, but can also combine human, artefacts, technologies and social elements. According to (Latour, 2005) the actors are elements of the situation that perform an action which meet or align with their own interests. Actors are also phenomena created by a network of heterogeneous interacting objects or artifacts.

The concept of an actor does not point at the source of an action in the network theory expressions, but it is an expression of the interest of an entity instead. The notion of ‘actor’ is applied equally to all human and non-human elements within an actor-network, such as people, technologies, objects, resources and others. During the generation of actor network some effective actors may convince other actors to be a part of an entity. They could agree or deny based on the following principles:

1. Actors who are not part of a network and don't have any objectives can agree because the controlling actor enrolled them and they accepted their purpose or interest.
2. Some actors may refuse the idea or the role they are assigned to play as unsuitable for their capabilities and abilities.
3. Actors who are offensive reject the objectives of the network.
4. Actors who work on behalf of controlling actor.

On the other hand, association which do not impact the process of controlling a specific network are not actors in that network (Latour, 2005).

Actor Network: actors have individual existence, while actor networks are groups of actors connected with each other through different relationships within the heterogeneous material network. The use of the notion of " network" here is basically different from its meaning in sociology, because it is not originally about linking or interaction between individuals, but it is concerned with the exploration of how different actors identify and hand out roles, how they are persuaded to perform these roles that can be technical, social, political, or educational. In other meaning, it consists of different entities or actors that are joined in an alliance to satisfy their individual aims. Within the entity every actor is working according to his level of involvement to enroll others through convincing them to support their own interests. The strength and the durability of any network depends on the length of the period of time and the number of entities enrolled in.

The objects that are bound to accomplish their roles are heterogeneous and can be identified as people, entities, artifacts, machines or scientific inventions. The actor-network is completed through the process called ‘enrollment’ of human and non-human actors into a network through negotiation and adjustment of their interests. The alignment can't be accomplished before the translation of the interests and the enrolment of the actors is completed within the network. The translation has to guarantee that the interests become fully aligned.

To reach the target, the controlling actors should negotiate with those who are selected to be enrolled on the network. The stability of actor’s network depends on the adjustment of the interests between the controlling actor and the others striving to achieve their own aims (Richerd Heekes, 2013).

Symmetry: in ANT the meaning of symmetry refers to the link between objects and concepts, refusing strict separation of human and non-human, material and non-material actors which should be described or treated the same way, in other words it is "*treatment of humans and nonhumans as a priori equal* " (Tatnall and Gilding, 1999).

Mediators: any technologies that never work as passive objects and that never transfer effects from one actor to another. According to (Latour, 2005) mediators "*transform, translate, distort, and modify the meaning or the elements they are supposed to carry*". Moreover, this concept allows to investigate how the technology produces its effect.

A black box: a group of actors, either human or non- human (device, system, or technology) whose internal functioning or processing system remains invisible for users and does not matter how it works. This concept applies when an object functions perfectly but the requirement is to focus on its inputs and outputs and not on its internal processing system (Bueger and Stockbruegger, 2016).

There are five different ways that a black-boxed actor could use to enroll other actors to have the black box established. They were summarized by Latour as follows:

1. (You w*ant what only you want*), to invoke the other's straightforward interests.
2. (*You want what I want*), to convince the others to accept our interests.
3. (*I will take care of your interests, if you fol1ow me*), to suggest work around.
4. (*We all want this*), to modify goals and interests to reshuffle interests and goals within a new strategy by creating new goals and new groups
5. (*You need me to get what you want*), by becoming essential to the others (Mahring et al, 2004).

Convergence and irreversibility are the two main characteristics by which the connection to one another behavior or action forces the creation of black boxes. But the convergence and irreversibility depend on the effective processes of enrolment and the percentage that the actors have aligned.

According to (latour, 2005) the Black boxing is a complicated relationship of the different actors participating in the overall scheme of action which becomes invisible, so Black boxing is the reflection of the networking in general.

- **Control:** the key actors developing their own plans and strategies to convince others to take specific roles. Whenever actors within the network have been persuaded, their activities support the key strategy of the main actor (the controlling actor) to accomplish their goals that have been set previously for the actor-network (González, 2013).

- **Event:** any type of activities or behavior which should lead to achieving the aim as planned.

- **Affordance:** this is the warranty that objects or non-human artifacts support, encourage, or give facilities to human actions, "action possibilities".

- **Translation (Delegation):** is considered a core concept of ANT; it identifies the type of relations and associations. It is a method for exploring how the heterogeneous networks are formed. Also, this concept explains how different not yet enrolled actors who have never interacted with the network became part of it and start acting as enrolled actors. In other words, the concept of translation is totally about links and relations. Moreover, it is a tool to explore the development of new relations, the role and position of the actors in that relationship, and how they maintain the shape and purpose of their relationship (Bueger and Stockbruegger, 2016). According to (Latour, 2005), translation is the process "***during which the identity of actors, the possibility of interaction and the margins of manoeuvre are negotiated and delimited*". In simple words, translation is "*an attempt to define and control others***" (Leah and Horowitz, 2012).

- **Inscription:** it is the second key concept in ANT's terminology. It analyzes the results of actors' successful translation process. Also this concept shows the stability of the relationship between different actors within the heterogeneous network with identified roles. This concept focuses on how the technology interferes in different practices and becomes part of them and how the technology controls the way that actions are executed. The concept of inscription sometimes refers to a power relationship in which an actor controls the activity of another actor. In general, any heterogeneous network component such as objects, artifacts, practices, skills, organizational arrangements, texts and instructions can be the material for inscriptions (Bueger and Stockbruegger, 2016).

According to (Mahring et al, 2004) inscriptions can be organized around four axes:

1. Identification of clear expectation, view and objectives from which the inscriptions start.

2. How these expectation are transferred and engraved to capture the interest of the actors.
3. Conroler actors who undertake the inscriptions.

4. The power of the inscriptions and their ability to form irreversible networks.

Irreversibility: it is a stage where returning to a point of alternative possibilities is not possible (Walsham, 1997).

2.5.3 The process of ANT.

The establishment of an actor network passes through a process of translations. This process needs different actors in the network to accept the network roles, interests and aims. Michel Callon, together with Bruno Latour one of the leading corroborators of Actor Network Theory (ANT) mentioned in his research that the process of translation is a process of "persuading" which can be categorized into four different phases, called "moments": problematization, interposition, enrolment, and mobilization. The stability of the established actor network can be described through these moments which are overlapped and interrelated.

1. **Problematization:** it is the first step of ANT translation process where some of the actors within the network are looking for definition of the issues or problems and present applicable solution for solving this problem to other actors. In this process step the roles and activities are defined for both human and not human actors (Heeks, 2013).

   During this process the main actor determines the identities and interests of other actors which match his own interest and goals and defines himself as " obligatory passage point (OPP)". The OPP is present as a solution to a problem where all the resources are available to the actors to achieve target aims. OPP also controls the resources that are required to achieve the actors' results. For example in traffic system the OPP is precisely a passage which contains different traffic rules, instructions, objects and roads which make them a strong reliable network (Jessen et al, 2014).

Moreover, in this situation the main actor tries to make himself indispensable for the other actors within the network by introducing the nature of the problem which they are going to face in achieving their goals and aims (Heeks, 2013).

2. **Interposition:** It is the second step of the translation which relates to a series of processes where the main actor convinces other actors that the solutions defined by him is matching their interest and these interests are in line with their own interests. It is another a set of instructions or activities by which an entity tries to force and stabilize the identity of other actors as defined through its problematization. Different objects are submitted and used in these actions for different actors. For example in traffic network the interpositioncan be done by applying the penalty for disobeying the law or the control rules of the traffic, the instructions and signs during the learning processes in which the actor got the driving license (Gunawong and Gao, 2010).

3. **Enrollment:** it is the third process of the translation after the successful interposition which leads to enrolment. This means that the main action in this process of translation is "**negotiation**" that leads to enrolment, where the actors identify their roles and accept them. It is the point where the actor network is involved in defining the roles and setting the strategies which the main actors are looking for and convincing the other actors to join and accept the main aim of the actor network. The moments of enrolment include ***"set of multilateral arguments, strength and power experiments and skillful act or scheme that support the interessements and enable them to succeed. In brief, it is action belong to the other actors acceptance of the aims and goals or interests which defined by a control actor through the process of negotiation and persuading and making concessions"*** (Gunawong and Gao, 2010).

4. **Mobilization:** it is the final process of translation. it is a set of methods and manners where the main actor uses it only to ensure that all member of the network act as planned according to their agreement and will not be deceived that just to achieves network stability. According to (Callon, 1986) Mobilization is a:

> "***Set of methods used by the prime actors to ensure that supposed spokesmen for various relevant collectivities are able to represent those collectivities and not betray them***".

These processes represent the different stages of the main process of translation in which the actors are identified, the possibility of interaction is deliberated, and the boundaries of maneuvering are negotiated and limited.

The above four processes can overlap, but at the end a restrict network of relationships leads to building the actor network. Of course this relationships and the alliances can be broken at any time. The translation becomes disloyalty when an enrolled actor rejects to enter the actor network in order to expand it into the direction of others. It cannot always be taken for granted, and the plans, designs and strategies rely on specific circumstances in which they develop. A brief summary of the four translation processes is shown as follows (Danchao Hu, 2011):

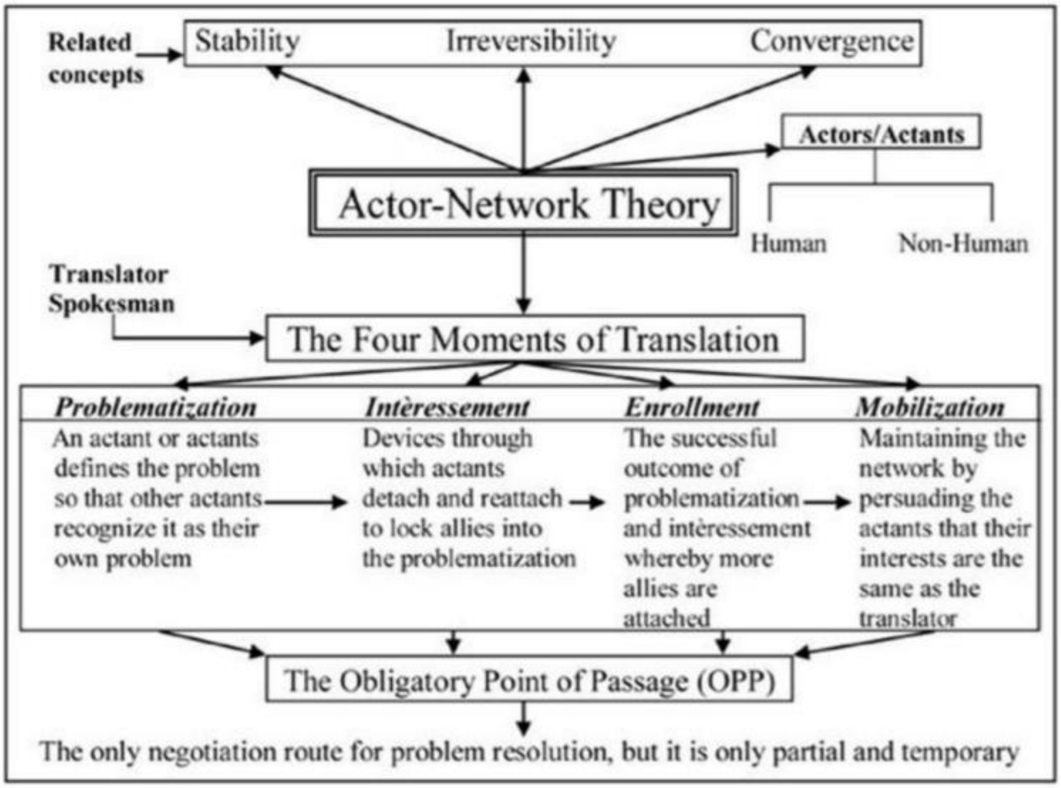

Related concepts
Stability
Irreversibility
Convergence
Actors/Actants
Actor-Network Theory
Human
Non-Human
Translator Spokesman
The Four Moments of Translation
Problematization
Intèressement
Enrollment
Mobilization
An actant or actants defines the problem so that other actants recognize it as their own problem
Devices through which actants detach and reattach to lock allies into the problematization
The successful outcome of problematization and intèressement whereby more allies are attached
Maintaining the network by persuading the actants that their interests are the same as the translator
The Obligatory Point of Passage (OPP)
The only negotiation route for problem resolution, but it is only partial and temporary

Figure 2.18: The Four Moments of Translation.

2.5.4 ANT in Information Infrastructure Research.

ANT has built very strong foundation based on the IS field. Long time back to the beginning of Actor Network Theory (ANT) the researchers knew about the potential of using it to examine the successes and failures of technological innovations. Recently, different Information System (IS) researchers made tremendous efforts to prove the strength of ANT in the field of IS. This is very different from the case of adopting models, such as Technology Acceptance Model (TAM), the Theory of Reasoned Action (RA) and the theory of diffusion of innovation.

A large number of IS researchers rely on ANT. They concentrate their interests mainly on the relationship between Information Technology (IT) and the actors. An ANT concept allows different approaches to study these relationships while looking at IIs. There are, for example, different views of how some basic characteristics of the factors affect the selected delegation network. A list worth mentioning is as follows:

- (Grint and Woolgar, 1997) employed the Actor Network Theory (ANT) to analyze the Luddite movement in England during the 19th century.
- (Monteiro and Hanseth, 1996) researched the role of standards in electronic data interchange systems (EDIs) by applying ANT to critical information infrastructures.
- (Wagner, 2003) did research on the design and application of enterprise resource planning (ERP) systems in schools and universities based on ANT.
- (Spanoli, 2004) also used ANT in analysis of company's conflicts in negotiating and legitimizing new network technology.
- (Vidgen and McMaster, 1996) used ANT to examine the success and failure of car parking systems.
- (Nijland, 2004) did a PhD research on how organisations use IT evaluation methods.
- (Silva et al, 1997) used the concepts of ANT to explain the failure to institutionalise the London Ambulance Service information system.
- (Monteiro and Hanseth, 1996) used ANT for understanding the role of standards in shaping of big Information Infrastructure System (IIS). They also

tried to explore the effects of standards on the accomplishment of resilience in the actor network that is shaped by the TCP-IP protocol.

- (Timmermans and Berg, 1997) Analyze how medical protocols affect emergency medical intervention practices. On the other hand, (Bowker and Star, 1994) try to find out the effect of using the International Classification of Diseases (ICD) within different ANT.

(Cordella and Shaikh, 2006) state that Actor Network Theory (ANT) is widely used today as an analytical framework to assist the Information Security (IS) research as theory which give a sound treatment of the technology artifacts.

According to (Kam, 2015), the security advisor at International Association of Privacy Professionals (IAPP) which is the largest and most comprehensive global information privacy community with resources across Europe that cover more than (70%) of healthcare and business organizations, the negligence of the employees is the biggest insider threat to critical information infrastructure security. On the other hand, Prof. William Buchanan from Napier University declared that top three threats in the computer and information security is "people, people and people", while a famous hacker between 1980s and 1990s stated in a BBC interview that **"*The lethal combination is when you exploit both people and technology. What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time, organizations overlook that human element* "(**Kam, 2015).

There is some misconception that ANT has very little to do with the study of social networks. These studies don't care how interests evolve with the increased social connections of individual human actors but with their distribution, frequency, proximity and homogeneity (Latour, 2005).

2.5.5 Motivation for using ANT.

The Actor Network Theory (ANT) which came into existence in the 1980s was introduced as a conceptual framework for examining the collection of socio-technical processes by Bruno Latour, Michael Callon and John Law. Bruno Latour focused further on how to adapt social, technology and information technology approach as he mentioned in his notes "***The theory is concerned with investigating the social and the technical together***" (Latour, 2005).

The Actor Network Theory (ANT) can be used as a framework that provides the security specialists and administrators with a perfect analysis tool and method to protect IT technology and critical information infrastructure systems. Another useful idea is that ANT eliminates the difference between humans and non-humans. By positioning of the actor in the context of the network it avoids creating discrimination between the agency and the structure. The key concept of ANT is the translation. This is an essential concept of ANT and is one main reason for why the theory is considered to be useful for the logical analysis of the threats.

In ANT, the researchers are involved in analysis mainly to find out the relation between different actors within the network, rather than their inherent nature (M. Aanestad, 2003). This allows ANT to be a relevant tool for understanding the links between different malicious actors since the information infrastructure components work in a consistent relationship with the actors that build up the network.

According to (M. Aanestad, 2003) the actor networks are not only defined by the common interest of the actors who accepted their roles within the network, but also by the conflicts inherent from the power position. The disparate and often controversial interests of the actors give a clear view of the relationship between them, because the stability of the ANT can be achieved only by acceptance and refusal of the interest translation. If the actor's role is accepted it should align the motivation, interest and intentions with the other actors within the network.

Further, the non-human actors within the information infrastructure or information system network may include network elements, servers, databases, hardware, interface and software which together create a platform that is the typical context of information security.

Each of these actors work together in synchronous way to allow the human actors to achieve their goals and to enable a service that is soiled and is consistent with the targets and interests of the different actors and the motivations of these actors can be observed in the appearance of the successful network within an organization.

2.5.6 The Limitation and criticisms of Actor Network Theory.

In spite of Actor Network Theory (ANT) being useful, flexible and widely used in different applications, ANT has also some clear limitation and is subject of criticisms. The researcher, who introduced ANT - Latour himself - observed that while ATN is a "***powerful tool to destroy spheres and domains, to regain the sense of heterogeneity and to bring interobjectivity back*****", it is "*****an extremely bad tool for differentiating associations***" (Latour, 1996).

Actor network theory is suitable for identifying and exploring existing elements such as networks acting as actors and actors acting as networks. ANT studies recognize different practices such as characterization, interpretation and research method that expand or spread out of the specific network in question. At the same time, ANT is not concerned with any type of design and is not interested in establishing any new environment, It is not concerned with the " narrative" while it uses the word "narrative path" which (Latour, 2005) used when they introduced the theory.

There are several limitations and criticisms mentioned by different researchers regarding ANT which include the following points:

1. It is unreasonable to assign agency to nonhuman actors. ATN insists on the agency of objects or nonhuman factors and elements, while such properties are *essentially* differentiating the humans, animals and other objects. Most of the ANT researchers and users claim that they do not refer deliberately to intentions in order to avoid ascribing such properties to non-human objects (Brey, 2005).

2. ANT is amoral, because the creator of the theory considered all actors are equal and similar within the network.

3. ANT has some difficulty in distinguishing between associations in the sense of identifying the differences between network connections. Some researchers modified ANT in their researches, like for example (Ruuskanen, 2003), who modified the ANT model by adopting Granovetter's concept of strong and weak ties to identify the different relationships between actors.

Chapter 3: Conceptual Framework.

3.1 Introduction.

This chapter outlines the theoretical conceptual framework which supports the present research on minimizing the critical information infrastructure threats from insiders. It begins by discussing the importance of actor's involvement and outlines the benefits of adopting the ANT approach specifically and the different stages of actor involvement.

ANT is used as a critical theoretical component in this study to understand insider users' threats and to identify different types of attack in order to minimize CII attacks.

3.2 Actor-network perspective.

An important analytical move offered by actor-network research is the understanding that the social behavior is just a pattern of heterogeneous material network (Law, 1992). The Critical Information Infrastructure (CII) network can be considered a network of heterogeneous materials, and in this case the proposed framework provides a method for analyzing the relationship between different actors which is present only when they endeavor to achieve similar aims and interests.

3.3 Actors enrollment factors.

To explain the components of the theoretical framework and their relationships, it is very important to start giving brief idea about the model state and the psychological aspects related to the actor. In most of the organizations the actors are classified as individuals who can be full or part-time employees, contractors or trusted third party, who have legitimate or privileged access to the organizational networks, systems or data. It is normally anticipated that malicious actors may use their privileges to access the resources within their reach in an inappropriate way due to different reasons.

To explain the different elements of the theoretical framework and their relationships, it is very important to mention the factors of behavioral and psychological influence related to the actor. These factors can be considered as absolutely necessary to understand an individual's tendency to be involved in different malicious activities and to align his intentions with key actors who consider themselves as Obligatory Point of Passage (OPP).

The main factors which are motivating the users to be part of malicious network or malicious behavior are related to the fact that the main actor can rely or can convince others to adopt his interest as shown in diagram below:

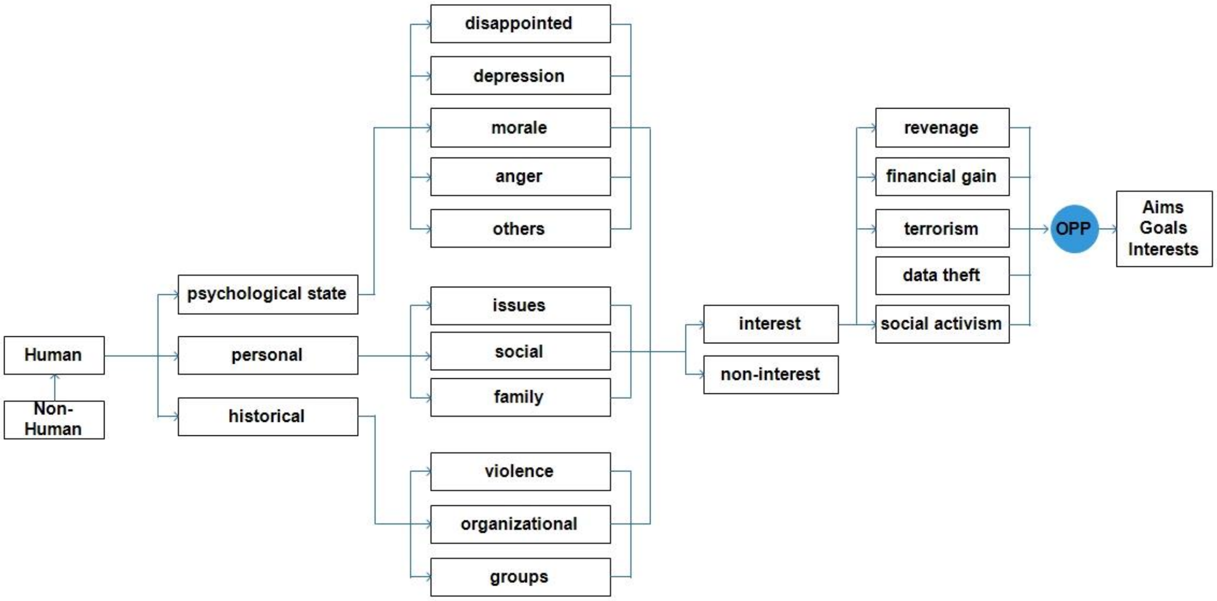


Figure 3.1: Obligatory Point of Passage.

The behaviors mentioned in the diagram are strictly human, and they are divided into three different categories. It is worth observing that these psychosocial, personal and historical factors strongly contribute to the identified level of acceptance.

The key actors who are following external criminal agenda try to find the users who are useful for their aims especially the ones who have experience and feel uncomfortable due to some reasons related to their personal issues. The users' status within the organization gives clear idea about the employee's initial intentions for participating in some type of attacks or causing some damage. Also, the behavior of authorized users within the organization reflects their negative or positive attitude toward the work, which makes the job of the main actor in trying to persuade them to join the network much easier.

The primary actor who puts himself as OPP can control the actors using their motivation factors. According to ANT the main actor who is Obligatory Passage Point rely totally on these user-related factors because they influence their behavior to activate maliciously against their organizations. They are briefly described as follows:

1. Psychological state of the inside users
   a. Anger
   b. Disappointment
   c. Depression
   d. Morale
   e. Other

2. Personal tendencies due to:
   a. Negative attitude
   b. Social issues
   c. Family problems

3. Historical records of previous behavior
   a. Violence
   b. Membership in organizations
   c. Belonging to informal groups

These behavior factors give a clear idea about the employee's initial intentions for potential undertaking of malicious attacks or causing damage. The behavior of the insider users reflect their attitude for working with negative attitude which may lead to malicious activities or joining malicious networks to satisfy their desires through Revenge, Financial Gain, Terrorism, Data Thefts or Social Activism. The malicious intent leads to exploiting existing vulnerabilities, breaches or weakness of organization Information Infrastructure (II) or Internet and Communication Technology (ICT), or even planning attacks like:

1. **Passive attacks:** eavesdropping without modifying the message stream.

2. **Active Attack:** The hacker tries to make changes in the original data of the target or the data routing to the target.

3. **Distributed Attack:** like distributed denial-of-service (DDoS) attack where a group of computer systems attack a single target to affect its availability of service.

4. **Insider Attack:** happens thanks to a person with authorized system access from inside the organization.

5. **Close-in Attack:** in this type of attack the attacker is physically too close to the target system.

The main purpose of these attacks is causing shortage of the service availability through exploiting the Databases, Servers or any physical elements. This would inevitably lead to huge losses in either income or reputation.

So based on his social skills the key or primary actor (OPP) will start searching for users who have the same interest in order to convince them to join his group and use them as tool for malicious activities. The ANT helps in analyzing the different users by classifying them into groups based on their interest and activities. This would allow to apply restricted security policies for preventative purposes.

According to (Callon, 1986) the Obligatory passage point (OPP) is ***"predicated on controlling all of the actors and variables in order to make them perform a predetermined course of action*"**. The OPP will translate his own interest to users who betray their organization due to discontent, dissatisfaction or offence. As a result they will participate in his network in which all activities should pass through him in order to be sure that the processes are under control; in other words, the OPP actor will becomes functionally indispensable to the network.

The obligatory passage point (OPP) in reality is a chain of measurements and execution points. OPP plays the role of a proxy for malicious activities which can lead to harm on Critical Information Infrastructure (CII). The proper addressing of the OPP plays an important role for minimizing the threats to CII from insiders. It starts with identifying the key actor and the network actors. This has been investigated by several researchers to the extent it has been ‘black-boxed’.

The word ‘black box’ used here has been also used by several researchers in situations where a piece of machinery or a set of commands are too complicated without particular need to be investigated in details. In such situations they are labelled with a small box which hints at the lack of information besides only input and output (Latour, 1987). The black box in this study describes aligning of the interests on all processes by matching the goals and the actor’s interests. A black box here shows part of a complicated system which doesn’t have to be explored, is stable and can be ignored by all network actors within that system with focus only on the input and output (Latour, 1999).

3.4 Proposed Theoretical Framework.

The stability of operational processes within secured Critical Information Infrastructures (CIIs) is crucial for any country economy and society growth and welfare of the citizens. This forces many organizations to give the protection of their CIIs highest priority and to spend more and more on integral protection solution like a CIIP framework that has a real time protection ability. In the previous chapters we mentioned various concepts which strongly justify the need of integral protection like the proposed framework for minimizing the critical information infrastructure threats from insiders.

Actor Network Theory (ANT) demonstrates how the simultaneous consideration of material artefacts (devices and people) and concepts (networks) can be joint together to become one complex entity. For example, CII or ICT system include both network and users or an actor which are interdependent, but for specific objective, intent, aim or goal act as one entity. So the main actor will search for strategies to join and link different elements together in a network that they will form one solid entity.

In this study the use of ANT as theoretical framework is not intended to illustrate “'why”' a network will take the specific form of a malicious activity, but is concerned with examining how actor networks align the interests to hold the actors together as one entity, letting them achieve the planned goals.

The ANT approach is not considered a real theory in the true sense. While theories typically aim to demonstrate why some type of phenomena occurs, ATN is more like a base for explanation. It explains how different relations or connections are assembled or gathered together in one place for a common purpose (Law, 2008).

Based on literature review reported in chapter 2 and the ANT discussion in chapter 3, I decided to use ATN as a theoretical framework for finding out the key insider actor and the malicious actors within the organization. The ANT approach focuses on the behavior of insider actors within the Critical Information Infrastructure (CII) and ICT network from the perspective of access to the resources, and deals with both humans and non-humans. In this case the users are using their legitimate access via computer to the resources to access various facilities. On the other hand, Information and Communication System (ICT) usually keep track of all user activities in log file format for the purpose of auditing. Based on the audit activities the generated attacks can be easily extracted from the corresponding ICT component log files. This chapter explains the actor's personal trails and motivations which can be considered as a main factor that influences the actors to take part in malicious activities. This is followed by description of the ANT translation process which is a core of the conceptual framework proposed here.

The proposed framework applies two different techniques for protecting the whole Critical Information Infrastructure (CII), including Information and Communication Technology (ICT). Based on the literature study, we have developed a theoretical framework which is outlined in Figure 3.2.

The theoretical framework which is aiming to reduce the threats to CIIP from insiders is builds using the conceptual language of ANT that depend on the translation, as well as the key concepts of problematisation, interposition (interessement) and enrolment which will be explained in more detail in the next chapter.

In this study the theoretical framework was built on the base of two concepts from ATN which are relevant to our case, namely: inscription and translation.

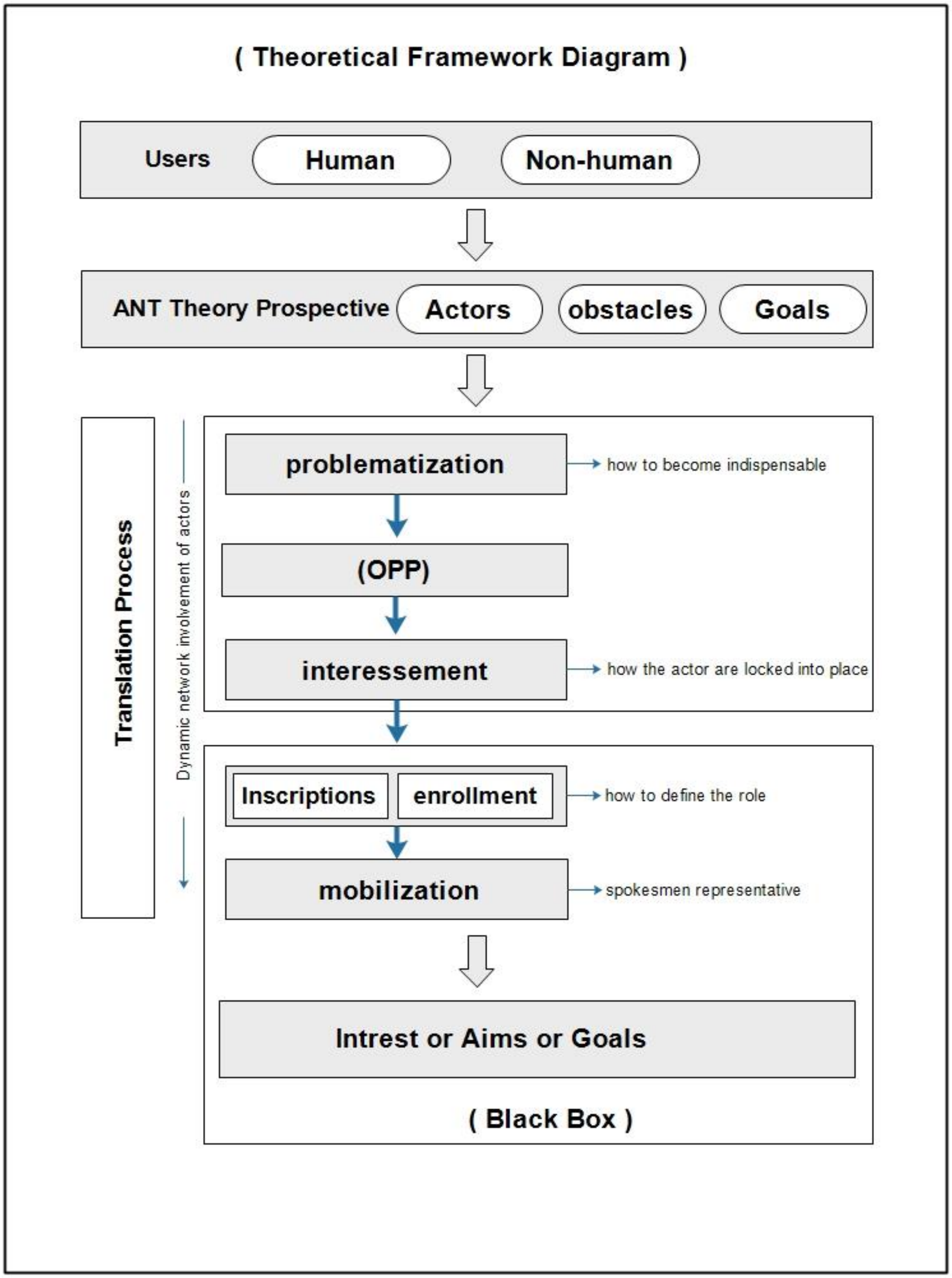


Figure 3.2: Proposed Theoretical Framework.

3.5 Theoretical Framework

As mentioned in chapter 3 of this research, (Callon, 1986) enhanced the theoretical framework to understand the development of an actor network, which relies on four stages called the four moments of translation - problematization, interposition, enrolment and mobilization, which they used in their analysis of the process of creating a network of different actors.

ANT concepts in this study are the most appropriate theory to analyze and identify the key actor and the network actors who are considered malicious insiders. The main aim of the key actor is to align the interests of the actor network and to have all their motivation fit together. The alignment of the network is acquired through successful process of translation which means that the primary actor's interests is aligning with the interests of other actors within the network of the organization. The proposed theoretical framework describes how different actors align their interests with the main actor’s interest, aiming to enroll in order to ensure the existence of malicious threats.

According to (Latour, 1987) actor networks are formed by negotiation and enrollment of different users or actors, while the enrollment of network participant occurs during the process of translation. (Callon, 1999) states that the translation process includes four different steps: problematization, interposition, enrolment and mobilization where interposition and enrolment concentrate on negotiating the guidelines and roles for the human actors.

The translations takes place as the main aims and interests within the network are accepted and adapted by the individual actors, and their goals are planned. The success of the translation process totally depends on aligning the network actor interests with the main actor (OPP) interests. The translation process visualizes the involvement of the actor network in Critical Information Infrastructure (CII). It is very important for the involved actors to know that to achieve target goals they need more efforts just to ensure that the network is alignment with their interest.

The successful translation process requires clear understanding of the interchange activities which take place between different networks. This can be done by displaying the details of all links and connections through which a primary actor (OPP) identifies other network actors and tides them up to connect to each other. The translation process needs to concentrate on realizing how various actor networks are formed and develop, becoming more strong or weak, rather than focus on the causes and effects. In the translation process, the primary or key actor initially has a legitimate access to the privileged network and resources and intends to use them in a certain manner. This is then inscribed into malicious activities through the network devices. For example, once a piece of information system is accessed, this devices becomes an actor and imposes its inscription on its users. When studying the use of technical or network system we necessarily need to shift back and forth between the main actor and the network actor in order to describe this dynamic negotiation process.

As drawn in the diagram of the proposed theoretical framework above, the primary actor translation process has four phases of involvement of other users arranged as: Problematization, Interposition, Enrolment, and Mobilisation. These four phases are not consecutive and can overlap.

-Problematization phase:

Before analyzing the network of Critical Information Infrastructure (CII) systems, the first thing is to identify what and who makes up the network. Based on Actor Network Theory (ANT) and its definition of actors, the users can classify into two different groups of entities identified as heterogeneous network as shown in table 3-1 below:

Human Actors	
Formal employee	Full time or part time
Contractors	
Third party	
Agents	
Trainee	
Non-human	
Personal Computers	
Servers	
Applications	
Database	
Remote nodes	

Table 3-1: Classification of ANT actors identified as heterogeneous network.

In this phase the most important actors emerge (both human and not human). They define different actor problems so that other actors accept, agree and consider these problems as their own problems. In this stage various actors identify their own problems and issues that are related to their jobs which need to be solved. As different problems and issues cannot be solved by the actors individually, they will try to find other related actors. After aligning their interests with the group of actors, they will select one representative that will work as a center point for passing all activities, appearing as a proxy.

The primary actor during this phase will do his best to persuade different actors within the network to identify themselves and reveal their roles in the a way that will allow him to consider himself as an Obligatory Passage Point (OPP) between the group actors and the network. The obligatory passage point, as shown in the diagram above, is identified as a main contact point to link all activities of actors who are involved in the network.

This dual action by OPP, submitted to himself, makes him indispensable in the network and this is exactly what (Callon, 1986) calls problematization. Because defining the nature of the problem and the role of each dissatisfied actor guides towards desired solution it is crucial in the problematization phase that the primary actor selects the right actor in a right action, based on their skills and experience. It was recommended by (Callon, 1986) that the primary actor (OPP) negotiates with the other actors to modulate this issue, which means that the process in this stage basically initiates the malicious behavior or starts the activities against the CII. By identifying the actors involvements, the obligatory passage points (OPP) assigns roles and associations to form alliances between different network actors.

- Obligatory Passage Point (OPP).

The first questions which will appear in Problematization phase are: What is the problem that required to be resolve? Who are the relevant users? It is necessary to select representative which will represent the group of actors. Initially, the primary actor will represent different interested users or any users who are working within the Critical Information Infrastructure (CII) system, like contractors, third parties or agents. In the problematisation stage, the main actor will develop to make himself an obligatory passage point (OPP) between the other actors and the network, and this way becomes indispensable.

In general the Obligatory Passage Point (OPP) refers to a phenomena that has the aim to fulfill the malicious interests against CII and the coordinating representative is responsible for all actors. The primary actor becomes indispensable by defining himself as Obligatory Passage Point (OPP) where all activities like information collecting, transferring, copying, analyzing and attacking the CII system or ICT components should pass through him (Callon, 1986). The main actors usually consider themselves as indispensable and supported by other network actors which are totally dependent on him for progressing and enhancing the network.

The Obligatory Passage Point (OPP) in this study requires a new methodology to find out the main actor and the relevant network actors in order to minimize the Critical Information Infrastructure (CII) threats from insiders. The main actor who has malicious or criminal agenda, intends to attract and encourage various disappointed users by relying on their personal problems. He tries to lure them to join the network and to align their interests with it so that their aims become more fixable, easier and faster to achieve.

The OPP is setting up the objectives that must be aligned with different network actors, and makes his own effort to defeat obstacles and problems that actors have to overcome because they may affect the achievement of the goals, while each actor will perform specific attack relaying on his skills and experience. The success of his goals will make as a result the OPP successful.

Different actors will be assigned different attacks according to their position to achieve goals at high level of performance . The main benefit of Obligatory Passage Point (OPP) is that OPP is used as a powerful tool to keep the actors attached together as one entity in the actor– network item (Callon 1986).

- Interposition Phase.

It is the second phase of translation where the main actor who has been followed by outsiders with malicious intention adopts a collection of actions by which the actor interests strongly agree with the other network actors in the proposal to breach or threat the CII (Callon, 1986). At this stage of the process, he places the network motivated actors into suitable places, avoiding the influence of actors who can affect negatively the developing network. Callon mentioned in his research that

"Interposition is the group of actions by which an entity [a controlling actor] attempts to impose and stabilize the identity of the other actors it defines through its problematisation…to interest other actors is to build devices that can be placed between them and all other entities who want to define their identities

otherwise. A interests B by cutting or weakening all the links between B and the invisible (or at times quite visible) groups of other entities C, D, E, etc. who may want to link themselves to B (Callon, 1986)".

At this phase, most of the actors who are targeted for interposition are already involved in the problematisation phase of other networks, and they may be find their priorities in conflict with the interests of the emerging network. To achieve a stable interposition OPP actor looks for various tactics and strategies to be deployed. The best strategy to support his aims and goals is to use either a technology and physical elements, or political force and textual content that can be placed between the main or OPP actor and the relevant actors. Another successful strategy can be employed by the OPP through assigning roles of representatives within the network in which the OPP actor negotiates interposition with those actors who speak for him in front of other actors (Callon, 1986).

Instead of persuading and encouraging each individual actor who is part of a network, the actors who consider themselves representatives will act as spokesmen of the OPP actor. The OPP actor use this strategy to isolate other network actors from enrolling by mistake unskilled users that could affect the authenticity of the OPP. At the end, the success of interposition phase leads to fulfilling the goals of enrolled network actors (Callon, 1986).

In summary, the interposition explains how different actors are locked into positions. Interposition is a collection of processes in which the primary actor (OPP) searches for other actors, brings them to terms with the objectives, guides them, assigns them specific agenda and programs its submission outside the group.

- Enrolment phase.

Actor network theory (ANT) is known as the sociology of translation, or enrolment theory. ANT enrollment is a conceptual framework for identifying series of sociotechnical processes, whose representatives pay personal attention to scientific and technological activities.

The effective enrolment relies on the negotiation and the integration between interested actors during the Interposition stage. According to (Callon, 1986) the enrolment is achieved by a group of actors with different interests after negotiations between them, and at the end of the enrollment process they share common aims or goals. (Callon, 1986) states:

"***Why speak of enrolment? In using this term, we are not resorting to a functionalist or culturalist sociology, which defines society as an entity, made up of roles and holders of roles. Enrolment does not imply, nor does it exclude, preestablished roles. It designates the device by which a set of inter-related roles are defined and attributed to actors who accept them. 'Interposition' achieves enrolment if it is successful. To describe enrolment is thus to describe the group of multilateral negotiations, trials of strength and tricks that accompany the 'interposition' and enable them to succeed*** ".

To enroll different interested actors in an actor network (ANT) it is needed to pass across several common activities where actors can explore and share their own interests. So these actors can only be enrolled through identifying common interests between them and the Critical Information Infrastructure (CII) system or component.

So the enrolment stage gives a clear idea about how to submit and coordinate the guides and roles. Enrolment is a set of designed, planned and well organized strategies that the main actors look to expand by connecting different roles and assigning malicious activities to others.

In the enrolment process the main or key actor searches through the physical activities and investigates how to synchronize the roles with other network actors. The physical behavior in this case includes installation of malicious applications or software on different PCs or performing of other types of unauthorized actions that lead to harming the CII system.

To enroll different actors in the malicious network, they are expected to demonstrate personal desire. Mostly main actors use negotiation to convince and attract different external users.

- Mobilization phase.

The fourth and last stage of the translation is the mobilization of different participating actors. This stage is totally accomplished when the three other phases of the translation are passed and the users accept the agent that has ability to represent the group by sharing the same aims and goals with it (Callon, 1986). Mobilization consist of a group of processes and procedures that can be used by the primary or key actor to guarantee that all network actors have followed their guidelines and roles which have been assigned to them according to the agreement, and they do not deceive or resist the interest of the main actor.

According to the network actor theory, the main actor is required to provide ongoing support for the main ideas of other enrolled actors to achieve their mobilization, which will lead to stability of the actor network. This stability gives the actor network ability to institutionalize implicit aims and goals, so that they are no longer likely to cause rising of public disagreement. (Callon, 1986).

This is the phase in where the actors within the network use various tools for performing malicious activities. Each user follows his own instructions which have been given to him by the key actor based on his skills and experience, accepting the authority and responsibility of the organization resources and the position he holds in it. The intention to attack or threaten the CII, which is constructed in the previous stage, is supported by different type of applications or authorizations for access which gives the opportunity to steal or damage data which can affect directly the reputation of the organization.

- Inscription.

This is one of ANT concepts which refer to aligning the interests between the primary actor and the other enrolled within the network actors. Inscriptions and translations go simultaneously in the same path during the ANT process. Inscriptions are consequences of a chain of different translation phases, which reflect clearly that the high quality of translations will result into high quality inscriptions**.**

In the translation process, the main actor who planned to use artefact in a specific manner, is going to engrave them into a tool, while the process will support it and will ensure that the actor's interests are protected (Latour, 1992).

Inscriptions are the methods used by actors to obtain a competitive advantage in enrolment and present different processes during translation. They are applied through different technical artifacts to improve and develop the interests of an actor's inscriptions. In the Critical Information Infrastructure (CII) system the successful translation is inscribed into a main plan, procedure and activities which attempts to identify the malicious behavior and actions of insiders through using different technical artefacts like applications, software, scripts or physical actions.

The concept of inscription in this theoretical framework indicate the way technical artefacts shape the manner used by the primary and the network actors: ***"Technical objects thus simultaneously embody and measure a set of relations between heterogeneous elements"*** (Akrich, 1992). The word inscription sounds almost inevitable to state that malicious behavior or activities which target to harm the organization is consolidated or achieved by permanent connection to an artifact.

In our case the translations and inscriptions are used as dual processes. The number of translations is extracted from the user profile which contains all registered activities in the log files, both malicious and non-malicious. These security logs are inscribed in data analysis which reveals the intentional behavior and the manner of attacking CII which supports the objectives of other interested network actors. Different tools and applications used by human and non-human actors for inscribing malicious application for brute force attack, for example, fail the access authorization from different PCs, fail remote access from inside and outside the CII, create a new admin account and accesses different organization resources in odd hours.

Another task of the translation and inscription is the activity targeting to use admin privileges to create fake accounts and their use for brute force applications which affect the availability of some of the services.

- Black Box.

The phrase “black box” defines a technical component (object) and is commonly used in studies based on ANT. Most historical, philosophical and sociological studies focused on the technology use the term “black box" to identify the studied object. This ANT concept was identified in the study of information technology in particular to make unambiguous the complexity of Internet technologies especially.

A black box in Critical Information Infrastructure (CII) system can be any non-human object, technical or non-technical, like computers, servers, applications, databases, network devices and any other components that contain ICT. When human and non-human objects are involved simultaneously to achieve specific aims, the complicated socio-technical link between the components will shape it, remaining invisible (i.e., black-boxed). It was essential to realize in our study that hiding more complexities under the cover of black-boxes would add to the organizational network, system or devices gathering, saving, analyzing and transferring data among different network actors (Esnault et al, 2006) .

The Actor Network Theory (ANT) concept introduces the black-boxing at the end of the translation process. They are considered as "sealed actor-networks", which indicates that the alignment of interest has been achieved, so that the aligned interests are inscribed and stable while the involved actors are satisfied that this is no longer questionable. In our case this means, that the plan for an attack becomes a black-box that has been sealed off after successful interest translation process, which aligned the goals of the network actors (Stalder, 1997).

Chapter 4: Research Methodology.

4.1 Research Approach.

This chapter's initial aim is to clarify the philosophical standpoint used in this thesis. It then explains the research methodology and data enquiry technique used as a means to answer research questions. After that, the quality of the research is debated, which relates to the reliability and validity of this research.

As supposed in the introduction more specific research methodology is required to define how to construct a proper framework that can increase the protection of Critical Information Infrastructures which from any type of threats, especially insiders.

Quantitative research is an approach that is more appropriate for research in which the researchers begin with theory and hypotheses. Then they collect the row data which can be used to verify by observation or experience as an evidence the degree to which the proposed security framework for minimizing the Critical Information Infrastructure (CII) threats from insiders is successful in producing a desired result. So the quantitative approach is the best method for examining the theory by identifying the relationship between different elements which can be measured using existing or created on purpose tools. The data can be then analyzed using statistical methods.

In the field of Information and Communication Technology (ICT), as it is in our case, the quantitative approach depend totally on collected or extracted information and the tools used in the scientific methods for data analysis. The main aim of the quantitative approach in our research would be to elaborate and utilize the models which are based on Socio-technical approach, so that they can be included in the framework for CII protection built upon the ANT for protecting Critical Information Infrastructure (CII) and Information and Communication Technology (ICT).

The steps of the proposed framework are clearly converging through the quantitative approach, because the relationship which exists between the data, produced through empirical observation and the models, result of the mathematical analysis.

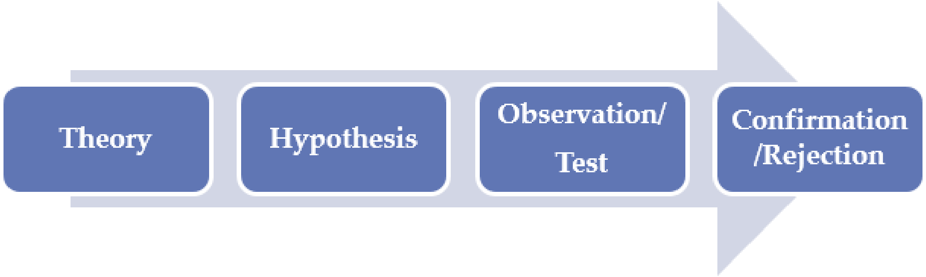


Figure 4.1: Quantitative Research Method.

To accomplish this, a methodical search of the literature was undertaken to find an appropriate theory. Different papers and articles were used to complement the Actor Network Theory (ANT). One of the best articles found was (GUNAWONG, 2011). The Actor Network Theory (ANT) analysis was used to find out the percentage of success that could be achieved in the use of smart ID cards issued by the government of Thailand, which planned to use single multi-propose ID card in all Thai public services. The concept of ANT identified different causes for failure that resulted from the ANT problematization process, which directly related to the role of the main actor, the council and other actors involved in forming the actor network of the Smart ID Card project.

(Silic, 2015) used the concept of ANT to identify the dark side of computer underground which specifically impact on electronic security in the dual use context. He used ANT to give a complete anatomy of the different contemporary hacker organizations and to explore the hacker culture within the large cultural context which includes beliefs, interests, and gang formation and translation process from Actor Network Theory perspective.

(Pieters, 2011) used the theory in system modeling to evaluate the vulnerability of physical infrastructure and the security threats by comparing with an attacker who is threatening the system. Pieters introduced a graph-based model for monitoring the human behavior during the access of system model based on lens of sociological Actor Network Theory (ANT). He considered both human and not human agents. He also created an algorithm for finding the attacks. Thanks to that the model is as a solid tool for representing the human behavior using system analysis methods rather than using graph theory methods.

Actor-Network Theory (ANT) is a best analytical tool that can be used for deeper understanding of how the malicious groups are formed and how different members activate and assume roles. As mentioned in the previous chapter these members are behaving secretly and it is difficult to know their inner intentions just by observation while they are cooperating with each other to achieve planned aims which are sealed in a black box. So it is very important to open this black box and extract the different activities to analyze them and reveal their own malicious intention against CII or ICT component.

The proposed framework is built out of several component as follows:

1. **Data source:** the data source most often is an ICT component which keeps its activities in the form of log files at various locations which can be

    a. **PCs:** machines with multipurpose functions for individual use.

    b. **Servers:** entities which empower the computer software or hardware devices that provide services to other applications or devices within application architecture called “**client/server**".

    c. **Application entities:** either basic or more complex software which is considered a part of another computer system to do a specific job.

    d. **Databases:** collection of interrelated data that contains tables, reports, schemas, queries and views as well other elements.

    e. **Firewalls, anti-virus software, and intrusion detection and prevention systems:** security devices which monitor the incoming and outgoing network traffic and take decision whether to allow or block particular traffic based on a predefined security policies and rules.

    f. **Network devices:** various devices which build the structure of the network connect to other networks for information exchange through routing the packets, such as Modems, Hubs, Switches, NICs, Repeaters, Bridges, Routers, and Gateways.

2. **Log files (logs):** files that keep record of all events which take place on operating system or application level, as well as all messages exchanged among various users of communication software. According to WhatIs dictionary the log in computing context "***is the automatically produced and time-stamped documentation of*** *events* ***relevant to a particular system. Virtually all software applications and systems produce log files***". Log files can be compared with the black boxes of airplanes which record all incidents and events that accrued during flying.

There are many different type of log files that can be considered based on the location:

1. **Server side log files:** text files which contains all activities performed by the Web Server.

2. **Client side log files:** contain data collected from client side machine through execution of a script.

3. **Proxy side log files:** the center point which links the client machine with the server machine that logs the user activities while surfing specific web site.

4. **Firewall side log files:** contain events that are denied by the system.

5. **Network side log files:** has all activities which occur on network components like routers, switches and firewalls for helping security analysis.

6. **System side log files:** has all activities captured by the operating system (Deokar and Hazarnis, 2012).

According to (Alspaugh et al, 2014) the log analysis is a process of converting the raw logs which contain data into usable information that helps solving different problems. There are two different types of log file analysis, namely qualitative log file analysis that is analyzed manually by person interpreting the logs and quantitative log file analysis that is performed either manually by administrator, or automatically by the machine.

The security log analysis is the process of detecting attacks in different environments based on security and warning logs as an information source, also known as Log-based Intrusion Detection System (LIDS). LIDS can be used also to detect malicious activities like computer misuse and policy violation (Gupta, 2012).

The Log events are considered crucial information since they contain records of most of system and network activities. This Logs are very important due to several reasons that can be summarize as follows:

- ✓ Unauthorized Access can be easily prevent or detect as well insider abuse.

- ✓ Meet the Organization regulatory needs.
- ✓ Affective to in forensic analysis.
- ✓ Give the insurance for organization regulatory compliance.
- ✓ Best tool for suspicious behavior tracking.
- ✓ Help IT administrators in failure or problems troubleshooting and operation.
- ✓ Help Network Admin in user activity monitoring.
- ✓ Help in daily event and incidents reports.
- ✓ Powerful tool for appliance and application performance measurements (Gupta, 2012).

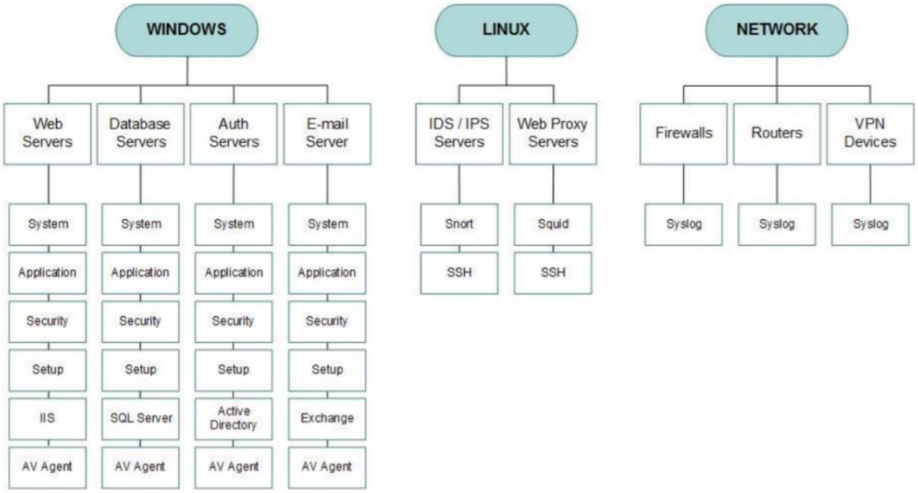


Figure 4.2: Events Log Source.

3. **Log & Event Manager Tools:** powerful software applications that can extract and analyze different type of events from log sources. There are several different managers used in this research:

    a. **User Behaviour Analytic (UBA):** type of complex software which gives ability to different organizations to find out all type of threats by using multi-dimensional behavior analysis by identifying starting points and peer groups and applying machine learning to explore compromised or misused privileges as well as unauthorized access. UBA dive deeply in the human behavior patterns to apply some algorithms and to produce statistically significant analysis to find out anomalies which visualize potential threats especially from insiders.

b. **Security Information Event Management (SIEM):** is type of software used for extracting, analyzing, archiving, reporting, and correlating data acquired from the different network resources. SIEM technology combines two different technologies, namely Security Event Management (SEM) that is used for monitoring real time network devices activities of Routers, Switches, firewalls, proxy server, VPN, IDS etc. Usually administrators use SEM for enhancing the daily incident response ability of the network devices through network behavioral analysis. Security Information Management (SIM) uses it for collecting the data from logs to store it in central repository for security analysis.

4. **User Profile:** contain all user behavior characteristics, interests and preferences. User profiling is involved in gathering user information, classifying, analyzing and interpreting behavior. The user profile may also contain information about different malicious activities which is the best source for analysis.

5. **Analysis:** event logs analysis is often used to find out the relationships or connections and to prove that specific behavior of individuals happens at specific times (Iglesias and Antonio, 2012). The analysis technique, the method and algorithm which are used will be described in the next section.

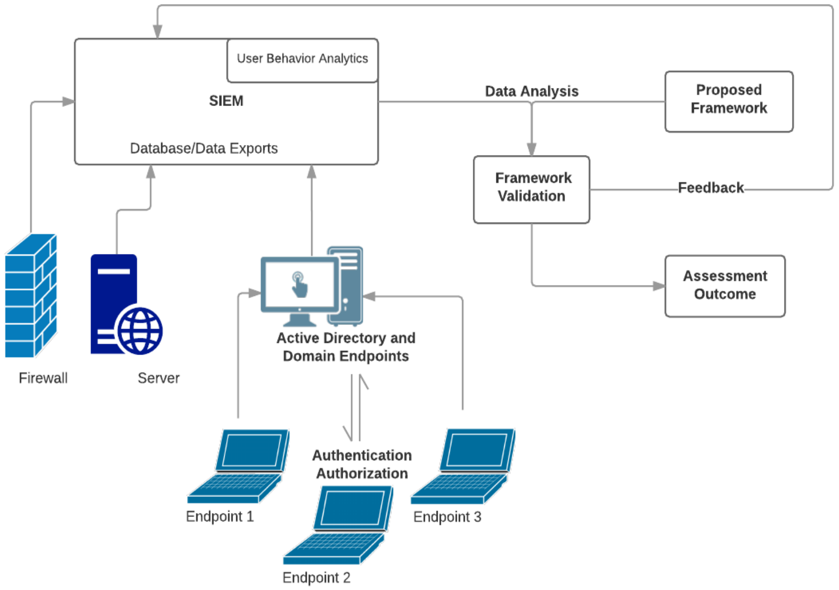


Figure 4.3: Framework Lab Setup.

4.2 Methodology.

This Section aims to illustrate the philosophical point of view used in this research. It also presents a brief idea about the research methodology and data collection technique which is used to formulate the research question. In general, a method represents the procedure and technique which has been used to examine some process in a systematic and logical way.

4.2.1 Overview

As is mentioned in pervious chapter the malicious Actor Network (ANT) groups are formed and their members are working in hidden manner inside a black box. Best solution to open the black box and visualize all malicious activities to reveal the behaviors through analyzing the events. To achieve the objective of this study in a scientific way it was very important to find the proper environment for applying, collecting, analyzing and processing the data. The first choice was the organization which I am working at due the type, size and quality of data that it has, but unfortunately most of my requests were refused.

To test the proposed framework it was very important to find out suitable environment or laboratories for real life data that has all ICT components and is equipped with Security Information Event Management (SIEM) and User Behavior Analytic (UBA) software which are very expensive and not easy to hold except by big profitable organizations. The meetings and discussion with specialists in the field of information security from more than 25 different IT private organizations and establishments failed because they were interested only in selling solutions and applications they are familiar with.

The test implementation of the framework was successfully scheduled as a Prove of Concept (POC) project after the long search finally found one of the overseas laboratories which has more than 60 employee from different IT fields. It took four months of work and weekly video conference meetings due to the unavailability of UBA at the laboratory because UBA is a considerably new technology which was released for the first time in 2014 and is very expensive. This obstacle was solved after long argument with IBM who accepted to provide IBM Qradar (SIEM and UBA) for five weeks only.

4.2.2 Case Study.

The Proof of Concept (POC) experiment was organized to validate for Insider threat protection by using both SIEM and UBA technology, on one hand, and the proposed framework, on the other hand. Several use cases were configured to generate correlated normal events and suspicious events and to raise offenses. These use cases were configured just to validate the proposed framework with Actor Network Theory (ANT) in consideration. The following insider threat detection scenarios were tested as part of this PoC:

- Unauthorized access to systems / apps / firewalls.
- Malicious configuration changes / backdoor / DDOS attacks by employees.
- Undesirable guest account creation in admin group.
- Malicious Exploit triggered (at odd hours).

4.2.2.1 SIEM Lab.

A QRadar Security Information Events Management (SIEM) system and User Behavior Analytics Application (UBA) from IBM was set up integrated with multiple different log sources mentioned in previous section. The integrated devices included:

- Windows Domain Controller (***DC***)
- Fortinet Fortigate 100D Firewall (***FortiGate* 100D*).***
- Windows 10 Server-grade Machine.
- Windows 7 Server-grade Machine.

4.2.2.2 Installation

The Lab setup required for the case study included the following ICT components:

- **VMware Workstation Pro Version 12**
- **IBM QRadar 7.2.8 (5 weeks evaluation license)**

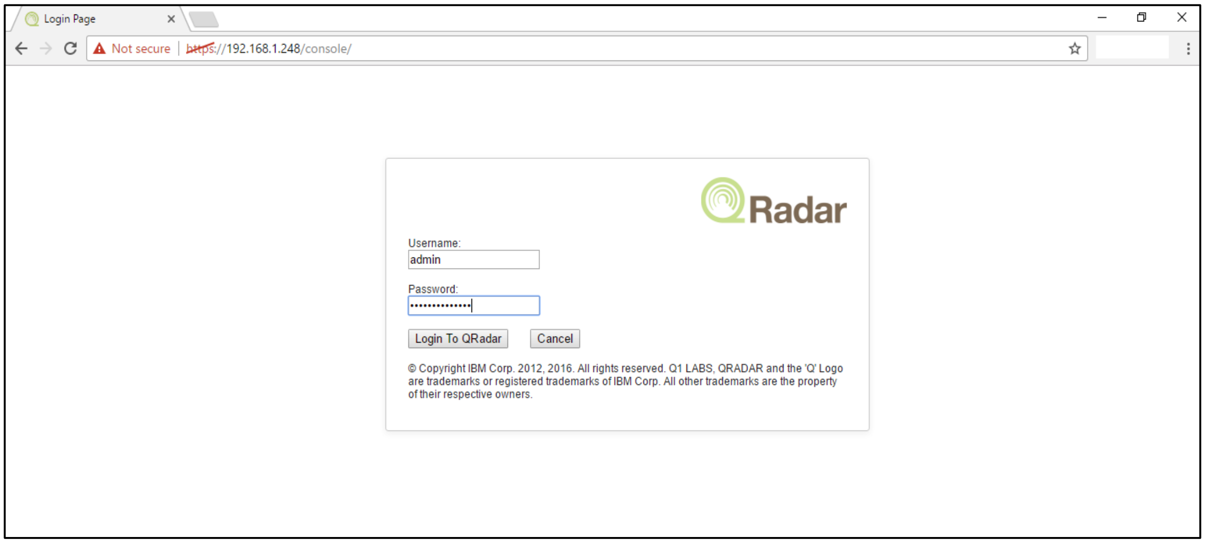
VMware Workstation Pro Version 12 was installed on a Windows 10-based server-grade machine and the IBM QRadar 7.2.8 was installed on top of VMware Workstation Pro with following hardware specifications:

Memory (RAM)	10 GB
Processors	4
Hard Disk	100 GB
Network Adapter	Bridged (Automatic)

Table 4-1: VMware Workstation Pro hardware specifications.

4.2.2.3 Configuration

The IBM QRadar SIEM and UBA were configured using step-by-step configuration dialog ultimately leading to a network connectivity configuration. The successful configuration led to successful connectivity which was tested by reaching the QRadar server through SSH or using HTTPS connection from a browser (Fig. 4.4).



~~https~~://192.168.1.248/console/

Username: admin

Password: ••••••••••••••

© Copyright IBM Corp. 2012, 2016. All rights reserved. Q1 LABS, QRADAR and the 'Q' Logo are trademarks or registered trademarks of IBM Corp. All other trademarks are the property of their respective owners.

Figure 4.4: **A Full-fledge Installed QRadar Login Page View**

4.2.2.4 User Consideration.

The life data was recorded for the analysis detailed in this research. All users were employees who sit inside and outside the network to perform network level operations. None of the other network users should be trusted, they must be controlled. A total of 40 users were considered, from 1 to from 25 registered in an Active Directory and 15 random users used to login to server-grade machines.

4.2.2.5 Log Source Integration.

As feasible log sources were identified, they were subsequently integrated in an attempt to validate the Proposed Framework:

1. Windows-based Domain Controller
   - ✓ A list of 25 distinct users were registered to record the user activity

2. Fortinet Fortigate 100D Firewall
   - ✓ Firewall, as a perimeter security device collecting logs of all network users initiating outgoing or incoming connection requests.

3. Windows 10 based Server-grade Machine
   - ✓ With remote logins enabled.

4. Windows 7 based Server-grade Machine
   - ✓ With remote logins enabled.

4.2.3 User Behavior Analytics and Security Information Event Management.

User Behavior Analytics (UBA) was the key component along with Security Information Event Management (SIEM) for analyzing users' interaction with the entities in a network and observing whether any interaction is an insider threat or a normal behavior. According to " *Verizon's Data Breach Investigation Report 2017"* 76 percent of data breaches or cyber-crimes were committed by insiders - employees, contractors, or terminated employees and contractors. The combination or SIEM and UBA is a very strong and powerful tool which can be perform the following tasks:

- ✓ **C**ollect,
- ✓ **A**nalyze,
- ✓ **I**dentify,
- ✓ **R**espond, and
- ✓ **S**trategize to **M**itigate insider threat in a believed-to-be highly-secured network.

Based on reality experienced by various large or huge corporations such as Accenture (professional services organization providing consulting and digital technology solutions) and HfS Research (provides strategic guidance to most complex projects) almost 69 percent of enterprise security executives reported a theft or corruption of data by insiders during 2016. Focusing on the emerging insider threats and the need to mitigate them, we tested a list of scenarios.

Below are some of the most significant insider threat activities which can bring down the so-called/believed to be the most secure network.

- Unauthorized access to systems / apps / firewalls
  - ➢ Multiple Login Failures (Intrusion Attempt)
  - ➢ Successful Login Preceded by Multiple Login Failures (Brute Force)
  - ➢ Remote Login Failures

- Malicious configuration changes / backdoor / DDOS attacks by employees on notice period (resigned / laid off)
  - ➢ Malicious Exploit
  - ➢ Privilege Escalation
  - ➢ A Laid-off employee’s login attempt

- Undesirable guest account creation in admin group
  - ➢ A guest account is added

- Malware triggered at odd hours (Time-Bomb)
  - ➢ A chain of activities to execute a malicious software or carry out a malicious operation

4.2.3.1 Event Logging.

One of the most crucial and valued sources of evidence for security breaches indicators for many organizations, the event logging has always been there to prove malicious behavior or untrusted activities generated within any network or infrastructure.

These repercussions range from heavy storage demand to backup of data for performing historical search in order to identify what has been identified on a much later stage. This is typically destructive for an entire network which relies on availability.

Further, from the event logs one can be discover what might cause disruptions. But let’s look with a broader view at those scenarios:

- Users with high count of remote login failure have a higher chance of malicious activity.

    - ➢ A user, as per compliance of any organization, must be limited to certain access attempts, especially remote logins, to regulate and enforce the policy. If it is found beyond the permissible failure count and is followed by successful attempts, it may be deemed as an uncertainty or insider threat.

- Users with high count of remote login failure in odd hours have higher chance of malicious activity.

    - ➢ The odd hours denote the out-of-office or non-business hours, during which a high count of remote login attempts is suspicion.

- The higher the count of firewall denies for a user, the higher is the chance for suspicious activity.

    - ➢ A user may be attempting to bypass the perimeter defense (firewall) of the network with high number of requests. The higher the number of denials, the higher the suspicion of insider threat in attempt to bypass the access control and commit an illegal activity.

Respectively, another challenging assumption may be drawn from the hypothesis formulated on the base of the possibility of occurrence of insider threat activities.

- The higher the number of brute force successful logins in odd hours from a user, the higher is the chance for suspicious activity.
- Users with high number of brute force logins along with high number of login failures have higher chance of malicious activity.
- The higher the count of successful logins at odd hours, the higher is the chance of malicious activity.
- Users with high count of login failures have higher chance for malicious activity.
- Users with high count of login failures in odd hours have higher chance for malicious activity.
- Users having high number of malicious exploits have higher chance of malicious activity.
- Users having high number of malicious exploits at odd hours have higher chance of malicious activity.
- The higher the count of account privilege changes in odd hour the higher is the probability of malicious activity.
- Users with accounts added to Admin group in odd hours have higher chance of suspicious activity.

4.2.3.2 Data Collection.

Quantitative data collection methods rely on random sampling and structured data collection instruments that fit diverse experiences into predetermined response categories. They produce results that are easy to summarize, compare, and generalize. Quantitative research is concerned with testing hypotheses derived from theory and/or being able to estimate the size of a phenomenon of interest. Typical quantitative data gathering strategies include: experiments/clinical trials.

There are many methods and ways used to collect or obtain data for statistical analysis. Mainly there are three different popular methods which are:

- Direct Observation
- Experiments approaches.
- Surveys.

The main data collection technique used in this research study is totally based on experiment approach, where the Data collection tool was done through both the integration of SIEM and UBA. As it mentioned before the trail based license for QRadar SIEM and UBA from IBM was only five weeks and within this period of time the number of events collected was more than eighty thousand events (651718 records) which has both the malicious and non-malicious activities. The considered malicious activities based on twelve different proposed hypothesis which has ability to minimize or maximize as case required are subtracted from total events and the result was only 6689 malicious events.

For the purposes of this research and for the sake for providing more details the plan to collect row data was divided into three different phases which are:

- Phase (1): Lab preparing.

The laboratory of Aujas Company in city of Banglor (India) was selected to test the proposed Framework. This company has more than 60 employees and is a suitable Laboratory for applying the real data collection tool for research analysis.

The proposed framework built on different component which was prepared in Aujas LAB within two weeks and contains:

- Data source tools:

a. **PCs:** are machines with multipurpose functions which have features practical for individual use.

b. **Servers:** are entities which could be a power computer software or a hardware device that provides services to other applications or devices and this architecture called "**client server model**".

c. **Application entities:** is mainly either basic or complicated type of software, and considered as part of a computer system which is based on data or instructions to perform specific jobs.

d. **Databases:** collection of interrelated or related data that contain series of tables, reports, schemas, queries and views as well other elements.

e. **Firewalls, anti-virus software, Intrusion Detection and prevention systems:** are security devices which monitor all type of incoming and outgoing network traffic and take decision whether to allow or block particular type of traffic based on a predefined collection or group of security policies and rules.

f. **Network devices:** Is the different type of devices which are used for arranging into a structured a network, connecting to other different networks for information exchange through routing the packets like: Modem, Hub, Switch, NIC, Repeater, Bridge, Router, and Gateway.

- Data collection tools:

Log & Event Manager Tools: are types of powerful application or software that can extract and analyze different type of events from several log sources. There to different type are manager are used in this research study which are:

a. **User Behavior Analytic (UBA):** QRADAR is a type of complicated software which gives ability to different organizations to find out all type of threats by using multi-dimensional behavior starting point used for figure, effective peer group analysis, and auto machine learning just to explore compromised and misused privileges as well unauthorized access. UBA dive deeply in a human behavior patterns to apply some type of algorithms and statistical significance analysis to find out anomalies which visualize potential threats especially from insiders.

b. **Security Information Event Management (SIEM):** also from QRADAR which is a type of software used for extracting, analyzing, archiving, reporting, and correlating data or information acquired from all the different network resources. SIEM technology is combination of two different technologies, which are the Security Event Management (SEM) that is used for real time network devices activities monitoring, like Routers, Switches, firewalls, proxy server, VPN, IDS etc. Usually administrators use SEM for enhancing the daily incident response ability of the network devices through network behavioral analysis. While, Security Information Management (SIM) which is used for collecting data form typically logs to store in central repository for security analysis.

- Phase (2): Performing the Malicious Activities.

The malicious activities performed from different Aujas employee PCs in different period of time without informing them to make the scenario as real. The different malicious activities are mainly dependent on the research hypothesis which was as a follows:

1. General Authentication Failed.
2. Remote Login Failure.
3. Remote Login Success – Odd hour.
4. User Login Failure.
5. Excessive Firewall Denies Between Hosts.
6. UBA: New Account Use Detected.

7. Malicious Exploit.
8. UBA: User Access at Unusual Times.
9. Multiple login failure.
10. Admin Login Successful – Odd hour.
11. General Authentication Successful – Odd hour.
12. Brute Force.

- Phase (3): Data Collecting.

The deployment of proposed Framework relies on both UBA and SIEM tool to collect all malicious and non-malicious activities which exist in different ICT component Log files. Log data generated by large numbers of devices, they generally relate to one of four source classes in the LAB:

- Services that provide functionality to users.
- Infrastructure supporting the network.
- Host devices.
- Remote connection services.

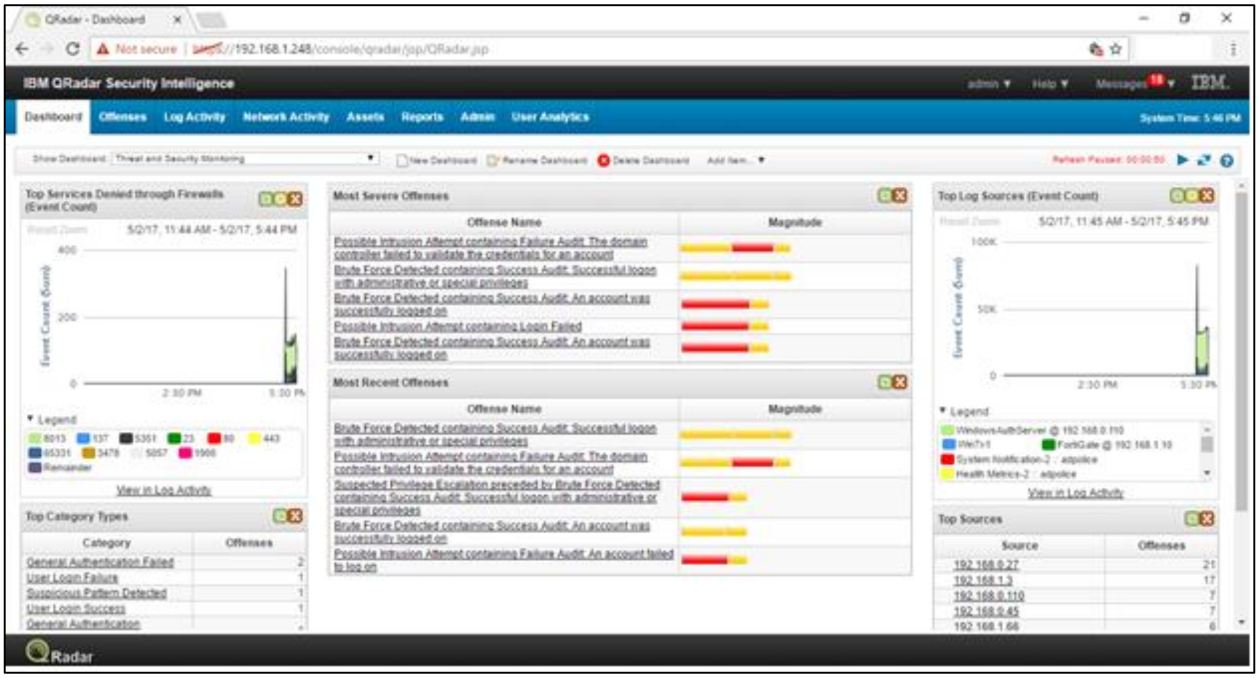
Those instantly record the running state of hardware and software activities. Correlation of log events across a range of devices is a critical part of any incident response activity as it assists an organization in assessing the extent and impact of a network compromise and informing what steps may be necessary for mitigation. Network security appliances may provide elements of the picture during an attack, but may not have full visibility over a network or possess the correlation capabilities to fully describe the attacker's activities. Different malicious and non-malicious activities stored in different users profile for analysis later.

4.2.3.3 Experimental Results.

The result of the experiment was very important to validate our work as shown in the analysis section. The experiment set-up was presented in the previous section.

The accuracy of these experimental results is considered as a benchmark and the compression point of the analysis is based on the algorithm of centrality from Graph Theory (GT).

These scenarios lead to the generation of user behavior, which may be deemed as an outcome of manipulation the accessible resources inside an environment, which could be secured from the outside threats, but when the users become target, they may be exploited in several cases. This is presented in Fig. 4.5 below.



Most Severe Offenses

Offense Name	Magnitude
Possible Intrusion Attempt containing Failure Audit: The domain controller failed to validate the credentials for an account	
Brute Force Detected containing Success Audit: Successful logon with administrative or special privileges	
Brute Force Detected containing Success Audit: An account was successfully logged on	
Possible Intrusion Attempt containing Login Failed	
Brute Force Detected containing Success Audit: An account was successfully logged on	

Most Recent Offenses

Offense Name	Magnitude
Brute Force Detected containing Success Audit: Successful logon with administrative or special privileges	
Possible Intrusion Attempt containing Failure Audit: The domain controller failed to validate the credentials for an account	
Suspected Privilege Escalation preceded by Brute Force Detected containing Success Audit: Successful logon with administrative or special privileges	
Brute Force Detected containing Success Audit: An account was successfully logged on	
Possible Intrusion Attempt containing Failure Audit: An account failed to log on	

Top Category Types

Category	Offenses
General Authentication Failed	2
User Login Failure	1
Suspicious Pattern Detected	1
User Login Success	1
General Authentication	

Top Sources

Source	Offenses
192.168.0.27	21
192.168.1.3	17
192.168.0.110	7
192.168.0.45	7
192.168.1.66	6

Figure 4.5: Summary of severe offenses displayed in QRadar Threat and Security.

The malicious activities initiate the next-step of processing the alerts that can be taken care of by an external or SIEM-embedded UBA engine. The UBA and SIEM engines along with the Actor Network Theory help and understand how a user may attempt to damage a network through malicious or suspicious or unwarranted activities.

The data logged by the log collector of the SIEM is analyzed by the processing engine of User and Entity Behavior Analytics (UBA). This brings the power of decision-making through factor-mapping or mapping of users in a representational format. An actor is identified based on the two main factors which are extracted from ANT: interactions and actions with any number of entities in an ideal network.

The following steps have been followed to perform exploratory data analysis:

- Creating master - user level dataset by rolling up the provided events data at user level.
- Calculating the user level count of metrics such as remote login failures count, total malicious events count, login failure count, etc. in master- user level dataset.
- Analyzing the user level metrics to identify key metrics for the deep dive as shown in the chart below (Fig. 4.6).

To produce the chart we used the number of interaction links and the number of activities by various users selected only on the basis of high number of activities on the scale of 1 to 7. We tested them through coding the logic in R and manipulating the data in excel.

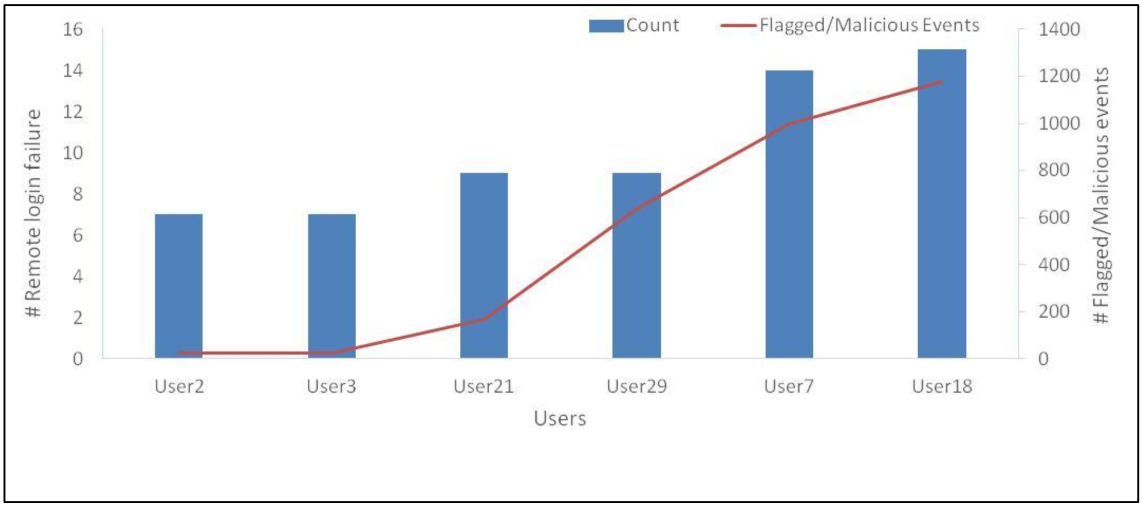


Figure 4.6: Users with high count of remote login failure have higher chance of malicious activity

Out of the hundreds of flagged for being potentially malicious events; the users listed in the representational format have certain amount of remote login failures. The high number of failed attempts raises question for the credibility of the intentions of that user. Both User7 and User18 show significant count of remote login failures out of all the flagged/malicious events. A suspicion is highly likely.

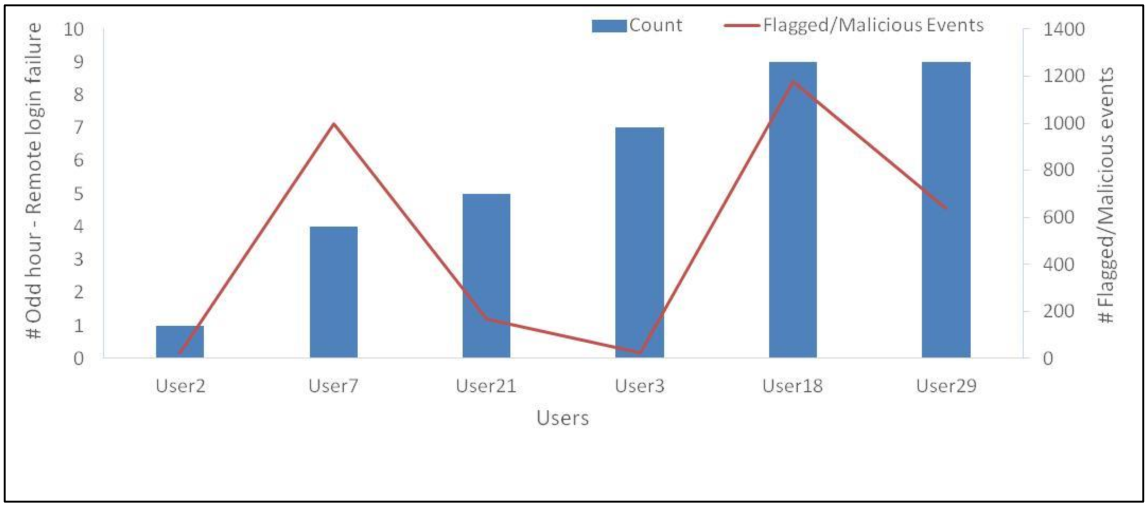


Figure 4.7: **Users with high count of remote login failure in odd hours have a higher chance of malicious activity.**

Remote login failures may look like normal, but when they are observed at an odd or out-of-office hours; it should concern the network administrators. If a network is not supposed to permit such attempts, as in this arrangement, it is observed to be highly alarming, and deemed as an insider threat.

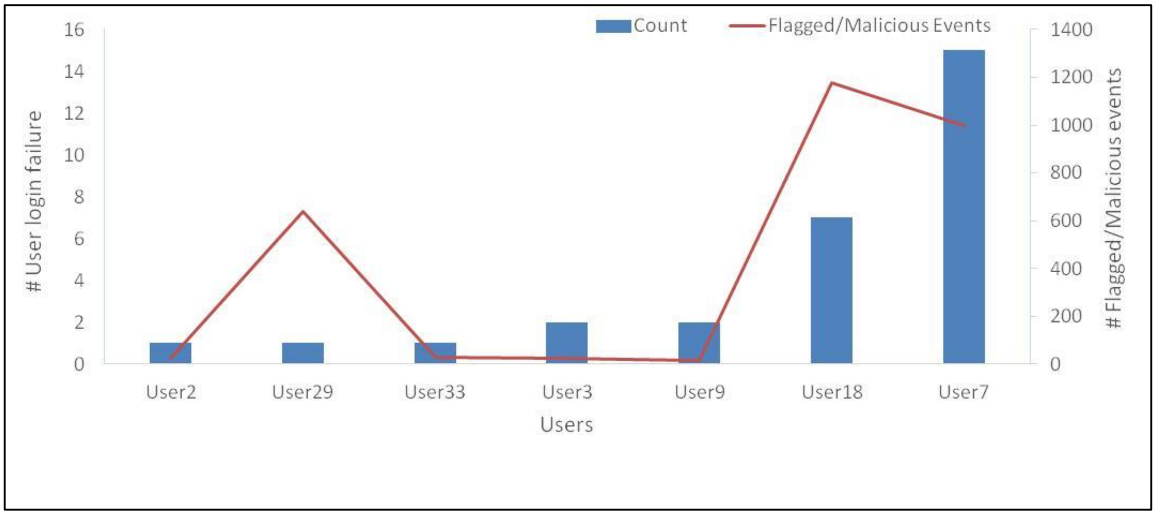


Figure 4.8: Users with high count of login failure have higher chance for malicious activity

User attempts to authenticate their credentials with Active Directory, which in turn validates them and grants certain level of access, is defined by the granting server/machine. In the case of login failures this means that high number of login failures leads to a high level of suspicion.

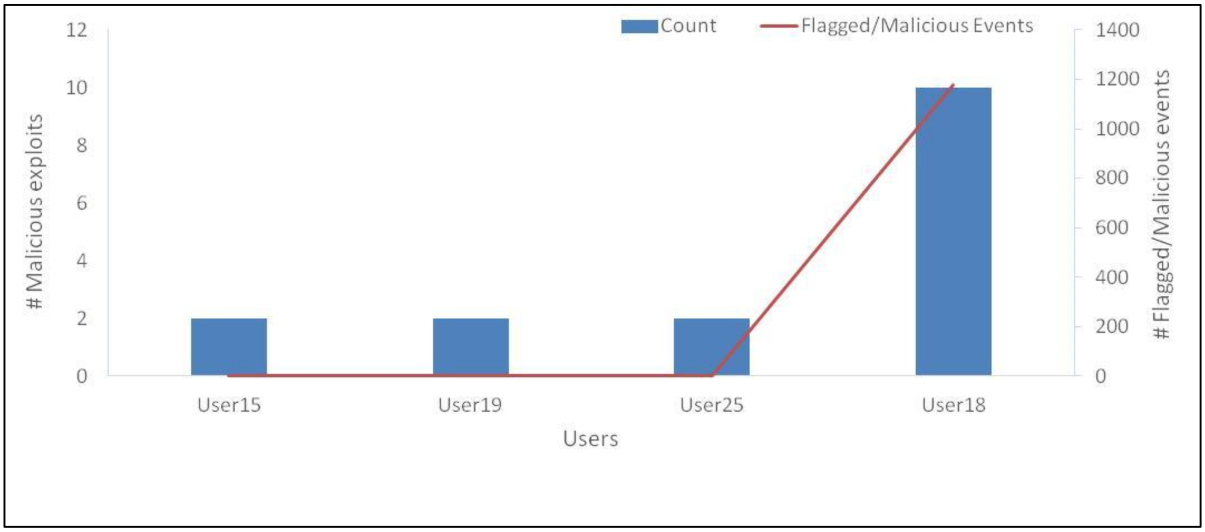


Figure 4.8.1: Users having high number of malicious exploits have higher chance of malicious activity

Users with high malicious exploits have high number of flagged/malicious events. User18 has significantly high number of malicious exploits and flagged events in comparison to other users. Therefore, logs of the users with high malicious exploits should be analyzed in detail to identify the interactions between them, and then identify the actor. Based on the above study and the general business logic, 12 hypotheses or key KPIs have been formulated to identify the suspicious user, hence the actor:

13. General Authentication Failed
14. Remote Login Failure
15. Remote Login Success – Odd hour
16. User Login Failure
17. Excessive Firewall Denies Between Hosts
18. UBA: New Account Use Detected
19. Malicious Exploit

20.UBA: User Access at Unusual Times

21.Multiple login failure

22.Admin Login Successful – Odd hour

23.General Authentication Successful – Odd hour

24.Brute Force

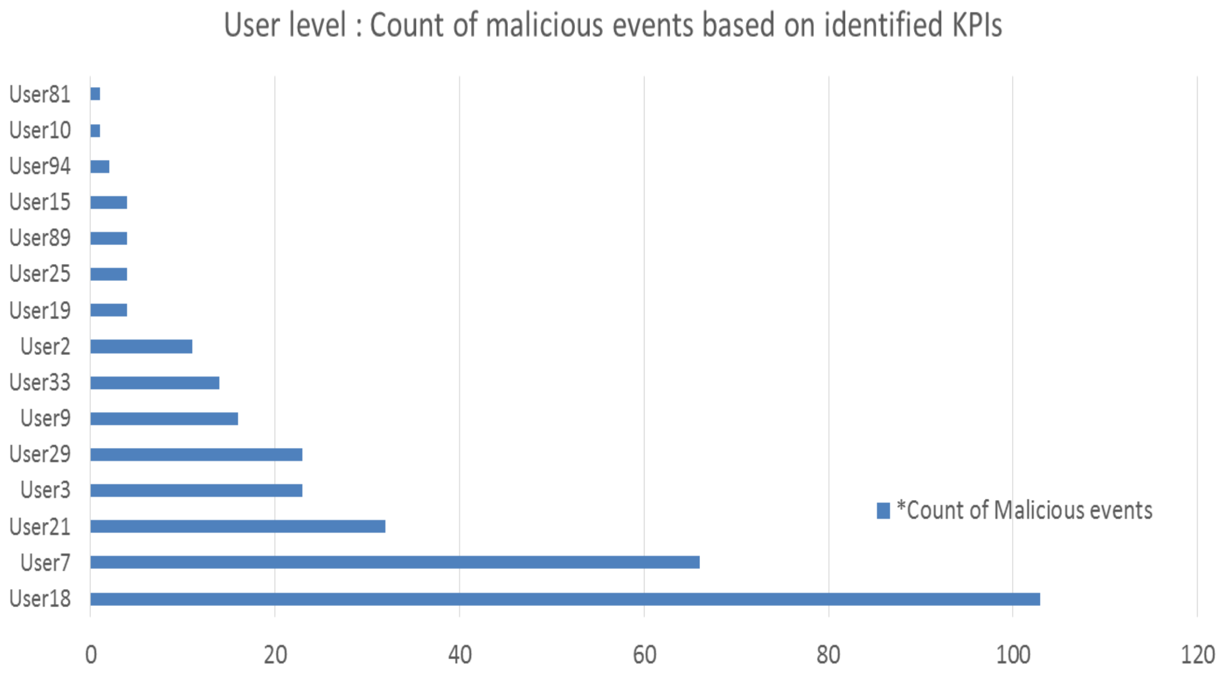


Figure 4.9: Total Count of Malicious events-1

Based on the count of identified KPIs, six users (User 9, User 29, User 3, User 21, User 7, and User 18) have high number of malicious events compared to other users. User 7 and User 18 have the highest count of malicious events of 66 and 103 respectively. These 6 highlighted users should be deep dived further to figure out the main actor.

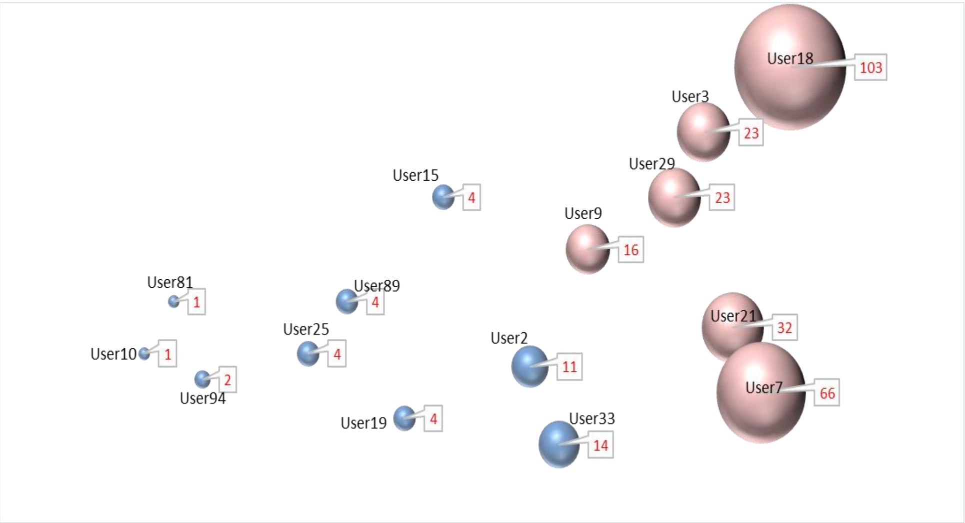


Figure 4.10: Total Count of Malicious events-2

To find the interaction between different users it was very important to find out the common or matching activities, which indicate the relation between various users. More Key Performance Indicator (KPIs) between different users is a match that means more interaction. For the identified KPIs, User level count of the KPIs is shown in Table 4-2 below.

KPI	User18	User7	User21	User3	User29	User9	User33	User2	User19	User25	User89	User15	User94	User10	User81	Total
General Authentication Failed	25	15		14	0	14	10	1								79
Remote Login Failure	15	14	9	7	9			7								61
Remote Login Success – Odd hour	3	11	13		12											39
User Login Failure	7	15		2	1	2	1	1								29
Excessive Firewall Denies Between Hosts	24				1											25
Malicious Exploit	10								2	2		2				16
UBA: New Account Use Detected	4		2						1	1	4	1	2	1		16
UBA: User Access at Unusual Times	3		5					2	1	1		1			1	14
Admin Login Successful – Odd hour	3	3	3													9
Multiple login failure	4	3					2									9
General Authentication Successful – Odd hour	3	3														6
Brute Force	2	2					1									5
Total	**103**	**66**	**32**	**23**	**23**	**16**	**14**	**11**	**4**	**4**	**4**	**4**	**2**	**1**	**1**	**308**

Table 4-2: User level count of the KPIs.

The data shows that User 18 has the highest count of malicious events of 103 events, followed by User 7 with 66 counts of malicious events for the identified

KPIs. Also, it can be seen that User 18, User 7 and User 21 have been flagged for almost all the identified KPIs, while other users have been flagged only for a very few of the KPIs. These three users combined (User 18, User 7 and User 21) have the count of 201 malicious events out of total 308 events, which is nearly 65% of the total malicious events count.

The next step of the analysis is to identify suspicious patterns or links based on the user interaction data and to identify the main actor. To identify the interaction between users, a network chart has been drawn by analyzing the interaction between these users for the identified KPIs.

In the network chart, users are shown as nodes and the size of the nodes is proportional to their count of malicious events. The following logic has been used to define the edges in the network chart:

1. Identify the users with the highest count of malicious events for each of these identified KPIs.

2. Connect the user with the highest count of that KPI to other users who have been flagged for the same metric

The set of interactions or activities by these users were tested through the coded logic and data manipulations written in R. The result is shown in Figure 4-11.

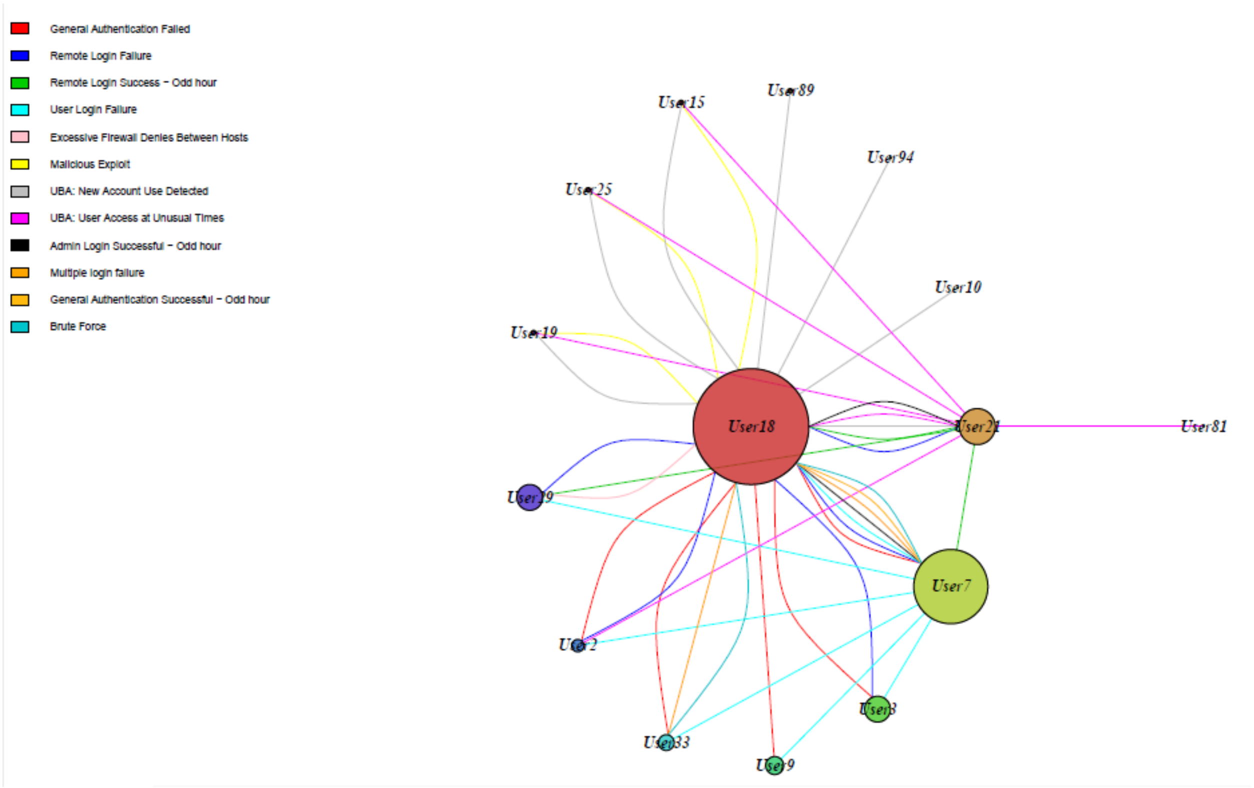

🟥 General Authentication Failed
🟦 Remote Login Failure
🟩 Remote Login Success - Odd hour
User Login Failure
Excessive Firewall Denies Between Hosts
🟨 Malicious Exploit
UBA: New Account Use Detected
UBA: User Access at Unusual Times
⬛ Admin Login Successful - Odd hour
🟧 Multiple login failure
General Authentication Successful - Odd hour
Brute Force
User15
User89
User94
User25
User10
User19
User18
User21
User81
User7
User2
User3
User33
User9

Figure 4.11: Final Lab Result OPP Graph.

This graph shows that User 18 has the highest malicious events count and also has the highest number of interactions for these KPIs. While User 7 and User 21 have almost the same level of interaction for the KPIs but the count of malicious events for User 7 is higher than User 21. Therefore, the size of user 7 is bigger than that of the user 21.

On the other hand, five different KPIs - General Authentication Failed, Remote Login Failure, User Login Failure, UBA: New Account Use Detected and UBA: User Access at Unusual Times - have the highest number of users with an average of 7-8 users, while the other KPIs have on an average 2-3 users. It can be seen also that User 81, User 10, User 94 and User 89 don’t have much interaction with other users for the identified KPIs.

4.2.4 Centrality.

In a network analysis and graph theory, a graph has several measures for the centrality of a vertex. The comparative significance of a vertex (for instance, the importance of an individual in a social group) can be shown on a separate diagram. The extensively used measures of centrality in a network analysis are divided into four categories: betweenness, closeness centrality, eigenvector centrality and degree of centrality (Lieberman et. al., 2014). Among these categories, betweenness, closeness centrality and degree of centrality are the three most extensively used measures of centrality (Valente et. al., 2015). On the basis of non-directed and directed links some of them vary in their applicability (Worrell et. al., 2013).

4.2.4.1 Degree of Centrality.

Degree of centrality is a straightforward and simple measure of the importance of the location and can be described by the connections involving a node (for instance the total number of links present at the nodes). On the basis of the risk estimation for a given node, the degree of centrality is often interpreted to mean the information about what is passing through the system (for example data, virus etc.) (Mercer et. al., 2015). In the case of a directed network (i.e., all links are direct) there are typically 2 different procedures for estimating the in-degree and out-degree for degree of centrality (Burt et. al., 2013). In-degree can be defined as the total links that are incident to a node, while out-degree is defined as the total links directed to other through that node (Crossley et. al., 2015). For constructive relationships, like advice and companionship, in-degree is regularly deciphered as a type of fame, and out-degree as potential to socialize (Nikolaev et. al., 2015).

A set having high degree of centrality frequently keeps up various links with other network (Mercer et. al., 2015). A higher degree of centrality is found in sets where the nodes can access as well as can have an impact on a number of other nodes (Luo et. al., 2015). An auxiliary position is occupied by the main performing actor (who organizes) who works as a controller for data and other assets exchanges and who has huge capacities for working with other actors. In a social pool, they are found at the center or close to the focus of the network graph (Palonen et. al., 2013). Interestingly, an actor having a minor role has no or few relations only and along these lines a peripheral actor is found at the boundaries of a network graph (Burt et. al., 2013).

A degree of centrality of a non-directed graph is just the total of the degrees of each actor (Valente et. al., 2015). The degree of centrality index is characterized more specifically with the maximum likelihood of the in-degrees to normalize or stabilize it. This allows different size networks to be compared by showing the outcome in terms of a percentage or a proportion (Crossley et. al., 2015).

The distribution or difference of the individual centralities is quantified by group degree of centrality (Nikolaev et. al., 2015). For instance, the difference between the degree of centrality of the main actor and the centrality of the rest is measured by the general index (Valente et. al., 2015). Its value is in the range of 0 to 1 that reaches its maximum if all other actors select one central actor (forming a star configuration) and reaches its minimum if all other actors possess identical centralities (forming a circle).

Degree of centrality indexes can be also applied to directed graphs. In such a case, the actor set is uneven (Crossley et. al., 2015). Traditionally, out-degree is used to mirror the choice of every actor by summing up the centrality degrees of the sets to which the access is directed (Burt et. al., 2013).

$$degree\_centrality(i) \overset{def}{=} k(i)$$

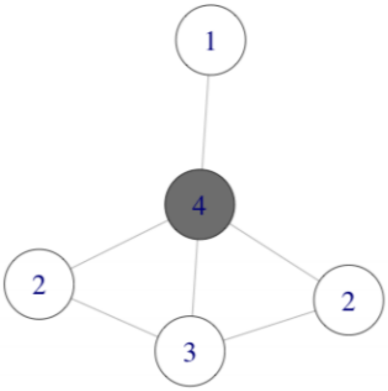
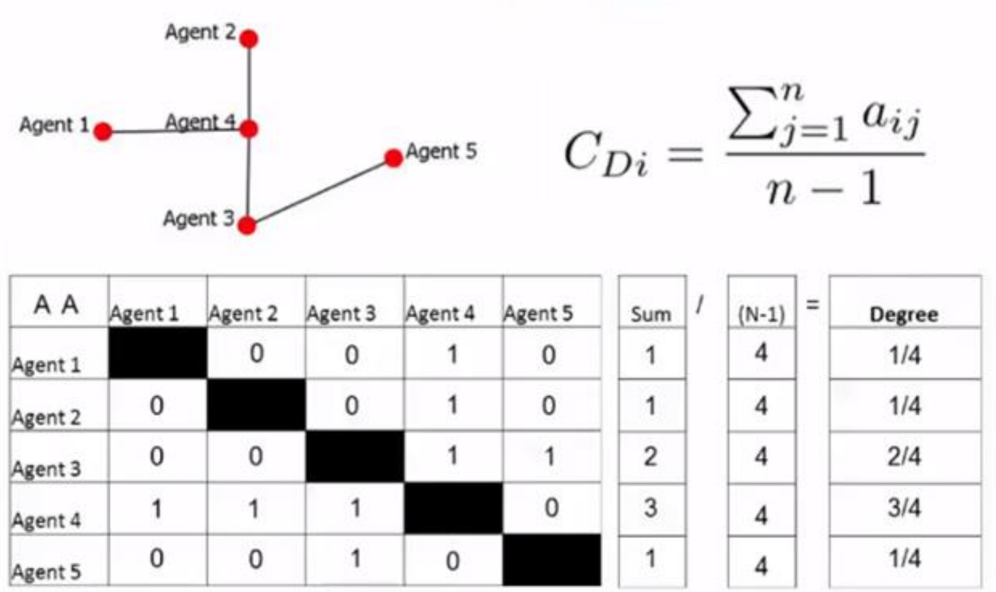


Figure 4.12: Degree of Centrality.

The maximum centrality value possible = n − 1 (so values are all between 0 and 1).



$$C_{Di} = \frac{\sum_{j=1}^{n} a_{ij}}{n-1}$$

A A	Agent 1	Agent 2	Agent 3	Agent 4	Agent 5	Sum	/	(N-1)	=	Degree
Agent 1		0	0	1	0	1		4		1/4
Agent 2	0		0	1	0	1		4		1/4
Agent 3	0	0		1	1	2		4		2/4
Agent 4	1	1	1		0	3		4		3/4
Agent 5	0	0	1	0		1		4		1/4

Figure 4.13: Degree of Centrality-1.

4.2.4.2 Closeness to Centrality.

In the concept of closeness, minimum path distances are held by a central actor from the g-1 actors (Crossley et. al., 2015). A performing actor can quickly connect and speak with many others without experiencing numerous intermediaries, if it is close to them (Burt et. al., 2013). Along these lines, it is significant to accomplish higher closeness to centrality in the case when two sets are not linked directly and require few intermediate steps to reach each other (Lieberman et. al., 2014).

Closeness to centrality of an actor is the opposite to the total geodesic displacements (shortest path) of an actor i to the other actors g-1 (Worrell et. al., 2013). Since the distance is "infinite", the closeness to centrality of an actor is calculated just for a linked diagram because parts of the node pairing might not be reachable (amongst i and j there is no path). By characterizing of the closeness index with maximum likely distance in terms of proportion/percentage, it can be standardized (Mercer et. al., 2015).

The geodesic distance of two actors is different in directed graphs - for instance (ni,nj) are not the same as (nj,ni). A standard closeness index can be calculated using similar formula as in the case of non-directed graph (Worrell et. al., 2013). However, if the graph is directed, the closeness isn't defined (because of directed routes in the opposite directions).

$$closeness\_centrality(i) \overset{def}{=} \left(\frac{\sum_{j\neq i} d(i,j)}{n-1}\right)^{-1} = \frac{n-1}{\sum_{j\neq i} d(i,j)}$$

The node can be close to other nodes and can also have ability to be reached from others easily or to reach others quickly.

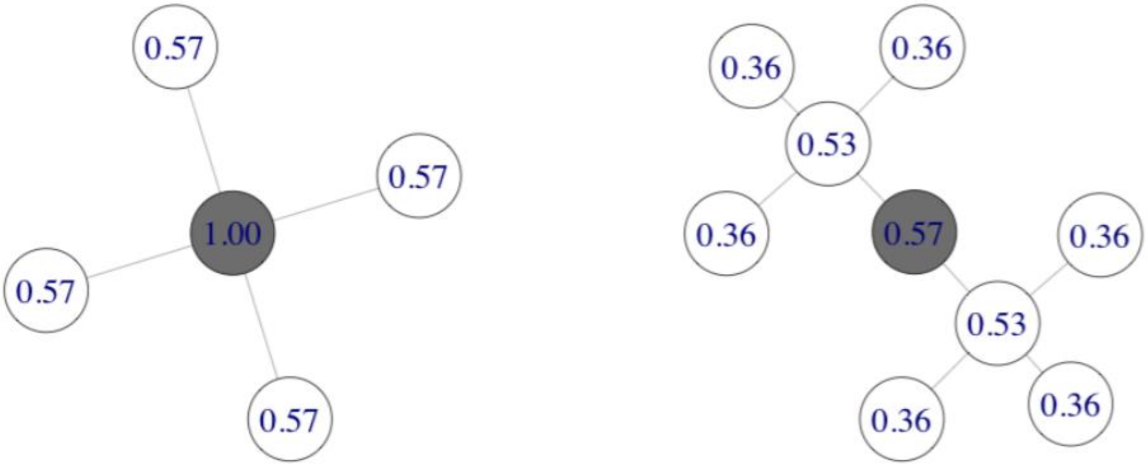


Figure 4.14: Closeness to Centrality.

4.2.4.3 Betweenness.

A degree of vertex's centrality in a graph is called betweeness (the edge betweeness is not debated here). It quantifies how frequently a node is acting like a link on the smallest path of other nodes (Bourbousson et. al., 2015). Betweenness was presented as an estimate for evaluating the control of a person on the correspondence of different people inside an interpersonal organization (Worrell et. al., 2013). Vertices which bear high betweenness have a high likelihood to be on the shortest path between two arbitrarily selected vertices (Nikolaev et. al., 2015).

There is a central actor which shows a "between" position at geodesics and associates with different other actors' sets in a system (Palonen et. al., 2013). Middle actors are cutting points in the shortest distance linking two nodes. They may control the stream of data or the substitution of assets, and may charge an expense or business commission for exchanging management. In our case, a couple of actors possess more than one geodesic links, expecting that each of these smallest displacements has an equivalent likelihood to be utilized (Lieberman et. al., 2014).

For a pair of Actors j and k, the betweenness for an actor i which is between them is the total proportion for all sets having actor i included within the pair's geodesic distance. Likewise with the other centrality standards, the betweenness scores are standardized through grouping them by the greatest believable betweenness (Marshall et. al., 2015).

The actor measurements are accurately shown on the diagrams, despite the fact that betweenness was calculated for non-directional relations (Worrell et. al., 2013). The standard system level index has to be increased by multiplying it by factor 2 to account for the most extreme cases (Burt et. al., 2013).

The three degrees of centrality provide a quantitative scale to measure the role of the actors within networks (Crossley et. al., 2015). For real complex networks, this integral measure is additionally an important element of the analyses (Bourbousson et. al., 2015). In any case, a substantive attention should be paid to measure the centrality (Nikolaev et. al., 2015).

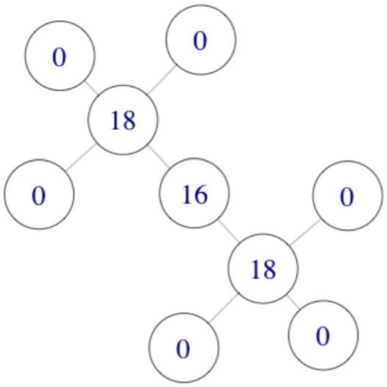


Figure 4.15: Betweenness.

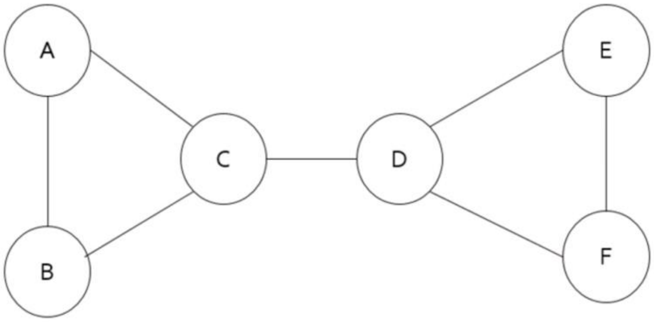


Figure 4.16: Betweenness.

A node is considered very effective or important if he is situated in many shortest paths as shown on Figure 4.15, so that different networks can pass information through it.

$$betweenness\_centrality(i) \overset{def}{=} \sum_{j<k} \frac{g_{jk}(i)}{g_{jk}}$$

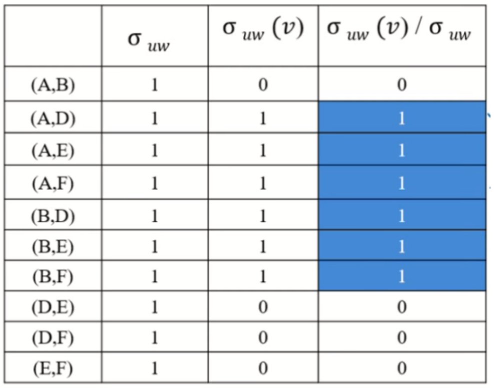
$$C_B'(i) = C_B(i\ )/[(n-1)(n-2)/2]$$

Where

(gjk) is the total number of shortest paths between node j and k.
(gjk (i)) is the total number of shortest paths node j and k through i.

4.2.5 Graph Theory.

In mathematics, graph theory is a growing area with a huge variations in the terminology (Crossley et. al., 2015). The terms are used by different authors with different meaning while some of the authors use different words with the same meaning (Valente et. al., 2015).



	σ_{uw}	$\sigma_{uw}(v)$	$\sigma_{uw}(v) / \sigma_{uw}$
(A,B)	1	0	0
(A,D)	1	1	1
(A,E)	1	1	1
(A,F)	1	1	1
(B,D)	1	1	1
(B,E)	1	1	1
(B,F)	1	1	1
(D,E)	1	0	0
(D,F)	1	0	0
(E,F)	1	0	0

Betweenness Centrality for C = 6

4.2.5.1 Basics.

A *graph* g has vertices and edges (Palonen et. al., 2013). In the set of vertices, each edge possesses two endpoints, which connect them pairwise (Lieberman et. al., 2014). Edges are defined as a pair of two vertices (Worrell et. al., 2013). There are alternate models of graphs; for instance a graph can be a square (0,1)-matrix over the set of vertices, or a binary Boolean function (Nikolaev et. al., 2015).

A *apex* g can be drawn as a set of nodes (Mercer et. al., 2015) and it is denoted as v (g), or v in absence of risk of misperception (Burt et. al., 2013). In the graphs the order is attributed to the vertices and is denoted as |v (g).| (Luo et. al., 2015).

Edge is a line which associates 2 vertices (an arrangement of two components) known as endpoints and also end vertices (Bourbousson et. al., 2015). An edge is denoted as xy, having end vertices x and y. The edge set of g is normally denoted as either e (g) or simply e if the condition is not present (Lieberman et. al., 2014).

The *size* of a graph g is the sum of all of its edges v(g), and is denoted as |e (g).| (Crossley et. al., 2015).

Loop is defined when an edge has endpoints in a single vertex (Valente et. al., 2015). Connections have for endpoints different end vertices (Palonen et. al., 2013). An aggregate of various edges having similar end vertices is the multiplicity of an edge (Nikolaev et. al., 2015). A graph is *simple* in the case when there are no multiple connections and loops, a *pseudo graph* we have in the case of multiple edges and loops without connections (literature is exceedingly conflicting on this) and a *multigraph* - in the case when there are multiple edges without loops (Palonen et. al., 2013). A chart is just a graph without any qualification (Crossley et. al., 2015).

Graphs having edges and vertices can be labeled (Nikolaev et. al., 2015). Those with named edges are edge-labelled, graphs with named vertices are vertex-labelled (Worrell et. al., 2013). The distinction between unlabeled and labeled graphs is that the unlabeled ones do not have labelled edges or vertices (Valente et. al., 2015).

An edgeless graph is a graph without any edges but zero or more vertices (Bourbousson et. al., 2015). An empty or a null graph is a graph which is without vertices and edges; this graph on n vertices without any edges and vertices is called null diagram (Luo et. al., 2015) (no consistency in the terminology).

A graph can be infinite, but most graphs are finite (Marshall et. al., 2015). An infinite graph is locally finite graph having finite degree for every index (Valente et. al., 2015). A chart is assumed finite, when formulated without qualification (Mercer et. al., 2015).

For example, if there is a graph g which is homomorphic to graph h and the mapping is a homomorphism from v(g) to v(h) in a way so that 2 vertices are present very near to each other in g then the vertices which are equivalent in the graph h are also near to each other.

4.2.5.2 Subgraphs.

A subgraph of g is a subset of g with adjacent subgroup limited to this subgroup (Palonen et. al., 2013). On the other end, the diagram is a super graph of a chart g of which it is a subgraph (Lieberman et. al., 2014). A diagram g comprises of another chart h in case a subgraph of g is isomorphic to h, or h is a subgraph of g. In this case, we say that h traverses g.

Diagram g has a subgraph of h which is actuated if xy is an edge of h, and for any of the vertices x and y of h, edge of g is xy (Mercer et. al., 2015). In such a case, h is initial subgraph of diagram g, if it has edges that can be shown in g with vertex set and h can be composed as g[s]. When the set of vertices of h is a subset s of v(g), we are saying that g is prompted by s. A chart having no h as an actuated subgraph is considered without h. Inside a class k of diagrams a universal graph is a straightforward chart having each component in k as a subgraph (Lieberman et. al., 2014).

4.2.5.3 Trees.

It is a connected non-cyclic straightforward diagram (Palonen et. al., 2013). A leaf is a vertex of degree 1, or also pendant vertex (Nikolaev et. al., 2015). A leaf edge is an edge occurrence to a leaf, or also pendant edge (Valente et. al., 2015). An inner vertex is a non-leaf vertex (Worrell et. al., 2013). In some cases, any one vertex of the tree can be its root; and if this is the case then the tree is rooted (Nikolaev et. al., 2015). These are the trees which are regarded as coordinated non-cyclic diagrams with the edges directing far away from the root (Valente et. al., 2015).

Strongly linked component has similar but weaker definition (Burt et. al., 2013). Casually, the components where all the present hubs can be in reach by every other hub in the subgraph is a subgraph which a strongly connected part of a coordinated diagram (Luo et. al., 2015). The presence of node paths establishes the reachability of the hubs (Palonen et. al., 2013).

By running the (dfs) calculation twice a directed graph can be decomposed into strongly linked components. It starts with one on the graph and another on the transposition of the outline which is in decreasing order of completing instances of the principal dfs (Worrell et. al., 2013). Assuming a directed chart g, its transposition gt has the edge directions reversed (Bourbousson et. al., 2015).

4.2.5.4 Adjacency Degree

In diagrams, especially when it is a vertex, various degrees are frequently used to measure the prompt contiguousness (Worrell et. al., 2013). Two vertices connected by an edge are termed as incident upon that edge; if this is not the case then the edge becomes incident to the two vertices (Marshall et al., 2015). All of these ideas are related to the degree of *adjacency* (Burt et. al., 2013).

Within a graph g, the degree of adjacency dg(v), or *valency* of a vertex v, is the sum of its edges in v, with loops being checked two times (Mercer et. al., 2015). Isolated vertex has degree 0 and a leaf vertex has degree 1 (Lieberman et. al., 2014). The aggregate level of a graph is equivalent to twice the sum of its edges, including the loops (Crossley et. al., 2015). The aggregated degree would be six for a chart with 3 vertices having every vertex of level two (a triangle).

Sequence of degrees is termed as a *rundown* of degrees having a diagram in decreasing order (Nikolaev et. al., 2015).

Two of the vertices u and v are *contiguous* in case when there is an edge of u and v. It is denoted as u ~ v or u ↓ v. The pair of branches of a v-shaped subgraph v is called neighborhood of vertex v and is denoted as ng (v) meaning they are vertices adjoining v but excluding v. A closed neighborhood is when v is included denoted as ng[v]. An area is termed as open, when it is denoted without qualifications (Palonen et. al., 2013). The subscript g in the notations is often dropped; as opposed to relating induced subgraphs, a similar neighborhood representation may likewise be utilized to allude to sets of nearby vertices (Marshall et al., 2015).

A vertex subset with close neighborhood incorporating all vertices of the graph is a *dominating set* of a diagram (Lieberman et. al., 2014). The domination number γ(g) is the size of a dominating set (Lieberman et. al., 2014).

A finite graph having n directed or undirected vertices is frequently characterized by an adjacency matrix of n*n values in which entries indexed ij (where i is row and j is column) represent the total edges from vertex at row i to vertex at column.

4.2.5.5 Independence

In a graph theory, independence means the absence of mutually nonadjacent or pairwise disjoints (Palonen et. al., 2013). It is another term for lack of adjacency (Luo et. al., 2015). A *segregated vertex* is a type of vertex which is not directed to any boundaries (Worrell et. al., 2013). *Independent set*, also termed as a stable set, is defined as a group of apexes having no adjacent pair (Crossley et. al., 2015). Subsequently a *void graph* is the *graph* prompted by any independent set (Nikolaev et. al., 2015).

If two sub graphs have no edges they are *edge disjoint* (Valente et. al., 2015). Similarly, two subgraphs having no vertices are *vertex disjoint* (and in this way, additionally without edges) (Marshall et. al., 2015). A disjoint set of subgraphs are *pairwise vertex disjoint*, if not qualified otherwise (Worrell et. al., 2013).

In a graph g, the *independence number* α(g) is termed as the biggest measure of an independent set of graph g. There are free sets of graphs g because complete vertex set is able to be apportioned into disconnected independent subsets pairwise (Bourbousson et. al., 2015). Independent subsets of this kind are termed as *partitioned sets* or parts (Luo et. al., 2015).

4.2.5.6 Connectivity.

It is basically a measure of concatenated adjacency and it expands the idea of contiguousness (Mercer et. al., 2015). The diagram is connected, if it builds up a way from vertex to the other vertex; the chart is disjoint otherwise (Valente et. al., 2015). A diagram is *absolutely disjoint* in case there is no way interfacing any combination of vertices (Nikolaev et. al., 2015). It is simply another name for portraying an independent set or an empty graph (Crossley et. al., 2015).

A *vertex cut* is a vertex which is removed from a subgraph (Lieberman et. al., 2014). A vertex cut is also called a *separating set*, since it groups vertices removed from the other subgraph (Luo et. al., 2015).

The diagram is a *k-vertex-linked* or k-linked, if it is likely to be build up from a vertex to some other vertex of a diagram even with the elimination of k - 1 vertices (Mercer et. al., 2015). If the k disjoint vertices are present in the middle then the diagram is termed as k-connected (Palonen et. al., 2013). According to our hypothesis, the network is a connected subgraph containing a dominant part of the nodes of the whole diagram (Crossley et. al., 2015).

4.2.5.7 Distance

The distance D (u, v) is called *displacement* between vertices u and v in the diagram; it is defined as the distance of the shortest path from u to v. Distance of u to v is 0, when u and v are inaccessible from each vertex; when u and v vertices are equal the displacement of them is infinite (Worrell et. al., 2013).

4.3 Proposed Framework.

The proposed solution for the analysis is based on the analytical tools from Social Network Theory and Graph Theory. The main goal of this analysis is to identify the individual who plays the main role in the malicious activities within the organization.

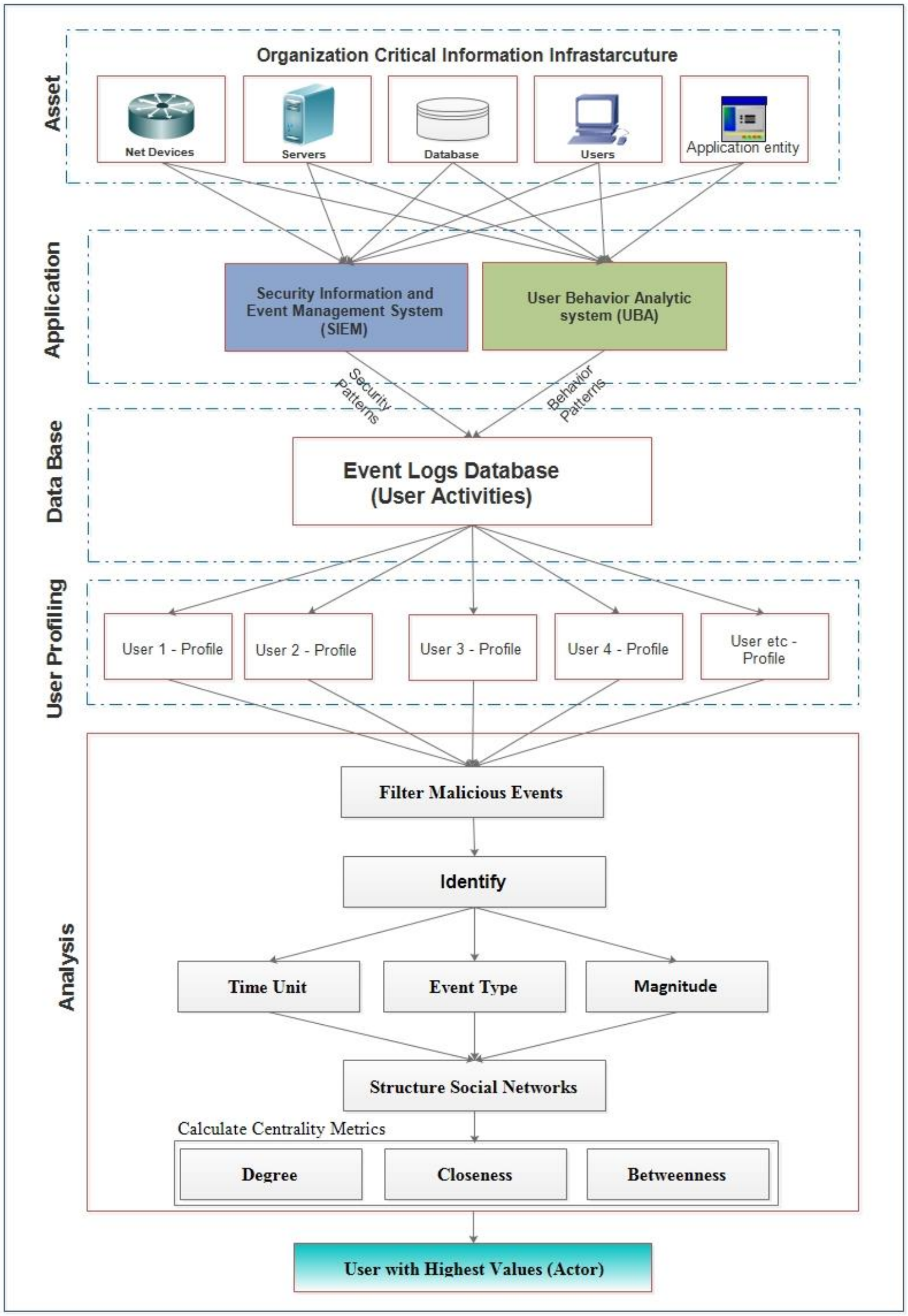


Figure 4.17: Proposed Framework for the Analysis.

The proposed framework tries to utilize the exiting data that is usually collected by all computer system administrators. Then this data should be filtered to include only malicious activities relevant to the analysis. After that, three main categories are proposed to be identified: time unit in hours, event type which describes the application and magnitude. Other types can be used as well. The next step is to establish networks where the users who have appear in the same category in the logs also have a link between themselves in the network graph. For example, if two users were active in the same hour, then they will be linked. After that, discussed centrality metric should be calculated. The individual who has the highest value for these metrics is the most probable to be the main actor.

The magnitude in the framework is used to prioritize offenses and help to determine, which offenses should be investigated first while the rating of an offense is calculated based on relevance, severity, and credibility.

- Relevance determines the impact of the offense on your network, like some ports are open, the relevance is high.

- Credibility indicates the integrity of the offense as determined by the credibility rating that is configured in the log source. Credibility increases as multiple sources report the same event.

- Severity indicates the level of threat that a source poses in relation to how prepared the destination is for the attack.

Chapter 5: Implementation, Results and Discussions.

5.1 General Description.

There are 651718 events in the data set. Recording these **events** started on 2017-04-13 16:50:23 and finished on 2017-04-16 15:51:25. There are 62 distinct event types. Event 'User Account Removed' has the minimum activities count with percentage of 0.0002 %. On the other end, event 'Information' has the maximum count of 324665 with percentage of 49 %. The average count of all different Events is 10511.6, with standard deviation of the events from the average 45919.5.

Respectively, there are 91 distinct users providing inputs in the data set. **User** 'User34' has the minimum count of one appearance with percentage of 0.0002 %. On the other end, user 'User_NA' has the maximum count of 621748 appearances with percentage of 95 %. The average count of all different users is 7161.7 with standard deviation 64791.6.

In addition, there are 9 distinct activity magnitudes. **Magnitude** '10' has the minimum count of one with percentage of 0.0002 %. Conversely, Magnitude '5' has the maximum count of 403619 with percentage of 61 %. The average count of all different Magnitudes is 72413.1; while the standard deviation is 124396.5.

Moreover, there are 11 distinct operation hours. **Hour** '1' has the minimum count of 29 with percentage of 0.0044 %. Instead, Hour '13' has the maximum count of 139130 with percentage of 21 %. The average count of all different Hours is 59247.1; while the standard deviation is 51279.4.

5.2 Users and Malicious Activities.

There are 6689 malicious events with percentage of 10.0264 %. The following figure shows the distribution of these events over Users.

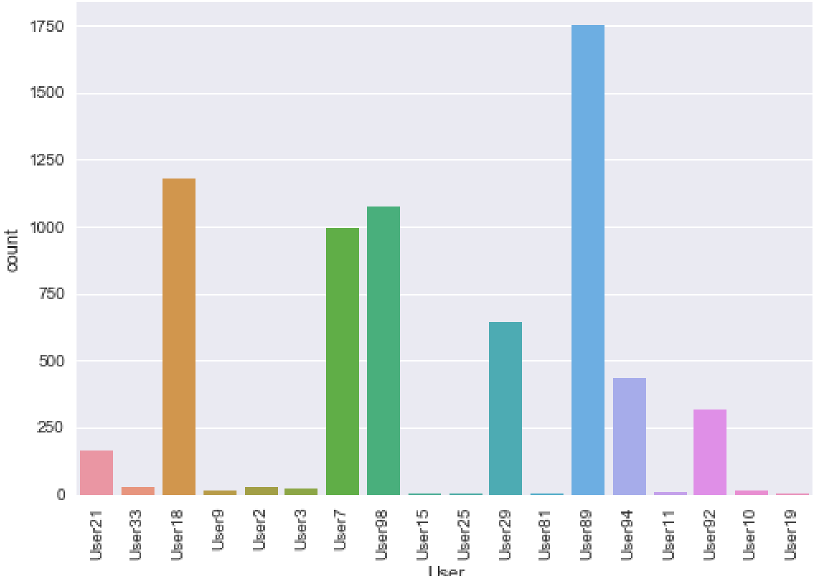


Figure 5.1: Distribution of the Malicious Activities across Users.

User 'User81' has the minimum count of 3 with percentage of 0.0448 %. On the other hand, User 'User89' has the maximum count of 1753 with percentage of 26 %. The average count of all different Users is 371.6; while the standard deviation is 518.9.

5.3 Hour.

The following figure shows the distribution of these malicious events over Hours.

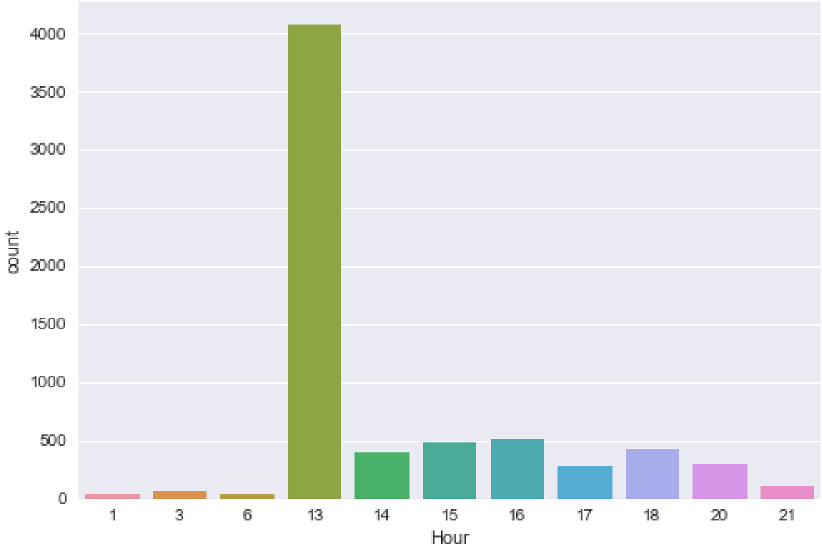


Figure 5.2: malicious activities distribution over Hour.

Hour '1' has the minimum count of 29 with percentage of 0.4335 %. Then again, Hour '13' has the maximum count of 4077 with percentage of 60 %. The average count of all different Hours is 608.1; while the standard deviation is 1110.3. The following sub-sections will build the social network for each one of these hours with regard to other categories in the data set (i.e. magnitude and event types etc.).

- Average value and Standard division.

To characterize or describe a bulk of dataset, it is very important to learn the meaning and purpose of different types of statistical values. There are two different and important statistics which are measures of Average value and Standard deviation.

The average is the sample mean and is measured as the sum of all the observed outcomes from the sample and divided by the total number of events. The (x) is used as a symbol for average. In math terms,

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x$$

Where (n) are the sample size and the (x) corresponding to the observed value, for example the average for numbers (34, 43, 81, 106, 106 and 115):

We compute the sample mean by adding and dividing by the number of samples by 6.

$$\frac{34 + 43 + 81 + 106 + 106 + 115}{6} = 80.83$$

The purpose of the average value in this network graphs is to show how much the different users or nodes are involved in the activity mean the nearest value of different centrality measurements (degree, closeness and between) of users to the average are more involved.

While, Standard deviation is a measure that summarizes the amount by which every value within a dataset varies from the average or mean. Exactly it is show

how tightly the values in the dataset are linked into a compact group around the mean value.

In other meaning, Standard Deviation usually shows the variation in data. If the data is close together, the standard deviation will be small and, if the data is diffused then standard deviation will be large. The standard deviation formula can be represented using Sigma Notation:

$$\sigma = \sqrt{\frac{\sum (x-\mu)^2}{n}}$$

For example the SD for the following five numbers which are: 92,88,80,68 and 52:

1. Find the mean: (92+88+80+68+52)/5 = 76.
2. Find the deviation from the mean:
   a. 92-76=16
   b. 88-76=12
   c. 80-76=4
   d. 68-76= -8
   e. 52-76= -24
3. Square the deviation from the:

$$(16)^2 = 256$$
$$(12)^2 = 144$$
$$(4)^2 = 16$$
$$(-8)^2 = 64$$
$$(-24)^2 = 576$$

4. Find the sum of the squares of the deviation from the mean: 256+144+16+64+576= 1056
5. Divide by the number of data items: 1056/5 = 211.2
6. Find the square root of the variance:

$$\text{variance: } \sqrt{211.2} = 14.53$$

5.3.1 Hour and Magnitude.

Graphs model the connections in a network and are widely applicable in several fields like physical, biological, and information systems. The graphs can be used to model the neurons in a brain, the flight patterns of an airline, and much more. The structure of a graph is comprised of “nodes” and “edges”. Each node represents an entity, and each edge represents a connection between two nodes or context which made up of vertices, nodes that are connected to each other by edges, arcs, or lines.

The network graph in this section represents several users (nodes or vertex) in certain time of period from (hour 1, 3, 15, 16, 20, 21), while the links connected between them (edge) represented different level of magnitude which are variable between (magnitude1 to magnitude10).

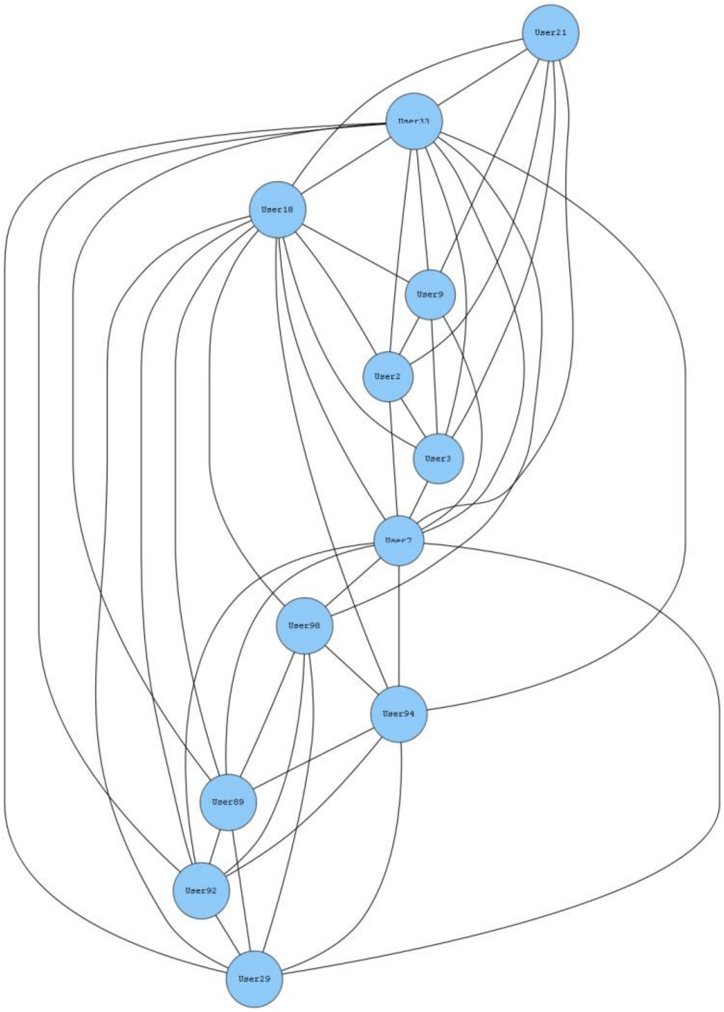


Figure 5.3: Users associations for Hour 16.

Figure 5.3 illustrates different component of graph at hour 16, where the circles represent different users as nodes while the links between them (vertex) are represented as magnitude and differ from 1 to 10 reflecting the relationship between different users.

The maximum value of **degree of centrality** of one has been realized by users User33, User18, and User7. Users User21, User9, User2, and User3 have achieved the minimum value of 0.55 for degree of centrality. Its average value is 0.7; while the standard deviation value is 0.18.

Betweenness centrality has a maximum value of 0.12 which was achieved by users User33, User18, and User7. The minimum value of zero for the same measure has been realized by users User21, User9, User2, User3, User98, User94, User89, User92, and User29. Both of 0.03 and 0.05 are the average and the standard deviation values for betweenness centrality in this network graph.

Users User33, User18, and User7 have achieved the maximum value of one for **closeness** centrality. It has a minimum value of 0.69 which was achieved by users User21, User9, User2, and User3. It has an average value of 0.78 for all users. Moreover, it has a standard deviation value of 0.13.

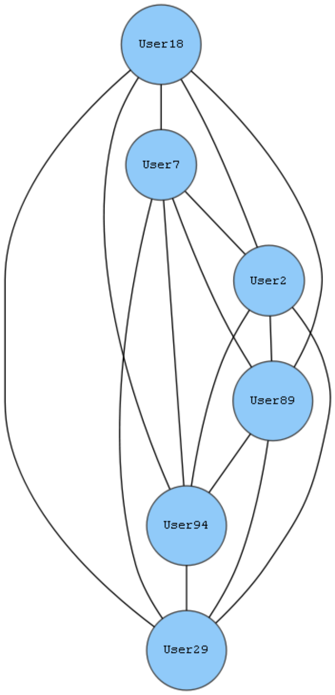


Figure 5.4: Users associations for Hour 15.

Figure 5.4 illustrates the different component of the graph at hour 15, where the circles represents different users as nodes while the links between them (vertex) are represented as magnitude and differ from 1 to 10 reflecting the relationship between different users.

Degree of centrality has a value of one for all users in Hour '15'. They have the same betweenness centrality for all of them as well as the same closeness centrality.

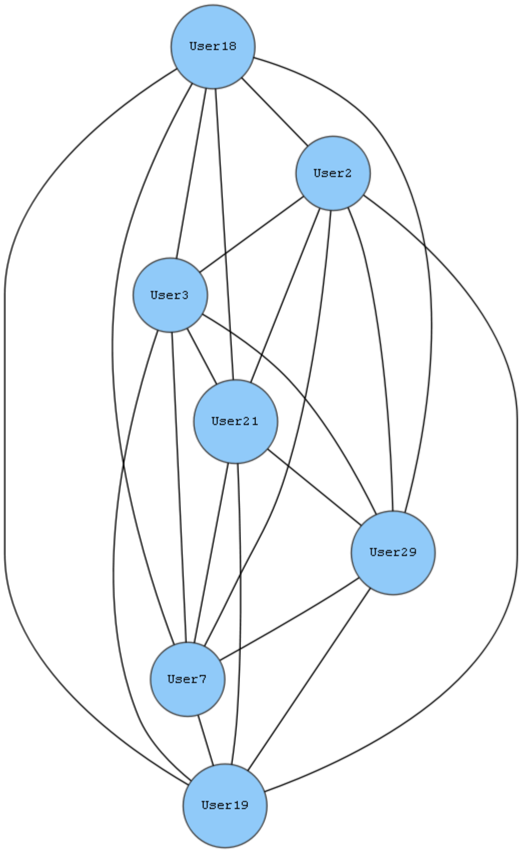


Figure 5.5: Users associations for Hour 3.

Figure 5.5 illustrates different components of the graph at hour 3, where the circles represent different users as nodes while the links between them (vertex) are represented as magnitude and differ from 1 to 10 reflecting the relationship between different users.

Users in Hour '3' have the same degree of centrality for all of them. Also, they have betweenness centrality of zero. Conversely, all users have closeness centrality of one.

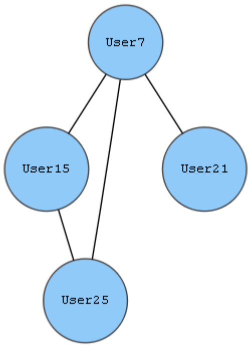


Figure 5.6: Users associations for Hour 1.

Figure 5.6 illustrates the different components of the graph at hour 1, where the circles represent different users as nodes while the links between them (vertex) are represented as magnitude and differ from 1 to 10 reflecting the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by user User7. User User21 has degree of centrality of 0.33 which is at the same time the minimum in this graph for Hour '1'. Its average value is 0.67; while the standard deviation value is 0.24.

The maximum value of betweenness centrality of 0.67 has been realized by user User7. Users User15, User25, and User21 have achieved the minimum value of zero for the same measure. Both of 0.17 and 0.29 are the average and the standard deviation values for betweenness centrality in this network graph.

User User7 has closeness centrality of one which is at the same time the maximum in this graph for Hour '1'. Value 0.6 is the minimum for the same metric that has been achieved by user User21. It has an average value of 0.78 for all users. Moreover, it has a standard deviation value of 0.14.

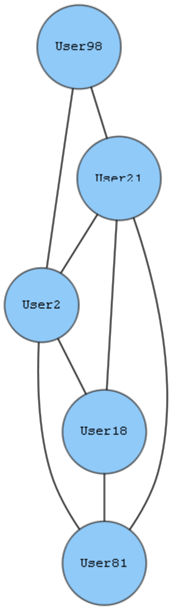


Figure 5.7: Users associations for Hour 20.

Figure 5.7 illustrates the different components of the graph at hour 20, where the circles represent different users as nodes while the links between them (vertex) are represented as magnitude and differ from 1 to 10 reflecting the relationship between different users.

The maximum value of degree of centrality of one has been realized by users User21, and User2. User User98 has achieved the minimum value of 0.5 for degree of centrality. Both of 0.8 and 0.19 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality has a maximum value of 0.17 which was achieved by users User21, and User2. The minimum value of zero for the same measure has been realized by users User98, User18, and User81. It has an average value of 0.07 for all users. Also, it has a standard deviation value of 0.08.

Users User21 and User2 have achieved the maximum value of one for closeness centrality. It has a minimum value of 0.67 which was achieved by user User98. Its average value is 0.85; while the standard deviation value is 0.13.

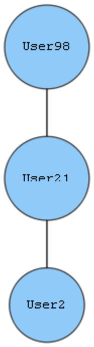


Figure 5.8: Users associations for Hour 21.

Figure 5.8 illustrates the different components of the graph at hour 21, where the circles represent different users as nodes while the links between them (vertex) are represented as magnitude and differ from 1 to 10 reflecting the relationship between different users.

User User21 has achieved the maximum value of one for degree of centrality. It has a minimum value of 0.5 which was achieved by users User98, and User2. Its average value is 0.67; while the standard deviation value is 0.24.

Value one is the maximum of betweenness centrality that has been achieved by user User21. Users User98 and User2 have betweenness centrality of zero which is at the same time the minimum in this graph for Hour '21'. Both of 0.33 and 0.47 are the average and the standard deviation values for betweenness centrality in this network graph.

Closeness centrality has a maximum value of one which was achieved by user User21. The minimum value of 0.67 for the same metric has been realized by users User98, and User2. It has an average value of 0.78 for all users. Moreover, it has a standard deviation value of 0.16.

5.3.2 Hour and Event.

The network graph in this section represents several users (nodes or vertex) in certain period of time with a range of (hour 1, 3, 13, 14, 15, 16 and 18), while the links connected between them (edge) represented different type of malicious activities which are resulting from:

- Brute force successful logins in odd hours.
- Brute force logins along with high number of login failure.
- Successful login at odd hours.
- Login failure.
- Login failure in odd hours.
- Malicious exploits.
- Malicious exploits at odd hours.
- Account privilege changes in odd hour.

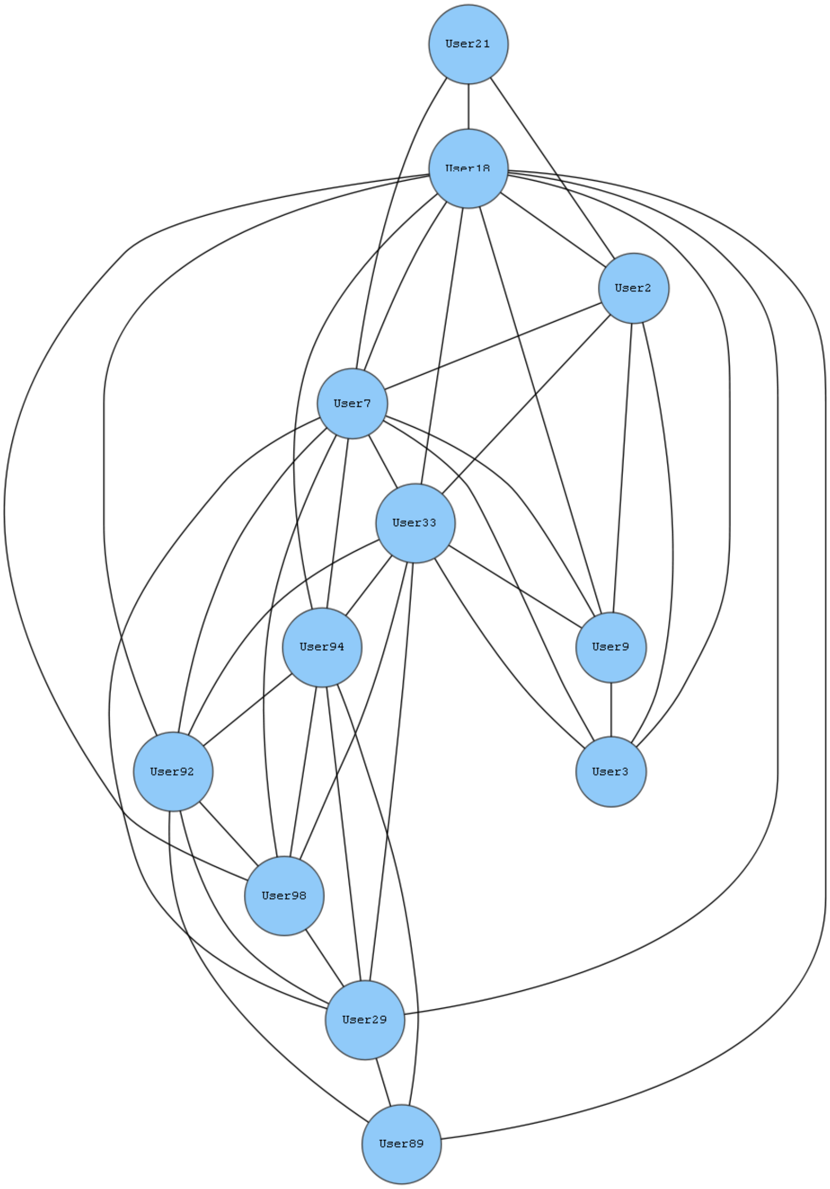


Figure 5.9: Users associations for Hour 16.

Figure 5.9 illustrates the different components of the graph at hour 16, where the circles represent different users as nodes while the links between them (vertex) are represented as different type of malicious activities mentioned above reflecting the relationship between different users.

User User18 has achieved the maximum value of one for degree of centrality. It has a minimum value of 0.27 which was achieved by user User21. Both of 0.61 and 0.21 are the average and the standard deviation values for degree of centrality in this network graph.

Value 0.21 is the maximum of betweenness centrality that has been achieved by user User18. Users User21, User9, User3, User98, and User89 have betweenness centrality of zero which is at the same time the minimum in this graph for Hour '16'. It has an average value of 0.04 for all users. Also, it has a standard deviation value of 0.06.

Closeness centrality has a maximum value of one which was achieved by user User18. The minimum value of 0.58 for the same metric has been realized by user User21. Its average value is 0.74; while the standard deviation value is 0.12.

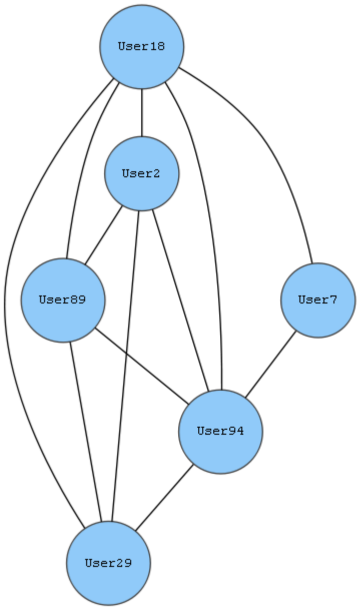


Figure 5.10: Users associations for Hour 15.

Figure 5.10 illustrates the different components of the graph at hour 15, where the circles represent different users as nodes while the links between them (vertex) are represented as different type of malicious activities mentioned above reflecting the relationship between different users.

Degree of centrality has a maximum value of one which was achieved by users User18, and User94. The minimum value of 0.4 for the same metric has been realized by user User7. Its average value is 0.8; while the standard deviation value is 0.2.

Users User18 and User94 have betweenness centrality of 0.15 which is at the same time the maximum in this graph for Hour '15'. Value zero is the minimum the same measure that has been achieved by users User7, User2, User89, and User29. Both of 0.05 and 0.07 are the average and the standard deviation values for betweenness centrality in this network graph.

Value one is the maximum of closeness centrality that has been achieved by users User18, and User94. User User7 has closeness centrality of 0.62 which is at the same time the minimum in this graph for Hour '15'. It has an average value of 0.85 for all users. Moreover, it has a standard deviation value of 0.13.

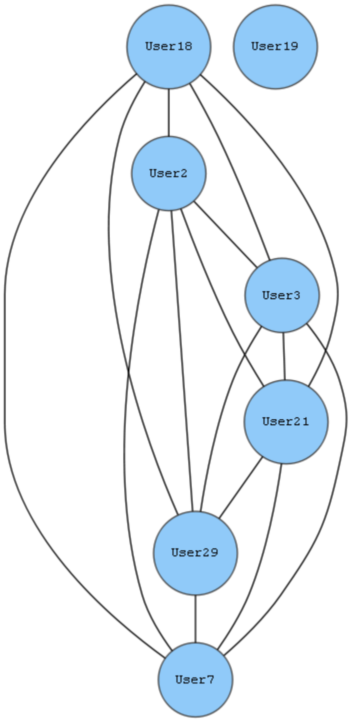


Figure 5.11: Users associations for Hour 3.

Figure 5.11 illustrates the different components of the graph at hour 3, where the circles represent different users as nodes while the links between them (vertex) are represented as different type of malicious activities mentioned above reflecting the relationship between different users.

Value 0.83 is the maximum of degree of centrality that has been achieved by users User18, User2, User3, User21, User29, and User7. User User19 has degree of centrality of zero which is at the same time the minimum in this graph for Hour '3'. It has an average value of 0.71 for all users. And, it has a standard deviation value of 0.29.

Betweenness centrality is zero for all users in this graph.

Users User18, User2, User3, User21, User29, and User7 have closeness centrality of 0.83 which is at the same time the maximum in this graph for Hour '3'. Value zero is the minimum for the same metric that has been achieved by user User19. Both of 0.71 and 0.29 are the average and the standard deviation values for closeness centrality in this network graph.

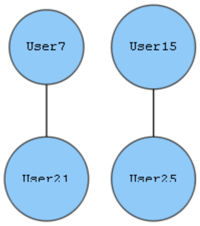


Figure 5.12: Users associations for Hour 1.

Figure 5.12 illustrates the different components of the graph at hour 1, where the circles represent different users as nodes while the links between them (vertex) are represented as different type of malicious activities mentioned above reflecting the relationship between different users.

Users User7, User21, User15, and User25 have degree of centrality of 0.33 which is at the same time the maximum in this graph for Hour '1'. Value 0.33 is the minimum of the same metric that has been achieved by users User7, User21, User15, and User25. Both of 0.33 and zero are the average and the standard deviation values for degree of centrality in this network graph.

In this graph, all users achieve betweenness centrality of zero.

The maximum value of closeness centrality of 0.33 has been realized by users User7, User21, User15, and User25. Users User7, User21, User15, and User25 have achieved the minimum value of 0.33 for the same metric. Its average value is 0.33; while the standard deviation value is 0.0.

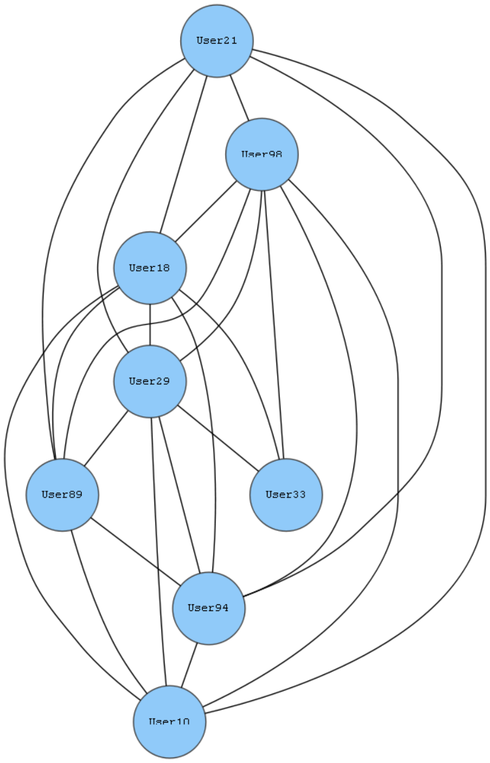


Figure 5.13: Users associations for Hour 18.

Figure 5.13 illustrates the different components of the graph at hour 18, where the circles represent different users as nodes while the links between them (vertex) are represented as different type of malicious activities mentioned above reflecting the relationship between different users.

The maximum value of degree of centrality of one has been realized by users User98, User18, and User29. User User33 has achieved the minimum value of 0.43 for degree of centrality. Its average value is 0.86; while the standard deviation value is 0.17.

Betweenness centrality has a maximum value of 0.06 which was achieved by users User98, User18, and User29. The minimum value of zero for the same measure has been realized by users User21, User89, User94, User10, and User33. Both of 0.02 and 0.03 are the average and the standard deviation values for betweenness centrality in this network graph.

Users User98, User18, and User29 have achieved the maximum value of one for closeness centrality. It has a minimum value of 0.64 which was achieved by user User33. It has an average value of 0.89 for all users. Moreover, it has a standard deviation value of 0.11.

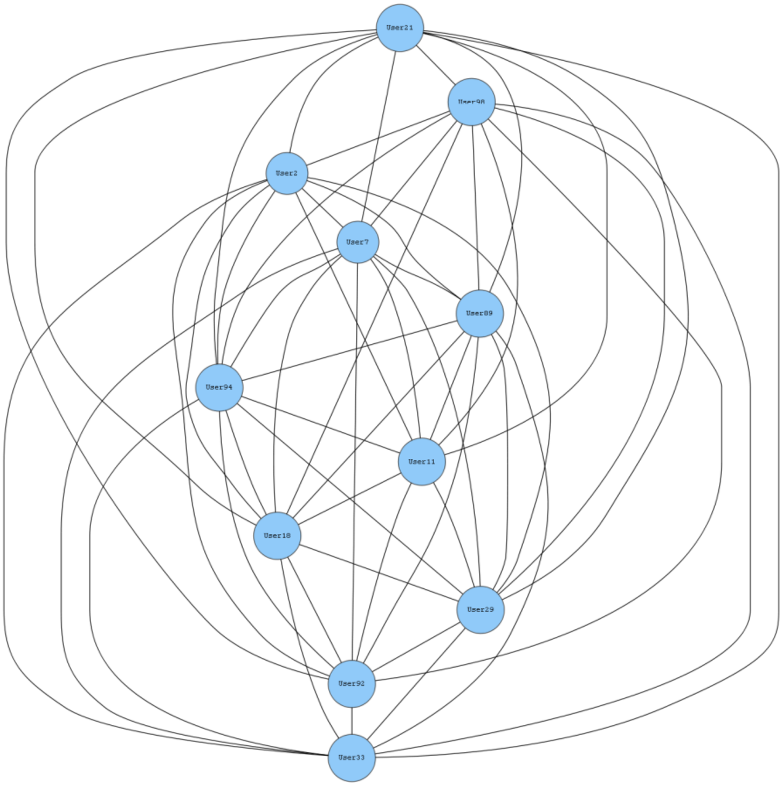


Figure 5.14: Users associations for Hour 13.

Figure 5.14 illustrates the different components of the graph at hour 13, where the circles represent different users as nodes while the links between them (vertex) are represented as different type of malicious activities mentioned above reflecting the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by users User21, User98, User2, User7, User89, User94, User18, User29, and User92.

Users User11, and User33 have degree of centrality of 0.9 which is at the same time the minimum in this graph for Hour '13'. Its average value is 0.98; while the standard deviation value is 0.04.

The maximum value of betweenness centrality of zero has been realized by users User21, User98, User2, User7, User89, User94, User18, User29, and User92. Users User11, and User33 have achieved the minimum value of zero for the same measure. Both of zero and zero are the average and the standard deviation values for betweenness centrality in this network graph.

Users User21, User98, User2, User7, User89, User94, User18, User29, and User92 have closeness centrality of one which is at the same time the maximum in this graph for Hour '13'. Value 0.91 is the minimum for the same metric that has been achieved by users User11, and User33. It has an average value of 0.98 for all users. Moreover, it has a standard deviation value of 0.04.

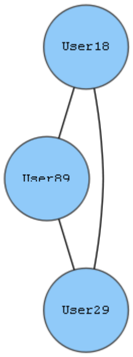


Figure 5.15: Users associations for Hour 14.

Figure 5.15 illustrates the different components of the graph at hour 14, where the circles represent different users as nodes while the links between them (vertex) are represented as different type of malicious activities mentioned above reflecting the relationship between different users.

Degree of centrality is one for all users in this graph, while the achieved betweenness centrality is zero for all users and finally achieved closeness centrality for all users is one.

5.3.3 Hour and Source IP Address.

The network graphs in this section represents several users (nodes or vertex) in a certain period of time ranging from (hour 3, 13, 14, 15, 16, 17, 18 and 20), while the links connected between them (edge) represent different source IP address which could be servers, firewalls, database or host. In this case any node has a connection to the same source IP address which means that this node has a link between them.

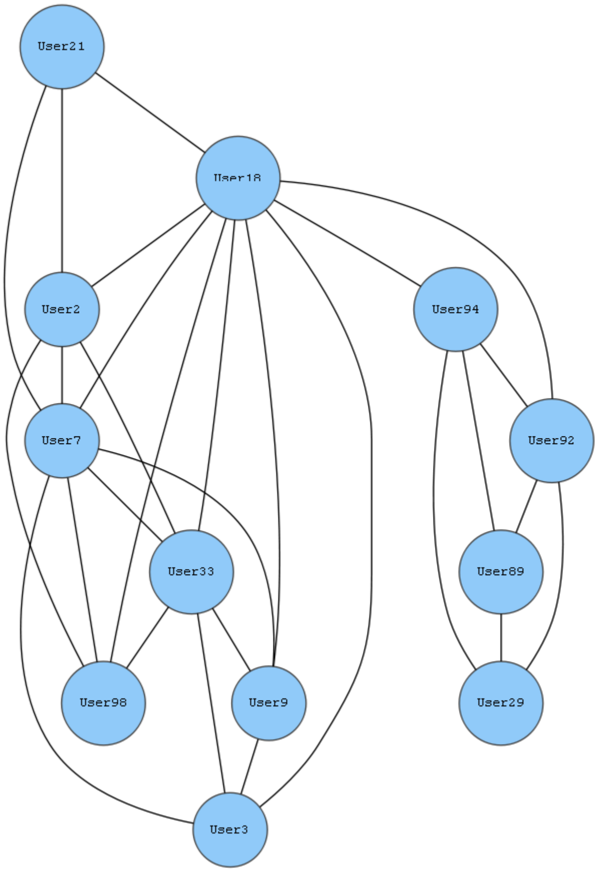


Figure 5.16: Users associations for Hour 16.

Figure 5.16 illustrates different components of the graph at hour 16, where the circles represents different users as node while the links between them (vertex) are presented as a different source IP Addresses reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.82 which was achieved by user User18. The minimum value of 0.27 for the same metric has been realized by users User21, User89, and User29. It has an average value of 0.42 for all users. And, it has a standard deviation value of 0.16.

User User18 has betweenness centrality of 0.56 which is at the same time the maximum in this graph for Hour '16'. Value zero is the minimum the same measure that has been achieved by users User21, User9, User3, User98, User89, and User29. Its average value is 0.08; while the standard deviation value is 0.16.

Value 0.85 is the maximum of closeness centrality that has been achieved by user User18. Users User89, and User29 have closeness centrality of 0.42 which is at the same time the minimum in this graph for Hour '16'. Both of 0.58 and 0.11 are the average and the standard deviation values for closeness centrality in this network graph.

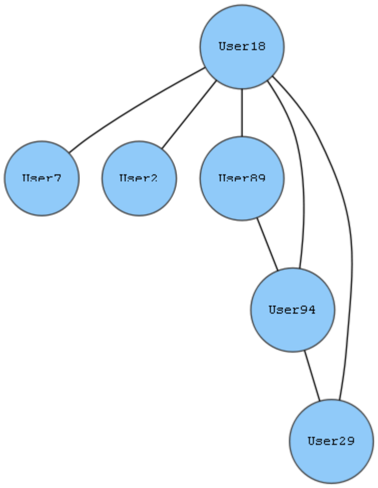


Figure 5.17: Users associations for Hour 15.

Figure 5.17 illustrates different components of the graph at hour 15, where the circles represents different users as node while the links between them (vertex) are presented as a different source IP Addresses reflecting the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by user User18. Users User7, and User2 have degree of centrality of 0.2 which is at the same time the minimum in this graph for Hour '15'. Both of 0.47 and 0.27 are the average and the standard deviation values for degree of centrality in this network graph.

The maximum value of betweenness centrality of 0.75 has been realized by user User18. Users User7, User2, User89, and User29 have achieved the minimum value of zero for the same measure. It has an average value of 0.13 for all users. Also, it has a standard deviation value of 0.28.

User User18 has closeness centrality of one which is at the same time the maximum in this graph for Hour '15'. Value 0.56 is the minimum for the same metric that has been achieved by users User7, and User2. Its average value is 0.68; while the standard deviation value is 0.15.

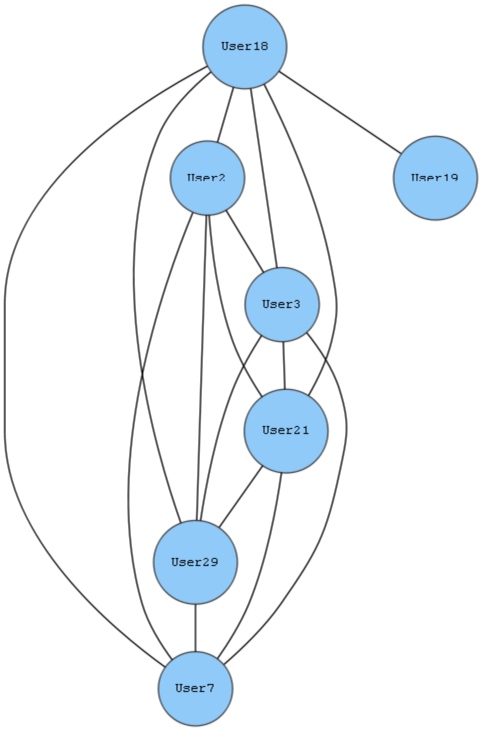


Figure 5.18: Users associations for Hour 3.

Figure 5.18 illustrates different components of the graph at hour 3, where the circles represents different users as node while the links between them (vertex) are presented as a different source IP Addresses reflecting the relationship between different users.

User User18 has degree of centrality of one which is at the same time the maximum in this graph for Hour '3'. Value 0.17 is the minimum of the same metric that has been achieved by user User19. Its average value is 0.76; while the standard deviation value is 0.25.

User User18 has achieved the maximum value of 0.33 for betweenness centrality. It has a minimum value of zero which was achieved by users User2, User3, User21, User29, User7, and User19. Both of 0.05 and 0.12 are the average and the standard deviation values for betweenness centrality in this network graph.

The maximum value of closeness centrality of one has been realized by user User18. User User19 has achieved the minimum value of 0.55 for the same metric. It has an average value of 0.83 for all users. Moreover, it has a standard deviation value of 0.13.

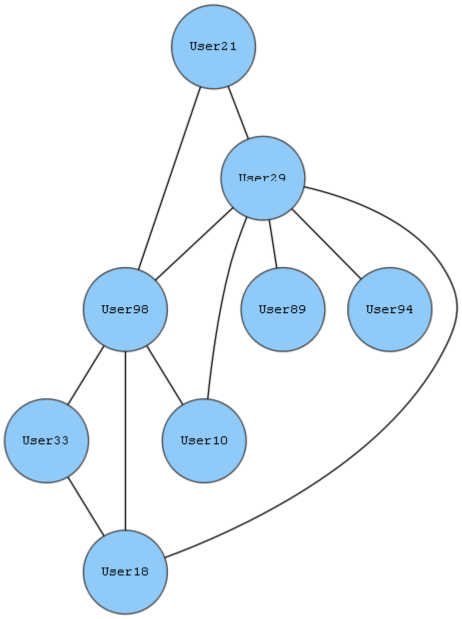


Figure 5.19: Users associations for Hour 18.

Figure 5.19 illustrates different components of the graph at hour 18, where the circles represents different users as node while the links between them (vertex) are presented as a different source IP Addresses reflecting the relationship between different users.

User User29 has achieved the maximum value of 0.86 for degree of centrality. It has a minimum value of 0.14 which was achieved by users User89, and User94. Both of 0.39 and 0.24 are the average and the standard deviation values for degree of centrality in this network graph.

Value 0.6 is the maximum of betweenness centrality that has been achieved by user User29. Users User21, User10, User33, User89, and User94 have betweenness centrality of zero which is at the same time the minimum in this graph for Hour '18'. It has an average value of 0.11 for all users. Also, it has a standard deviation value of 0.2.

Closeness centrality has a maximum value of 0.88 which was achieved by user User29. The minimum value of 0.5 for the same metric has been realized by users User33, User89, and User94. Its average value is 0.62; while the standard deviation value is 0.13.

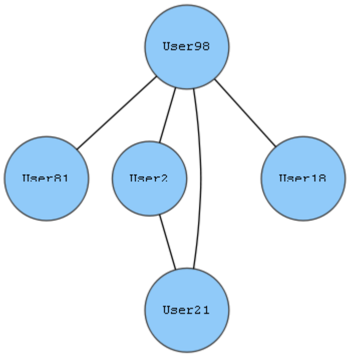


Figure 5.20: Users associations for Hour 20.

Figure 5.20 illustrates different components of the graph at hour 20, where the circles represents different users as node while the links between them (vertex) are presented as a different source IP Addresses reflecting the relationship between different users.

Degree of centrality has a maximum value of one which was achieved by user User98. The minimum value of 0.25 for the same metric has been realized by users User81, and User18. Its average value is 0.5; while the standard deviation value is 0.27.

User User98 has betweenness centrality of 0.83 which is at the same time the maximum in this graph for Hour '20'. Value zero is the minimum the same measure that has been achieved by users User81, User2, User21, and User18. Both of 0.17 and 0.33 are the average and the standard deviation values for betweenness centrality in this network graph.

Value one is the maximum of closeness centrality that has been achieved by user User98. Users User81, and User18 have closeness centrality of 0.57 which is at the same time the minimum in this graph for Hour '20'. It has an average value of 0.7 for all users. Moreover, it has a standard deviation value of 0.16.

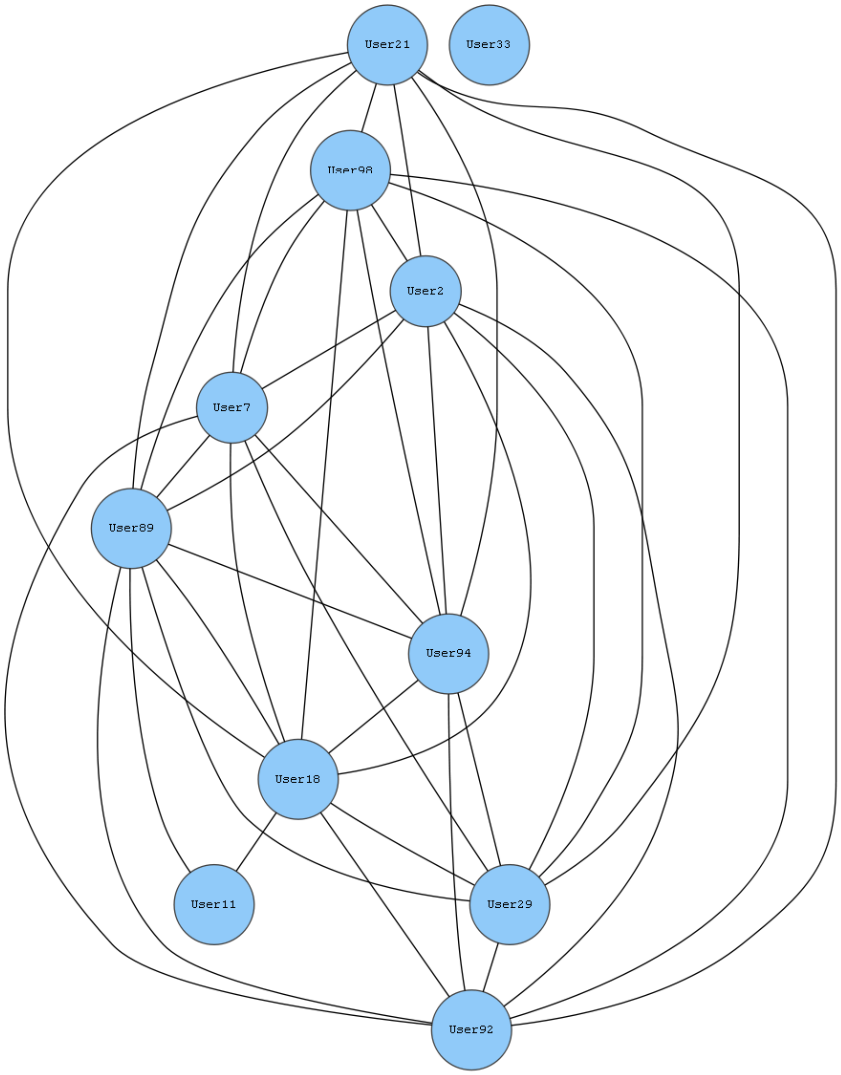


Figure 5.21: Users associations for Hour 13.

Figure 5.21 illustrates different components of the graph at hour 21, where the circles represents different users as node while the links between them (vertex) are presented as a different source IP Addresses reflecting the relationship between different users.

Users User 89 and User18 have degree of centrality of 0.9 which is at the same time the maximum in this graph for Hour '13'. Value zero is the minimum of the same metric that has been achieved by user User33. Both of 0.69 and 0.28 are the average and the standard deviation values for degree of centrality in this network graph.

Users User89 and User18 have achieved the maximum value of 0.08 for betweenness centrality. It has a minimum value of zero which was achieved by users User21, User98, User2, User7, User94, User29, User92, User11, and User33. It has an average value of 0.01 for all users. Also, it has a standard deviation value of 0.03.

The maximum value of closeness centrality of 0.9 has been realized by users User89, and User18. User User33 has achieved the minimum value of zero for the same metric. Its average value is 0.73; while the standard deviation value is 0.25.

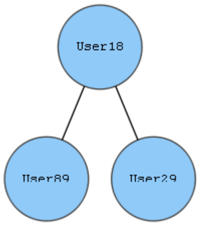


Figure 5.22: Users associations for Hour 14.

Figure 5.22 illustrates different components of the graph at hour 14, where the circles represents different users as node while the links between them (vertex) are presented as a different source IP Addresses reflecting the relationship between different users.

The maximum value of degree of centrality of one has been realized by user User18. Users User89 and User29 have achieved the minimum value of 0.5 for degree of centrality. Its average value is 0.67; while the standard deviation value is 0.24.

Betweenness centrality has a maximum value of one which was achieved by user User18. The minimum value of zero for the same measure has been realized by users User89, and User29. Both of 0.33 and 0.47 are the average and the standard deviation values for betweenness centrality in this network graph.

User User18 has achieved the maximum value of one for closeness centrality. It has a minimum value of 0.67 which was achieved by users User89, and User29. It has an average value of 0.78 for all users. Moreover, it has a standard deviation value of 0.16.

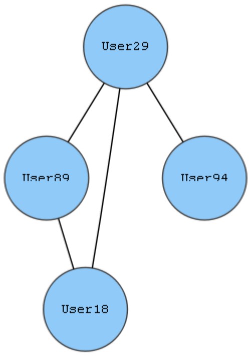


Figure 5.23: Users associations for Hour 17.

Figure 5.23 illustrates different components of the graph at hour 17, where the circles represents different users as node while the links between them (vertex) are presented as a different source IP Addresses reflecting the relationship between different users.

User User29 has achieved the maximum value of one for degree of centrality. It has a minimum value of 0.33 which was achieved by user User94. It has an average value of 0.67 for all users. And, it has a standard deviation value of 0.24.

Value 0.67 is the maximum of betweenness centrality that has been achieved by user User29. Users User89, User18, and User94 have betweenness centrality of zero which is at the same time the minimum in this graph for Hour '17'. Its average value is 0.17; while the standard deviation value is 0.29.

Closeness centrality has a maximum value of one which was achieved by user User29. The minimum value of 0.6 for the same metric has been realized by user User94. Both of 0.78 and 0.14 are the average and the standard deviation values for closeness centrality in this network graph.

5.3.4 Hour and Source Port.

The network graphs in this section represents several users (nodes or vertex) in certain period of time ranging from (hour 3, 6, 13, 14, 15, 16, 17, 18 and 20), while the links connected between them (edge) represent different source ports of different services. In this case any node has a connection to the same source ports which means that these nodes have a link between them.

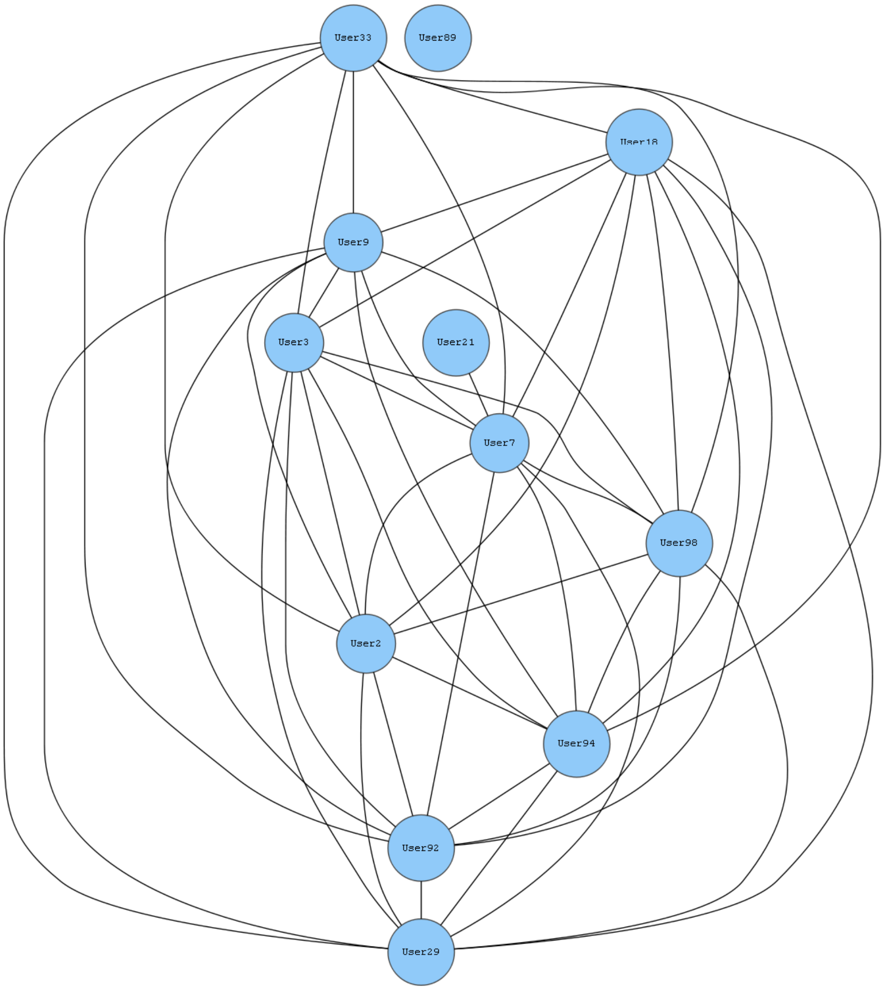


Figure 5.24: Users associations for Hour 16.

Figure 5.24 illustrates different component of graph at hour 16, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

Value 0.91 is the maximum of degree of centrality that has been achieved by user User7. User User89 has degree of centrality of zero which is at the same time the minimum in this graph for Hour '16'. Its average value is 0.7; while the standard deviation value is 0.29.

The maximum value of betweenness centrality of 0.16 has been realized by user User7. Users User21, User33, User18, User9, User3, User98, User2, User94, User92, User29, and User89 have achieved the minimum value of zero for the same measure. Both of 0.01 and 0.05 are the average and the standard deviation values for betweenness centrality in this network graph.

User User7 has closeness centrality of 0.91 which is at the same time the maximum in this graph for Hour '16'. Value zero is the minimum for the same metric that has been achieved by user User89. It has an average value of 0.74 for all users. Moreover, it has a standard deviation value of 0.24.

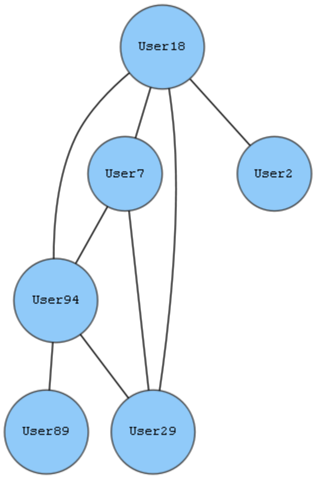


Figure 5.25: Users associations for Hour 15.

Figure 5.25 illustrates different component of graph at hour 15, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

Users User 18, and User94 have degree of centrality of 0.8 which is at the same time the maximum in this graph for Hour '15'. Value 0.2 is the minimum of the same metric that has been achieved by users User2, and User89. It has an average value of 0.53 for all users. And, it has a standard deviation value of 0.25.

Users User18, and User94 have achieved the maximum value of 0.4 for betweenness centrality. It has a minimum value of zero which was achieved by users User7, User29, User2, and User89. Its average value is 0.13; while the standard deviation value is 0.19.

The maximum value of closeness centrality of 0.83 has been realized by users User18, and User94. Users User2, and User89 have achieved the minimum value of 0.5 for the same metric. Both of 0.68 and 0.14 are the average and the standard deviation values for closeness centrality in this network graph.

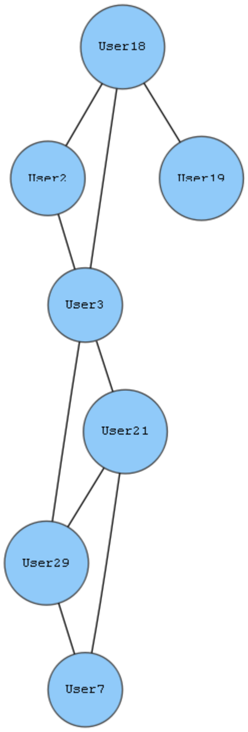


Figure 5.26: Users associations for Hour 3.

Figure 5.26 illustrates different component of graph at hour 3, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

The maximum value of degree of centrality of 0.67 has been realized by user User3. User User19 has achieved the minimum value of 0.17 for degree of centrality. Both of 0.43 and 0.15 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality has a maximum value of 0.6 which was achieved by user User3. The minimum value of zero for the same measure has been realized by users User2, User7, and User19. It has an average value of 0.17 for all users. Also, it has a standard deviation value of 0.21.

User User3 has achieved the maximum value of 0.75 for closeness centrality. It has a minimum value of 0.4 which was achieved by user User19. Its average value is 0.56; while the standard deviation value is 0.11.

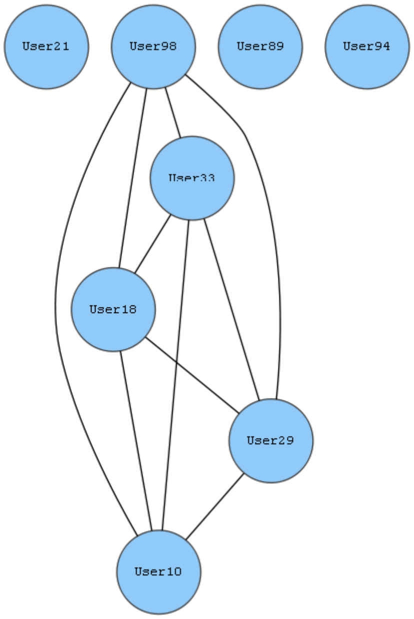


Figure 5.27: Users associations for Hour 18.

Figure 5.27 illustrates different component of graph at hour 18, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.57 which was achieved by users User98, User33, User18, User29, and User10. The minimum value of zero for the same metric has been realized by users User21, User89, and User94. It has an average value of 0.36 for all users. And, it has a standard deviation value of 0.28.

With regard to Hour '18', all users have betweenness centrality of zero.

Value 0.57 is the maximum of closeness centrality that has been achieved by users User98, User33, User18, User29, and User10. Users User21, User89, and User94 have closeness centrality of zero which is at the same time the minimum in this graph for Hour '18'. Both of 0.36 and 0.28 are the average and the standard deviation values for closeness centrality in this network graph.

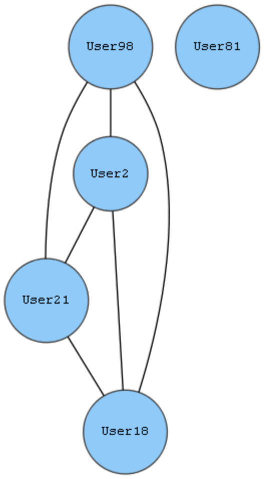


Figure 5.28: Users associations for Hour 20.

Figure 5.28 illustrates different component of graph at hour 20, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

Value 0.75 is the maximum of degree of centrality that has been achieved by users User98, User2, User21, and User18. User User81 has degree of centrality of zero which is at the same time the minimum in this graph for Hour '20'. Both of 0.6 and 0.3 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality is zero for all users in this graph.

Users User98, User2, User21, and User18 have closeness centrality of 0.75 which is at the same time the maximum in this graph for Hour '20'. Value zero is the minimum for the same metric that has been achieved by user User81. Its average value is 0.6; while the standard deviation value is 0.3.

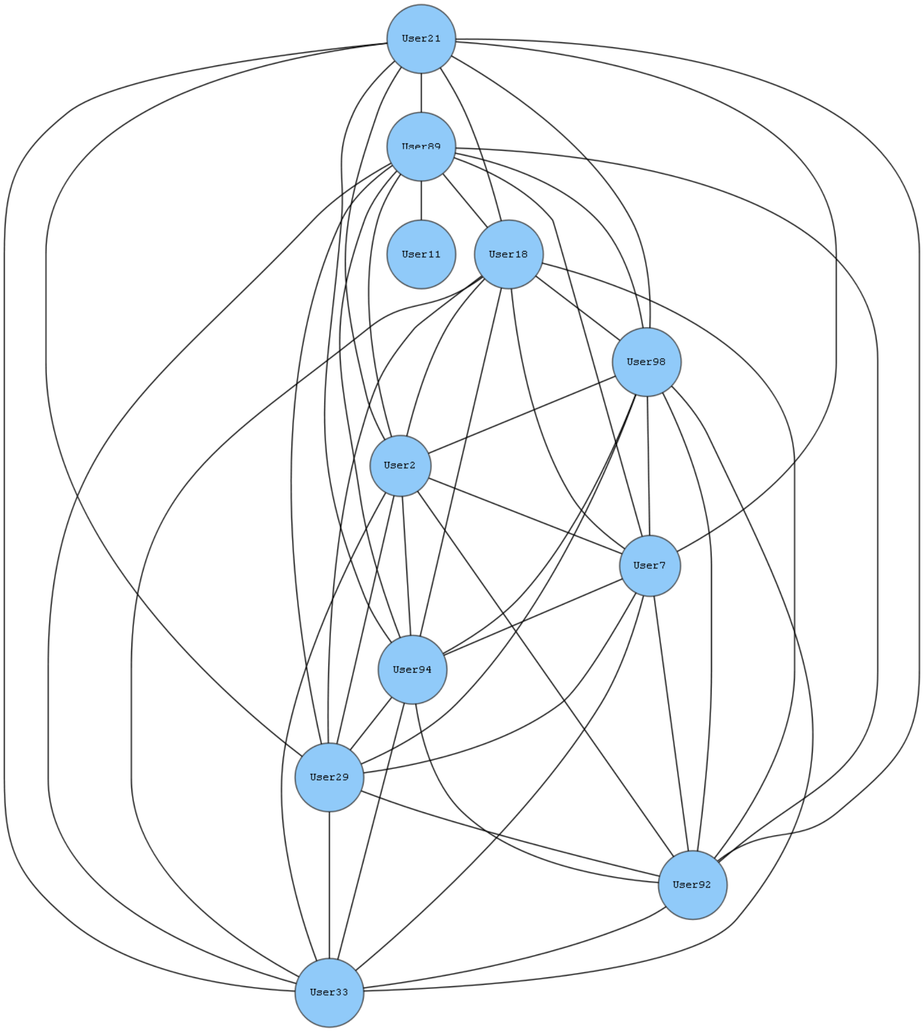


Figure 5.29: Users associations for Hour 13.

Figure 5.29 illustrates different component of graph at hour 13, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

The maximum value of degree of centrality of one has been realized by user User89. User User11 has achieved the minimum value of 0.1 for degree of centrality. It has an average value of 0.84 for all users. And, it has a standard deviation value of 0.23.

Betweenness centrality has a maximum value of 0.2 which was achieved by user User89. The minimum value of zero for the same measure has been realized by users User21, User18, User98, User2, User7, User94, User29, User92, User33, and User11. Its average value is 0.02; while the standard deviation value is 0.06.

User User89 has achieved the maximum value of one for closeness centrality. It has a minimum value of 0.53 which was achieved by user User11. Both of 0.88 and 0.12 are the average and the standard deviation values for closeness centrality in this network graph.

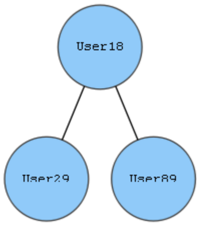


Figure 5.30: Users associations for Hour 14.

Figure 5.30 illustrates different component of graph at hour 14, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

User User18 has achieved the maximum value of one for degree of centrality. It has a minimum value of 0.5 which was achieved by users User29, and User89. Both of 0.67 and 0.24 are the average and the standard deviation values for degree of centrality in this network graph.

Value one is the maximum of betweenness centrality that has been achieved by user User18. Users User29, and User89 have betweenness centrality of zero which is at the same time the minimum in this graph for Hour '14'. It has an average value of 0.33 for all users. Also, it has a standard deviation value of 0.47.

Closeness centrality has a maximum value of one which was achieved by user User18. The minimum value of 0.67 for the same metric has been realized by users User29, and User89. Its average value is 0.78; while the standard deviation value is 0.16.

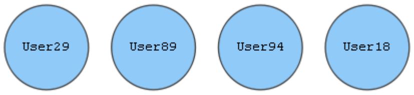


Figure 5.31: Users associations for Hour 17.

Figure 5.31 illustrates different component of graph at hour 17, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

Users in Hour '17' have the same degree of centrality for all of them.

With regard to Hour '17', all users have betweenness centrality of zero.

With regard to Hour '17', all users have closeness centrality of zero.

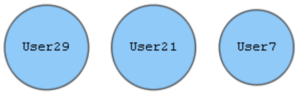


Figure 5.32: Users associations for Hour 6.

Figure 5.32 illustrates different component of graph at hour 6, where the circles represents different users as a node while the links between them (vertex) is represented as a different Source Port reflecting the relationship between different users.

With regards to Hour '6', all users have degree of centrality of zero.

Betweenness centrality is zero for all users in this graph.

Closeness centrality is zero for all users in this graph.

5.3.5 Hour and Destination IP Address.

The network graphs in this section represents several users (nodes or vertex) in certain period of time ranging from (hour 3, 13, 15, 16, 17 and 18), while the links connected between them (edge) represent different source ports of different Destination IP Address which could be IP address of Servers, Firewalls, Database or Hosts. In this case any node has a connection to the same Destination IP Address which means these nodes have a link between them.

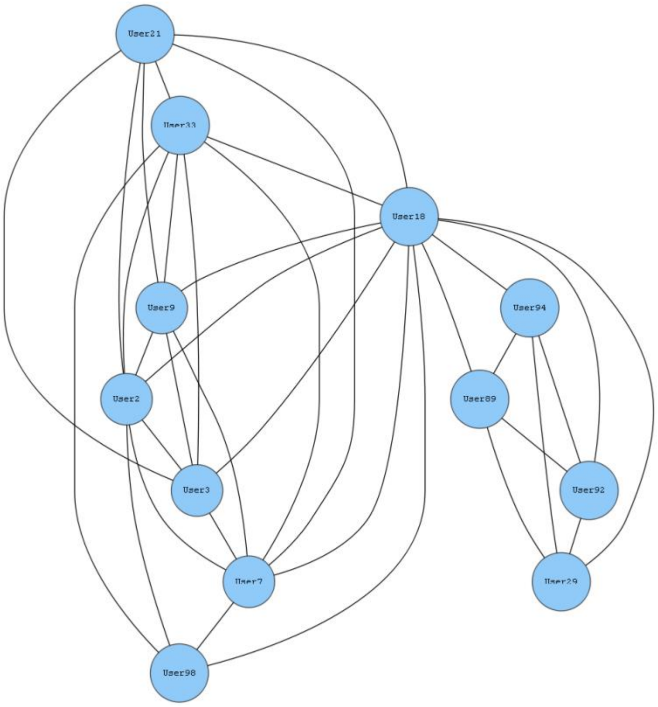


Figure 5.33: Users associations for Hour 16.

Figure 5.33 illustrates different components of the graph at hour 16, where the circles represents different users as a node while the links between them (vertex) are represented as a destination IP address reflecting the relationship between different users.

User User18 has degree of centrality of one which is at the same time the maximum in this graph for Hour '16'. Value 0.36 is the minimum of the same metric that has been achieved by users User98, User94, User89, User92, and

User29. Both of 0.53 and 0.18 are the average and the standard deviation values for degree of centrality in this network graph.

User User18 has achieved the maximum value of 0.52 for betweenness centrality. It has a minimum value of zero which was achieved by users User21, User9, User3, User98, User94, User89, User92, and User29. It has an average value of 0.05 for all users. Also, it has a standard deviation value of 0.14.

The maximum value of closeness centrality of one has been realized by user User18. Users User98, User94, User89, User92, and User29 have achieved the minimum value of 0.61 for the same metric. Its average value is 0.69; while the standard deviation value is 0.11.

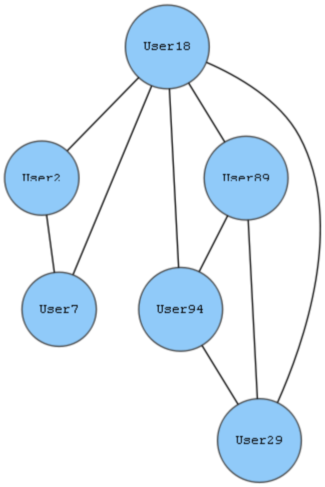


Figure 5.34: Users associations for Hour 15.

Figure 5.34 illustrates different components of the graph at hour 15, where the circles represents different users as a node while the links between them (vertex) are represented as a destination IP address reflecting the relationship between different users.

The maximum value of degree of centrality of one has been realized by user User18. Users User2, and User7 have achieved the minimum value of 0.4 for degree of centrality. Its average value is 0.6; while the standard deviation value is 0.2.

Betweenness centrality has a maximum value of 0.6 which was achieved by user User18. The minimum value of zero for the same measure has been realized by users User2, User7, User89, User94, and User29. Both of 0.1 and 0.22 are the average and the standard deviation values for betweenness centrality in this network graph.

User User18 has achieved the maximum value of one for closeness centrality. It has a minimum value of 0.62 which was achieved by users User2, and User7. It has an average value of 0.73 for all users. Moreover, it has a standard deviation value of 0.13.

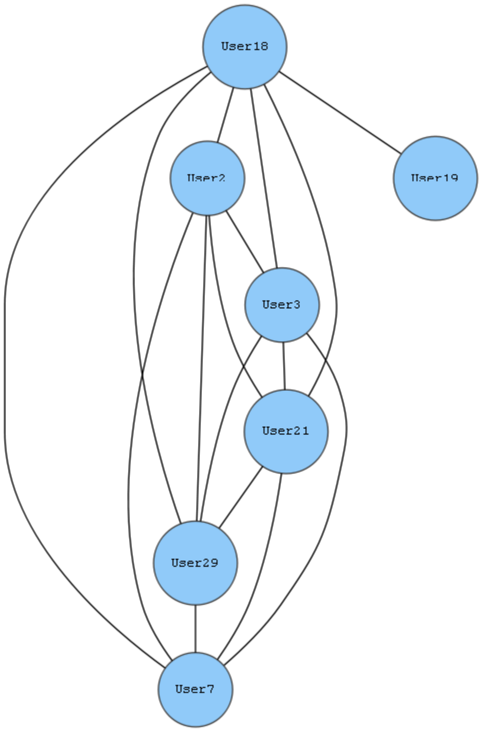


Figure 5.35: Users associations for Hour 3.

Figure 5.35 illustrates different components of the graph at hour 3, where the circles represents different users as a node while the links between them (vertex) are represented as a destination IP address reflecting the relationship between different users.

User User18 has achieved the maximum value of one for degree of centrality. It has a minimum value of 0.17 which was achieved by user User19. It has an average value of 0.76 for all users. And, it has a standard deviation value of 0.25.

Value 0.33 is the maximum of betweenness centrality that has been achieved by user User18. Users User2, User3, User21, User29, User7, and User19 have betweenness centrality of zero which is at the same time the minimum in this graph for Hour '3'. Its average value is 0.05; while the standard deviation value is 0.12.

Closeness centrality has a maximum value of one which was achieved by user User18. The minimum value of 0.55 for the same metric has been realized by user User19. Both of 0.83 and 0.13 are the average and the standard deviation values for closeness centrality in this network graph.

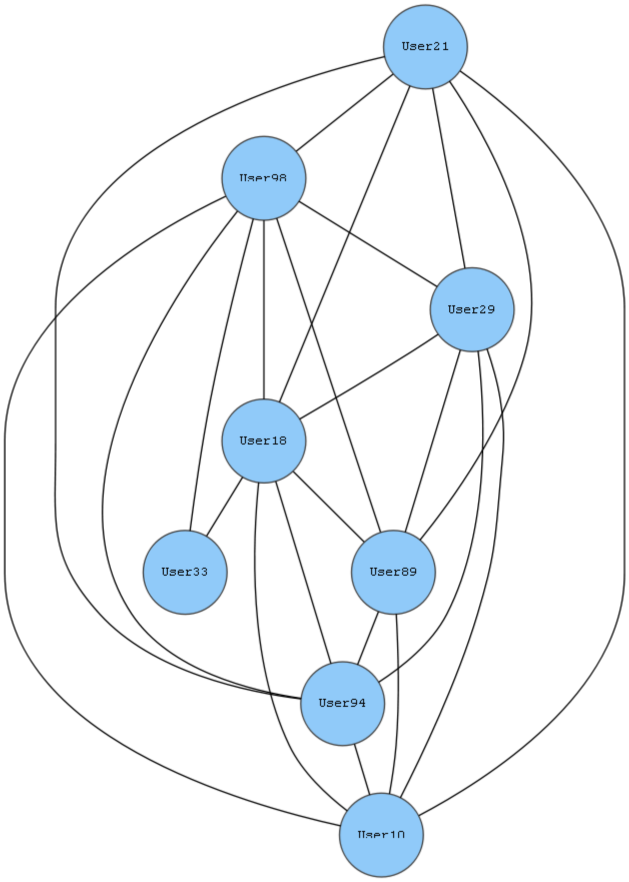


Figure 5.36: Users associations for Hour 18.

Figure 5.36 illustrates different components of the graph at hour 18, where the circles represents different users as a node while the links between them (vertex) are represented as a destination IP address reflecting the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by users User98, and User18. User User33 has degree of centrality of 0.29 which is at the same time the minimum in this graph for Hour '18'. Its average value is 0.82; while the standard deviation value is 0.21.

The maximum value of betweenness centrality of 0.12 has been realized by users User98, and User18. Users User21, User29, User89, User94, User10, and User33 have achieved the minimum value of zero for the same measure. Both of 0.03 and 0.05 are the average and the standard deviation values for betweenness centrality in this network graph.

Users User98, and User18 have closeness centrality of one which is at the same time the maximum in this graph for Hour '18'. Value 0.58 is the minimum for the same metric that has been achieved by user User33. It has an average value of 0.87 for all users. Moreover, it has a standard deviation value of 0.12.

Closeness centrality has a value of one for all users in Hour '21'.

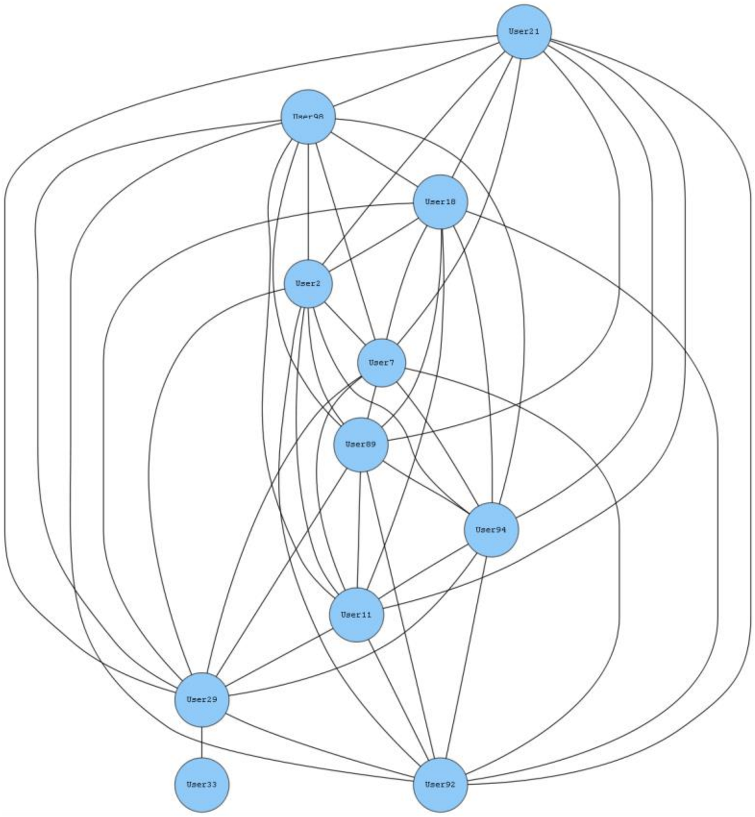


Figure 5.37: Users associations for Hour 13.

Figure 5.37 illustrates different components of the graph at hour 13, where the circles represents different users as a node while the links between them (vertex) are represented as a destination IP address reflecting the relationship between different users.

User User29 has achieved the maximum value of one for degree of centrality. It has a minimum value of 0.1 which was achieved by user User33. Its average value is 0.84; while the standard deviation value is 0.23.

Value 0.2 is the maximum of betweenness centrality that has been achieved by user User29. Users User21, User98, User18, User2, User7, User89, User94, User11, User92, and User33 have betweenness centrality of zero which is at the same time the minimum in this graph for Hour '13'. Both of 0.02 and 0.06 are the average and the standard deviation values for betweenness centrality in this network graph.

Closeness centrality has a maximum value of one which was achieved by user User29. The minimum value of 0.53 for the same metric has been realized by user User33. It has an average value of 0.88 for all users. Moreover, it has a standard deviation value of 0.12.

5.4 Magnitude.

The following figure shows the distribution of these events over Magnitudes.

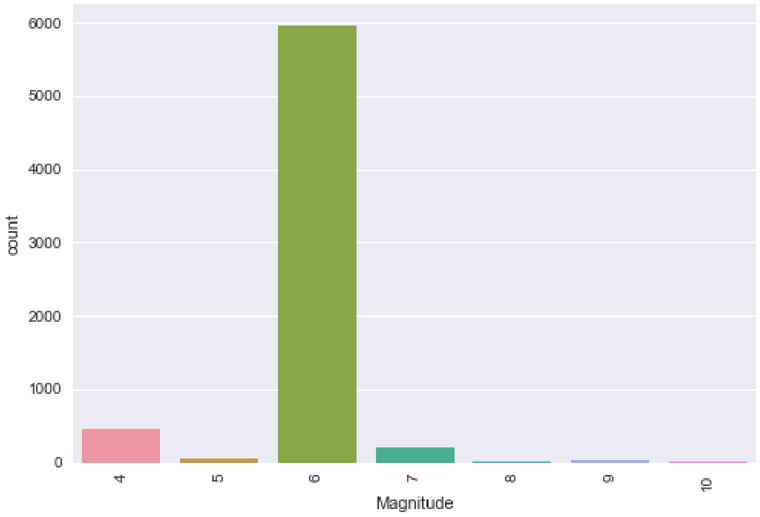


Figure 5.38: activities distribution over Magnitude.

Magnitude '10' has the minimum count of one with percentage of 0.0149 %. On the other hand, Magnitude '6' has the maximum count of 5969 with percentage of 89 %. The average count of all different Magnitudes is 955.6; while the standard deviation is 2052.1.

5.4.1 Magnitude and Hour.

Magnitude is a special value created by Q-radar User Behavior Analytic Tool (UBA) and it is a measurement of the relative importance of a specific offense, and also it is a weighted value that totally depends on relevance, severity, and credibility.

The network graphs in this section represents several users (nodes or vertex) at different Magnitude range from level 1 to level 10 and the highest the level likely to more critical or malicious activities, while the links connected between them (edge) representing different period of time or hours during the day from hour 1 am to 21 pm. In this case any tow nodes or more has the same magnitude at any period to time mean has linked or connection between them.

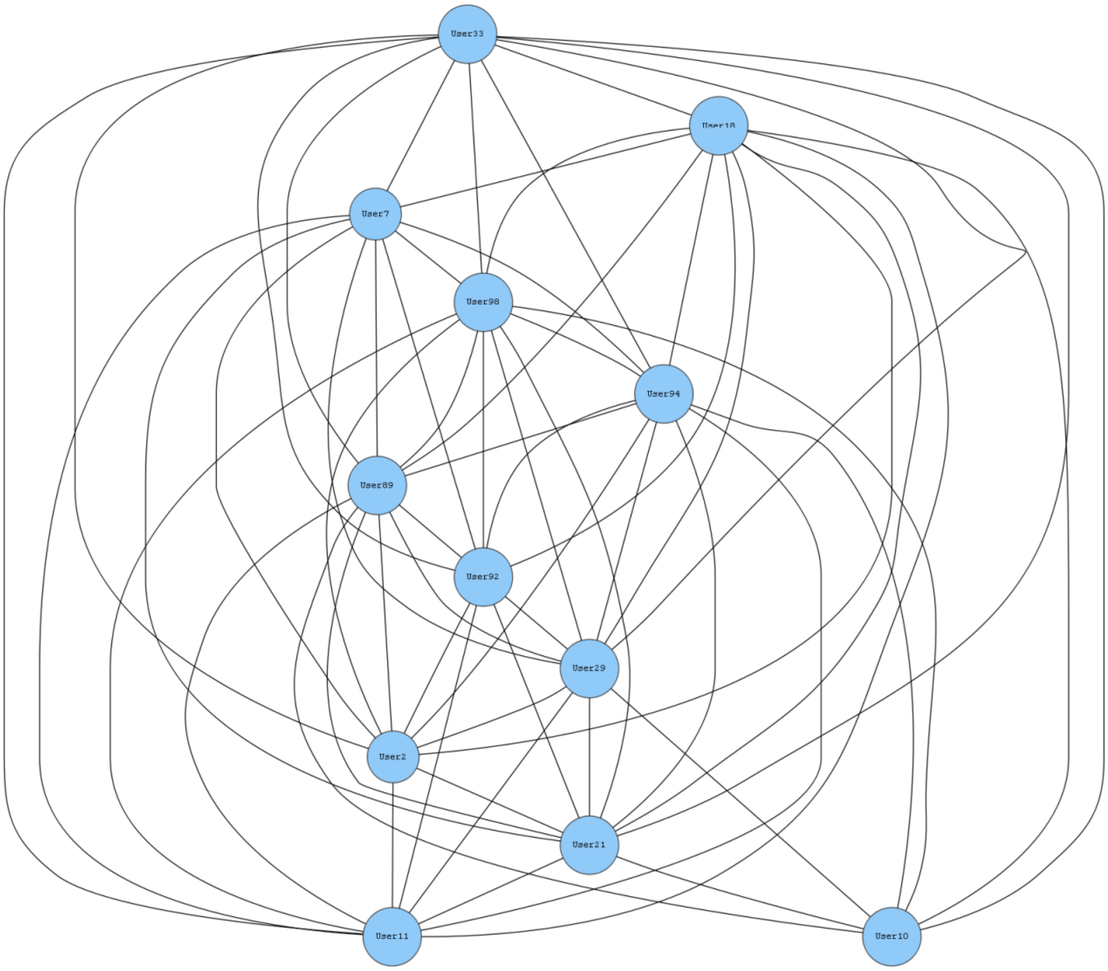


Figure 5.39: Users associations for Magnitude 6.

Figure 6.39 illustrates different components of the graph at Magnitude (6) in a Logs database, where the circles represent different users as node while the links between them vertex as a different time period from hour 1 am to 21 pm reflecting the relationship between different users.

Users User33, User18, User98, User94, User89, User29, and User21 have achieved the maximum value of one for degree of centrality. It has a minimum value of 0.64 which was achieved by user User10. Its average value is 0.94; while the standard deviation value is 0.1.

Value 0.01 is the maximum of betweenness centrality that has been achieved by users User33, User18, User98, User94, User89, User29, and User21. Users User7, User92, User2, User10, and User11 have betweenness centrality of zero which is at the same time the minimum in this graph for Magnitude '6'. Both of 0.01 and 0.01 are the average and the standard deviation values for betweenness centrality in this network graph.

Closeness centrality has a maximum value of one which was achieved by users User33, User18, User98, User94, User89, User29, and User21. The minimum value of 0.73 for the same metric has been realized by user User10. It has an average value of 0.95 for all users. Moreover, it has a standard deviation value of 0.08.

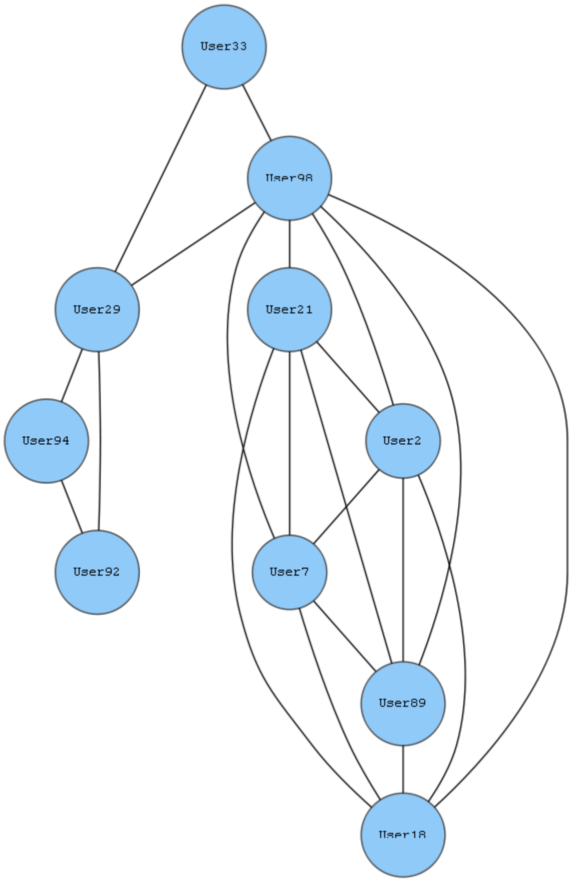


Figure 5.40: Users associations for Magnitude 4.

Figure 6.40 illustrates different components of the graph at Magnitude (4) in a Logs database, where the circles represent different users as node while the links between them vertex as a different time period from hour 1 am to 21 pm reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.78 which was achieved by user User98. The minimum value of 0.22 for the same metric has been realized by users User33, User94, and User92. It has an average value of 0.47 for all users. And, it has a standard deviation value of 0.18.

User User98 has betweenness centrality of 0.56 which is at the same time the maximum in this graph for Magnitude '4'. Value zero is the minimum the same measure that has been achieved by users User33, User21, User2, User7, User89, User18, User94, and User92. Its average value is 0.09; while the standard deviation value is 0.19.

Value 0.82 is the maximum of closeness centrality that has been achieved by user User98. Users User94, and User92 have closeness centrality of 0.43 which is at the same time the minimum in this graph for Magnitude '4'. Both of 0.59 and 0.1 are the average and the standard deviation values for closeness centrality in this network graph.

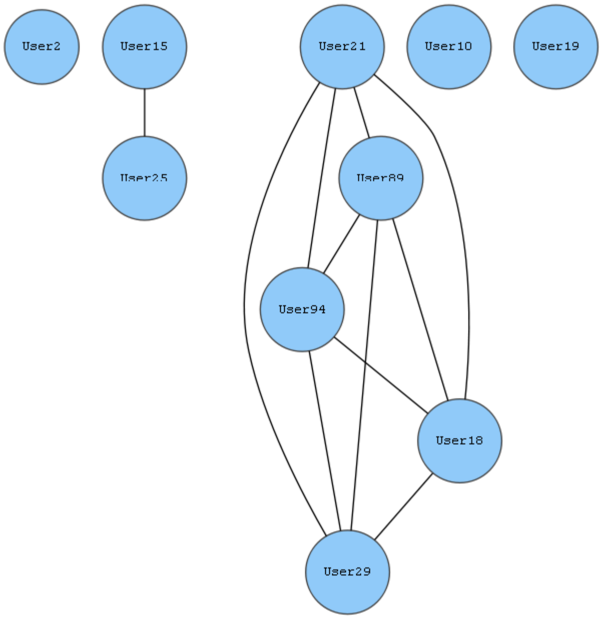


Figure 5.41: Users associations for Magnitude 5.

Figure 6.41 illustrates different components of the graph at Magnitude (5) in a Logs database, where the circles represent different users as node while the links between them vertex as a different time period from hour 1 am to 21 pm reflecting the relationship between different users.

Value 0.44 is the maximum of degree of centrality that has been achieved by users User21, User89, User94, User18, and User29. Users User2, User10, and User19 have degree of centrality of zero which is at the same time the minimum in this graph for Magnitude '5'. Both of 0.24 and 0.2 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality is zero for all users in this graph. Users User21, User89, User94, User18, and User29 have closeness centrality of 0.44 which is at the same time the maximum in this graph for Magnitude '5'. Value zero is the minimum for the same metric that has been achieved by users User2, User10, and User19. Its average value is 0.24; while the standard deviation value is 0.2.

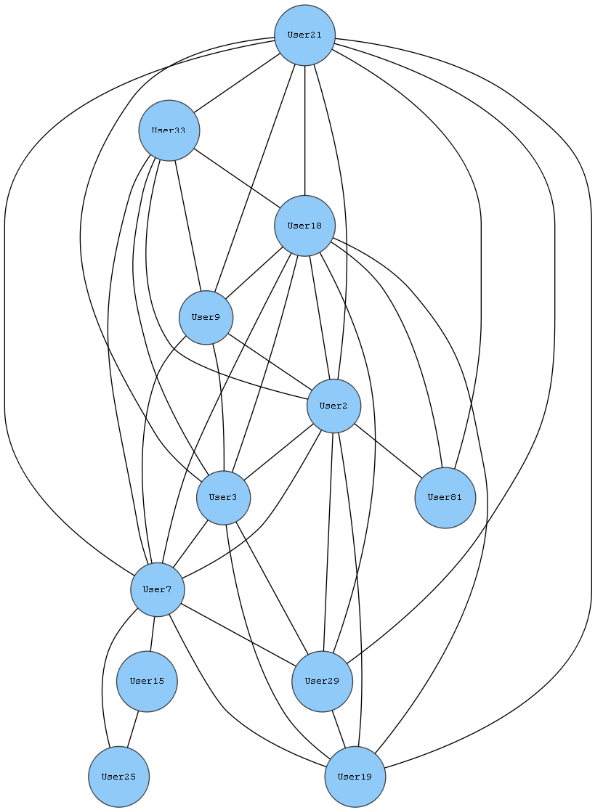


Figure 5.42: Users associations for Magnitude 7.

Figure 6.42 illustrates different components of the graph at Magnitude (7) in a Logs database, where the circles represent different users as node while the links between them vertex as a different time period from hour 1 am to 21 pm reflecting the relationship between different users.

User User7 has degree of centrality of 0.91 which is at the same time the maximum in this graph for Magnitude '7'. Value 0.18 is the minimum of the same metric that has been achieved by users User15, and User25. Its average value is 0.58; while the standard deviation value is 0.24.

User User7 has achieved the maximum value of 0.34 for betweenness centrality. It has a minimum value of zero which was achieved by users User33, User9, User15, User25, User29, User19, and User81. Both of 0.05 and 0.09 are the average and the standard deviation values for betweenness centrality in this network graph.

The maximum value of closeness centrality of 0.92 has been realized by user User7. Users User15, User25, and User81 have achieved the minimum value of 0.52 for the same metric. It has an average value of 0.71 for all users. Moreover, it has a standard deviation value of 0.13.

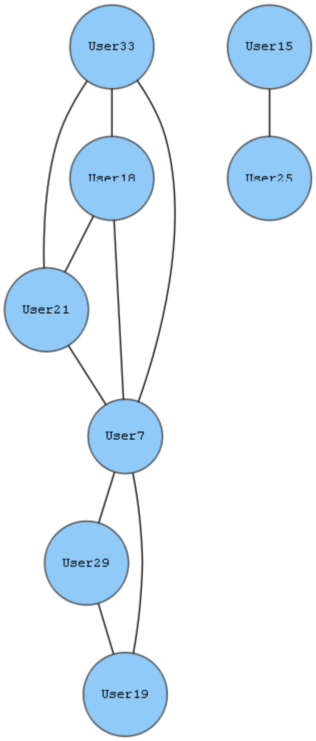


Figure 5.43: Users associations for Magnitude 9.

Figure 6.43 illustrates different components of the graph at Magnitude (9) in a Logs database, where the circles represent different users as node while the links between them vertex as a different time period from hour 1 am to 21 pm reflecting the relationship between different users.

The maximum value of degree of centrality of 0.71 has been realized by user User7. Users User15, and User25 have achieved the minimum value of 0.14 for degree of centrality. It has an average value of 0.36 for all users. And, it has a standard deviation value of 0.17.

Betweenness centrality has a maximum value of 0.29 which was achieved by user User7. The minimum value of zero for the same measure has been realized by users User33, User18, User21, User15, User25, User29, and User19. Its average value is 0.04; while the standard deviation value is 0.09.

User User7 has achieved the maximum value of 0.71 for closeness centrality. It has a minimum value of 0.14 which was achieved by users User15, and User25. Both of 0.43 and 0.18 are the average and the standard deviation values for closeness centrality in this network graph.

5.4.2 Magnitude and Event.

The network graphs in this section represents several users (nodes or vertex) at a different Magnitude ranging from level 1 to level 10 and the highest level is likely to be subjected to more critical or malicious activities, while the links connected between them (edge) represent different malicious type of events. In this case any two nodes or more has malicious activities with same level of magnitude which means has linked or connection between them.

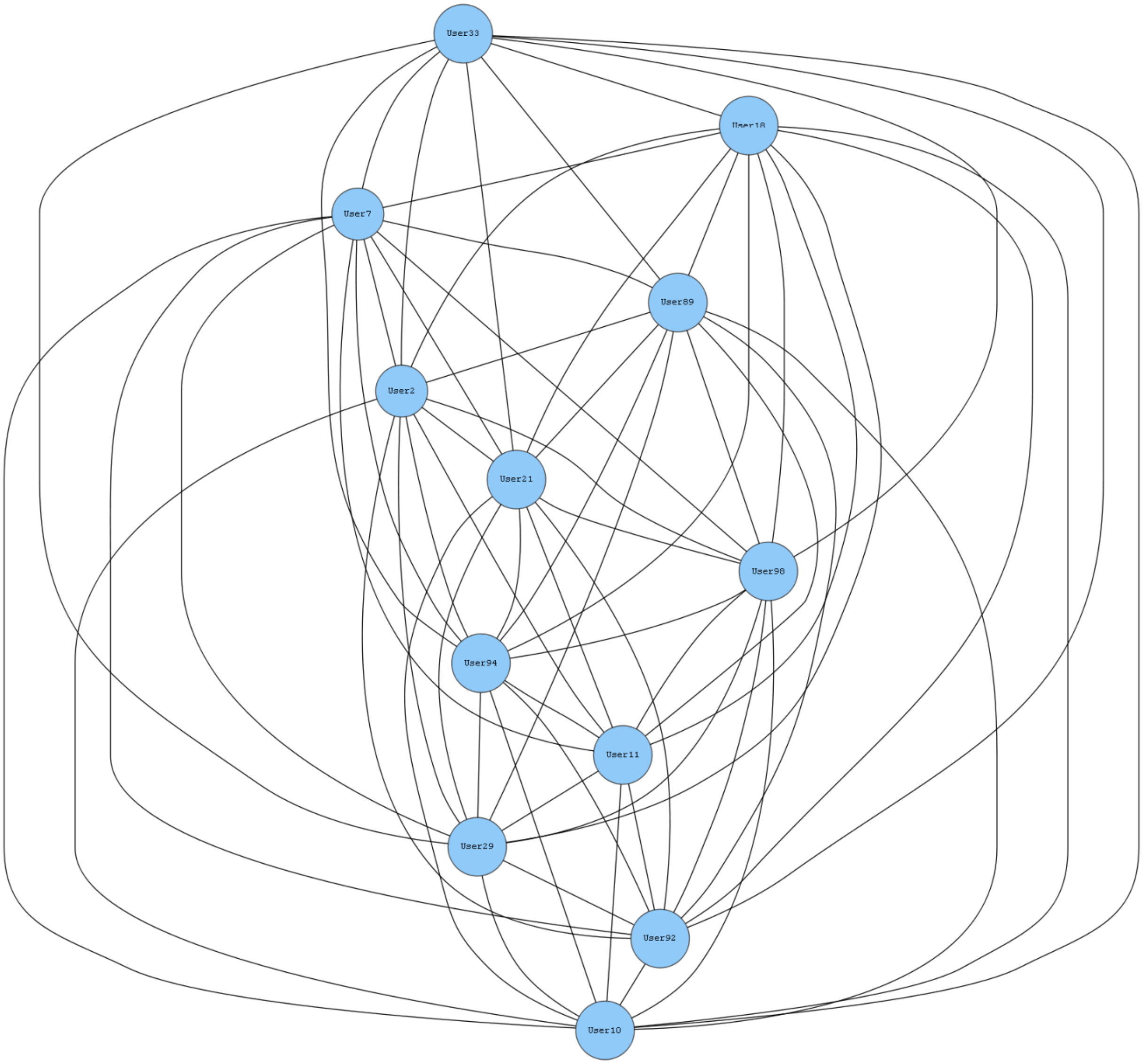


Figure 5.44: Users associations for Magnitude 6.

Figure 5.44 illustrates different components of the graph at a Magnitude (6) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different malicious activities reflecting the relationship between different users.

Degree of centrality has a maximum value of one which was achieved by users User18, User7, User89, User2, User21, User98, User94, User29, User92, and User10. The minimum value of 0.91 for the same metric has been realized by users User33, and User11. Its average value is 0.98; while the standard deviation value is 0.03.

Users User18, User7, User89, User2, User21, User98, User94, User29, User92, and User10 have betweenness centrality of zero which is at the same time the maximum in this graph for Magnitude '6'. Value zero is the minimum the same measure that has been achieved by users User33, and User11. Both of zero and zero are the average and the standard deviation values for betweenness centrality in this network graph.

Value one is the maximum of closeness centrality that has been achieved by users User18, User7, User89, User2, User21, User98, User94, User29, User92, and User10. Users User33, and User11 have closeness centrality of 0.92 which is at the same time the minimum in this graph for Magnitude '6'. It has an average value of 0.99 for all users. Moreover, it has a standard deviation value of 0.03.

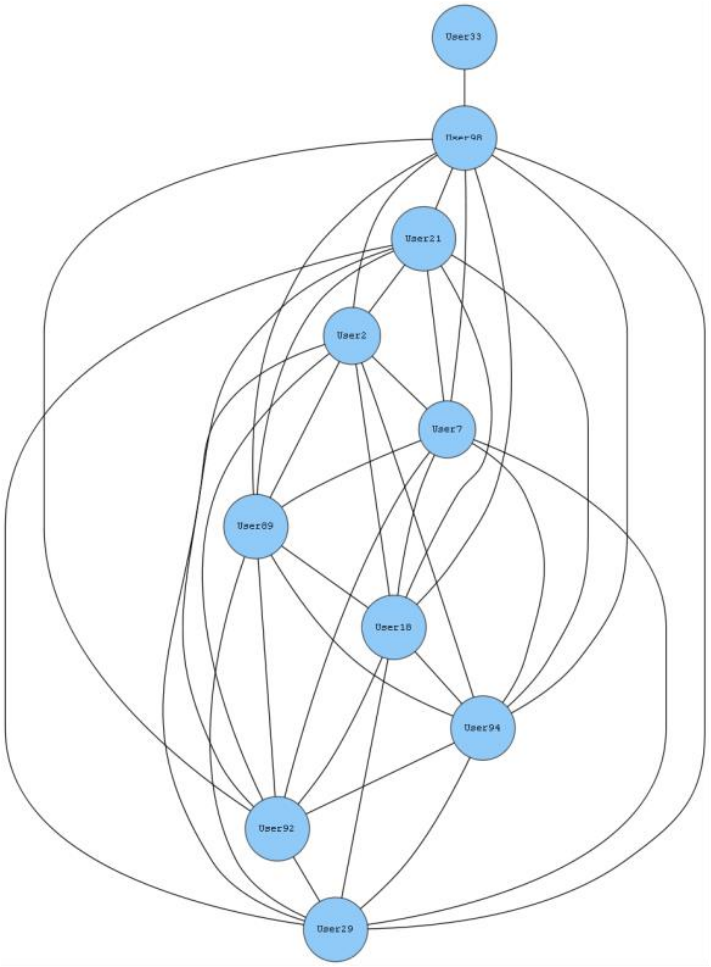


Figure 5.45: Users associations for Magnitude 4.

Figure 5.45 illustrates different components of the graph at a Magnitude (4) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different malicious activities reflecting the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by user User98. User User33 has degree of centrality of 0.11 which is at the same time the minimum in this graph for Magnitude '4'. It has an average value of 0.82 for all users. And, it has a standard deviation value of 0.24.

The maximum value of betweenness centrality of 0.22 has been realized by user User98. Users User33, User21, User2, User7, User89, User18, User94, User92, and User29 have achieved the minimum value of zero for the same measure. Its average value is 0.02; while the standard deviation value is 0.07.

User User98 has closeness centrality of one which is at the same time the maximum in this graph for Magnitude '4'. Value 0.53 is the minimum for the same metric that has been achieved by user User33. Both of 0.87 and 0.12 are the average and the standard deviation values for closeness centrality in this network graph.

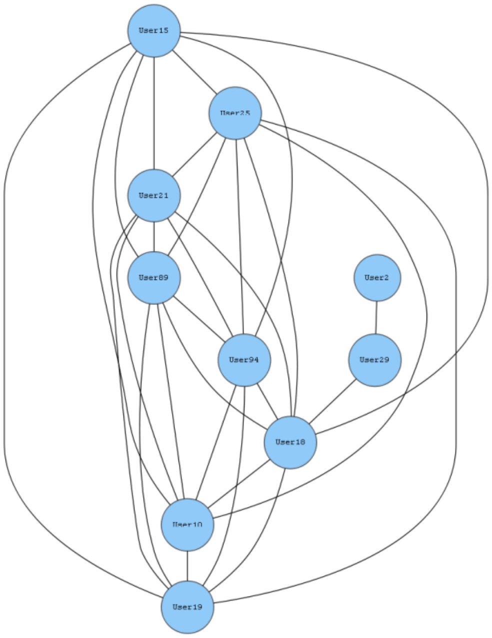


Figure 5.46: Users associations for Magnitude 5.

Figure 5.46 illustrates different components of the graph at a Magnitude (5) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different malicious activities reflecting the relationship between different users.

User User18 has degree of centrality of 0.89 which is at the same time the maximum in this graph for Magnitude '5'. Value 0.11 is the minimum of the same metric that has been achieved by user User2. Both of 0.67 and 0.25 are the average and the standard deviation values for degree of centrality in this network graph.

User User18 has achieved the maximum value of 0.39 for betweenness centrality. It has a minimum value of zero which was achieved by users User2, User15, User25, User21, User89, User94, User10, and User19. It has an average value of 0.06 for all users. Also, it has a standard deviation value of 0.13.

The maximum value of closeness centrality of 0.9 has been realized by user User18. User User2 has achieved the minimum value of 0.38 for the same metric. Its average value is 0.71; while the standard deviation value is 0.13.

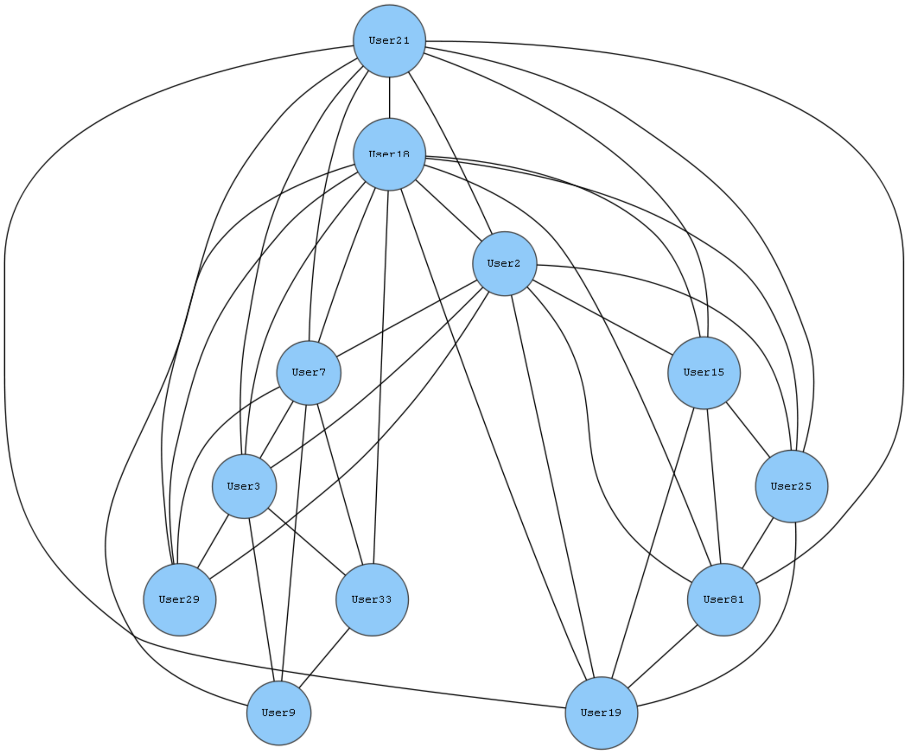


Figure 5.47: Users associations for Magnitude 7.

Figure 5.47 illustrates different components of the graph at a Magnitude (7) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different malicious activities reflecting the relationship between different users.

The maximum value of degree of centrality of one has been realized by user User18. Users User33, and User9 have achieved the minimum value of 0.36 for degree of centrality. Its average value is 0.61; while the standard deviation value is 0.18.

Betweenness centrality has a maximum value of 0.25 which was achieved by user User18. The minimum value of zero for the same measure has been realized by users User29, User33, User9, User15, User25, User81, and User19. Both of 0.04 and 0.07 are the average and the standard deviation values for betweenness centrality in this network graph.

User User18 has achieved the maximum value of one for closeness centrality. It has a minimum value of 0.61 which was achieved by users User33, and User9. It has an average value of 0.73 for all users. Moreover, it has a standard deviation value of 0.11.

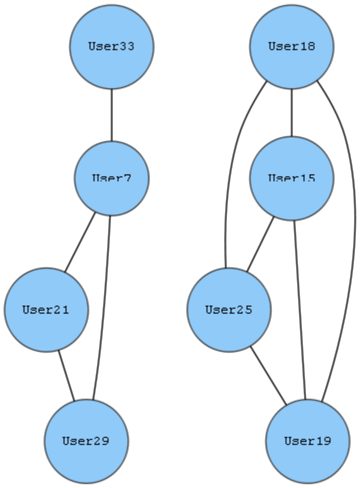


Figure 5.48: Users associations for Magnitude 9.

Figure 5.48 illustrates different components of the graph at a Magnitude (9) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different malicious activities reflecting the relationship between different users.

Users User7, User18, User15, User25, and User19 have achieved the maximum value of 0.43 for degree of centrality. It has a minimum value of 0.14 which was achieved by user User33. It has an average value of 0.36 for all users. And, it has a standard deviation value of 0.1.

Value 0.1 is the maximum of betweenness centrality that has been achieved by user User7. Users User33, User18, User21, User29, User15, User25, and User19 have betweenness centrality of zero which is at the same time the minimum in this graph for Magnitude '9'. Its average value is 0.01; while the standard deviation value is 0.03.

Closeness centrality has a maximum value of 0.43 which was achieved by users User7, User18, User15, User25, and User19. The minimum value of 0.26 for the same metric has been realized by user User33. Both of 0.38 and 0.06 are the average and the standard deviation values for closeness centrality in this network graph.

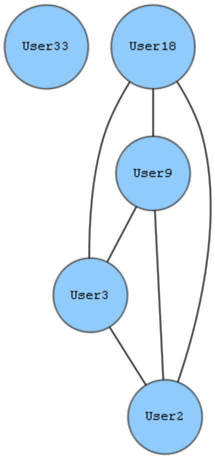


Figure 5.49: Users associations for Magnitude 8.

Figure 5.49 illustrates different components of the graph at a Magnitude (8) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different malicious activities reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.75 which was achieved by users User18, User9, User3, and User2. The minimum value of zero for the same metric has been realized by user User33. Both of 0.6 and 0.3 are the average and the standard deviation values for degree of centrality in this network graph.

With regard to Magnitude '8', all users have betweenness centrality of zero.

Value 0.75 is the maximum of closeness centrality that has been achieved by users User18, User9, User3, and User2. User User33 has closeness centrality of zero which is at the same time the minimum in this graph for Magnitude '8'. Its average value is 0.6; while the standard deviation value is 0.3.

5.4.3 Magnitude and Source IP Address.

The network graphs in this section represents several users (nodes or vertex) at different Magnitude ranging from level 1 to level 10 and the highest the level is likely to be subjected to more critical or malicious activities, while the links connected between them (edge) representing different source IP address belonging to different entities within the organization Information Infrastructure. In this case any two nodes or connected or exchanged information with the same source IP address mean they has same type of link or connection between them.

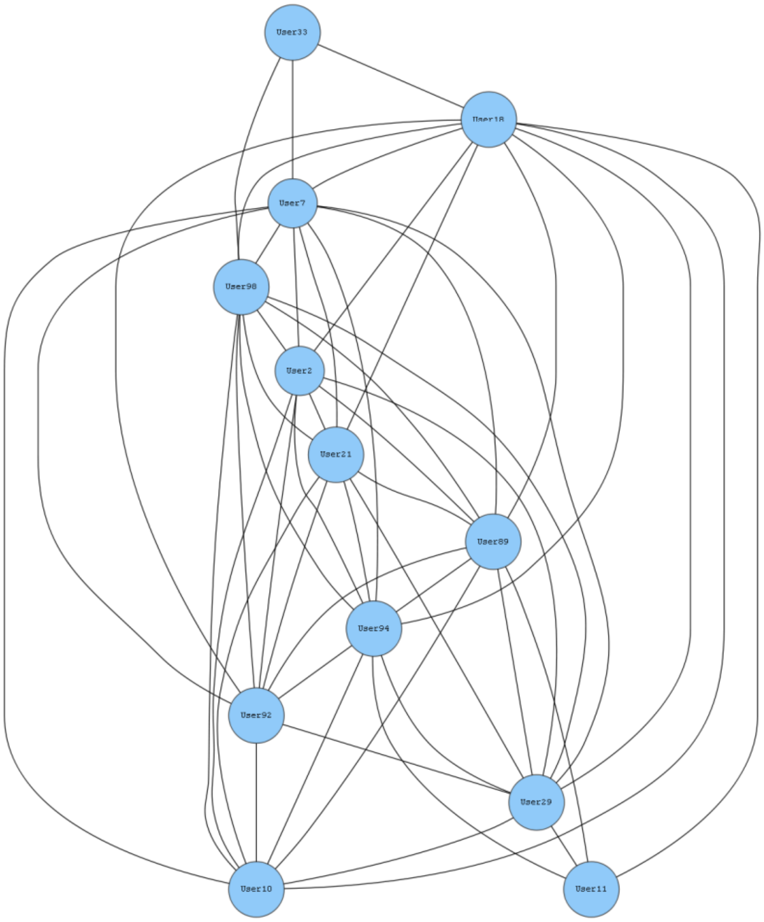


Figure 5.50: Users associations for Magnitude 6.

Figure 5.50 illustrates different components of graph at a Magnitude (6) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source IP Address reflecting the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by user User18. User User33 has degree of centrality of 0.27 which is at the same time the minimum in this graph for Magnitude '6'. Its average value is 0.79; while the standard deviation value is 0.22.

The maximum value of betweenness centrality of 0.09 has been realized by user User18. Users User33, User2, User21, User92, User10, and User11 have achieved the minimum value of zero for the same measure. Both of 0.02 and 0.03 are the average and the standard deviation values for betweenness centrality in this network graph.

User User18 has closeness centrality of one which is at the same time the maximum in this graph for Magnitude '6'. Value 0.58 is the minimum for the same metric that has been achieved by user User33. It has an average value of 0.85 for all users. Moreover, it has a standard deviation value of 0.12.

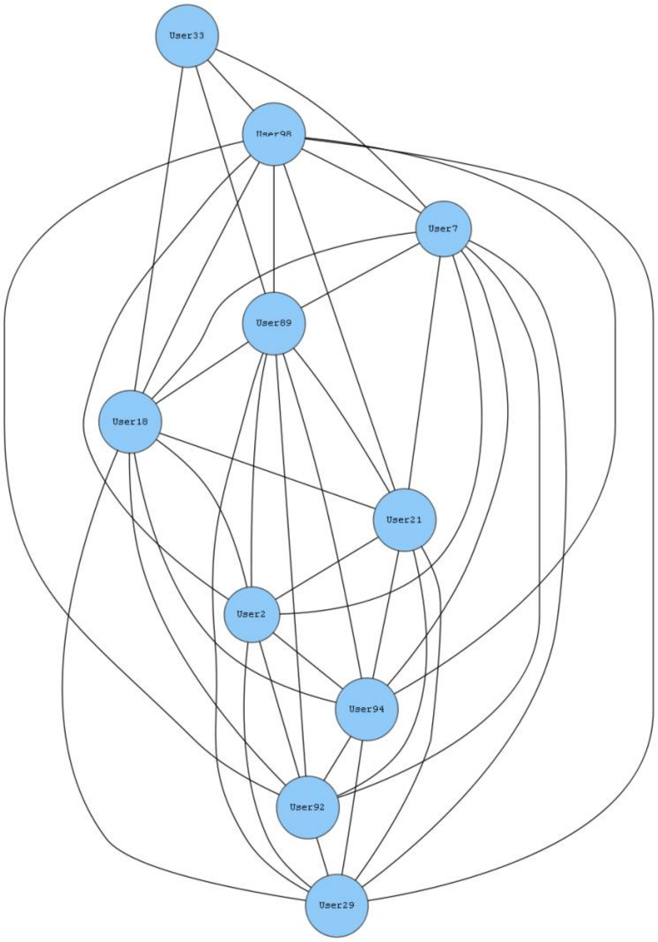


Figure 5.51: Users associations for Magnitude 4.

Figure 5.51 illustrates different components of graph at a Magnitude (4) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source IP Address reflecting the relationship between different users.

Users User98, User7, User89, and User18 have degree of centrality of one which is at the same time the maximum in this graph for Magnitude '4'. Value 0.44 is the minimum of the same metric that has been achieved by user User33. It has an average value of 0.89 for all users. And, it has a standard deviation value of 0.16.

Users User98, User7, User89, and User18 have achieved the maximum value of 0.03 for betweenness centrality. It has a minimum value of zero which was achieved by users User33, User21, User2, User94, User92, and User29. Its average value is 0.01; while the standard deviation value is 0.02.

The maximum value of closeness centrality of one has been realized by users User98, User7, User89, and User18. User User33 has achieved the minimum value of 0.64 for the same metric. Both of 0.91 and 0.1 are the average and the standard deviation values for closeness centrality in this network graph.

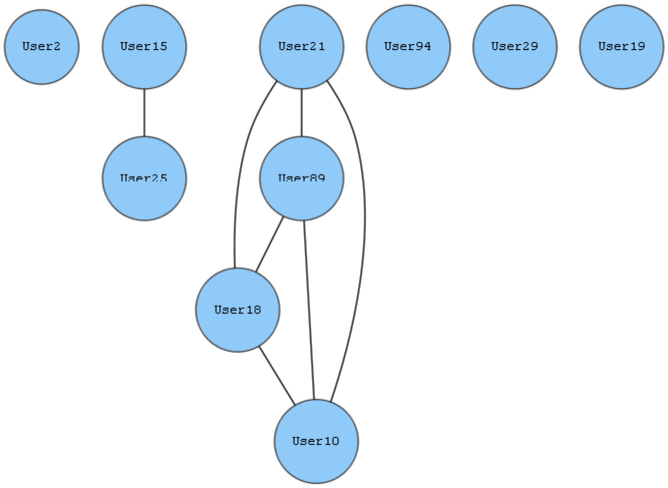


Figure 5.52: Users associations for Magnitude 5.

Figure 5.52 illustrates different components of graph at a Magnitude (5) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source IP Address reflecting the relationship between different users.

The maximum value of degree of centrality of 0.33 has been realized by users User21, User89, User18, and User10. Users User2, User94, User29, and User19 have achieved the minimum value of zero for degree of centrality. Both of 0.16 and 0.15 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality has a value of zero for all users in Magnitude '5'.

Users User21, User89, User18, and User10 have achieved the maximum value of 0.33 for closeness centrality. It has a minimum value of zero which was achieved by users User2, User94, User29, and User19. Its average value is 0.16; while the standard deviation value is 0.15.

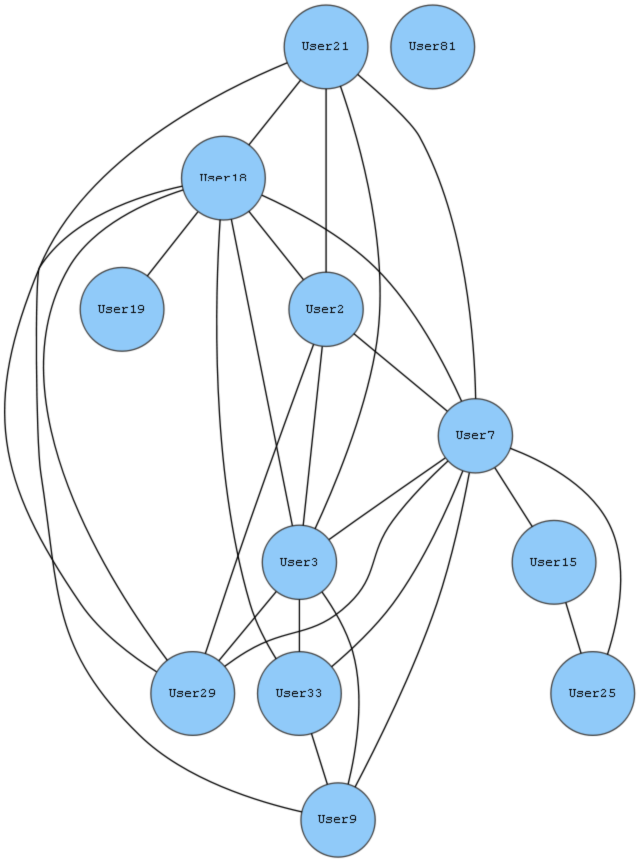


Figure 5.53: Users associations for Magnitude 7.

Figure 5.53 illustrates different components of graph at a Magnitude (7) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source IP Address reflecting the relationship between different users.

User User7 has achieved the maximum value of 0.82 for degree of centrality. It has a minimum value of zero which was achieved by user User81. Its average value is 0.39; while the standard deviation value is 0.24.

Value 0.33 is the maximum of betweenness centrality that has been achieved by user User7. Users User21, User2, User29, User33, User9, User15, User25, User81, and User19 have betweenness centrality of zero which is at the same time the minimum in this graph for Magnitude '7'. Both of 0.05 and 0.1 are the average and the standard deviation values for betweenness centrality in this network graph.

Closeness centrality has a maximum value of 0.83 which was achieved by user User7. The minimum value of zero for the same metric has been realized by user User81. It has an average value of 0.55 for all users. Moreover, it has a standard deviation value of 0.2.

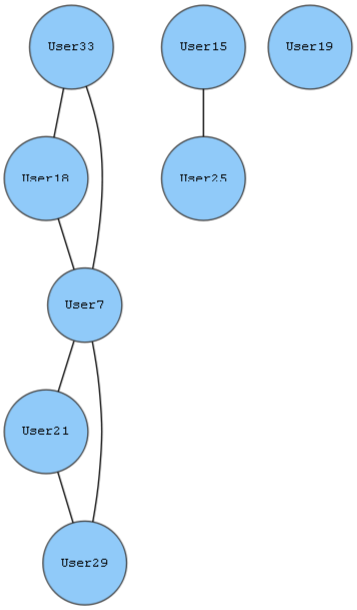


Figure 5.54: Users associations for Magnitude 9.

Figure 5.54 illustrates different components of graph at a Magnitude (9) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source IP Address reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.57 which was achieved by user User7. The minimum value of zero for the same metric has been realized by user User19. It has an average value of 0.25 for all users. And, it has a standard deviation value of 0.16.

User User7 has betweenness centrality of 0.19 which is at the same time the maximum in this graph for Magnitude '9'. Value zero is the minimum the same measure that has been achieved by users User33, User18, User21, User29, User15, User25, and User19. Its average value is 0.02; while the standard deviation value is 0.06.

Value 0.57 is the maximum of closeness centrality that has been achieved by user User7. User User19 has closeness centrality of zero which is at the same time the minimum in this graph for Magnitude '9'. Both of 0.3 and 0.17 are the average and the standard deviation values for closeness centrality in this network graph.

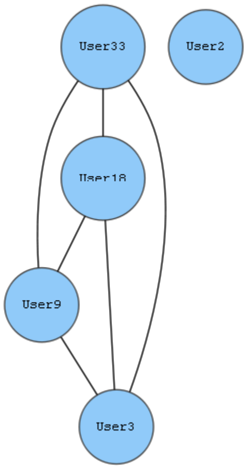


Figure 5.55: Users associations for Magnitude 8.

Figure 5.55 illustrates different components of graph at a Magnitude (8) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source IP Address reflecting the relationship between different users.

Value 0.75 is the maximum of degree of centrality that has been achieved by users User33, User18, User9, and User3. User User2 has degree of centrality of zero which is at the same time the minimum in this graph for Magnitude '8'. Both of 0.6

and 0.3 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality is zero for all users in this graph.

Users User33, User18, User9, and User3 have closeness centrality of 0.75 which is at the same time the maximum in this graph for Magnitude '8'. Value zero is the minimum for the same metric that has been achieved by user User2. Its average value is 0.6; while the standard deviation value is 0.3.

5.4.4 Magnitude and Source Port.

The network graphs in this section represents several users (nodes or vertex) at different Magnitude ranging from level 1 to level 10 and the highest the level is likely to be subjected to more critical or malicious activities, while the links connected between them (edge) representing different Source Port belong to different entities with different services within the organization Information Infrastructure. In this case any two nodes or more connected or exchanged information with the same source port mean has linked or connection between them.

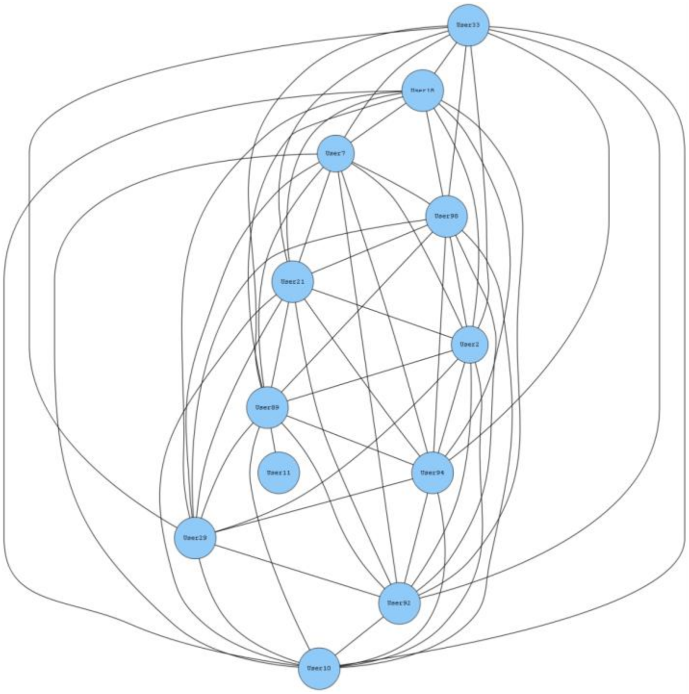


Figure 5.56: Users associations for Magnitude 6.

Figure 5.56 illustrates different components of the graph at Magnitude (6) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source Port reflecting the relationship between different users.

User User89 has degree of centrality of one which is at the same time the maximum in this graph for Magnitude '6'. Value 0.09 is the minimum of the same metric that has been achieved by user User11. Its average value is 0.85; while the standard deviation value is 0.23.

User User89 has achieved the maximum value of 0.18 for betweenness centrality. It has a minimum value of zero which was achieved by users User33, User18, User7, User98, User21, User2, User94, User29, User92, User10, and User11. Both of 0.02 and 0.05 are the average and the standard deviation values for betweenness centrality in this network graph.

The maximum value of closeness centrality of one has been realized by user User89. User User11 has achieved the minimum value of 0.52 for the same metric. It has an average value of 0.89 for all users. Moreover, it has a standard deviation value of 0.11.

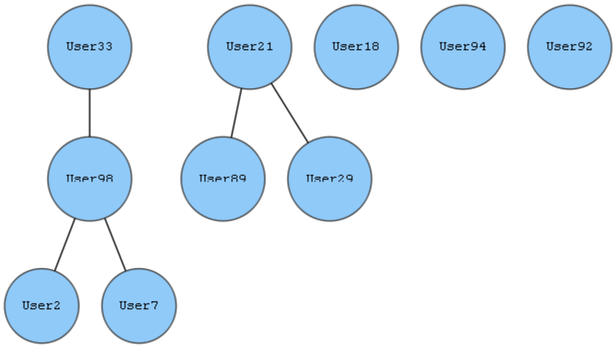


Figure 5.57: Users associations for Magnitude 4.

Figure 5.57 illustrates different components of the graph at Magnitude (4) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source Port reflecting the relationship between different users.

The maximum value of degree of centrality of 0.33 has been realized by user User98. Users User18, User94, and User92 have achieved the minimum value of zero for degree of centrality. It has an average value of 0.11 for all users. And, it has a standard deviation value of 0.1.

Betweenness centrality has a maximum value of 0.08 which was achieved by user User98. The minimum value of zero for the same measure has been realized by users User33, User2, User7, User89, User18, User94, User92, and User29. Its average value is 0.01; while the standard deviation value is 0.03.

User User98 has achieved the maximum value of 0.33 for closeness centrality. It has a minimum value of zero which was achieved by users User18, User94, and User92. Both of 0.15 and 0.11 are the average and the standard deviation values for closeness centrality in this network graph.

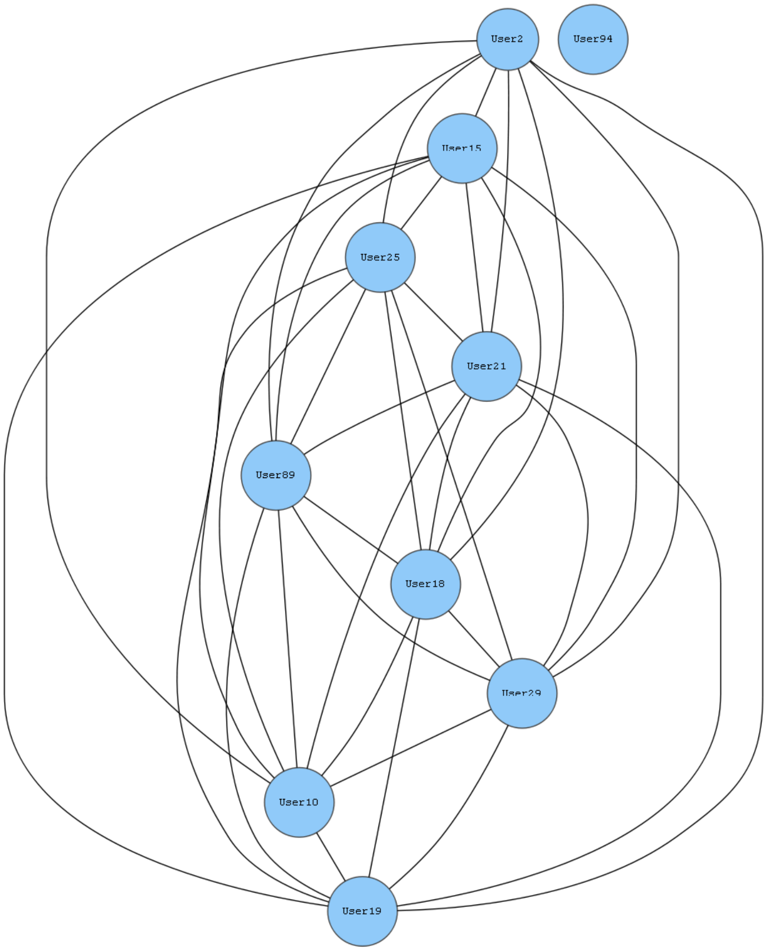


Figure 5.58: Users associations for Magnitude 5.

Figure 5.58 illustrates different components of the graph at Magnitude (5) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source Port reflecting the relationship between different users.Users User2, User15, User25, User21, User89, User18, User29, User10, and User19 have achieved the maximum value of 0.89 for degree of centrality. It has a minimum value of zero which was achieved by user User94. Both of 0.8 and 0.27 are the average and the standard deviation values for degree of centrality in this network graph.

Users in Magnitude '5' have the same betweenness centrality for all of them.

Closeness centrality has a maximum value of 0.89 which was achieved by users User2, User15, User25, User21, User89, User18, User29, User10, and User19. The minimum value of zero for the same metric has been realized by user User94. Its average value is 0.8; while the standard deviation value is 0.27.

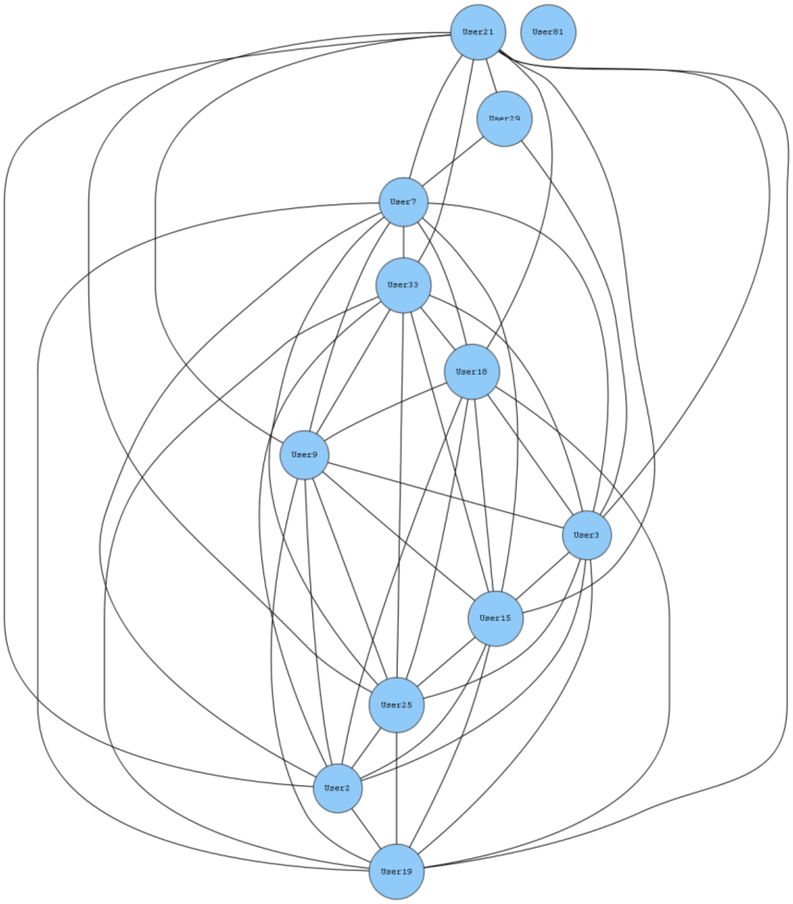


Figure 5.59: Users associations for Magnitude 7.

Figure 5.59 illustrates different components of the graph at Magnitude (7) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source Port reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.91 which was achieved by users User21, User7, and User3. The minimum value of zero for the same metric has been realized by user User81. Its average value is 0.73; while the standard deviation value is 0.27.

Users User21, User7, and User3 have betweenness centrality of 0.04 which is at the same time the maximum in this graph for Magnitude '7'. Value zero is the minimum the same measure that has been achieved by users User29, User33, User18, User9, User15, User25, User2, User19, and User81. Both of 0.01 and 0.02 are the average and the standard deviation values for betweenness centrality in this network graph.

Value 0.91 is the maximum of closeness centrality that has been achieved by users User21, User7, and User3. User User81 has closeness centrality of zero which is at the same time the minimum in this graph for Magnitude '7'. It has an average value of 0.75 for all users. Moreover, it has a standard deviation value of 0.25.

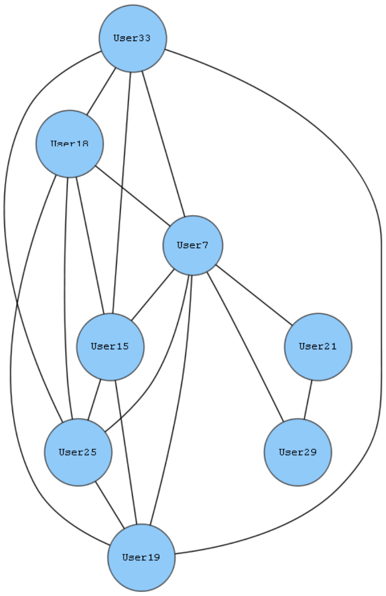


Figure 5.60: Users associations for Magnitude 9.

Figure 5.60 illustrates different components of the graph at Magnitude (9) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Source Port reflecting the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by user User7. Users User21, and User29 have degree of centrality of 0.29 which is at the same time the minimum in this graph for Magnitude '9'. It has an average value of 0.64 for all users. And, it has a standard deviation value of 0.23.

The maximum value of betweenness centrality of 0.48 has been realized by user User7. Users User33, User18, User15, User25, User19, User21, and User29 have achieved the minimum value of zero for the same measure. Its average value is 0.06; while the standard deviation value is 0.16.

User User7 has closeness centrality of one which is at the same time the maximum in this graph for Magnitude '9'. Value 0.58 is the minimum for the same metric that has been achieved by users User21, and User29. Both of 0.76 and 0.12 are the average and the standard deviation values for closeness centrality in this network graph.

5.4.5 Magnitude and Destination IP Address.

The network graphs in this section represents several users (nodes or vertex) at different Magnitude ranging from level 1 to level 10 and the highest the level is likely subjected to more critical or malicious activities, while the links connected between them (edge) represent different destination IP address belong to different entities within the organization Information Infrastructure. In this case any two nodes or connected or exchanged information with the same destination IP address mean they has same type of link or connection between them.

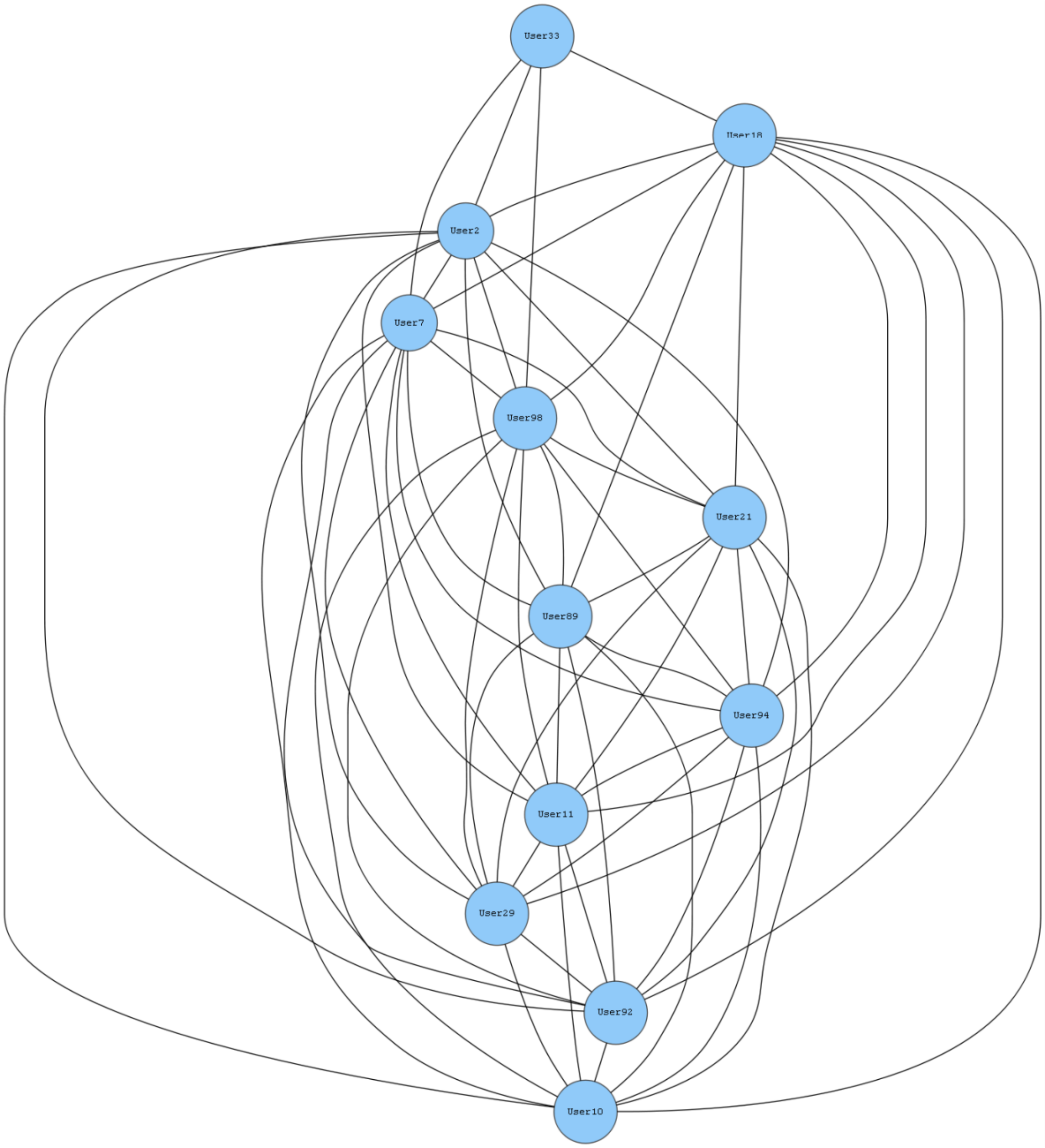


Figure 5.61: Users associations for Magnitude 6.

Figure 5.61 illustrates different components of the graph at Magnitude (6) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Destination IP Address reflecting the relationship between different users.

The maximum value of degree of centrality of one has been realized by users User18, User2, User7, and User98. User User33 has achieved the minimum value of 0.36 for degree of centrality. Its average value is 0.89; while the standard deviation value is 0.17.

Betweenness centrality has a maximum value of 0.03 which was achieved by users User18, User2, User7, and User98. The minimum value of zero for the same measure has been realized by users User33, User21, User89, User94, User11, User29, User92, and User10. Both of 0.01 and 0.01 are the average and the standard deviation values for betweenness centrality in this network graph.

Users User18, User2, User7, and User98 have achieved the maximum value of one for closeness centrality. It has a minimum value of 0.61 which was achieved by user User33. It has an average value of 0.92 for all users. Moreover, it has a standard deviation value of 0.1.

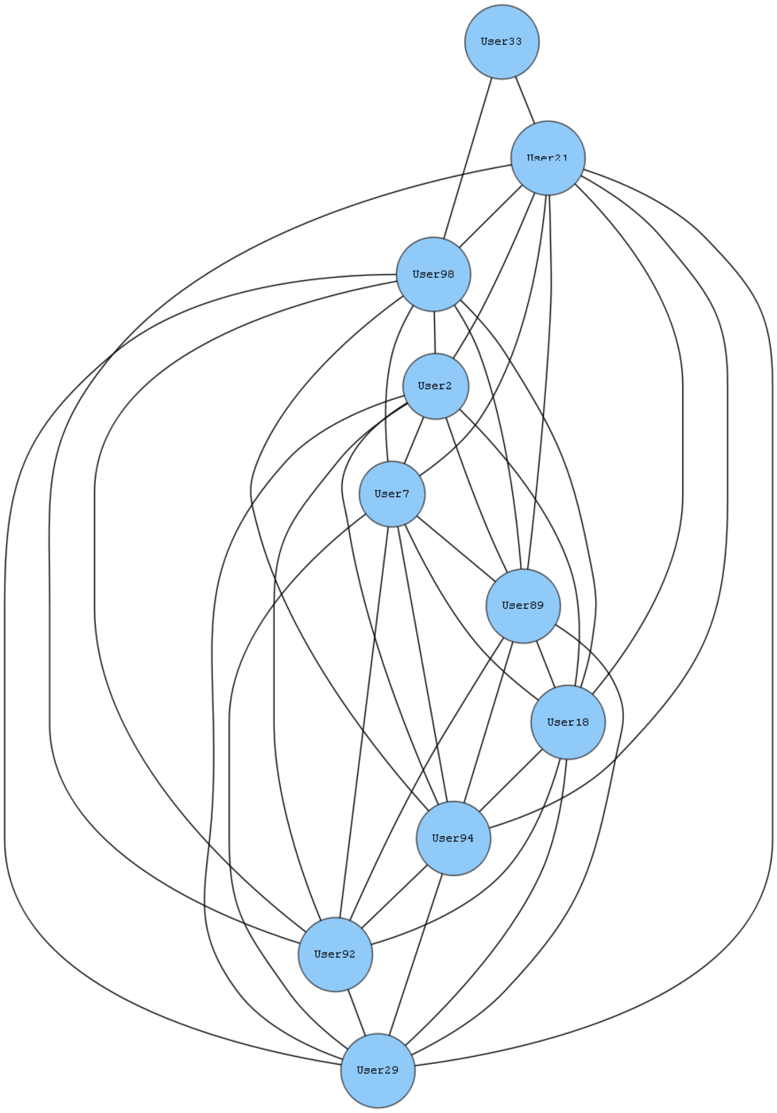


Figure 5.62: Users associations for Magnitude 4.

Figure 5.62 illustrates different components of the graph at Magnitude (4) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Destination IP Address reflecting the relationship between different users.

Users User21, and User98 have achieved the maximum value of one for degree of centrality. It has a minimum value of 0.22 which was achieved by user User33. It has an average value of 0.84 for all users. And, it has a standard deviation value of 0.21.

Value 0.1 is the maximum of betweenness centrality that has been achieved by users User21, and User98. Users User33, User2, User7, User89, User18, User94, User92, and User29 have betweenness centrality of zero which is at the same time the minimum in this graph for Magnitude '4'. Its average value is 0.02; while the standard deviation value is 0.04.

Closeness centrality has a maximum value of one which was achieved by users User21, and User98. The minimum value of 0.56 for the same metric has been realized by user User33. Both of 0.89 and 0.11 are the average and the standard deviation values for closeness centrality in this network graph.

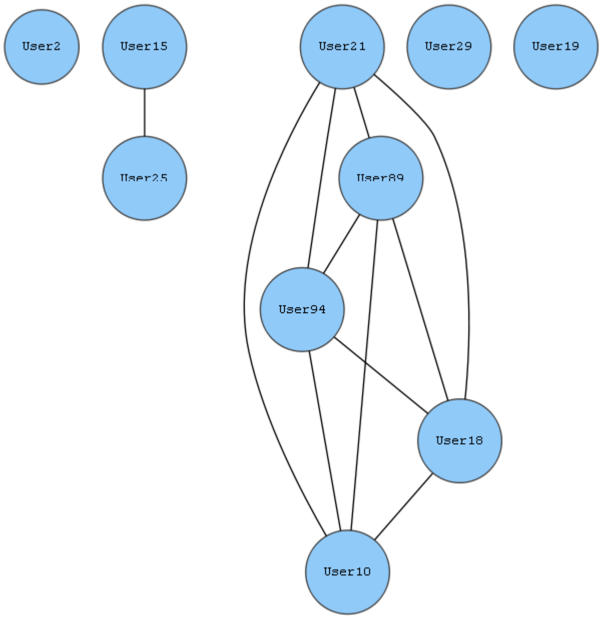


Figure 5.63: Users associations for Magnitude 5.

Figure 5.63 illustrates different components of the graph at Magnitude (5) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Destination IP Address reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.44 which was achieved by users User21, User89, User94, User18, and User10. The minimum value of zero for the same metric has been realized by users User2, User29, and User19. Both of 0.24 and 0.2 are the average and the standard deviation values for degree of centrality in this network graph.

With regard to Magnitude '5', all users have betweenness centrality of zero.

Value 0.44 is the maximum of closeness centrality that has been achieved by users User21, User89, User94, User18, and User10. Users User2, User29, and User19 have closeness centrality of zero which is at the same time the minimum in this graph for Magnitude '5'. Its average value is 0.24; while the standard deviation value is 0.2.

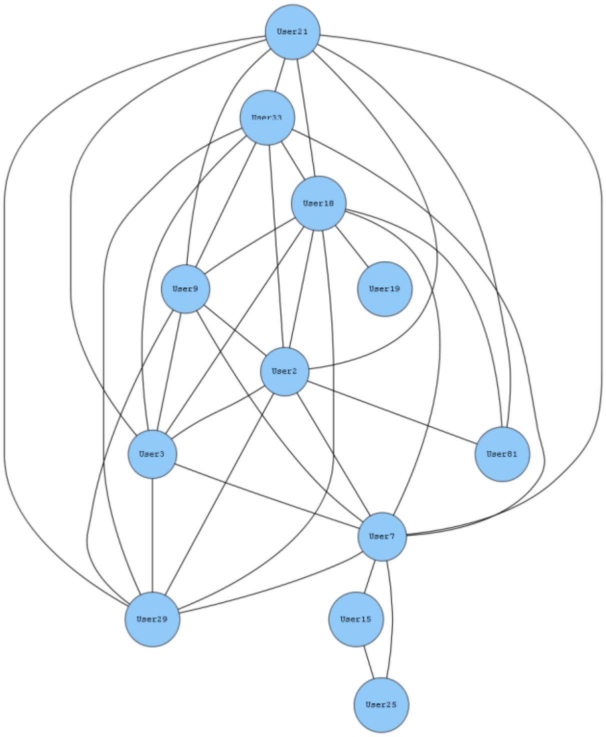


Figure 5.64: Users associations for Magnitude 7.

Figure 5.64 illustrates different components of the graph at Magnitude (7) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Destination IP Address reflecting the relationship between different users.

Value 0.82 is the maximum of degree of centrality that has been achieved by users User18, and User7. User User19 has degree of centrality of 0.09 which is at the same time the minimum in this graph for Magnitude '7'. Its average value is 0.53; while the standard deviation value is 0.26.

The maximum value of betweenness centrality of 0.33 has been realized by user User7. Users User33, User9, User3, User29, User15, User25, User81, and User19 have achieved the minimum value of zero for the same measure. Both of 0.05 and 0.1 are the average and the standard deviation values for betweenness centrality in this network graph.

Users User18, and User7 have closeness centrality of 0.85 which is at the same time the maximum in this graph for Magnitude '7'. Value 0.48 is the minimum for the same metric that has been achieved by user User19. It has an average value of 0.68 for all users. Moreover, it has a standard deviation value of 0.14.

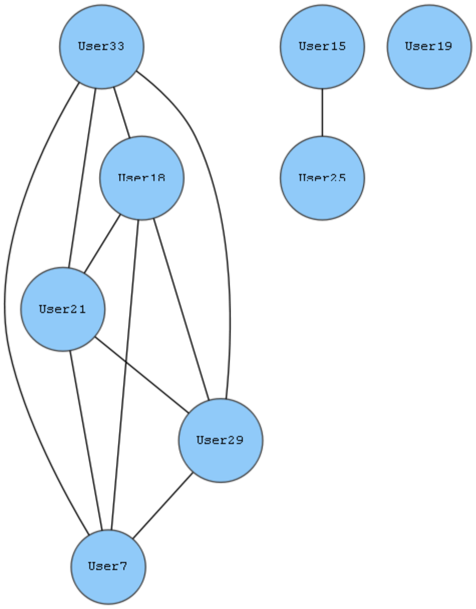


Figure 5.65: Users associations for Magnitude 9.

Figure 5.65 illustrates different components of the graph at Magnitude (9) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Destination IP Address reflecting the relationship between different users.

Users User33, User18, User21, User29, and User7 have degree of centrality of 0.57 which is at the same time the maximum in this graph for Magnitude '9'. Value zero is the minimum of the same metric that has been achieved by user User19. It has an average value of 0.39 for all users. And, it has a standard deviation value of 0.23.

In this graph, all users achieve betweenness centrality of zero.

The maximum value of closeness centrality of 0.57 has been realized by users User33, User18, User21, User29, and User7. User User19 has achieved the minimum value of zero for the same metric. Both of 0.39 and 0.23 are the average and the standard deviation values for closeness centrality in this network graph.

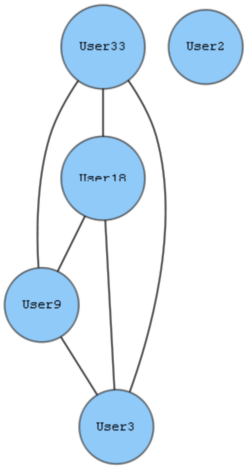


Figure 5.66: Users associations for Magnitude 8.

Figure 5.66 illustrates different components of the graph at Magnitude (8) in a Logs database, where the circles represents different users as a node while the links between them vertex as a different Destination IP Address reflecting the relationship between different users.

The maximum value of degree of centrality of 0.75 has been realized by users User33, User18, User9, and User3. User User2 has achieved the minimum value of zero for degree of centrality. Both of 0.6 and 0.3 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality has a value of zero for all users in Magnitude '8'.

Users User33, User18, User9, and User3 have achieved the maximum value of 0.75 for closeness centrality. It has a minimum value of zero which was achieved by user User2. Its average value is 0.6; while the standard deviation value is 0.3.

5.5 Event.

The following figure shows the distribution of these events over Events.

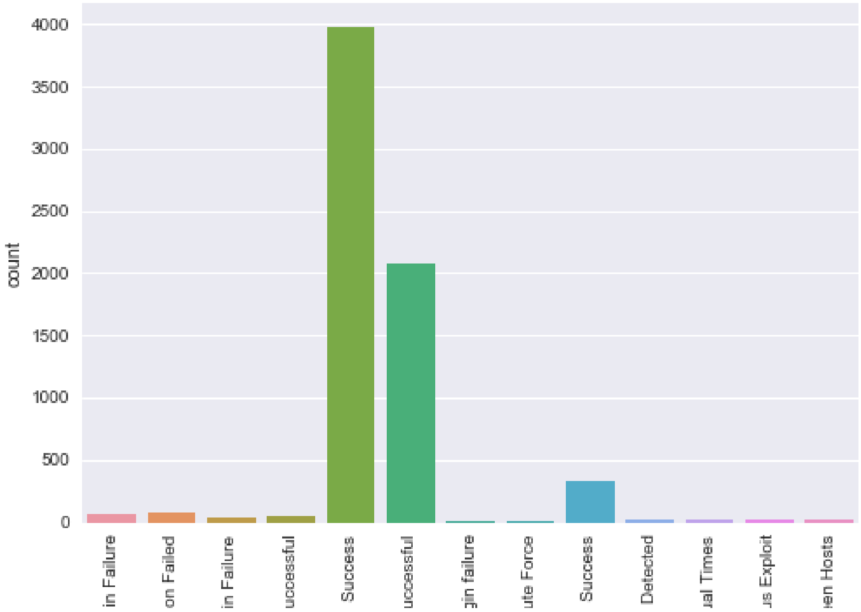


Figure 5.67: activities distribution over Event.

Event 'Brute Force' has the minimum count of 5 with percentage of 0.0747 %. On the other hand, Event 'Remote Login Success' has the maximum count of 3982 with percentage of 59 %. The average count of all different Events is 514.5; while the standard deviation is 1139.0.

One of the most crucial evidence source and valued security breaches indicators for many organizations, and event logging has always won its stand to prove any malicious or none trusted activities generated within any network or infrastructure arrangement.

These repercussions range from heavy storage demand to a backup of such data for performing a historical search to identify what has been identified on a much later stage now. This is typically believed to be destructive for an entire network relying on its availability.

Further from event logging, it can be discovered what might cause disruptions, but let us look at the broader view of those scenarios or hypothesis:

- Users with high count of remote login failure have a higher chance of malicious activity.
    - ➢ A user, as per compliance of any organization, must be limited to certain access attempts especially remote logins to regulate and enforce the policy, but if it is found beyond the permissible failure count and is followed by successful attempts, it may be deemed as an uncertainty or insider threat.
- Users with high count of remote login failure in odd hours have higher chance of malicious activity.
    - ➢ The odd hours denote the out-of-office or non-business hours, during which a high count of remote login attempts may arise suspicion.
- Higher the count of firewall denies from a user, higher is the chance for suspicious activity.
    - ➢ A user may be attempting to bypass the perimeter defense (firewall) of the network with high number of requests. Higher the number of denials, higher may be suspicion of insider threat to attempt to bypass and commit an illegal activity.

Similar, yet challenging assumptions may be drawn from the other hypothesis formulated from the possibility of occurrence of insider threat activities.

- Higher the number of brute force successful logins in odd hours from a user, higher is the chance for suspicious activity.

- Users with high number of brute force logins along with high number of login failure have higher chance of malicious activity.

- Higher the count of successful login at odd hours, higher is the chance of malicious activity.

- Users with high count of login failure have higher chance for malicious activity.

- Users with high count of login failure in odd hours have higher chance for malicious activity.

- Users having high number of malicious exploits have higher chance of malicious activity.

- Users having high number of malicious exploits at odd hours have higher chance of malicious activity.

- Higher the count of account privilege changes in odd hour higher is the probability of malicious activity.

- Users with account added to Admin group in odd hours have higher chance of suspicious activity.

5.5.1 Event and Hour.

The network graphs in this section represent several users (nodes or vertex) at different events (hypothesis) which are:

1. General Authentication Failed
2. Remote Login Failure
3. Remote Login Success – Odd hour

4. User Login Failure
5. Excessive Firewall Denies Between Hosts
6. UBA: New Account Use Detected
7. Malicious Exploit
8. UBA: User Access at Unusual Times
9. Multiple login failure
10. Admin Login Successful – Odd hour
11. General Authentication Successful – Odd hour
12. Brute Force

The links connected between them (edge) representing different period of time or hours. In this case any two nodes or more at specific event has same time stamp meant they have same type of link or connection.

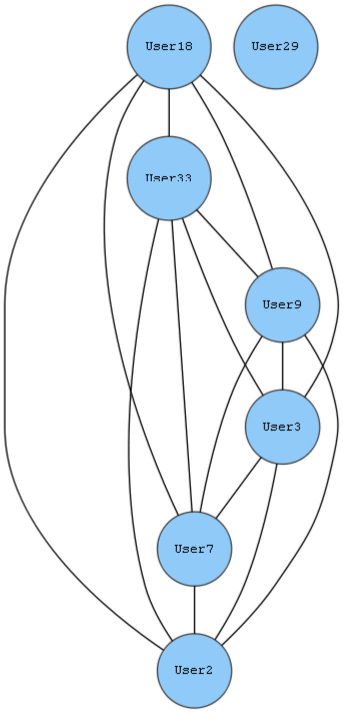


Figure 5.68: Users associations for Event User Login Failure.

Figure 5.68 illustrates different components of the graph at event called (Event User Login Failure), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

Users User18, User33, User9, User3, User7, and User2 have degree of centrality of 0.83 which is at the same time the maximum in this graph for Event 'User Login Failure'. Value zero is the minimum of the same metric that has been achieved by user User29. Both of 0.71 and 0.29 are the average and the standard deviation values for degree of centrality in this network graph.

In this graph, all users achieve betweenness centrality of zero.

The maximum value of closeness centrality of 0.83 has been realized by users User18, User33, User9, User3, User7, and User2. User User29 has achieved the minimum value of zero for the same metric. Its average value is 0.71; while the standard deviation value is 0.29.

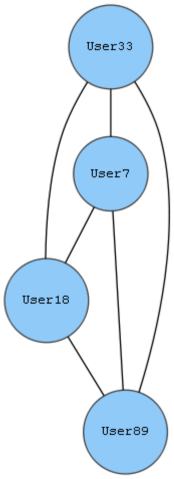


Figure 5.69: Users associations for Event General Authentication Successful.

Figure 5.69 illustrates different components of the graph at event called (General Authentication Successful), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

In this graph, all users achieve degree of centrality of one. Betweenness centrality has a value of zero for all users in Event 'General Authentication Successful'.

Closeness centrality has a value of one for all users in Event 'General Authentication Successful'.

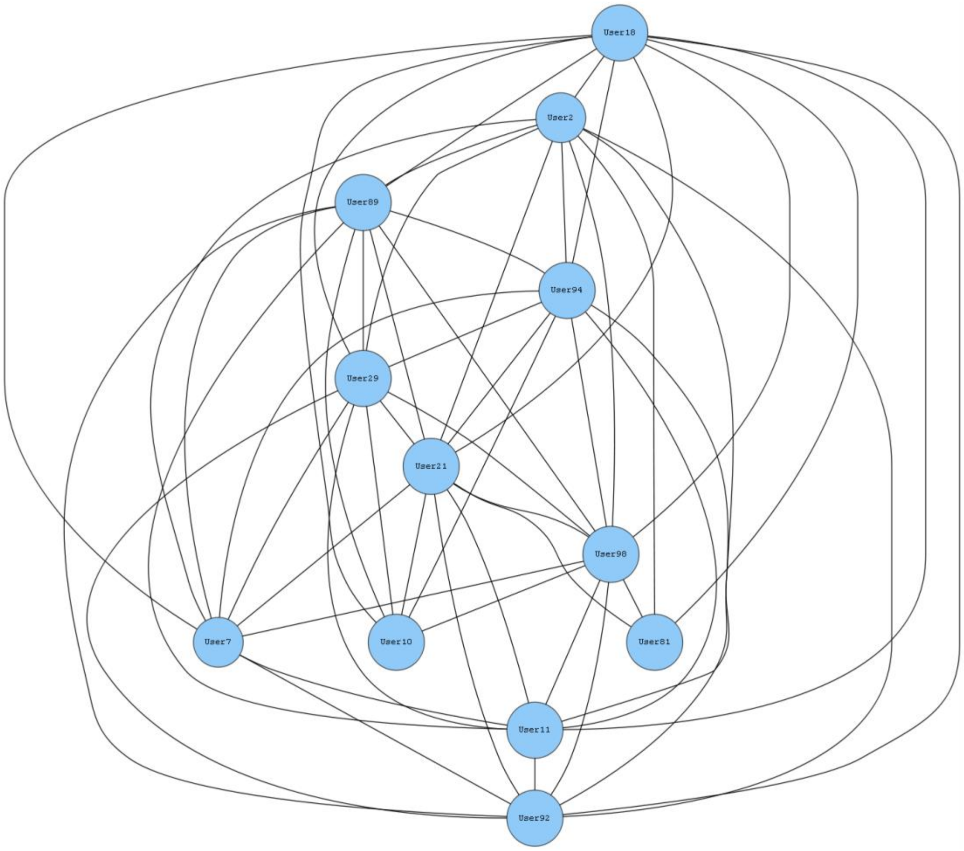


Figure 5.70: Users associations for Event Remote Login Success.

Figure 5.70 illustrates different components of the graph at event called (Event Remote Login Success), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

Users User18, User21, and User98 have achieved the maximum value of one for degree of centrality. It has a minimum value of 0.36 which was achieved by user User81. It has an average value of 0.83 for all users. And, it has a standard deviation value of 0.18.

Value 0.05 is the maximum of betweenness centrality that has been achieved by users User18, User21, and User98. Users User10, User81, User7, User11, and User92 have betweenness centrality of zero which is at the same time the minimum in this graph for Event 'Remote Login Success'. Its average value is 0.02; while the standard deviation value is 0.02.

Closeness centrality has a maximum value of one which was achieved by users User18, User21, and User98. The minimum value of 0.61 for the same metric has been realized by user User81. Both of 0.88 and 0.12 are the average and the standard deviation values for closeness centrality in this network graph.

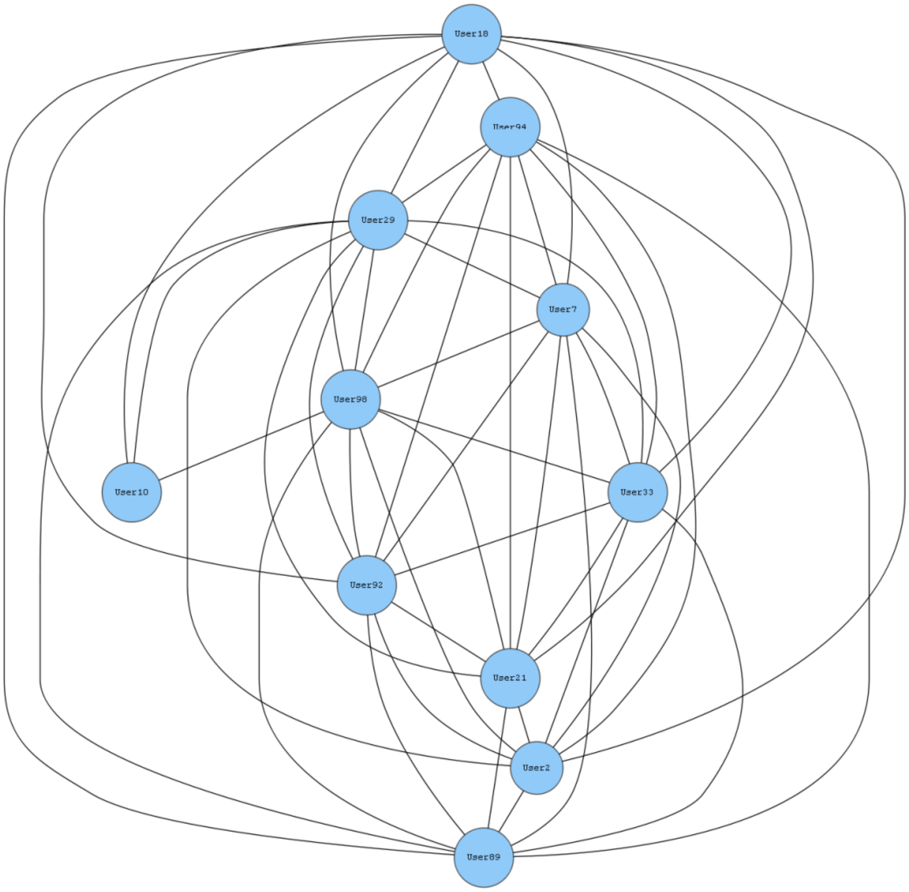


Figure 5.71: Users associations for Event Admin Login Successful.

Figure 5.71 illustrates different components of the graph at event called (Event Admin Login Successful), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

Degree of centrality has a maximum value of one which was achieved by users User18, User29, and User98. The minimum value of 0.3 for the same metric has been realized by user User10. Both of 0.87 and 0.19 are the average and the standard deviation values for degree of centrality in this network graph.

Users User18, User29, and User98 have betweenness centrality of 0.05 which is at the same time the maximum in this graph for Event 'Admin Login Successful'. Value zero is the minimum the same measure that has been achieved by users User94, User7, User33, User92, User21, User10, User2, and User89. It has an average value of 0.01 for all users. Also, it has a standard deviation value of 0.02.

Value one is the maximum of closeness centrality that has been achieved by users User18, User29, and User98. User User10 has closeness centrality of 0.59 which is at the same time the minimum in this graph for Event 'Admin Login Successful'. Its average value is 0.9; while the standard deviation value is 0.11.

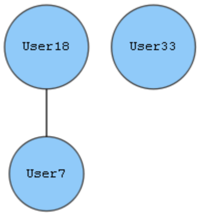


Figure 5.72: Users associations for Event Multiple login failure.

Figure 5.72 illustrates different components of the graph at event called (Event Multiple login failure), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

Value 0.5 is the maximum of degree of centrality that has been achieved by users User18, and User7. User User33 has degree of centrality of zero which is at the same time the minimum in this graph for Event 'Multiple login failure'. Its average value is 0.33; while the standard deviation value is 0.24. Betweenness centrality is zero for all users in this graph.

Users User18, and User7 have closeness centrality of 0.5 which is at the same time the maximum in this graph for Event 'Multiple login failure'. Value zero is the minimum for the same metric that has been achieved by user User33. It has an average value of 0.33 for all users. Moreover, it has a standard deviation value of 0.24.

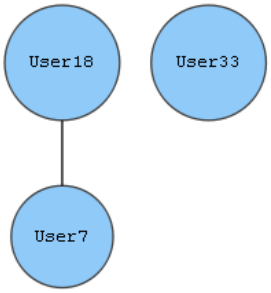


Figure 5.73: Users associations for Event Brute Force.

Figure 5.73 illustrates different components of the graph at event called (Event Brute Force), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

Users User18, and User7 have degree of centrality of 0.5 which is at the same time the maximum in this graph for Event 'Brute Force'. Value zero is the minimum of the same metric that has been achieved by user User33. It has an average value of 0.33 for all users. And, it has a standard deviation value of 0.24.

In this graph, all users achieve betweenness centrality of zero. The maximum value of closeness centrality of 0.5 has been realized by users User18, and User7. User User33 has achieved the minimum value of zero for the same metric. Both of 0.33 and 0.24 are the average and the standard deviation values for closeness centrality in this network graph.

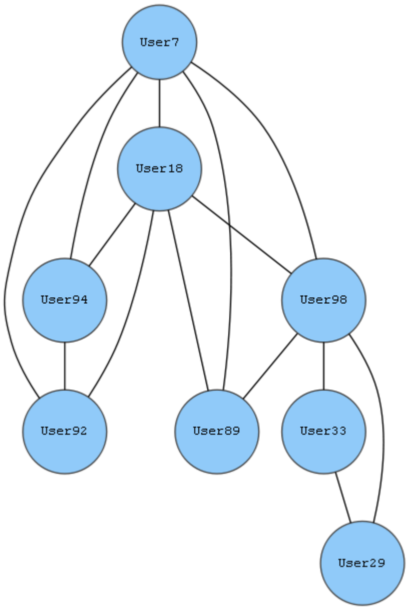


Figure 5.74: Users associations for Event User Login Success.

Figure 5.74 illustrates different components of the graph at event called (Event User Login Success), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

The maximum value of degree of centrality of 0.71 has been realized by users User7, User18, and User98. Users User33, and User29 have achieved the minimum value of 0.29 for degree of centrality. Both of 0.5 and 0.17 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality has a maximum value of 0.48 which was achieved by user User98. The minimum value of zero for the same measure has been realized by users User94, User92, User33, User29, and User89. It has an average value of 0.11 for all users. Also, it has a standard deviation value of 0.16.

Users User7, User18, and User98 have achieved the maximum value of 0.78 for closeness centrality. It has a minimum value of 0.5 which was achieved by users User33, and User29. Its average value is 0.63; while the standard deviation value is 0.12.

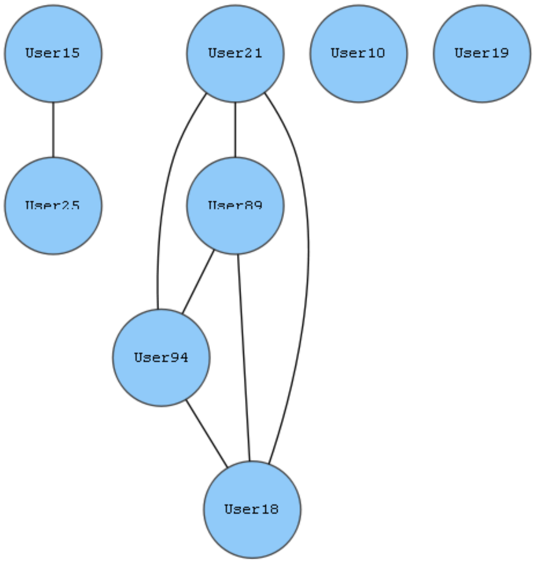


Figure 5.75: Users associations for Event UBA : New Account Use Detected.

Figure 5.75 illustrates different components of the graph at event called (New Account Use Detected), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

Users User21, User89, User94, and User18 have achieved the maximum value of 0.43 for degree of centrality. It has a minimum value of zero which was achieved by users User10, and User19. Its average value is 0.25; while the standard deviation value is 0.19.

Users in Event 'UBA : New Account Use Detected' have the same betweenness centrality for all of them.

Closeness centrality has a maximum value of 0.43 which was achieved by users User21, User89, User94, and User18. The minimum value of zero for the same metric has been realized by users User10, and User19. It has an average value of 0.25 for all users. Moreover, it has a standard deviation value of 0.19.

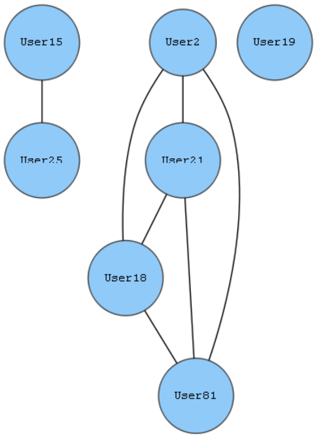


Figure 5.76: Users associations for Event UBA : User Access at Unusual Times.

Figure 5.76 illustrates different components of the graph at event called (User Access at Unusual Times), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.5 which was achieved by users User2, User21, User18, and User81. The minimum value of zero for the same metric has been realized by user User19. It has an average value of 0.33 for all users. And, it has a standard deviation value of 0.2.

With regard to Event ‘UBA: User Access at Unusual Times', all users have betweenness centrality of zero.

Value 0.5 is the maximum of closeness centrality that has been achieved by users User2, User21, User18, and User81. User User19 has closeness centrality of zero which is at the same time the minimum in this graph for Event 'UBA : User Access at Unusual Times'. Both of 0.33 and 0.2 are the average and the standard deviation values for closeness centrality in this network graph.

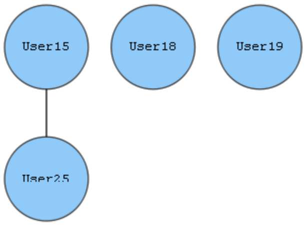


Figure 5.77: Users associations for Event Malicious Exploit.

Figure 5.77 illustrates different components of the graph at event called (Malicious Exploit), where the circles represents different users as a node while the links between them vertex as a different period of time from 1 AM to 21 PM reflecting the relationship between different users.

Value 0.33 is the maximum of degree of centrality that has been achieved by users User15, and User25. Users User18, and User19 have degree of centrality of zero which is at the same time the minimum in this graph for Event 'Malicious Exploit'. Both of 0.17 and 0.17 are the average and the standard deviation values for degree of centrality in this network graph.

Betweenness centrality is zero for all users in this graph.

Users User15, and User25 have closeness centrality of 0.33 which is at the same time the maximum in this graph for Event 'Malicious Exploit'. Value zero is the minimum for the same metric that has been achieved by users User18, and User19. Its average value is 0.17; while the standard deviation value is 0.17.

5.5.2 Event and Magnitude.

The network graphs in this section represent several users (nodes or vertex) at different events (hypothesis), while links connected between them (edge) represent different level of magnitude ranging between 1 and 10 . In this case any two nodes or more at specific event has same magnitude meant they have same type of link or connection.

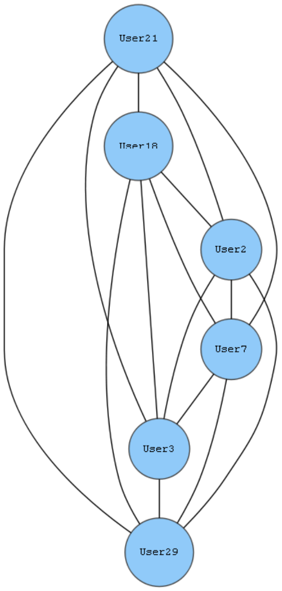


Figure 5.78: Users associations for Event Remote Login Failure.

Figure 5.78 illustrates different components of the graph at event called (Remote Login Failure), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users.

In this graph, all users achieve degree of centrality of one. Betweenness centrality has a value of zero for all users in Event 'Remote Login Failure'. Closeness centrality has a value of one for all users in Event 'Remote Login Failure'.

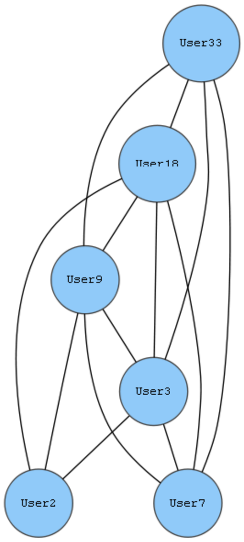


Figure 5.79: Users associations for Event General Authentication Failed.

Figure 5.79 illustrates different components of the graph at event called (General Authentication Failed), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users.

Users User18, User9, and User3 have achieved the maximum value of one for degree of centrality. It has a minimum value of 0.6 which was achieved by user User2. Both of 0.87 and 0.15 are the average and the standard deviation values for degree of centrality in this network graph.

Value 0.07 is the maximum of betweenness centrality that has been achieved by users User18, User9, and User3. Users User33, User7, and User2 have betweenness centrality of zero which is at the same time the minimum in this graph for Event 'General Authentication Failed'. It has an average value of 0.03 for all users. Also, it has a standard deviation value of 0.03.

Closeness centrality has a maximum value of one which was achieved by users User18, User9, and User3. The minimum value of 0.71 for the same metric has been realized by user User2. Its average value is 0.9; while the standard deviation value is 0.11.

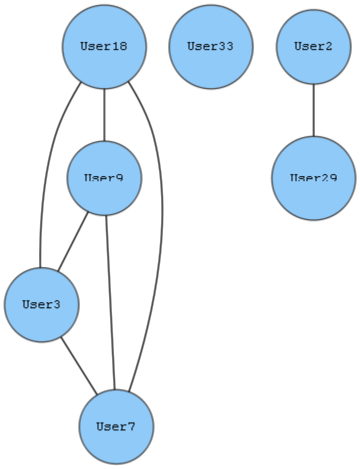


Figure 5.80: Users associations for Event User Login Failure.

Figure 5.80 illustrates different components of the graph at event called (User Login Failure), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users.

Degree of centrality has a maximum value of 0.5 which was achieved by users User18, User9, User3, and User7. The minimum value of zero for the same metric has been realized by user User33. Its average value is 0.33; while the standard deviation value is 0.2.

With regard to Event 'User Login Failure', all users have betweenness centrality of zero.

Value 0.5 is the maximum of closeness centrality that has been achieved by users User18, User9, User3, and User7. User User33 has closeness centrality of zero which is at the same time the minimum in this graph for Event 'User Login Failure'. It has an average value of 0.33 for all users. Moreover, it has a standard deviation value of 0.2.

Closeness centrality is one for all users in this graph.

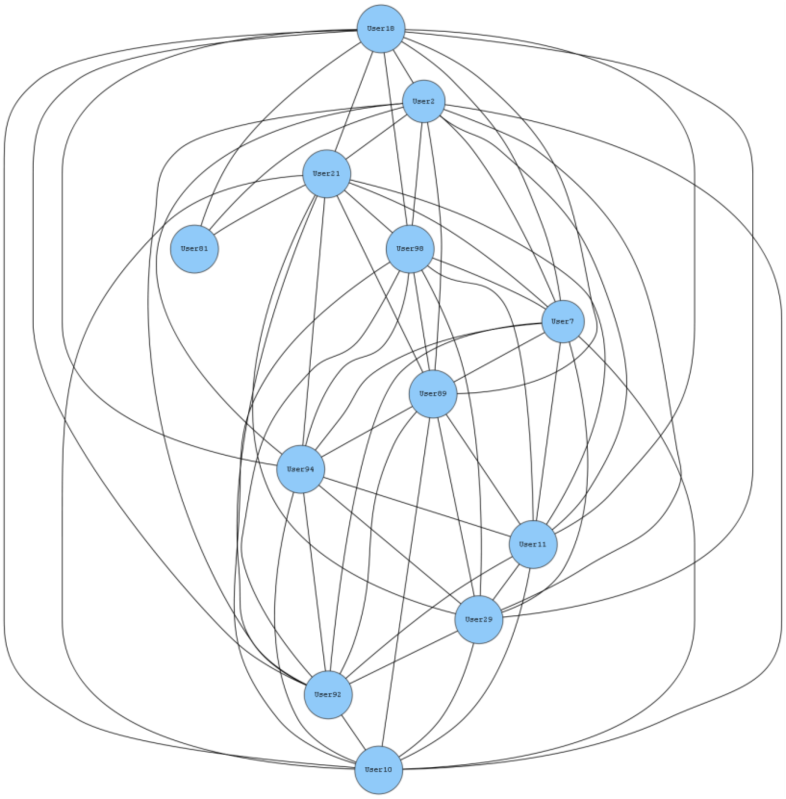


Figure 5.81: Users associations for Event Remote Login Success.

Figure 5.81 illustrates different components of the graph at event called (Event Remote Login Success), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users.

Users User18, User2, and User21 have degree of centrality of one which is at the same time the maximum in this graph for Event 'Remote Login Success'. Value 0.27 is the minimum of the same metric that has been achieved by user User81. Both of 0.88 and 0.19 are the average and the standard deviation values for degree of centrality in this network graph.

Users User18, User2, and User21 have achieved the maximum value of 0.05 for betweenness centrality. It has a minimum value of zero which was achieved by users User98, User7, User89, User94, User11, User29, User92, User10, and User81. It has an average value of 0.01 for all users. Also, it has a standard deviation value of 0.02.

The maximum value of closeness centrality of one has been realized by users User18, User2, and User21. User User81 has achieved the minimum value of 0.58 for the same metric. Its average value is 0.91; while the standard deviation value is 0.11.

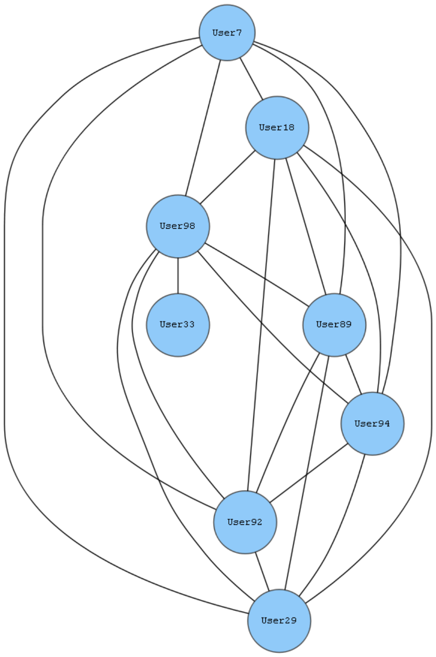


Figure 5.82: Users associations for Event User Login Success.

Figure 5.82 illustrates different components of the graph at event called (User Login Success), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by user User98. User User33 has degree of centrality of 0.14 which is at the same time the minimum in this graph for Event 'User Login Success'. Its average value is 0.79; while the standard deviation value is 0.25.

The maximum value of betweenness centrality of 0.29 has been realized by user User98. Users User7, User18, User89, User94, User92, User29, and User33 have achieved the minimum value of zero for the same measure. Both of 0.04 and 0.09 are the average and the standard deviation values for betweenness centrality in this network graph.

User User98 has closeness centrality of one which is at the same time the maximum in this graph for Event 'User Login Success'. Value 0.54 is the minimum for the same metric that has been achieved by user User33. It has an average value of 0.85 for all users. Moreover, it has a standard deviation value of 0.12.

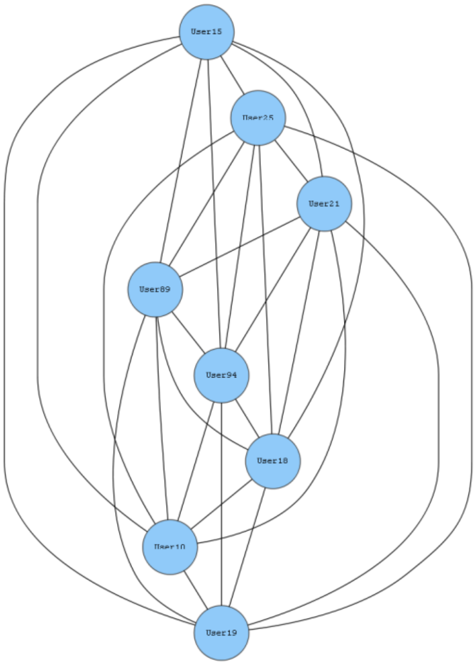


Figure 5.83: Users associations for Event UBA : New Account Use Detected.

Figure 5.83 illustrates different components of the graph at event called (New Account Use Detected), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users.

Degree of centrality is one for all users in this graph. In this graph, all users acheive betweenness centrality of zero. In this graph, all users acheive closeness centrality of one.

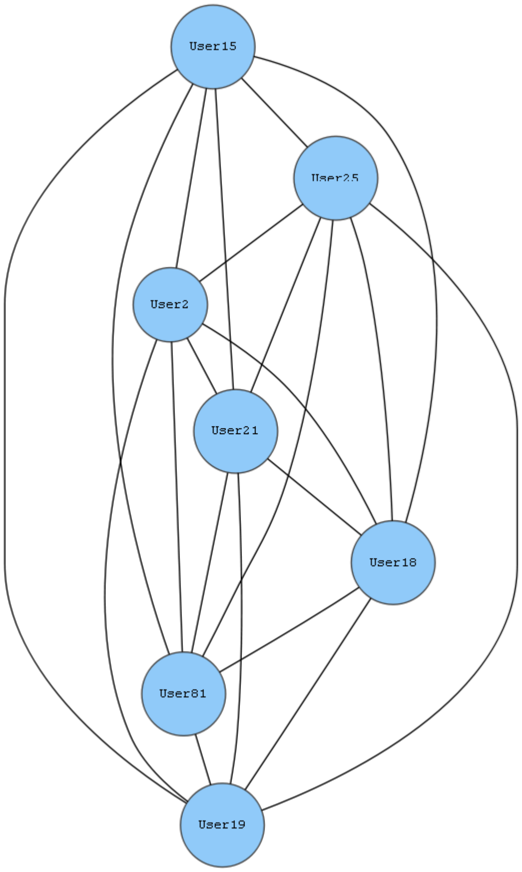


Figure 5.84: Users associations for Event UBA : User Access at Unusual Times.

Figure 5.84 illustrates different components of the graph at event called (User Access at Unusual Times), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users

In this graph, all users achieve degree of centrality of one. Betweenness centrality has a value of zero for all users in Event 'UBA : User Access at Unusual Times'. Also, Closeness centrality has a value of one for all users in Event 'UBA: User Access at Unusual Times'.

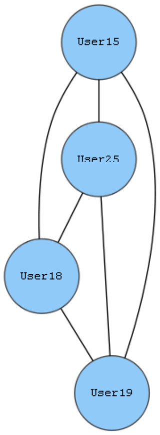


Figure 5.85: Users associations for Event Malicious Exploit.

Figure 5.85 illustrates different components of the graph at event called (Malicious Exploit), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users

Degree of centrality has a value of one for all users in Event 'Malicious Exploit'.

Users in Event 'Malicious Exploit' have the same betweenness centrality for all of them.

Users in Event 'Malicious Exploit' have the same closeness centrality for all of them.

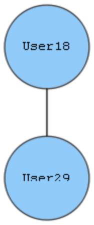


Figure 5.86: Users associations for Event Excessive Firewall Denies Between Hosts.

Figure 5.86 illustrates different components of the graph at event called (Firewall Denies between Hosts), where the circles represents different users as a node while the links between them vertex as a different Magnitude ranging from magnitude 1 to 10, which reflect the relationship between different users.

Users in Event 'Excessive Firewall Denies Between Hosts' have the same degree of centrality for all of them.

With regard to Event 'Excessive Firewall Denies Between Hosts', all users have betweenness centrality of zero.

With regard to Event 'Excessive Firewall Denies Between Hosts', all users have closeness centrality of one.

5.5.3 Event and Source IP Address.

The network graphs in this section represent several users (nodes or vertex) at different events (hypothesis), while links connected between them (edge) represent different Source IP Address. In this case any two nodes or more at specific event has same Source IP Address meant they have same type of link or connection.

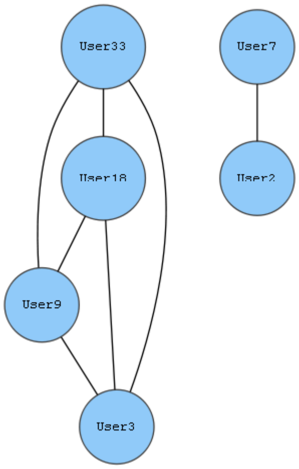


Figure 5.87: Users associations for Event General Authentication Failed.

Figure 5.87 illustrates different components of the graph at event called (Firewall Denies between Hosts), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

Users User33, User18, User9, and User3 have degree of centrality of 0.6 which is at the same time the maximum in this graph for Event 'General Authentication Failed'. Value 0.2 is the minimum of the same metric that has been achieved by users User7, and User2. Its average value is 0.47; while the standard deviation value is 0.19.

In this graph, all users achieve betweenness centrality of zero.

The maximum value of closeness centrality of 0.6 has been realized by users User33, User18, User9, and User3. Users User7, and User2 have achieved the minimum value of 0.2 for the same metric. It has an average value of 0.47 for all users. Moreover, it has a standard deviation value of 0.19.

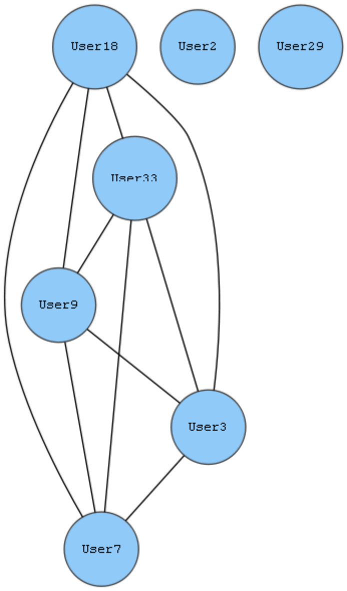


Figure 5.88: Users associations for Event User Login Failure.

Figure 5.88 illustrates different components of the graph at event called (Event User Login Failure), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

The maximum value of degree of centrality of 0.67 has been realized by users User18, User33, User9, User3, and User7. Users User2, and User29 have achieved the minimum value of zero for degree of centrality. It has an average value of 0.48 for all users. And, it has a standard deviation value of 0.3.

Betweenness centrality has a value of zero for all users in Event 'User Login Failure'.

Users User18, User33, User9, User3, and User7 have achieved the maximum value of 0.67 for closeness centrality. It has a minimum value of zero which was achieved by users User2, and User29. Both of 0.48 and 0.3 are the average and the standard deviation values for closeness centrality in this network graph.

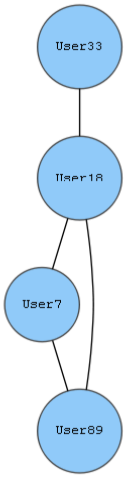


Figure 5.89: Users associations for Event General Authentication Successful.

Figure 5.89 illustrates different components of the graph at event called (Authentication Successful), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

User User18 has achieved the maximum value of one for degree of centrality. It has a minimum value of 0.33 which was achieved by user User33. Both of 0.67 and 0.24 are the average and the standard deviation values for degree of centrality in this network graph.

Value 0.67 is the maximum of betweenness centrality that has been achieved by user User18. Users User33, User7, and User89 have betweenness centrality of zero which is at the same time the minimum in this graph for Event 'General Authentication Successful'. It has an average value of 0.17 for all users. Also, it has a standard deviation value of 0.29.

Closeness centrality has a maximum value of one which was achieved by user User18. The minimum value of 0.6 for the same metric has been realized by user User33. Its average value is 0.78; while the standard deviation value is 0.14.

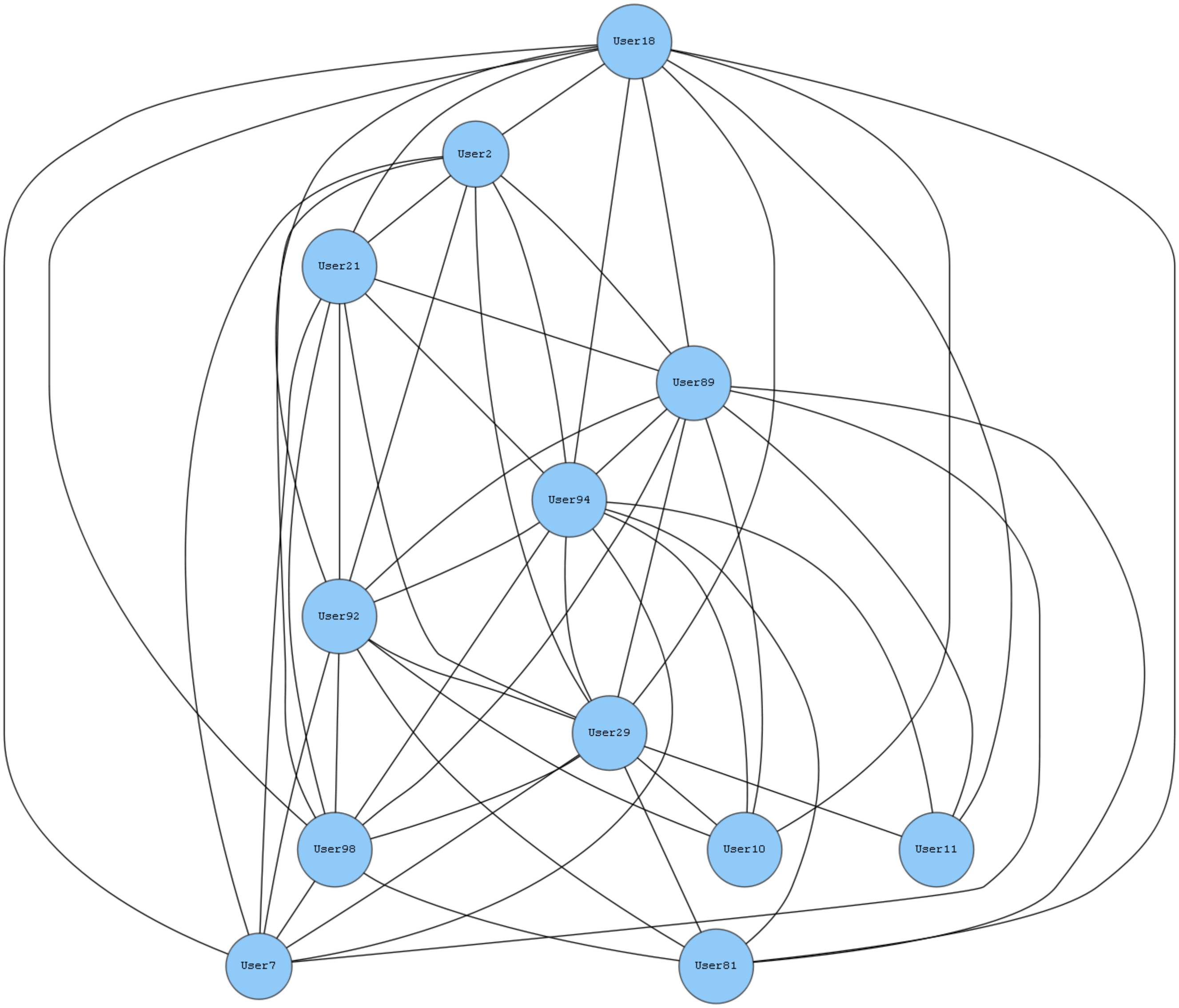


Figure 5.90: Users associations for Event Remote Login Success.

Figure 5.90 illustrates different components of the graph at event called (Remote Login Success), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

Degree of centrality has a maximum value of one which was achieved by users User18, User89, User94, and User29. The minimum value of 0.36 for the same metric has been realized by user User11. Its average value is 0.77; while the standard deviation value is 0.21.

Users User18, User89, User94, and User29 have betweenness centrality of 0.06 which is at the same time the maximum in this graph for Event 'Remote Login Success'. Value zero is the minimum the same measure that has been achieved by users User2, User21, User7, User81, User10, and User11. Both of 0.02 and 0.03 are the average and the standard deviation values for betweenness centrality in this network graph.

Value one is the maximum of closeness centrality that has been achieved by users User18, User89, User94, and User29. User User11 has closeness centrality of 0.61 which is at the same time the minimum in this graph for Event 'Remote Login Success'. It has an average value of 0.84 for all users. Moreover, it has a standard deviation value of 0.14.

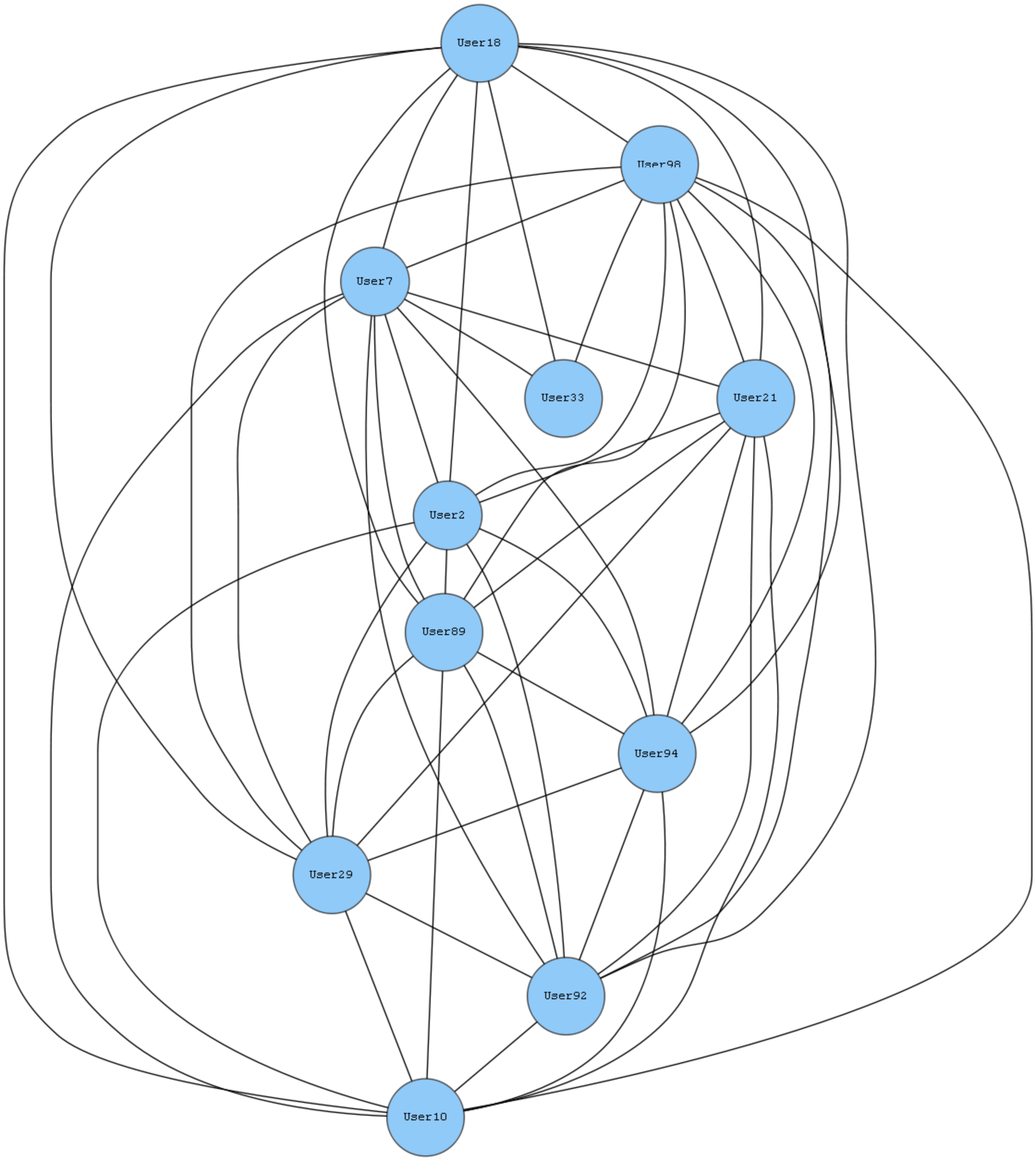


Figure 5.91: Users associations for Event Admin Login Successful.

Figure 5.91 illustrates different components of the graph at event called (Admin Login Successful), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

Value one is the maximum of degree of centrality that has been achieved by users User18, User98, and User7. User User33 has degree of centrality of 0.3 which is at the same time the minimum in this graph for Event 'Admin Login Successful'. It has an average value of 0.87 for all users. And, it has a standard deviation value of 0.19.

The maximum value of betweenness centrality of 0.05 has been realized by users User18, User98, and User7. Users User33, User21, User2, User89, User94, User29, User92, and User10 have achieved the minimum value of zero for the same measure. Its average value is 0.01; while the standard deviation value is 0.02.

Users User18, User98, and User7 have closeness centrality of one which is at the same time the maximum in this graph for Event 'Admin Login Successful'. Value 0.59 is the minimum for the same metric that has been achieved by user User33. Both of 0.9 and 0.11 are the average and the standard deviation values for closeness centrality in this network graph.

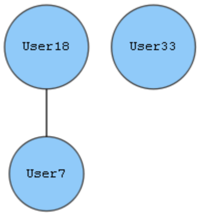


Figure 5.92: Users associations for Event Multiple login failure.

Figure 5.92 illustrates different components of the graph at event called (Multiple login failure), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

Users User18, and User7 have degree of centrality of 0.5 which is at the same time the maximum in this graph for Event 'Multiple login failure'. Value zero is the minimum of the same metric that has been achieved by user User33. Both of 0.33 and 0.24 are the average and the standard deviation values for degree of centrality in this network graph.

In this graph, all users acheive betweenness centrality of zero.

The maximum value of closeness centrality of 0.5 has been realized by users User18, and User7. User User33 has achieved the minimum value of zero for the same metric. Its average value is 0.33; while the standard deviation value is 0.24.

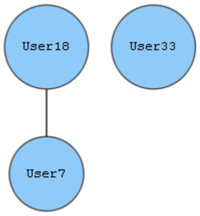


Figure 5.93: Users associations for Event Brute Force.

Figure 5.93 illustrates different components of the graph at event called (Brute Force), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

The maximum value of degree of centrality of 0.5 has been realized by users User18, and User7. User User33 has achieved the minimum value of zero for degree of centrality. Its average value is 0.33; while the standard deviation value is 0.24.

Betweenness centrality has a value of zero for all users in Event 'Brute Force'.

Users User18, and User7 have achieved the maximum value of 0.5 for closeness centrality. It has a minimum value of zero which was achieved by user User33. It has an average value of 0.33 for all users. Moreover, it has a standard deviation value of 0.24.

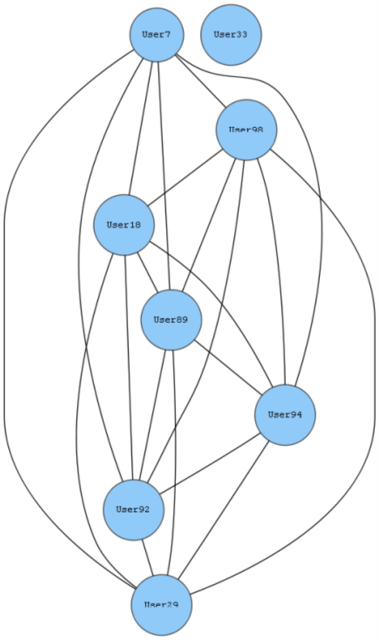


Figure 5.94: Users associations for Event User Login Success.

Figure 5.94 illustrates different components of the graph at event called (User Login Success), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

Users User7, User98, User18, User89, User94, User92, and User29 have achieved the maximum value of 0.86 for degree of centrality. It has a minimum value of zero which was achieved by user User33. It has an average value of 0.75 for all users. And, it has a standard deviation value of 0.28.

Users in Event 'User Login Success' have the same betweenness centrality for all of them.

Closeness centrality has a maximum value of 0.86 which was achieved by users User7, User98, User18, User89, User94, User92, and User29. The minimum value of zero for the same metric has been realized by user User33. Both of 0.75 and 0.28 are the average and the standard deviation values for closeness centrality in this network graph.

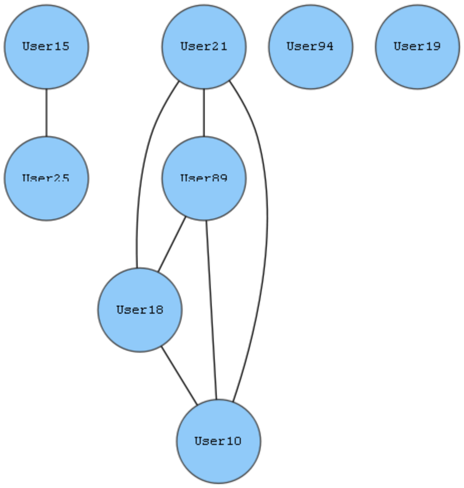


Figure 5.95: Users associations for Event UBA: New Account Use Detected.

Figure 5.95 illustrates different components of the graph at event called (UBA: New Account Use Detected),, where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

Degree of centrality has a maximum value of 0.43 which was achieved by users User21, User89, User18, and User10. The minimum value of zero for the same metric has been realized by users User94, and User19. Both of 0.25 and 0.19 are the average and the standard deviation values for degree of centrality in this network graph.

With regard to Event 'UBA: New Account Use Detected', all users have betweenness centrality of zero.

Value 0.43 is the maximum of closeness centrality that has been achieved by users User21, User89, User18, and User10. Users User94, and User19 have closeness centrality of zero which is at the same time the minimum in this graph for Event ‘UBA: New Account Use Detected'. Its average value is 0.25; while the standard deviation value is 0.19.

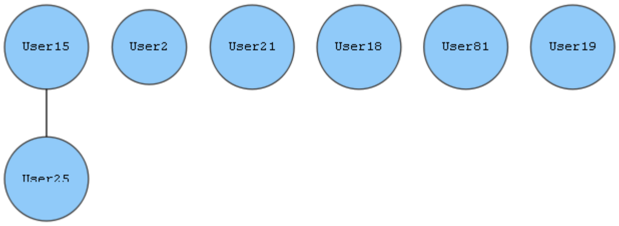


Figure 5.96: Users associations for Event UBA: User Access at Unusual Times.

Figure 5.96 illustrates different components of the graph at event called (UBA: User Access at Unusual Times), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

Value 0.17 is the maximum of degree of centrality that has been achieved by users User15, and User25. Users User2, User21, User18, User81, and User19 have degree of centrality of zero which is at the same time the minimum in this graph for Event 'UBA: User Access at Unusual Times'. Its average value is 0.05; while the standard deviation value is 0.08.

Betweenness centrality is zero for all users in this graph.

Users User15, and User25 have closeness centrality of 0.17 which is at the same time the maximum in this graph for Event 'UBA : User Access at Unusual Times'. Value zero is the minimum for the same metric that has been achieved by users User2, User21, User18, User81, and User19. It has an average value of 0.05 for all users. Moreover, it has a standard deviation value of 0.08.

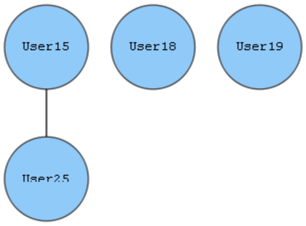


Figure 5.97: Users associations for Event Malicious Exploit.

Figure 5.97 illustrates different components of the graph at event called (Malicious Exploit), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

Users User15, and User25 have degree of centrality of 0.33 which is at the same time the maximum in this graph for Event 'Malicious Exploit'. Value zero is the minimum of the same metric that has been achieved by users User18, and User19. It has an average value of 0.17 for all users. And, it has a standard deviation value of 0.17.

In this graph, all users achieve betweenness centrality of zero.

The maximum value of closeness centrality of 0.33 has been realized by users User15, and User25. Users User18, and User19 have achieved the minimum value of zero for the same metric. Both of 0.17 and 0.17 are the average and the standard deviation values for closeness centrality in this network graph.

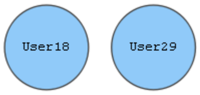


Figure 5.98: Users associations for Event Excessive Firewall Denies Between Hosts.

Figure 5.98 illustrates different components of the graph at event called (Excessive Firewall Denies between Hosts), where the circles represents different users as a node while the links between them vertex as a different source IP address, which reflecting the relationship between different users.

In this graph, all users achieve degree of centrality of zero.

Betweenness centrality has a value of zero for all users in Event 'Excessive Firewall Denies between Hosts'.

Closeness centrality has a value of zero for all users in Event 'Excessive Firewall Denies between Hosts'.

5.5.4 Event and Source Port.

The network graphs in this section represent several users (nodes or vertex) at different events (hypothesis), while links connected between them (edge) represent different Source Port. In this case any two nodes or more at specific event has same Source Port meant they have same type of link or connection.

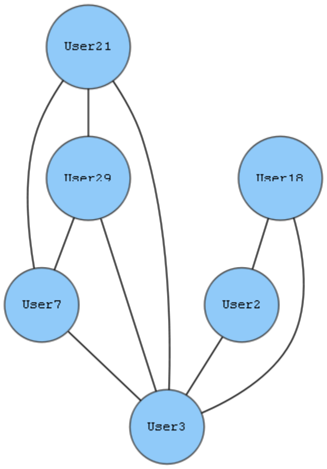


Figure 5.99: Users associations for Event Remote Login Failure.

Figure 5.99 illustrates different components of graph at event called (Remote Login Failure), where the circles represents different users as a node while the links between them vertex as a different Source Port, which reflect the relationship between different users.

User User3 has achieved the maximum value of one for degree of centrality. It has a minimum value of 0.4 which was achieved by users User18, and User2. Its average value is 0.6; while the standard deviation value is 0.2.

Value 0.6 is the maximum of betweenness centrality that has been achieved by user User3. Users User21, User29, User7, User18, and User2 have betweenness centrality of zero which is at the same time the minimum in this graph for Event 'Remote Login Failure'. Both of 0.1 and 0.22 are the average and the standard deviation values for betweenness centrality in this network graph.

Closeness centrality has a maximum value of one which was achieved by user User3. The minimum value of 0.62 for the same metric has been realized by users User18, and User2. It has an average value of 0.73 for all users. Moreover, it has a standard deviation value of 0.13.

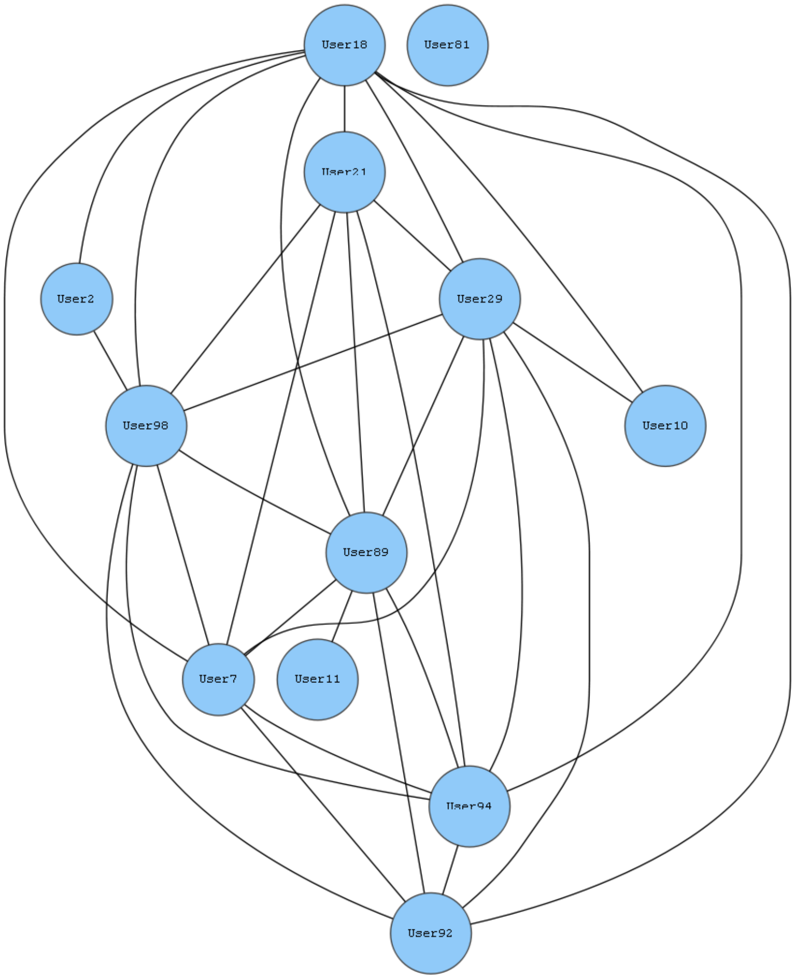


Figure 5.100: Users associations for Event Remote Login Success.

Figure 5.100 illustrates different components of graph at event called (Remote Login Success), where the circles represents different users as a node while the links between them vertex as a different Source Port, which reflect the relationship between different users.

The maximum value of degree of centrality of 0.82 has been realized by user User18. User User81 has achieved the minimum value of zero for degree of centrality. It has an average value of 0.48 for all users. And, it has a standard deviation value of 0.28.

Betweenness centrality has a maximum value of 0.17 which was achieved by user User89. The minimum value of zero for the same measure has been realized by users User2, User21, User92, User81, User11, and User10. Its average value is 0.04; while the standard deviation value is 0.06.

User User18 has achieved the maximum value of 0.83 for closeness centrality. It has a minimum value of zero which was achieved by user User81. Both of 0.6 and 0.22 are the average and the standard deviation values for closeness centrality in this network graph.

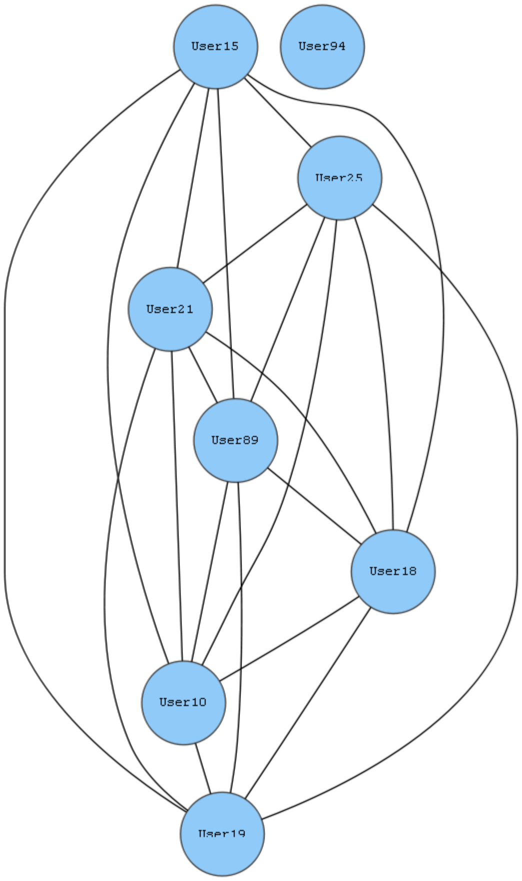


Figure 5.101: Users associations for Event UBA: New Account Use Detected.

Figure 5.101 illustrates different components of graph at event called (UBA: New Account Use Detected), where the circles represents different users as a node while the links between them vertex as a different Source Port, which reflect the relationship between different users.

The maximum value of degree of centrality of 0.86 has been realized by users User15, User25, User21, User89, User18, User10, and User19. User User94 has achieved the minimum value of zero for degree of centrality. Its average value is 0.75; while the standard deviation value is 0.28.

Betweenness centrality has a value of zero for all users in Event 'UBA : New Account Use Detected'.

Users User15, User25, User21, User89, User18, User10, and User19 have achieved the maximum value of 0.86 for closeness centrality. It has a minimum value of zero which was achieved by user User94. It has an average value of 0.75 for all users. Moreover, it has a standard deviation value of 0.28.

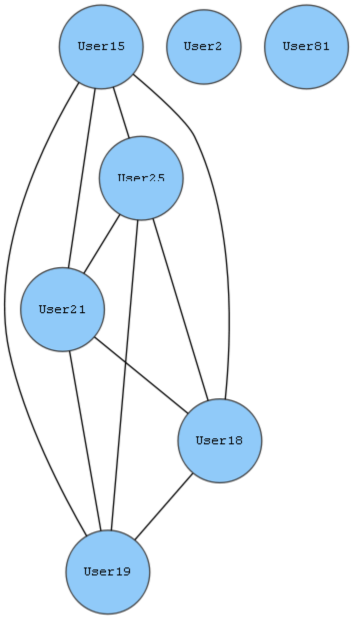


Figure 5.102: Users associations for Event UBA: User Access at Unusual Times.

Figure 5.102 illustrates different components of graph at event called (UBA: User Access at Unusual Times), where the circles represents different users as a node while the links between them vertex as a different Source Port, which reflect the relationship between different users.

Users User15, User25, User21, User18, and User19 have achieved the maximum value of 0.67 for degree of centrality. It has a minimum value of zero which was achieved by users User2, and User81. It has an average value of 0.48 for all users. And, it has a standard deviation value of 0.3.

Users in Event 'UBA: User Access at Unusual Times' have the same betweenness centrality for all of them.

Closeness centrality has a maximum value of 0.67 which was achieved by users User15, User25, User21, User18, and User19. The minimum value of zero for the same metric has been realized by users User2, and User81. Both of 0.48 and 0.3 are the average and the standard deviation values for closeness centrality in this network graph.

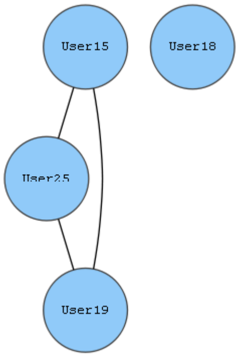


Figure 5.103: Users associations for Event Malicious Exploit.

Figure 5.103 illustrates different components of graph at event called (Event Malicious Exploit), where the circles represents different users as a node while the links between them vertex as a different Source Port, which reflect the relationship between different users.

Degree of centrality has a maximum value of 0.67 which was achieved by users User15, User25, and User19. The minimum value of zero for the same metric has been realized by user User18. Both of 0.5 and 0.29 are the average and the standard deviation values for degree of centrality in this network graph.

With regard to Event 'Malicious Exploit', all users have betweenness centrality of zero.

Value 0.67 is the maximum of closeness centrality that has been achieved by users User15, User25, and User19. User User18 has closeness centrality of zero which is at the same time the minimum in this graph for Event 'Malicious Exploit'. Its average value is 0.5; while the standard deviation value is 0.29.

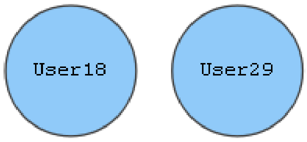


Figure 5.104: Users associations for Event Excessive Firewall Denies between Hosts.

Figure 5.104 illustrates different components of graph at event called (Excessive Firewall Denies between Hosts) where the circles represents different users as a node while the links between them vertex as a different Source Port, which reflect the relationship between different users.

With regard to Event 'Excessive Firewall Denies between Hosts', all users have degree of centrality of zero. Betweenness centrality is zero for all users in this graph. Moreover, Closeness centrality is zero for all users in this graph.

5.5.5 Event and Destination IP Address.

The network graphs in this section represent several users (nodes or vertex) at different events (hypothesis), while, links connected between them (edge) represent different Destination IP Address. In this case any two nodes or more at specific event has same Destination IP Address meant they have same type of link or connection.

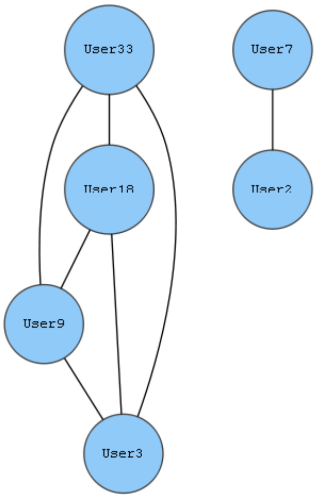


Figure 5.105: Users associations for Event General Authentication Failed.

Figure 5.105 illustrates different components of the graph at event called (General Authentication Failed), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

The maximum value of degree of centrality of 0.6 has been realized by users User33, User18, User9, and User3. Users User7, and User2 have achieved the minimum value of 0.2 for degree of centrality. Both of 0.47 and 0.19 are the average and the standard deviation values for degree of centrality in this network graph. Betweenness centrality has a value of zero for all users in Event 'General Authentication Failed'.

Users User33, User18, User9, and User3 have achieved the maximum value of 0.6 for closeness centrality. It has a minimum value of 0.2 which was achieved by users User7, and User2. Its average value is 0.47; while the standard deviation value is 0.19.

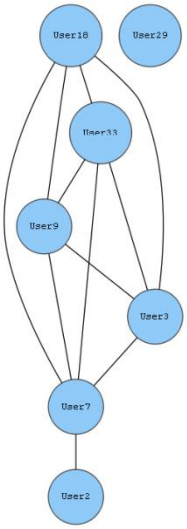


Figure 5.106: Users associations for Event User Login Failure.

Figure 5.106 illustrates different components of the graph at event called (User Login Failure), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

User User7 has achieved the maximum value of 0.83 for degree of centrality. It has a minimum value of zero which was achieved by user User29. Its average value is 0.52; while the standard deviation value is 0.29.

Value 0.27 is the maximum of betweenness centrality that has been achieved by user User7. Users User18, User33, User9, User3, User2, and User29 have betweenness centrality of zero which is at the same time the minimum in this graph for Event 'User Login Failure'. Both of 0.04 and 0.09 are the average and the standard deviation values for betweenness centrality in this network graph.

Closeness centrality has a maximum value of 0.83 which was achieved by user User7. The minimum value of zero for the same metric has been realized by user User29. It has an average value of 0.58 for all users. Moreover, it has a standard deviation value of 0.26.

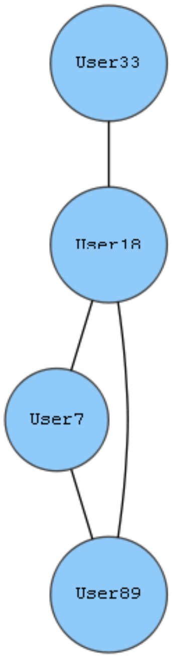


Figure 5.107: Users associations for Event General Authentication Successful.

Figure 5.107 illustrates different components of the graph at event called (General Authentication Successful), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

Degree of centrality has a maximum value of one which was achieved by user User18. The minimum value of 0.33 for the same metric has been realized by user User33. It has an average value of 0.67 for all users. And, it has a standard deviation value of 0.24.

User User18 has betweenness centrality of 0.67 which is at the same time the maximum in this graph for Event 'General Authentication Successful'. Value zero is the minimum the same measure that has been achieved by users User33, User7, and User89. Its average value is 0.17; while the standard deviation value is 0.29. Value one is the maximum of closeness centrality that has been achieved by user User18. User User33 has closeness centrality of 0.6 which is at the same time the minimum in this graph for Event 'General Authentication Successful'. Both of 0.78 and 0.14 are the average and the standard deviation values for closeness centrality in this network graph.

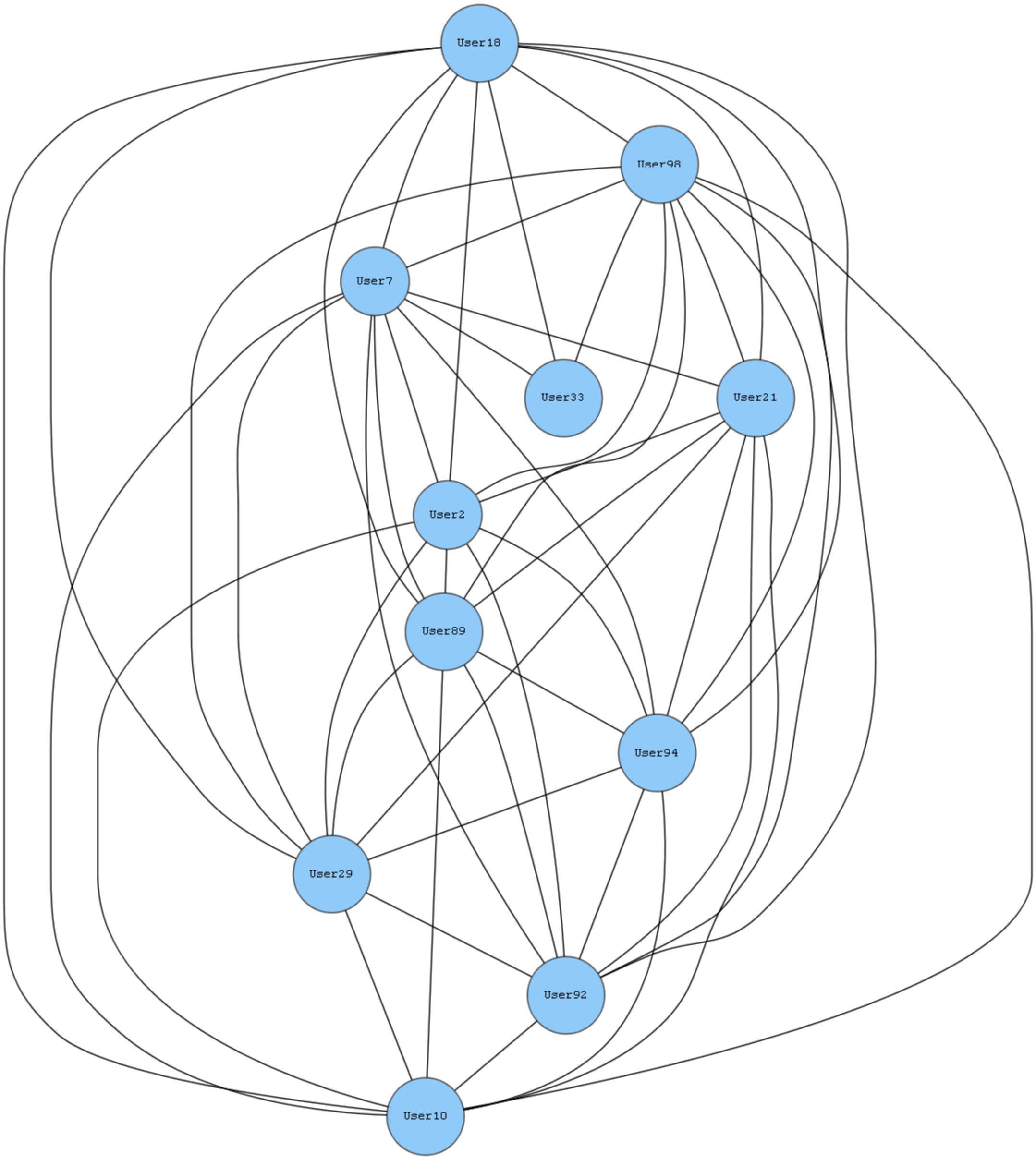


Figure 5.108: Users associations for Event Admin Login Successful.

Figure 5.108 illustrates different components of the graph at event called (Admin Login Successful), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

Users User18, User98, and User7 have degree of centrality of one which is at the same time the maximum in this graph for Event 'Admin Login Successful'. Value 0.3 is the minimum of the same metric that has been achieved by user User33. Its average value is 0.87; while the standard deviation value is 0.19.

Users User18, User98, and User7 have achieved the maximum value of 0.05 for betweenness centrality. It has a minimum value of zero which was achieved by users User33, User21, User2, User89, User94, User29, User92, and User10. Both of 0.01 and 0.02 are the average and the standard deviation values for betweenness centrality in this network graph.

The maximum value of closeness centrality of one has been realized by users User18, User98, and User7. User User33 has achieved the minimum value of 0.59 for the same metric. It has an average value of 0.9 for all users. Moreover, it has a standard deviation value of 0.11.

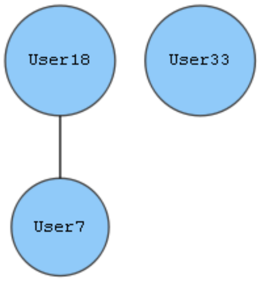


Figure 5.109: Users associations for Event Multiple login failure.

Figure 5.109 illustrates different components of the graph at event called (Multiple login failure), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

The maximum value of degree of centrality of 0.5 has been realized by users User18, and User7. User User33 has achieved the minimum value of zero for degree of centrality. It has an average value of 0.33 for all users. And, it has a standard deviation value of 0.24.

Betweenness centrality has a value of zero for all users in Event 'Multiple login failure'.

Users User18, and User7 have achieved the maximum value of 0.5 for closeness centrality. It has a minimum value of zero which was achieved by user User33.

Both of 0.33 and 0.24 are the average and the standard deviation values for closeness centrality in this network graph.

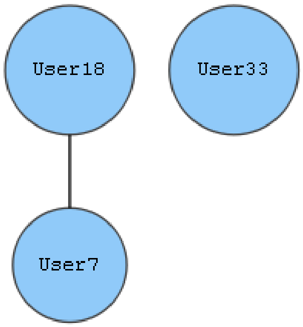


Figure 5.110: Users associations for Event Brute Force.

Figure 5.110 illustrates different components of the graph at event called (Event Brute Force), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

Users User18, and User7 have achieved the maximum value of 0.5 for degree of centrality. It has a minimum value of zero which was achieved by user User33. Both of 0.33 and 0.24 are the average and the standard deviation values for degree of centrality in this network graph.

Users in Event 'Brute Force' have the same betweenness centrality for all of them.

Closeness centrality has a maximum value of 0.5 which was achieved by users User18, and User7. The minimum value of zero for the same metric has been realized by user User33. Its average value is 0.33; while the standard deviation value is 0.24.

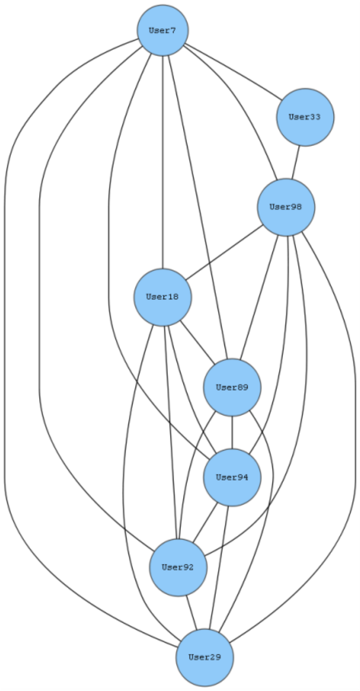


Figure 5.111: Users associations for Event User Login Success.

Figure 5.111 illustrates different components of the graph at event called (User Login Success), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

Degree of centrality has a maximum value of one which was achieved by users User7, and User98. The minimum value of 0.29 for the same metric has been realized by user User33. Its average value is 0.82; while the standard deviation value is 0.21.

Users User7, and User98 have betweenness centrality of 0.12 which is at the same time the maximum in this graph for Event 'User Login Success'. Value zero is the minimum the same measure that has been achieved by users User33, User18, User89, User94, User92, and User29. Both of 0.03 and 0.05 are the average and the standard deviation values for betweenness centrality in this network graph.

Value one is the maximum of closeness centrality that has been achieved by users User7, and User98. User User33 has closeness centrality of 0.58 which is at the same time the minimum in this graph for Event 'User Login Success'. It has an average value of 0.87 for all users. Moreover, it has a standard deviation value of 0.12.

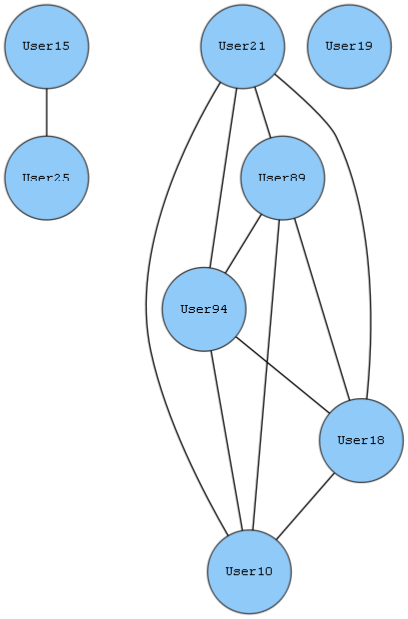


Figure 5.112: Users associations for Event UBA: New Account Use Detected.

Figure 5.112 illustrates different components of the graph at event called (UBA: New Account Use Detected), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

Value 0.57 is the maximum of degree of centrality that has been achieved by users User21, User89, User94, User18, and User10. User User19 has degree of centrality of zero which is at the same time the minimum in this graph for Event 'UBA: New Account Use Detected'. It has an average value of 0.39 for all users. And, it has a standard deviation value of 0.23.

Betweenness centrality is zero for all users in this graph.

Users User21, User89, User94, User18, and User10 have closeness centrality of 0.57 which is at the same time the maximum in this graph for Event 'UBA: New Account Use Detected'. Value zero is the minimum for the same metric that has been achieved by user User19. Both of 0.39 and 0.23 are the average and the standard deviation values for closeness centrality in this network graph.

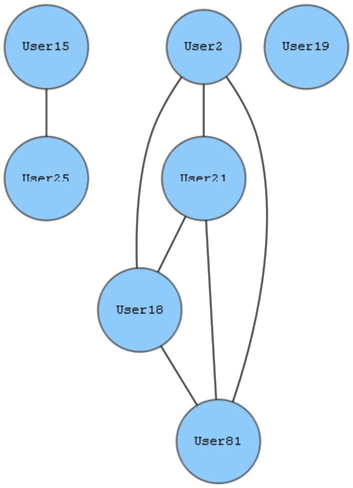


Figure 5.113: Users associations for Event UBA : User Access at Unusual Times.

Figure 5.113 illustrates different components of the graph at event called (UBA: User Access at Unusual Times), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

Users User2, User21, User18, and User81 have degree of centrality of 0.5 which is at the same time the maximum in this graph for Event 'UBA: User Access at Unusual Times'. Value zero is the minimum of the same metric that has been achieved by user User19. Both of 0.33 and 0.2 are the average and the standard deviation values for degree of centrality in this network graph.

In this graph, all users acheived betweenness centrality of zero.

The maximum value of closeness centrality of 0.5 has been realized by users User2, User21, User18, and User81. User User19 has achieved the minimum value of zero for the same metric. Its average value is 0.33; while the standard deviation value is 0.2.

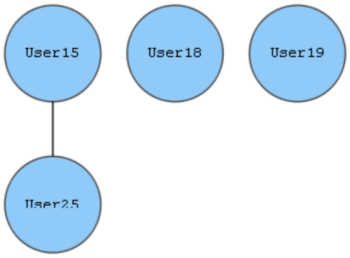


Figure 5.114: Users associations for Event Malicious Exploit.

Figure 5.114 illustrates different components of the graph at event called (Malicious Exploit), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

The maximum value of degree of centrality of 0.33 has been realized by users User15, and User25. Users User18, and User19 have achieved the minimum value of zero for degree of centrality. Its average value is 0.17; while the standard deviation value is 0.17.

Betweenness centrality has a value of zero for all users in Event 'Malicious Exploit'.

Users User15, and User25 have achieved the maximum value of 0.33 for closeness centrality. It has a minimum value of zero which was achieved by users User18, and User19. It has an average value of 0.17 for all users. Moreover, it has a standard deviation value of 0.17.

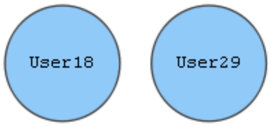


Figure 5.115: Users associations for Event Excessive Firewall Denies between Hosts.

Figure 5.115 illustrates different components of the graph at event called (Excessive Firewall Denies between Hosts), where the circles represents different users as a node while the links between them vertex as a different Destination IP Address, which reflect the relationship between different users.

Degree of centrality has a value of zero for all users in Event 'Excessive Firewall Denies between Hosts'.

Users in Event 'Excessive Firewall Denies Between Hosts' have the same betweenness centrality for all of them.

Users in Event 'Excessive Firewall Denies Between Hosts' have the same closeness centrality for all of them.

5.5.6 Event and Destination Port.

The network graphs in this section represent several users (nodes or vertex) at different events (hypothesis), while links connected between them (edge) represent different destination port. In this case any two nodes or more at specific event has same destination port meant they have same type of link or connection.

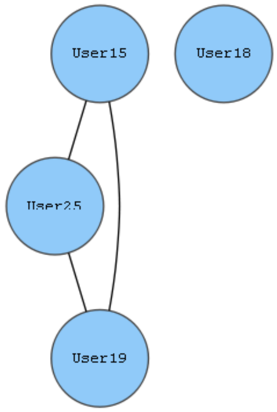


Figure 5.116: Users associations for Event Malicious Exploit.

Figure 5.116 illustrates different components of the graph at event called (Malicious Exploit), where the circles represents different users as a node while the links between them vertex as a different Destination Port, which reflect the relationship between different users.

Value 0.67 is the maximum of degree of centrality that has been achieved by users User15, User25, and User19. User User18 has degree of centrality of zero which is at the same time the minimum in this graph for Event 'Malicious Exploit'. It has an average value of 0.5 for all users. And, it has a standard deviation value of 0.29.

Betweenness centrality is zero for all users in this graph.

Users User15, User25, and User19 have closeness centrality of 0.67 which is at the same time the maximum in this graph for Event 'Malicious Exploit'. Value zero is the minimum for the same metric that has been achieved by user User18. Both of 0.5 and 0.29 are the average and the standard deviation values for closeness centrality in this network graph.

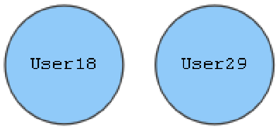


Figure 5.117: Users associations for Event Excessive Firewall Denies Between Hosts.

Figure 5.117 illustrates different components of the graph at event called (Excessive Firewall Denies between Hosts), where the circles represents different users as a node while the links between them vertex as a different Destination Port, which reflect the relationship between different users. Degree of centrality is zero for all users in this graph. In this graph, all users achieve betweenness centrality of zero and all users achieve closeness centrality of zero.

5.6 Locating the Center.

Locating the center in the social network will be based on the calculated centrality values from the previous network graphs.

User	Hour	Magnitude	Event	Average
User21	3.477	2.407	0.396	2.093
User33	1.117	1.993	0.436	1.182
User18	3.899	3.123	0.941	2.654
User9	0.339	0.997	0.159	0.498
User2	2.617	2.262	0.421	1.766
User3	0.809	1.088	0.256	0.718
User7	2.678	2.172	0.732	1.861
User98	2.306	1.214	0.275	1.265
User15	0.455	0.942	0.158	0.518
User25	0.455	0.942	0.158	0.518
User29	3.556	2.065	0.419	2.013
User89	2.36	1.572	0.417	1.45
User81	0.364	0.232	0.1	0.232
User94	2.055	1.365	0.309	1.243
User11	0.373	0.465	0.067	0.302
User19	0.227	0.91	0.127	0.421
User92	0.856	1.048	0.256	0.72
User10	0.416	0.969	0.21	0.532

Table 5-1: Average degree of centrality of all users.

Hour category has an average degree of centrality of 0.312 and standard deviation of 0.838. Its maximum observed value is 3.899 at user User18. Also, its minimum observed value is zero at user User_NA. On the other hand, Magnitude category has an average degree of centrality of 0.283 and standard deviation of 0.656. Its maximum observed value is 3.123 at user User18. Also, its minimum observed value is zero at user User_NA. Furthermore, Event category has an average degree of centrality of 0.064 and standard deviation of 0.161. Its maximum observed value is 0.941 at user User18. Likewise, its minimum observed value is zero at user User_NA. Finally, overall average degree of centrality has an average of 0.22 and standard deviation of 0.542. Its maximum observed value of this average is 2.654 at user User18. And, its minimum observed value is zero at user User_NA.

User	Hour	Magnitude	Event	Average
User21	0.118	0.04	0.002	0.053
User33	0.021	0.001	0.0	0.007
User18	0.605	0.144	0.033	0.261
User9	0.0	0.0	0.001	0.0
User2	0.019	0.024	0.001	0.015
User3	0.055	0.014	0.011	0.027
User7	0.104	0.248	0.011	0.121
User98	0.114	0.12	0.019	0.084
User29	0.152	0.072	0.003	0.076
User89	0.025	0.028	0.004	0.019
User94	0.069	0.004	0.001	0.025
User92	0.015	0.0	0.0	0.005
User10	0.0	0.0	0.0	0.0

Table 5-2: Average betweenness centrality of all users.

Moving to betweenness centrality, Hour category has an average betweenness centrality of 0.014 and standard deviation of 0.068. Its maximum observed value is 0.605 at user User18. Similarly, its minimum observed value is zero at user User_NA. In addition, Magnitude has an average betweenness centrality of 0.008 and standard deviation of 0.033. Its maximum observed value is 0.248 at user User7. Correspondingly, its minimum observed value is zero at user User_NA. Moreover, Event category has an average betweenness centrality of 0.001 and standard deviation of 0.004. Its maximum observed value is 0.033 at user User18. Also, its minimum observed value is zero at user User_NA. The overall average betweenness centrality has an average of 0.008 and standard deviation of 0.032. And, its maximum observed value of this average is 0.261 at user User18. Also, its minimum observed value is zero at user User_NA.

User	Hour	Magnitude	Event	Average
User21	3.674	2.503	0.4	2.192
User33	1.241	2.327	0.47	1.346
User18	3.976	3.169	0.947	2.697
User9	0.4	1.075	0.16	0.545
User2	2.803	2.345	0.437	1.862
User3	0.881	1.123	0.256	0.754
User7	2.788	2.207	0.741	1.912
User98	2.406	1.221	0.277	1.301
User15	0.462	1.069	0.158	0.563
User25	0.462	1.069	0.158	0.563
User29	3.703	2.294	0.426	2.141
User89	2.563	1.583	0.425	1.524
User81	0.397	0.304	0.111	0.271
User94	2.205	1.391	0.313	1.303
User11	0.441	0.543	0.078	0.354
User19	0.317	1.045	0.127	0.496
User92	0.922	1.081	0.261	0.755
User10	0.446	0.981	0.226	0.551

Table 5-3: Average closeness centrality of all users.

For closeness centrality, Hour has an average closeness centrality of 0.331 and standard deviation of 0.879. Its maximum observed value is 3.976 at user User18. Also, its minimum observed value is zero at user User_NA. Its Magnitude has an average closeness centrality of 0.3 and standard deviation of 0.691. The maximum observed value for this category is 3.169 at user User18. As well, its minimum observed value is zero at user User_NA. Besides, Event has an average closeness centrality of 0.066 and standard deviation of 0.164. Its maximum observed value is 0.947 at user User18. Moreover, its minimum observed value is zero at user User_NA. The overall average closeness centrality has an average of 0.232 and standard deviation of 0.567. Its maximum observed value of this average is 2.697 at user User18. And, its minimum observed value is zero at user User_NA.

From these results, we can conclude that **User18** plays a central role in malicious activities networks.

- Final results:

It is clearly observed from both the case study results which generated from Lab and the results extracted from Centrality algorithm (Degree, Closeness and Betweenness) calculation that the both results showing **User18** who is playing a main actor role in malicious activities within the networks while **User 7 and User 21** who is playing the role of reprehensive as it show in the table below:

User 18	Hour	Magnitude	Event	Average
Average degree of centrality	3.899	3.123	0.941	2.654
Average betweenness centrality	0.605	0.144	0.033	0.261
Average closeness centrality	3.976	3.169	0.947	2.697

Table 5-4: Average closeness, Betweenness and Degree of centrality of User 18.

User 7	Hour	Magnitude	Event	Average
Average degree of centrality	2.678	2.172	0.732	1.861
Average betweenness centrality	0.104	0.248	0.011	0.121
Average closeness centrality	2.788	2.207	0.741	1.912

Table 5-5: Average closeness, Betweenness and Degree of centrality of User 7.

User 21	Hour	Magnitude	Event	Average
Average degree of centrality	3.477	2.407	0.396	2.093
Average betweenness centrality	0.118	0.04	0.002	0.053
Average closeness centrality	3.674	2.503	0.4	2.192

Table 5-6: Average closeness, Betweenness and Degree of centrality of User 21.

The Labs experiments showing the same results are shown in the next figure.

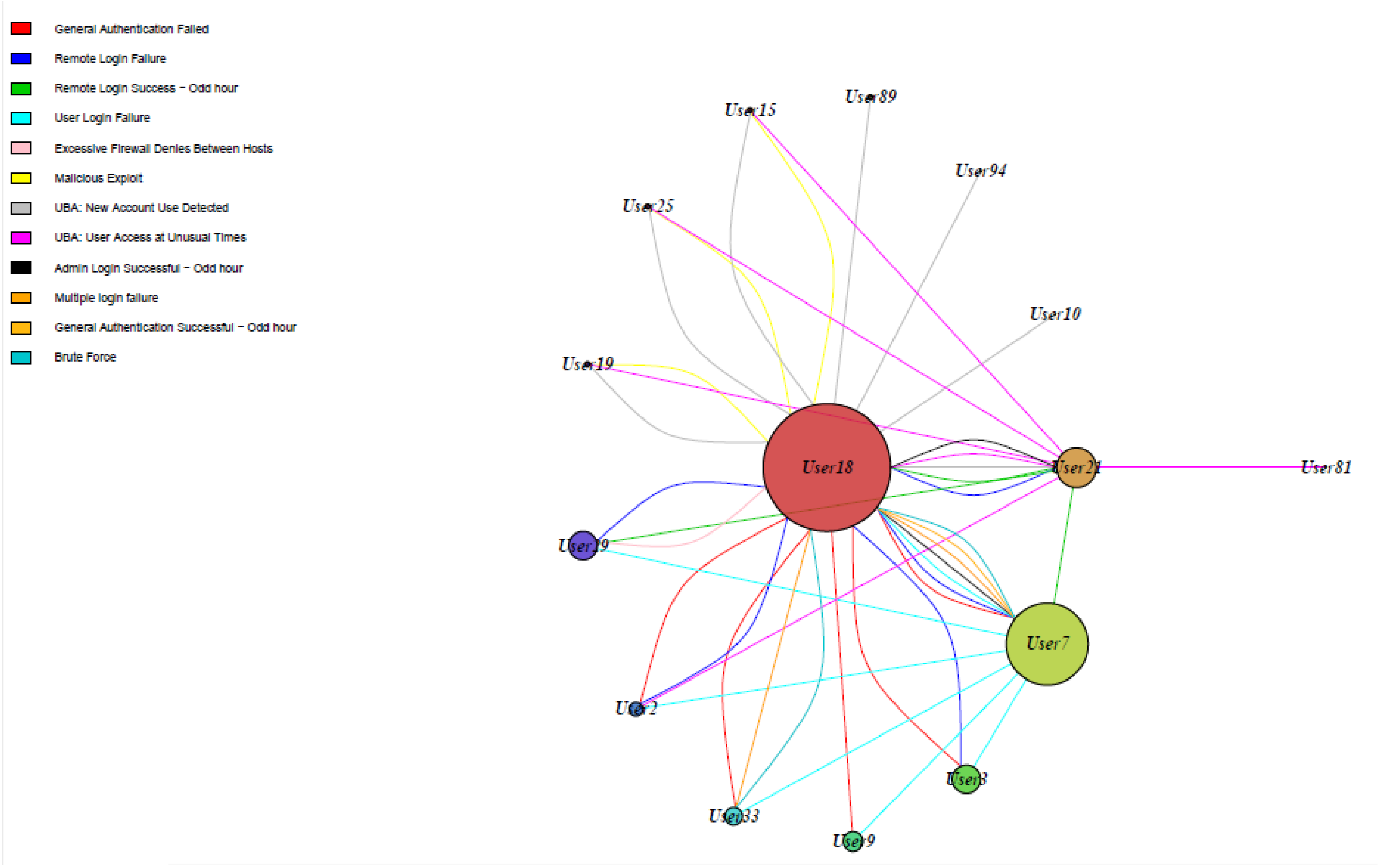

General Authentication Failed
Remote Login Failure
Remote Login Success – Odd hour
User Login Failure
Excessive Firewall Denies Between Hosts
Malicious Exploit
UBA: New Account Use Detected
UBA: User Access at Unusual Times
Admin Login Successful – Odd hour
Multiple login failure
General Authentication Successful – Odd hour
Brute Force
User15
User89
User94
User25
User10
User19
User18
User21
User81
User19
User7
User2
User8
User33
User9

Figure 5.118: Final Lab results.

Chapter 6: Conclusions and Recommendation for Future Work.

This Chapter introduces the conclusions of the study, briefly summarizing the achievements in studying the research question and the success in meeting the study objectives. The contribution to the world of education and knowledge is also explained and the directions for future research are specified.

6.1 Overview.

In today's world most of the world government, business and social communities are moving towards converting their crucial core services to online services, which increases the customer satisfaction, saving time and efforts. On the other hand, these crucial services depend mainly on **Critical Information Infrastructures** (CIIs) and any type of disruption could lead to service shortage, affecting directly the reputation of the organization.

Moreover, most of the servicing organizations focus on outsiders to protect their critical information assets rather than on insiders because of trust culture or other relevant reasons. Due to the recent events and disputes going on in this area at present, any insider employee can adapt malicious aims and goals from outside enemies, who are tempting him with money. He will form in turn a network to achieve malicious goals aimed at harming the organization. Forming this network group could take months or years to achieve loyalty to the network group and aims. Because the members are behaving in a hidden manner, it makes it extremely difficult to discover group intentions just by observing.

The literature review in the field of **Critical information Infrastructure Protection** (CIIP) and solution lead to the socio-organizational-technical theory called **Actor Network Theory** (ATN), which reflects exactly the scenario mentioned in the previous paragraph, which was adapted in this research. ANT is also known as enrolment theory or the sociology of translation. It does not explain why a network exists, but is suitable for analyzing the components of an actor networks and explaining how they are formed, how they fill gaps, assign responsibilities, take roles, etc.

The intentions and the unseen actor network malicious activities are hidden in a kind of a black box. In order to analyze them it was very impotent to find a technique that can extract and reveal all behaviors. From **Information Technology** (IT) perspective the best solution was to use the security event logs from different ICT components involved in the network operation. Such log files contain traces of all types of activities, time stamps, errors, IP addresses and many other useful pieces of information.

The proposed framework is built using a number of components with the most important being **User Behavior Analytic** (UBA) software and **Security Information Event Management** (SIEM) software. They are widely used for security analysis by security specialist worldwide. These two tools are used within the framework to collected both malicious and non-malicious activities and to store them in separate **User Profiles** for each user identified in the data sets.

The main issue in this research was how to analyze these malicious activities in order to find the links between different members of ANT group. Key for addressing this issue was the adoption of the ATN concept of a main user or actor called *Obligatory Passage Point* (OPP), who is characterized by a unique position within the network of agents, meaning that all activities should pass through him just to be sure that the planned aims are going in the correct way. Thus, OPP is the most active and interconnected user within the actor network group. The literature review found that the analysis can be further extended by another analytical tool, namely the **Graph Theory**, which was adopted to identify the OPP by analyzing the positions of different agents within the network.

Graph Theory (GT) is a theory used in applied mathematics and computer science to model pairwise relations between different nodes within a network. In GT the network analysis the concept of centrality plays very important role. GT considers several measures of centrality and provides algorithms for calculating them. Based on estimation of the degree of centrality the theory divides the relationships between the nodes of a network into four categories: *betweenness*, *closeness* to centrality, *eigenvector* of centrality and *degree* of centrality. Three of these measures are matching the concept of OPP in ANT, namely betweenness, closeness to centrality, and degree of centrality, which gave us the core key for the analysis in search for the main actor of the malicious network.

The core pre-requisite of the study was the availability of the data set of events, which was created in the form of an Excel spreadsheet extracted during normal work hour from live data over an extended period of time. The data set contains large variety of information but three main characteristics were analyzed, namely the *time*, *magnitude* and *event type*.

6.2 Objectives.

The initial aim of the research was to find the main actor who encourages other insider users to become involved in malicious activities. The next section explains how the study objectives were achieved and summarizes the conclusions that have been derived from the research.

6.2.1 Research Objective one:

Finding out the main actor who exploits the physical, psychological, personal, financial and historical state of some insiders to form a malicious network

As a final result the study found all malicious network members and different related malicious events performed by each member at specific time. The analysis of different measures led to find out the main actor who forms the network and who involves other users in different malicious activities which is a clear evidence of achieving the objective successfully.

6.2.2 Research Objective two:

Filling the gap in security policies and the guidelines for their implementation by monitoring the logs and auditing the applications

The framework can clearly identify the most experienced users who enjoy legitimate and privileged access to the network resources and therefore have good understanding of all gaps within the policies and guideline. Based on their expert knowledge the security policies can be tightened up and the corresponding guidelines can be put in place in order to prevent their exploitation for malicious purpose.

6.2.3 Research Objective three:

Improving the security information sharing to assist the information security specialist in investment decisions.

The results from different aspects of this study show different malicious activities from both outsiders and insiders. The estimation of the size and the density of both inside and outside attacks which affect the organization can help the security specialist in taking investment decision in order to neutralize such attacks and to protect the assets of the organization.

6.3 Contribution to Knowledge.

During the literature review it was clearly recognized that many researchers, especially the researchers who are doing research in the field of information security, are facing problem in finding real data containing information about malicious activities. This data is very expensive to collect and costly to generate due to the technological complexity and the need for dedicated setup of a specific Lab.

The research produced a new framework for security analysis built upon two different security technologies, namely UBA and SIEM. These two technologies are very expensive to implement or setup and this was leading to a different research approach, but through this research it was proven that the combination of the two technologies is the best source for security analysis.

By successful construction of the framework the study proved the possibility to complement the ANT and GT theories in order to empower the security analysis. This combined theory might also be useful in other areas of knowledge where the analysis of the leadership is of key importance for the success of the enterprise - project management, public administration, business management and politics.

6.4 Future Work

In many respects, it is our belief that this research has provided a starting point for the future use of socio-technical methodologies for security analytics by combining ANT and GT. The study has produced a clear understanding of the socio-technical methods using which the proposed framework was developed. This section summarizes in brief the possible continuations of this work in the future:

6.4.1 Automation

The research study used different techniques to proof the conceptual basis of the proposed framework for minimizing the damages and for protecting the critical information infrastructures from insiders. The tools which were used within this research were operated manually, especially the creation and the analysis of multiple graphs, which makes the work more complicated, tedious and time consuming. This limitation can be resolved by automating the process using suitable software applications. They can automate the calculation of various metrics used in the analysis as well as the creation of the corresponding graphs.

The automation of the entire framework can be achieved by integrating several software applications, developed specifically for collecting data, for filtering and identification of the relevant information, for analyzing the security patterns, for displaying the potential threats and providing reports which would make the process more easy and efficient. This would give the network and system administrators, security analysts and other parties an integral overview of the organization network that helps eliminating potential security breaches, defending from malicious activities and protecting critical assets.

6.4.2 Testing the Framework with More Algorithms

The proposed framework is based on a limited number of algorithms for calculating various measures using formulas from Graph Theory, but the framework is not limited to them and can be extended further by accounting more factors and incorporating more algorithms.

In this study the framework structure and the results totally depend on one single data measure, centrality, which can be measured in many different ways, while the calculations used in this research were produced only for estimating the degree of closeness and betweenness. By accounting more measures the accuracy of the results can be improved. By using different algorithms the sensitivity of the calculations can be also reduced.

References:

Omar, Marwan. "Insider Threats: Detecting and Controlling Malicious Insiders." New Threats and Countermeasures in Digital Crime and Cyber Terrorism. IGI Global, 2015.

Harris Poll, VORMETRIC INSIDER THREAT REPORT, Trends and Future Directions in Data Security, Vormetric Data Security, GLOBAL EDITION, USA, 2015.

Privileged User Abuse & The Insider Threat, Commissioned by Raytheon Company, Independently conducted by Ponemon Institute LLC, 2014.

Cziner et al, Critical Information Infrastructure Protection in the Baltic Sea Area: The Case of TETRA, Helsinki University of Technology, Communications Laboratory, 2007.

Omar , Insider Threats: Detecting and Controlling Malicious Insiders, New Threats and Countermeasures in Digital Crime and Cyber Terrorism, Nawroz University, Iraq, 2015.

Lyzhenkov , Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, Co-ordinator of Activities to Address Transnational Threats, Organization for Security and Co-Operation in Europe, 2013.

Roberto Baldoni, Critical Infrastructure Protection: Threats, Attacks and Countermeasures, TENACE Project Coordinator Center of Cyber Intelligence and Information Security Università degli Studi di Roma “La Sapienza”, 2014.

European union directive 2008/114/ec, 2008.

Ted G Lewis, Critical Infrastructure Protection in Homeland Security, ISBN-13: 978-0-471-78628-3 (2006)

CIR Strategy 2015 ,Critical Infrastructure Resilience strategy: PLAN, Commonwealth of Australia, 2015.

Novotný and Rostek, Perspective of Cross-Cutting Criteria as a Major Instrument to Determination of Critical Infrastructure in the Czech Republic, INTERNATIONAL DOCTORAL SEMINAR 2014, Zielona Góra, Poland, 2014.

Abgarowicz et al, Critical Infrastructure Security – the ICT Dimension, The Kosciuszko Institute, Poland, 2014.

Panek, Basic categories and taxonomies in studies of standard and quality of living, Poland, 2014.

Bennett and Gupta, Dealing in Security understanding vital services and how they keep you safe, 2010, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf.

Luiijf and Kernkamp, Sharing Cyber Security Information Good Practice Stemming from the Dutch Public-Private Participation Approach, Global Conference on Cyber Space (GCCS), 2015

Brocklehurst, Cyberterrorists Attack on Critical Infrastructure Could Be Imminent, Featured articles, THE STATE OF SECURITY, TRIPWIRE, 2015.

Pradhan, Cyber security: Need for an overall national cyber strategy, News, Blogs, India Blogs, Cyber security: Need for an overall national cyber strategy, India, 2016.

Gregory et al, Threats Impacting the Nation, GAO-09-661T Information Security, United States Government Accountability Office, USA, 2012.

Hon George Brandis ,Managing the insider threat to your business, A personnel security handbook, Commonwealth of Australia, Australia, 2014.

McAfee, McAfee Labs Threats Report December 2016, Intel Security, USA, 2016.

Wilshusen, Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies, INFORMATION SECURITY, United States Government Accountability Office, USA, 2015.

Nurse et al, Understanding Insider Threat: A Framework for Characterising Attacks, IEEE Security and Privacy Workshops, 2014.

Khazanchi et al, Information Availability. Handbook of Research on Information Security and Assurance. (2008).

Qadir and Quadri, Information Availability: An Insight into the Most Important Attribute of InformationSecurity, Journal of Information Security, India, 2016.

Zaballos and Jeun, Best Practices for Critical Information Infrastructure Protection (CIIP), Experiences from Latin America and the Caribbean and Selected Countries, Felipe Herrera Library, US, 2016.

Alcaraz, Zeadally, Critical Infrastructure Protection: Requirements and Challenges for the 21st Century, In International Journal of Critical Infrastructure Protection (IJCIP), vol. 8, Elsevier Science, 2015.

NTRO, Guidelines for Protection of National Critical Information Infrastructure, National Critical Information Infrastructure Protection Centre, National Technical Research Organization, VERSION 1.0, Government of India, 2013.

Pederson et al, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, The INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, US, 2006.

CascEff , Modelling of dependencies and cascading effects for emergency management in crisis situations SP Technical Research Institute of Sweden, 2016.

Stergiopoulos et al, Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures, International Journal of Critical Infrastructure Protection Volume 12, March 2016.

Luiijf et al, The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, The Global Forum on Cyber Expertise (GFCE), Netherlands, 2016)

KANG, A Critical cogitation on Critical Inform ation Infrastructure A Critical cogitation on Critical Information Infrastructure, Journal of Security Engineering, 2008.

Abgarowicz et al, Critical Infrastructure Security – the ICT Dimension, The Kosciuszko Institute Poland, 2014.

HÄMMERLI, PROTECTING CRITICAL INFRASTRUCTURE IN THE EU, CENTRE FOR EUROPEAN POLICY STUDIES, Brussels, ISBN: 978-94-6138-070-8, 2010.

Brdiczka, DECODING THE INSIDER THREAT, Insider Threats in critical US Infrastructure – Let me blow you up, computer world, Security, USA, 2014.

Silowash et al, Common Sense Guide to Mitigating Insider Threats 4 th Edition, CERT Program, Software Engineering Institute, Carnegie Mellon University, USA, 2012.

Gücüyener, Human Factor in Critical Infrastructure Security: The Insider Threat, Hazar Institute, Turkey , 2015.

Smith, Mitigating malicious insider cyber threat, Technical Report RHUL–ISG–2015–12 (RHUL–MA–2015–12), UK, 2015.

Cappelli et al, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft,Sabotage, Fraud). NJ, Addison-Wesley, 2012.

Noonan and Archuleta, The Insider Threats To Critical Infrastructures, Final Report And Recommendations, The National Infrastructure Advisory Council (NIAC),US,2008.

Munshi et al, Insider Threat Behavior Factors: A comparison of theory with reported incidents, 45th Hawaii International Conference on System Sciences (HICSS), USA, 2012.

Moore et al, The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures, Technical Report CMU/SEI-2008-TR-009, ESCTR-2008-009, Carnegie Mellon University, USA, 2008.

Hedstrom et al, Using Actor Network Theory to Understand Information Security Management, Kai Rannenberg; Vijay Varadharajan; Christian Weber. Security and Privacy - Silver Linings in the Cloud, IFIP Advances in Information and Communication Technology, HAL, Sweden, , 2010.

Huang and Hsieh, Protect Critical Information Infrastructure Systems in Financial and Healthcare Sectors: Actor Network Theory, The Sixth International Conference on Systems, ICONS, 2011.

Latour, Reassembling the Social: An Introduction to Actor-Network-Theory, Oxford: Oxford UP, 2005.

González, The use of Actor-Network Theory and a Practice-Based Approach to understand online community participation, A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy, The University of Sheffield, 2013.

Gunawong and Gao, Understanding eGovernment Failure: An Actor-Network Analysis of Thailand’s Smart ID Card Project, Pacific Asia Conference on Information Systems (PACIS), PACIS 2010 Proceedings, 2010.

Jessen et al, Games as Actors - Interaction, Play, Design, and Actor Network Theory, International Journal on Advances in Intelligent Systems, Denmark, 2017.

Richerd Heekes, Development Studies Research and Actor-Network Theory, Centre for Development Informatics, Institute for Development Policy and Management, SED, UK.2013.

Bueger and Stockbruegger, Actor-Network Theory: Objects and Actors, Networks and Narratives, Technology and World Politics: An Introduction, edited by Daniel R. McCarthy, Abingdon: Routledge, forthcoming, 2016.

Tatnall and Gilding, Actor-Network Theory and Information Systems Research, 10th Australasian Conference on Information Systems, 1999.

Leah and Horowitz, Translation alignment: actor-network theory and the power dynamics of alliance in New Caledonia, a Radical Journal of Geography (*Antipode*), (2012).

Jessen et al, Games as Actors - Interaction, Play, Design, and Actor Network Theory, International Journal on Advances in Intelligent Systems, 2014.

Walsham and Sahay, GIS for District-Level Administration in India: Problems and Opportunities, MIS Quarterly, 1999.

Danchao Hu, Using actor-network theory to understand inter-organizational network aspects for strategic information systems planning, Master thesis Business information technology School of Management and Governance (SMG), University of Twente Enschede, The Netherlands, 2011.

Elbanna, Actor Network Theory and IS Research, in Handbook of Research on Contemporary Theoretical Models in Information Systems, eds, IGI Global, 2009.

Cardella and Shaikh, From epistemology to ontology: Challenging the constructed truth and ANT, *Information Technology and People*, (2006).

Mahring et al, Trojan actor-networks and swift translation : bringing actor-network theory to IT project escalation studies, Information Technology & People, (2004).

M. Aanestad, The Camera as an Actor: Design-in-Use of Telemedicine Infrastructure in Surgery, Computer Supported Cooperative Work 12, Netherland, 2003.

Raila HEKKANEN, Fields, Networks and Finnish prose: A Comparison of Bourdieusian Field Theory and Actor-Network Theory in Translation Sociology, the CETRA Research Seminar in Translation Studies, Finland, 2004.

Latour, On actor-network theory. A few clarifications plus more than a few complications, CSI-Paris/Science Studies-San Diego, 1996.

Brey, Artifacts as Social Agents in Inside the Politics of Technology. Agency and Normativity in the CoProduction of Technology and Society, Amsterdam University, 2005.

Callon Michel, The Sociology of an Actor-Network: The Case of the Electric Vehicle. In Callon, Law & Rip Mapping the Dynamics of Science and Technology: Sociology of Science in the real World, MacMillan Press, London, 1986.

Thapa, The Role of ICT Actors and Networks in Development: The Case Study of a Wireless Project in Nepal, The Electronic Journal on Information Systems in Developing Countries, 2011.

Latour Bruno, Where are the Missing Masses? The Sociology of a Few Mundane Artifacts, Shaping Technology/Building Society: Studies in Sociotechnical Change, Cambridge: MIT Press, (1992).

Stalder, Actor-Network-Theory and Communcation Networks: Toward Convergence. Published by the Faculty of Information Studies, University of Toronto, 1997.

Esnault et al, On the Use of Actor-Network Theory for developing Web Services Dedicated to Communities of Practice. First European Conference on Technology Enhanced Learning, Crete, Greece, CEUR, 2006.

Akrich, The De-scription of Technical Objects, In Wiebe Bijker and John Law, eds, Shaping Technology/Building Society: Studies in Sociotechnical Change, Cambridge, MA: MIT Press, 1992.

Law, Actor Network Theory and Material Semiotics, in The New Blackwell Companion to Social Theory (ed B. S. Turner), Wiley-Blackwell, Oxford, UK, 2008.

Gunawong, Understanding eGovernment Failure: An Actor-Network Analysis of Thailand's Smart ID Card Project, Pacific Asia Conference on Information Systems, PACIS 2010, Taipei, Taiwan, 2010.

Silic, Using ANT to understand dark side of computing - Computer underground impact *on* eSecurity in the dual use context. University of St Gallen Institute of Information Management, Switzerland, 2015.

Iglesias and Antonio, Creating evolving user behavior profiles automatic, IEEE Transactions on Knowledge and Data Engineering, (May 2012).

Verizon, 2017-Data-Breach-Investigations-Report, Verizon Enterprise, 2017.

Bourbousson, J., R Kiouak, M., & Eccles, D, W, (2015), The dynamics of team coordination: a social network analysis as a window to shared awareness, European Journal of Work and Organizational Psychology, 24(5), 742-760.

Burt, R, S., Kilduff, M., & Tasselli, S, (2013), Social network analysis: Foundations and frontiers on advantage, Annual review of psychology, 64, 527-547.

Crossley, N., Bellotti, E., Edwards, G., Everett, M, G., Koskinen, J., & Tranmer, M, (2015), Social network analysis for ego-nets: Social network analysis for actor-centred networks, Sage.

Lieberman, M, (2014), Visualizing big data: Social network analysis, In Digital research conference (pp, 1-23).

Luo, Q., & Zhong, D, (2015), Using social network analysis to explain communication characteristics of travel-related electronic word-of-mouth on social networking sites, Tourism Management, 46, 274-282.

Marshall, D, J., & Staeheli, L, (2015), Mapping civil society with social network analysis: Methodological possibilities and limitations, Geoforum, 61, 56-66.

Mercer, S, (2015), Social network analysis and complex dynamic systems, Motivational dynamics in language learning, 73-82.

Nikolaev, A, G., Razib, R., & Kucheriya, A, (2015), On efficient use of entropy centrality for social network analysis and community detection, Social Networks, 40, 154-162.

Palonen, T., & Hakkarainen, K, (2013), Patterns of interaction in computersupported learning: A social network analysis, In Fourth International Conference of the Learning Sciences (pp, 334-339).

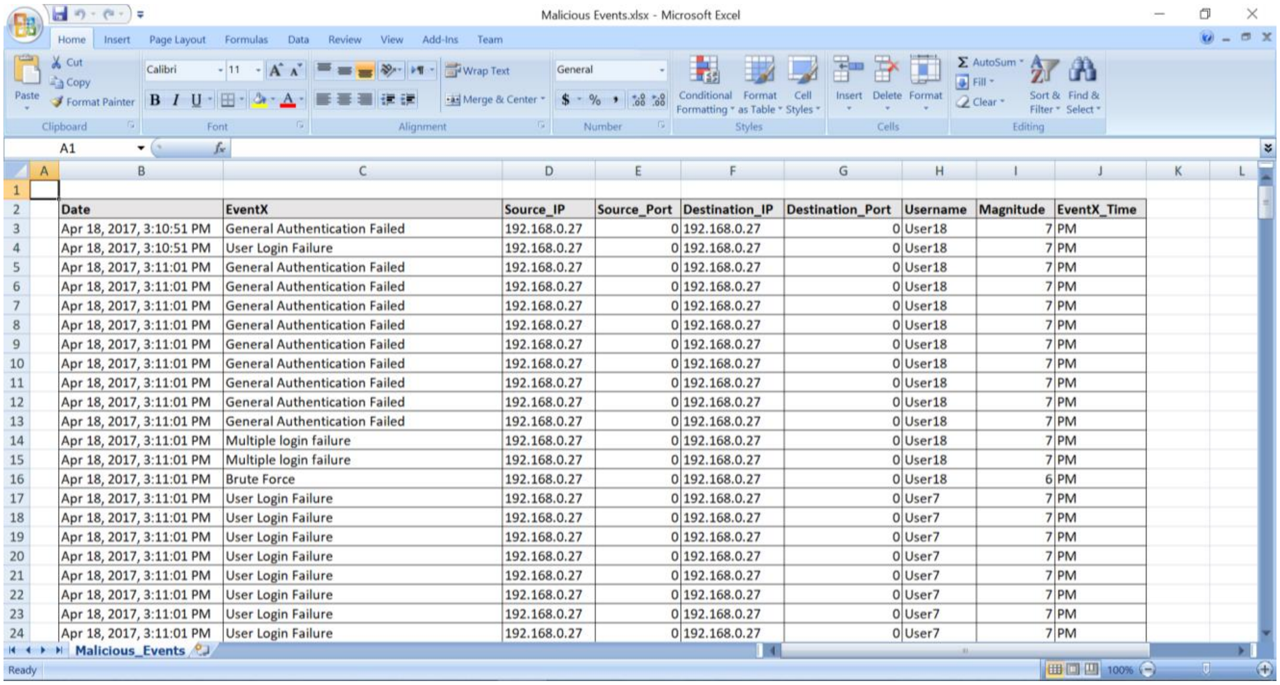
Valente, T, W., Palinkas, L, A., Czaja, S., Chu, K, H., & Brown, C, H, (2015), Social network analysis for program implementation, PloS one, 10(6), e0131712.

Worrell, J., Wasko, M., & Johnston, A, (2013), Social network analysis in accounting information systems research, International Journal of Accounting Information Systems, 14(2), 127-137.

Appendices

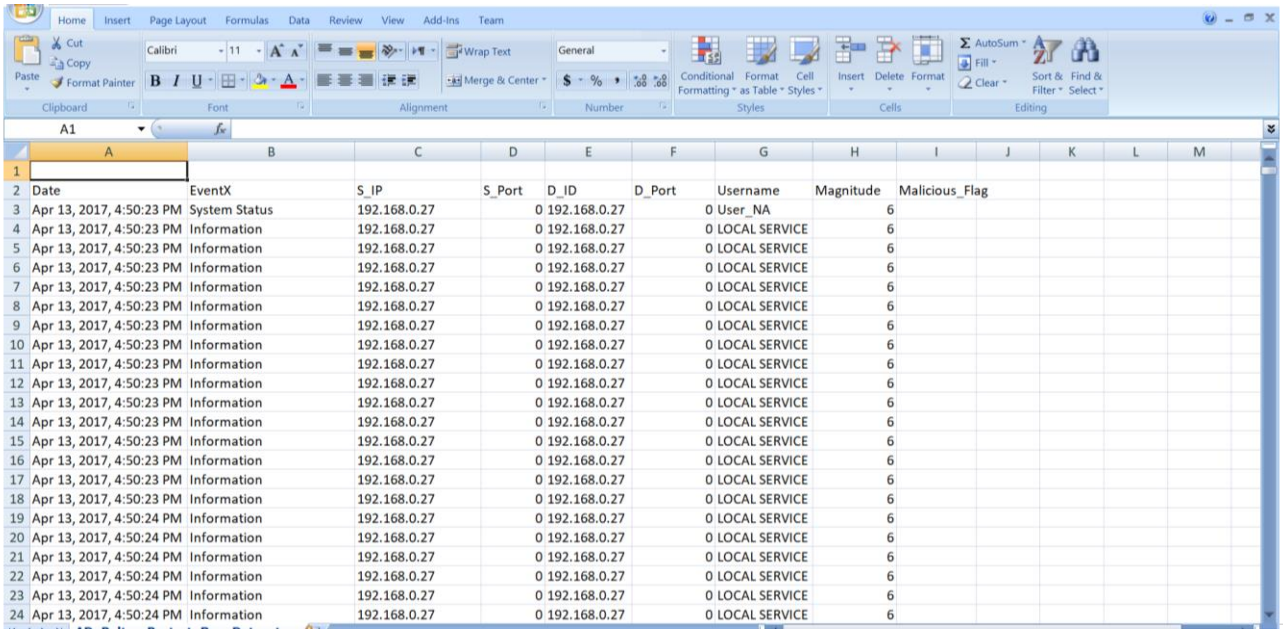
Appendix 1: Data Set.

A- Row Database - Excel Form.



	A	B	C	D	E	F	G	H	I	J
1										
2		Date	EventX	Source_IP	Source_Port	Destination_IP	Destination_Port	Username	Magnitude	EventX_Time
3		Apr 18, 2017, 3:10:51 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
4		Apr 18, 2017, 3:10:51 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User18	7	PM
5		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
6		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
7		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
8		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
9		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
10		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
11		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
12		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
13		Apr 18, 2017, 3:11:01 PM	General Authentication Failed	192.168.0.27	0	192.168.0.27	0	User18	7	PM
14		Apr 18, 2017, 3:11:01 PM	Multiple login failure	192.168.0.27	0	192.168.0.27	0	User18	7	PM
15		Apr 18, 2017, 3:11:01 PM	Multiple login failure	192.168.0.27	0	192.168.0.27	0	User18	7	PM
16		Apr 18, 2017, 3:11:01 PM	Brute Force	192.168.0.27	0	192.168.0.27	0	User18	6	PM
17		Apr 18, 2017, 3:11:01 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User7	7	PM
18		Apr 18, 2017, 3:11:01 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User7	7	PM
19		Apr 18, 2017, 3:11:01 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User7	7	PM
20		Apr 18, 2017, 3:11:01 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User7	7	PM
21		Apr 18, 2017, 3:11:01 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User7	7	PM
22		Apr 18, 2017, 3:11:01 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User7	7	PM
23		Apr 18, 2017, 3:11:01 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User7	7	PM
24		Apr 18, 2017, 3:11:01 PM	User Login Failure	192.168.0.27	0	192.168.0.27	0	User7	7	PM

B- Malicious Events Datasheet.



	A	B	C	D	E	F	G	H	I
1									
2	Date	EventX	S_IP	S_Port	D_ID	D_Port	Username	Magnitude	Malicious_Flag
3	Apr 13, 2017, 4:50:23 PM	System Status	192.168.0.27	0	192.168.0.27	0	User_NA	6	
4	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
5	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
6	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
7	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
8	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
9	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
10	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
11	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
12	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
13	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
14	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
15	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
16	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
17	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
18	Apr 13, 2017, 4:50:23 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
19	Apr 13, 2017, 4:50:24 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
20	Apr 13, 2017, 4:50:24 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
21	Apr 13, 2017, 4:50:24 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
22	Apr 13, 2017, 4:50:24 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
23	Apr 13, 2017, 4:50:24 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	
24	Apr 13, 2017, 4:50:24 PM	Information	192.168.0.27	0	192.168.0.27	0	LOCAL SERVICE	6	

Appendix 2: R Code for hypothesis testing

This R code was used for testing the user level hypothesis from the master log data

```
##########################Sub setting data columns##################################
Ad_police_Final_Dataset<-
 Ad_police_Final_Dataset[,2:11]
names(Ad_police_Final_Dataset)[9]<-"Odd_hour_Flag"
names(Ad_police_Final_Dataset)[10]<-"Event_X4"
##################Remote Login Failure############
###############Slide 3 Hypothesis 1st Graph#################
Remote_Login_Failure<-
sqldf("
select
a.*, b.total_events
from
(select Username, count(Eventx) as cnt_Remote_Login
from Ad_police_Final_Dataset
where EventX='Remote Login Failure'
group by Username)a
left join
(select Username, count(Eventx) as total_events
from Ad_police_Final_Dataset
group by Username)b
on a.Username=b.Username
order by cnt_Remote_Login ")


##################Remote Login Failure odd hours############
###############Slide 4 Hypothesis 2nd Graph#################
Remote_Login_Failure_odd_hours<-
  sqldf("
        select
        a.*, b.total_events
        from
        (select Username, count(Eventx) as cnt_Remote_Login_odd_hour
        from Ad_police_Final_Dataset
        where EventX='Remote Login Failure'
        and Odd_hour_Flag='AM'
        group by Username)a
        left join
        (select Username, count(Eventx) as total_events
        from Ad_police_Final_Dataset
        group by Username)b
        on a.Username=b.Username
        order by cnt_Remote_Login_odd_hour ")

##################Remote Login Failure odd hours############
###############Slide 5 Hypothesis 7th Graph#################
#unique(Ad_police_Final_Dataset$EventX)
User_Login_Failure<-
  sqldf("
        select
        a.*, b.total_events
        from
        (select Username, count(Eventx) as cnt_User_Login_Failure
        from Ad_police_Final_Dataset
        where EventX='User Login Failure'
        group by Username)a
        left join
        (select Username, count(Eventx) as total_events
        from Ad_police_Final_Dataset
        group by Username)b
        on a.Username=b.Username
        order by cnt_User_Login_Failure")

##################Malicious Exploit############
###############Slide 6 Hypothesis 9 Graph#################
Malicious_Exploit<-
  sqldf("
        select
        a.*, b.total_events
        from
        (select Username, count(Eventx) as cnt_Malicious_Exploit
        from Ad_police_Final_Dataset
        where EventX='Malicious Exploit'
        group by Username)a
        left join
        (select Username, count(Eventx) as total_events
        from Ad_police_Final_Dataset
        group by Username)b
        on a.Username=b.Username
        order by cnt_Malicious_Exploit")

##################Bubble Chart############
###############Slide 8 Bubble Chart#################
unique(Ad_police_Final_Dataset$EventX)
User_bubble_chart<-
  sqldf("select Username, count(Event_X4) as total_events
        from Ad_police_Final_Dataset
        where Event_X4 in (
       'General Authentication FailedPM',
        'User Login FailurePM',
        'Multiple login failurePM'
        ,'Brute ForcePM'
        ,'UBA : New Account Use DetectedPM'
        ,'UBA : User Access at Unusual TimesPM',
         'Malicious ExploitPM'
        ,'Excessive Firewall Denies Between HostsPM',
         'Remote Login FailureAM'
        ,'General Authentication FailedAM',
         'Multiple login failureAM'
        ,'General Authentication SuccessfulAM',
          'Brute ForceAM'
        ,'Admin Login SuccessfulAM',
        'UBA : New Account Use DetectedAM'
        ,'UBA : User Access at Unusual TimesAM',
          'Malicious ExploitAM',
           'Remote Login SuccessAM',
           'Remote Login FailurePM'
        )
        group by Username
        order by total_events desc
        ")
```

Appendix 3: R Code to identify business logics from events data

The below attached R code was used to identify the three defined patterns/business logics from events/logs data.

```
##########################Subsetting data columns##################################

Ad_police_Final_Dataset<-

  Ad_police_Final_Dataset[,2:8]

##########################Data Duplication#############################

Bck<-

  Ad_police_Final_Dataset

#####################Creating Patterns to be tested in dataset##########

Pattern<-

  as.data.frame(

    c("Brute Force",

      "Admin Login Successful",

      "UBA : New Account Use Detected",

      "UBA : User Access at Unusual Times","Malicious Exploit")

    )

names(Pattern)<-

  "Pattern1"

Pattern$Pattern2<-

  c("Admin Login Successful",

    "UBA : New Account Use Detected",

    "UBA : User Access at Unusual Times",

    "Malicious Exploit",

    ""

    )


Pattern$Pattern3<-
```

```
  c("Excessive Firewall Denies Between Hosts",
    "Multiple login failure",
    "Brute Force",
    "Admin Login Successful",
    ""   )
Pattern$sr<-"1"
a=aggregate(Pattern1 ~ sr, data = Pattern,paste, collapse = ",")[2]
b=aggregate(Pattern2 ~ sr, data = Pattern,paste, collapse = ",")[2]
c=aggregate(Pattern3 ~ sr, data = Pattern,paste, collapse = ",")[2]
b=substr(b,1,nchar(b)-1)
c=substr(c,1,nchar(c)-1)
Ad_police_Final_Dataset<-
  Ad_police_Final_Dataset[which(Ad_police_Final_Dataset$EventX %in% c("Brute Force",
                                                    "Admin Login Successful" ,
                                                    "UBA : New Account Use Detected",
                                                    "Malicious Exploit",
                                                    "UBA : User Access at Unusual Times",
                                                    "Excessive Firewall Denies Between Hosts",
                                                    "Multiple login failure")),]
Ad_police_Final_Dataset$Time_Stamp <-
  as.POSIXct(Ad_police_Final_Dataset$Time_Stamp, format = "%Y-%m-%d %I:%M:%S %p")
df<-Ad_police_Final_Dataset
names(df)[7]<-"TimeStamp"
df$sr<-"1"


######################Testing the pattern#######################
df1<-df[with(df, c(TRUE, diff(as.numeric(interaction(df$EventX,df$Username))) != 0)), ]
z=aggregate(EventX ~ sr, data = df1,paste, collapse = ",")[2]
grepl(a,z)
grepl(b,z)
grepl(c,z)

#######################################1st Pattern#################################

sapply(regmatches(substr(z,1,gregexpr(pattern =a,z)[[1]][1]), gregexpr(",",substr(z,1,gregexpr(pattern
=a,z)[[1]][1]))), length)

Case1<-Bck[min(row.names(df1[102:106,])):max(row.names(df1[102:106,])),]

sapply(regmatches(substr(z,1,gregexpr(pattern =a,z)[[1]][2]), gregexpr(",",substr(z,1,gregexpr(pattern
=a,z)[[1]][2]))), length)

Case2<-Bck[min(row.names(df1[108:111,])):max(row.names(df1[108:111,])),]

########################################2nd Pattern ###################
##################

sapply(regmatches(substr(z,1,gregexpr(pattern =b,z)[[1]][3]), gregexpr(",",substr(z,1,gregexpr(pattern
=b,z)[[1]][3]))), length)

Case3<-Bck[min(row.names(df1[113:116,])):max(row.names(df1[113:116,])),]

########################################3rd Pattern##############################

gregexpr(pattern =c,z)[[1]]

sapply(regmatches(substr(z,1,gregexpr(pattern =c,z)[[1]][1]), gregexpr(",",substr(z,1,gregexpr(pattern
=c,z)[[1]][1]))), length)

Case4<-Bck[min(row.names(df1[117:120,])):max(row.names(df1[117:120,])),]

##############################Checking Time Interval for identified cases############

Case1<-Case1[with(Case1, abs(difftime(Time_Stamp,Time_Stamp,units="mins")) <= 10 ),]

Case2<-Case2[with(Case2, abs(difftime(Time_Stamp,Time_Stamp,units="mins")) <= 10 ),]

Case3<-Case3[with(Case3, abs(difftime(Time_Stamp,Time_Stamp,units="mins")) <= 10 ),]


Case4<-Case4[with(Case4, abs(difftime(Time_Stamp,Time_Stamp,units="mins")) <= 10 ),]

##########################Exporting the data#################################
############

write.csv(Case1,"D:/Data Analysis/AD Police Analysis/Final Deliverable/Case1.csv")

write.csv(Case2,"D:/Data Analysis/AD Police Analysis/Final Deliverable/Case2.csv")

write.csv(Case3,"D:/Data Analysis/AD Police Analysis/Final Deliverable/Case3.csv")

write.csv(Case4,"D:/Data Analysis/AD Police Analysis/Final Deliverable/Case4.csv")

###############################End of Code#####################################
```

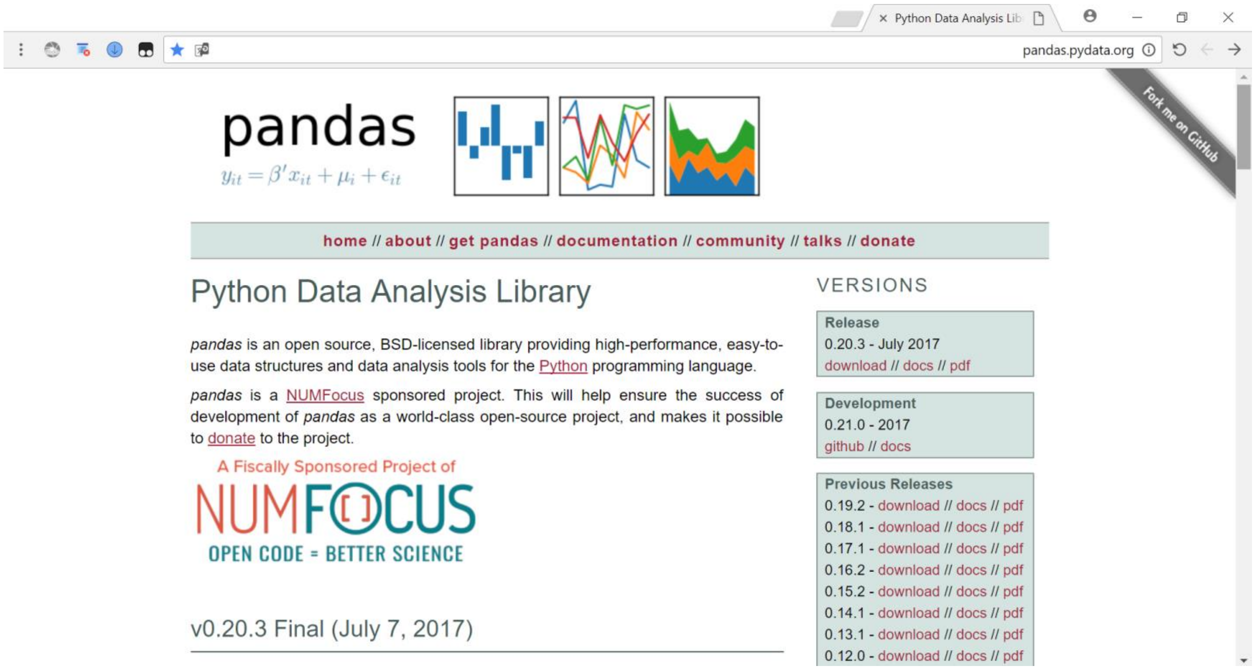
Appendix 4: R Code for network graph generation.

The below attached R code was used to generate the network chart from events/logs data.

```
#############Importing Libraries#####################

library(igraph)

library(readr)

#########Data Import##########################

Gephi_edges<- read_csv("D:/Data Analysis/Network Graph/Gephi2.csv")

relations<-Gephi_edges[,c(1,2,3,4)]

names(relations)<-c("from","to","weight","Metrics")

relations$weight<-"1"

g <- graph.data.frame(relations, directed=F)

############### Node Size Adjustment##############################

node.size<-
setNames(c(34.3333333,10.6666667,22.0000000,7.6666667,5.3333333,4.6666667,3.6666667,7.666666
7,1.3333333,1.3333333,1.3333333,1.3333333,
0.6666667,0.3333333,0.3333333),c("User18","User7","User21","User3","User29","User9","User33","U
ser2","User19","User25","User89","User15","User94","User10","User81"))

########3#####Assigning Edges Colours based on Metrics############

g1 <- barabasi.game(15, directed=FALSE)

library(qgraph)

e <- get.edgelist(g1)

l <- layout.reingold.tilford(g, circular=T)

E(g)$color[E(g)$Metrics == 1] <- "red"

E(g)$color[E(g)$Metrics == 2] <- "blue"

E(g)$color[E(g)$Metrics == 3] <- 'green3'
```

```
E(g)$color[E(g)$Metrics == 4] <- 'cyan'

E(g)$color[E(g)$Metrics == 5] <- 'pink'

E(g)$color[E(g)$Metrics == 6] <- 'yellow'

E(g)$color[E(g)$Metrics == 7] <- 'grey'

E(g)$color[E(g)$Metrics == 8] <- 'magenta'

E(g)$color[E(g)$Metrics == 9] <- 'black'

E(g)$color[E(g)$Metrics == 10] <- 'orange'

E(g)$color[E(g)$Metrics == 11] <- 'darkgoldenrod1'

E(g)$color[E(g)$Metrics == 12] <- 'turquoise3'

############Plotting Network Graph##################

plot(g,

    vertex.color = rainbow(10, .8, .8, alpha= .8),

    layout=l,

    edge.arrow.size=0.01,vertex.label.color = "black",vertex.size=as.matrix(node.size),

    vertex.label.font=4, vertex.label.cex=0.75

)

######Adding Legends to Network Graph#########

par(mar=c(0, 0, 0, 0))

legend("topleft","groups", fill =
c("red","blue","green3","cyan","pink","yellow","grey","magenta","black","orange","darkgoldenrod1","tu
rquoise3"),

       legend=c(

         "General Authentication Failed",

         "Remote Login Failure",

         "Remote Login Success - Odd hour",

         "User Login Failure",

         "Excessive Firewall Denies Between Hosts",

         "Malicious Exploit",

         "UBA: New Account Use Detected",

         "UBA: User Access at Unusual Times",
         "Admin Login Successful - Odd hour",
         "Multiple login failure",
         "General Authentication Successful - Odd hour",
         "Brute Force"
       ),ncol=1, bty ="n", cex=0.5)
```

Appendix 5: Python Data Analysis (PANDAS).



home // about // get pandas // documentation // community // talks // donate

Python Data Analysis Library

pandas is an open source, BSD-licensed library providing high-performance, easy-to-use data structures and data analysis tools for the Python programming language.

pandas is a NUMFocus sponsored project. This will help ensure the success of development of *pandas* as a world-class open-source project, and makes it possible to donate to the project.

A Fiscally Sponsored Project of NUMFOCUS OPEN CODE = BETTER SCIENCE

v0.20.3 Final (July 7, 2017)

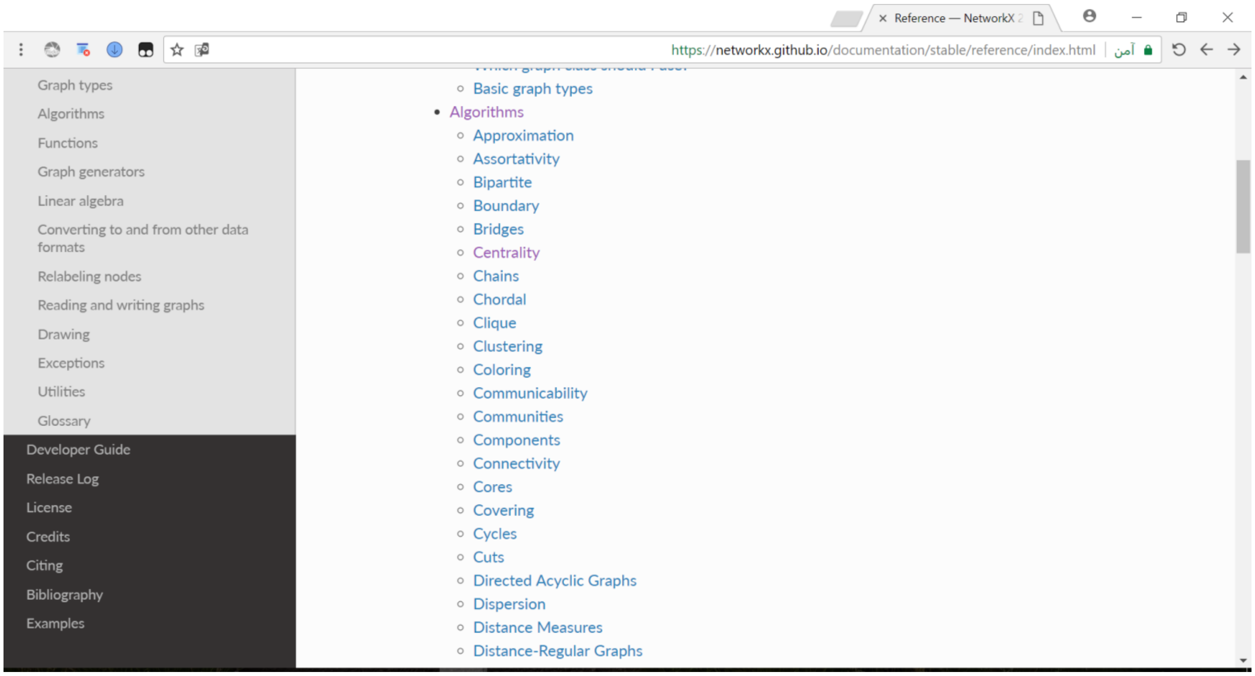
VERSIONS

Release
0.20.3 - July 2017
download // docs // pdf

Development
0.21.0 - 2017
github // docs

Previous Releases
0.19.2 - download // docs // pdf
0.18.1 - download // docs // pdf
0.17.1 - download // docs // pdf
0.16.2 - download // docs // pdf
0.15.2 - download // docs // pdf
0.14.1 - download // docs // pdf
0.13.1 - download // docs // pdf
0.12.0 - download // docs // pdf

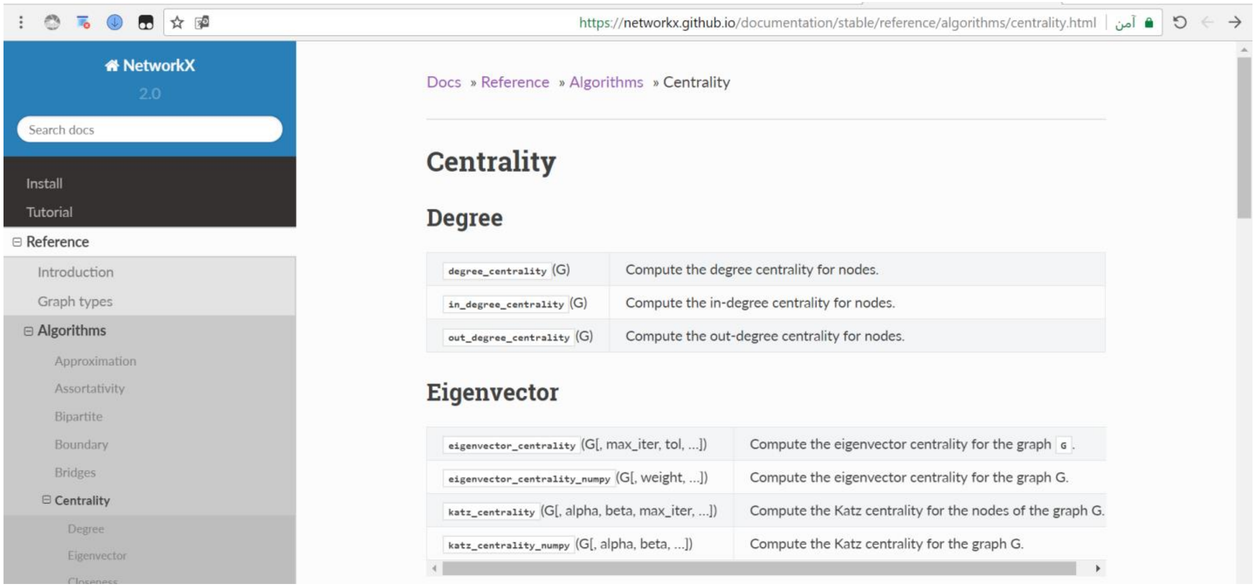
Appendix 6: NetworkX - Python package.



https://networkx.github.io/documentation/stable/reference/index.html

- Graph types
- Algorithms
- Functions
- Graph generators
- Linear algebra
- Converting to and from other data formats
- Relabeling nodes
- Reading and writing graphs
- Drawing
- Exceptions
- Utilities
- Glossary
- Developer Guide
- Release Log
- License
- Credits
- Citing
- Bibliography
- Examples

- Basic graph types
- Algorithms
  - Approximation
  - Assortativity
  - Bipartite
  - Boundary
  - Bridges
  - Centrality
  - Chains
  - Chordal
  - Clique
  - Clustering
  - Coloring
  - Communicability
  - Communities
  - Components
  - Connectivity
  - Cores
  - Covering
  - Cycles
  - Cuts
  - Directed Acyclic Graphs
  - Dispersion
  - Distance Measures
  - Distance-Regular Graphs



https://networkx.github.io/documentation/stable/reference/algorithms/centrality.html

- Install
- Tutorial
- ⊟ Reference
  - Introduction
  - Graph types
  - ⊟ Algorithms
    - Approximation
    - Assortativity
    - Bipartite
    - Boundary
    - Bridges
    - ⊟ Centrality
      - Degree
      - Eigenvector
      - Closeness

Docs » Reference » Algorithms » Centrality

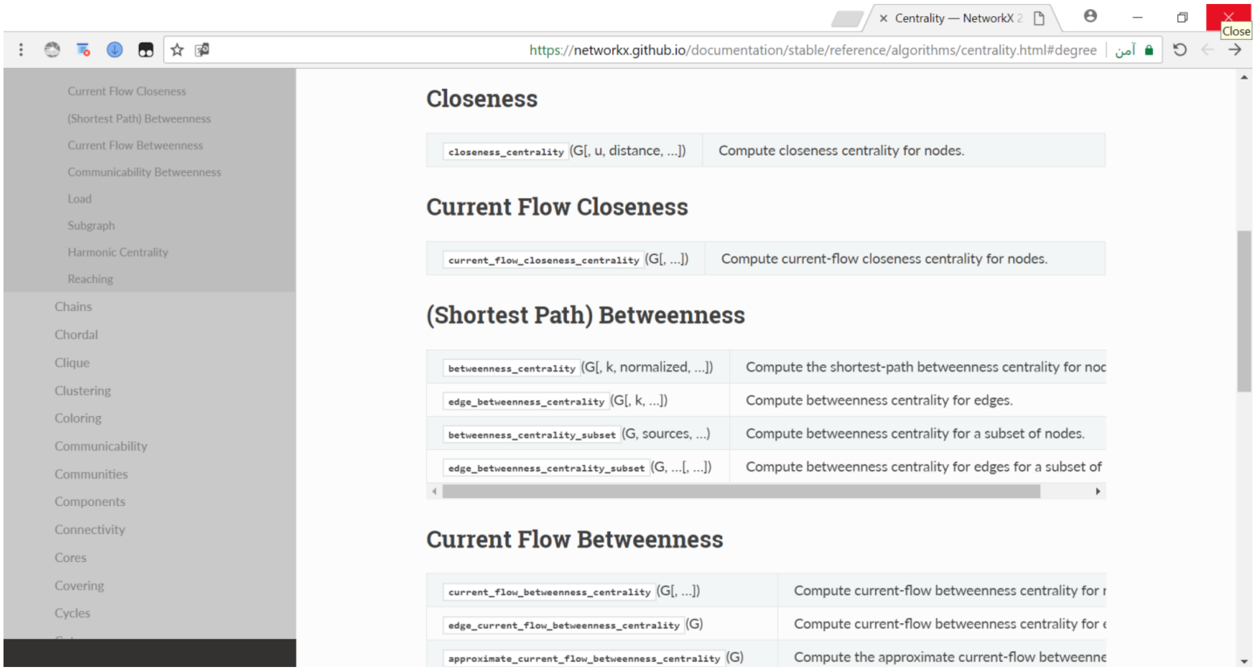
Centrality

Degree

`degree_centrality` (G)	Compute the degree centrality for nodes.
`in_degree_centrality` (G)	Compute the in-degree centrality for nodes.
`out_degree_centrality` (G)	Compute the out-degree centrality for nodes.

Eigenvector

`eigenvector_centrality` (G[, max_iter, tol, ...])	Compute the eigenvector centrality for the graph `G`.
`eigenvector_centrality_numpy` (G[, weight, ...])	Compute the eigenvector centrality for the graph G.
`katz_centrality` (G[, alpha, beta, max_iter, ...])	Compute the Katz centrality for the nodes of the graph G.
`katz_centrality_numpy` (G[, alpha, beta, ...])	Compute the Katz centrality for the graph G.



Closeness

`closeness_centrality` (G[, u, distance, ...])	Compute closeness centrality for nodes.

Current Flow Closeness

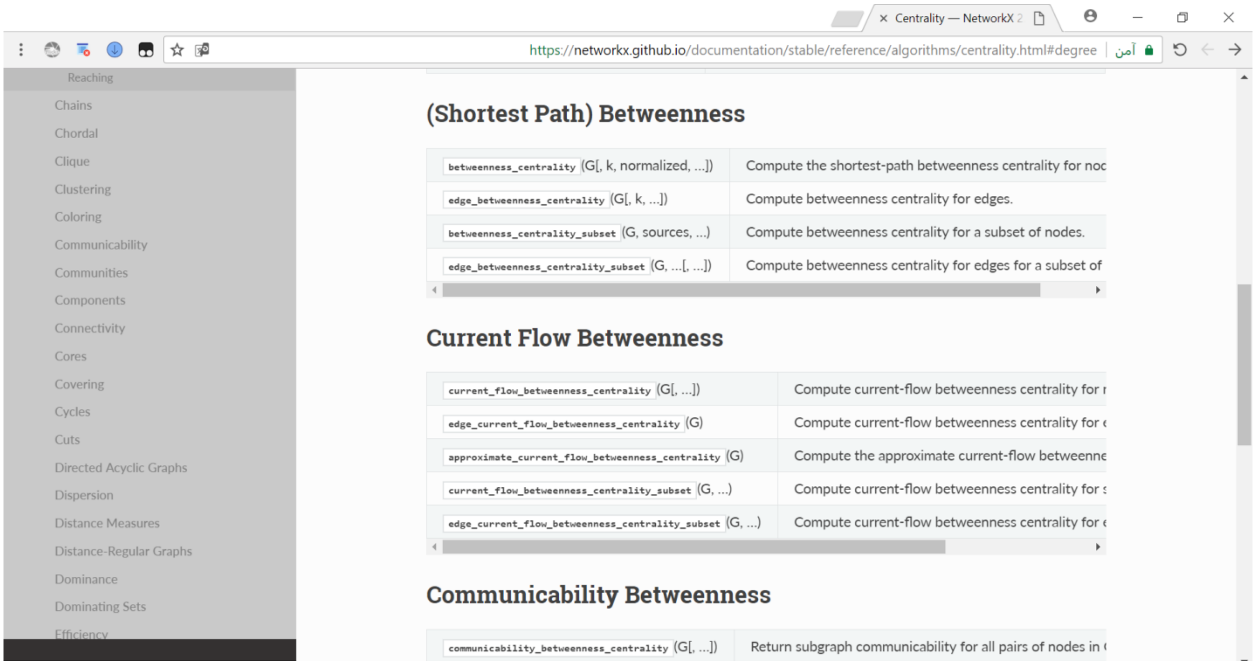
`current_flow_closeness_centrality` (G[, ...])	Compute current-flow closeness centrality for nodes.

(Shortest Path) Betweenness

`betweenness_centrality` (G[, k, normalized, ...])	Compute the shortest-path betweenness centrality for noc
`edge_betweenness_centrality` (G[, k, ...])	Compute betweenness centrality for edges.
`betweenness_centrality_subset` (G, sources, ...)	Compute betweenness centrality for a subset of nodes.
`edge_betweenness_centrality_subset` (G, ...[, ...])	Compute betweenness centrality for edges for a subset of

Current Flow Betweenness

`current_flow_betweenness_centrality` (G[, ...])	Compute current-flow betweenness centrality for r
`edge_current_flow_betweenness_centrality` (G)	Compute current-flow betweenness centrality for e
`approximate_current_flow_betweenness_centrality` (G)	Compute the approximate current-flow betweenne



(Shortest Path) Betweenness

`betweenness_centrality` (G[, k, normalized, ...])	Compute the shortest-path betweenness centrality for noc
`edge_betweenness_centrality` (G[, k, ...])	Compute betweenness centrality for edges.
`betweenness_centrality_subset` (G, sources, ...)	Compute betweenness centrality for a subset of nodes.
`edge_betweenness_centrality_subset` (G, ...[, ...])	Compute betweenness centrality for edges for a subset of

Current Flow Betweenness

`current_flow_betweenness_centrality` (G[, ...])	Compute current-flow betweenness centrality for r
`edge_current_flow_betweenness_centrality` (G)	Compute current-flow betweenness centrality for e
`approximate_current_flow_betweenness_centrality` (G)	Compute the approximate current-flow betweenne
`current_flow_betweenness_centrality_subset` (G, ...)	Compute current-flow betweenness centrality for s
`edge_current_flow_betweenness_centrality_subset` (G, ...)	Compute current-flow betweenness centrality for e

Communicability Betweenness

`communicability_betweenness_centrality` (G[, ...])	Return subgraph communicability for all pairs of nodes in (

Appendix 7: Final Graph Theory Centrality Graphs.

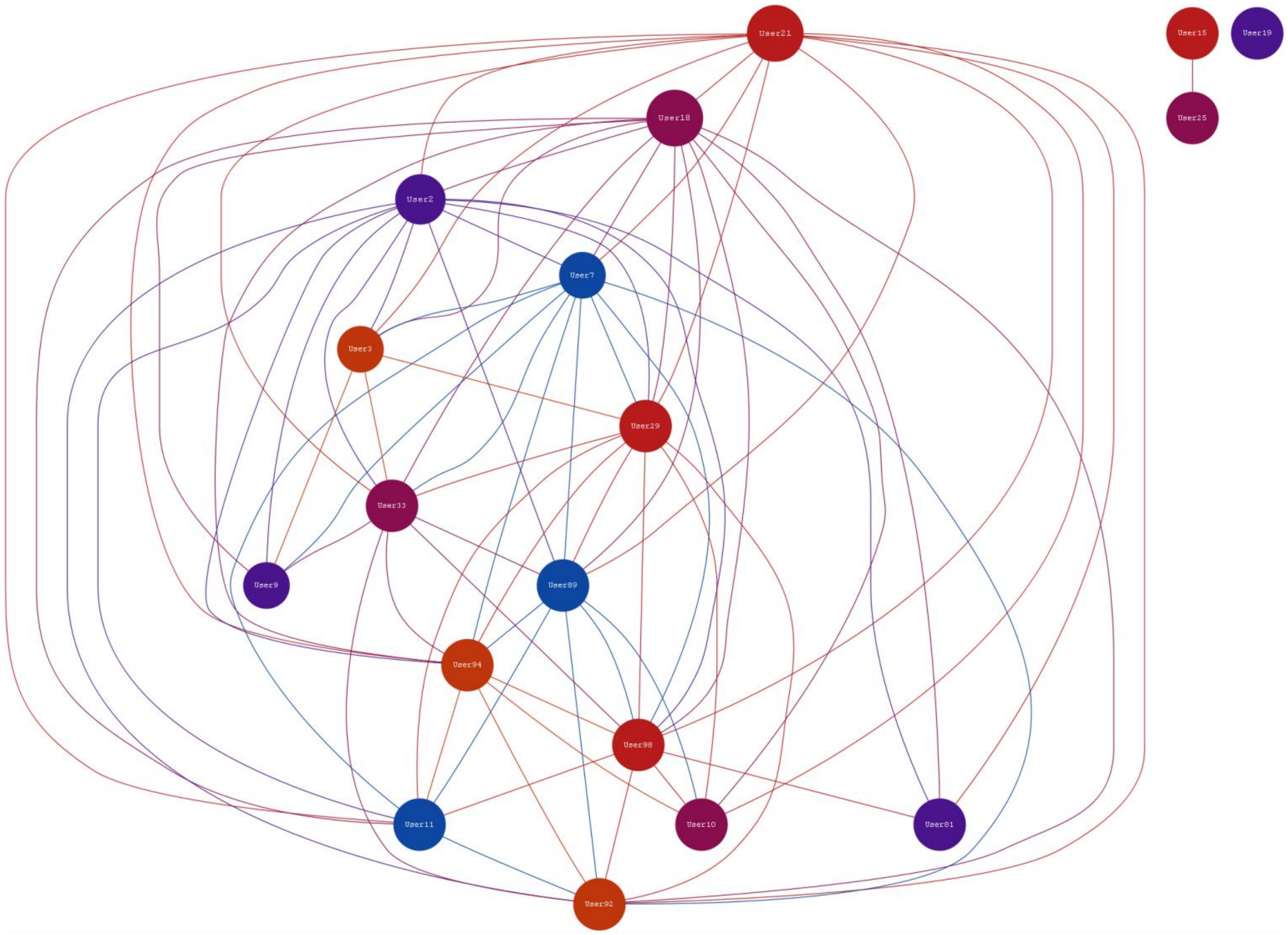


Figure APP-1: Betweenness Centrality Event and Hour.

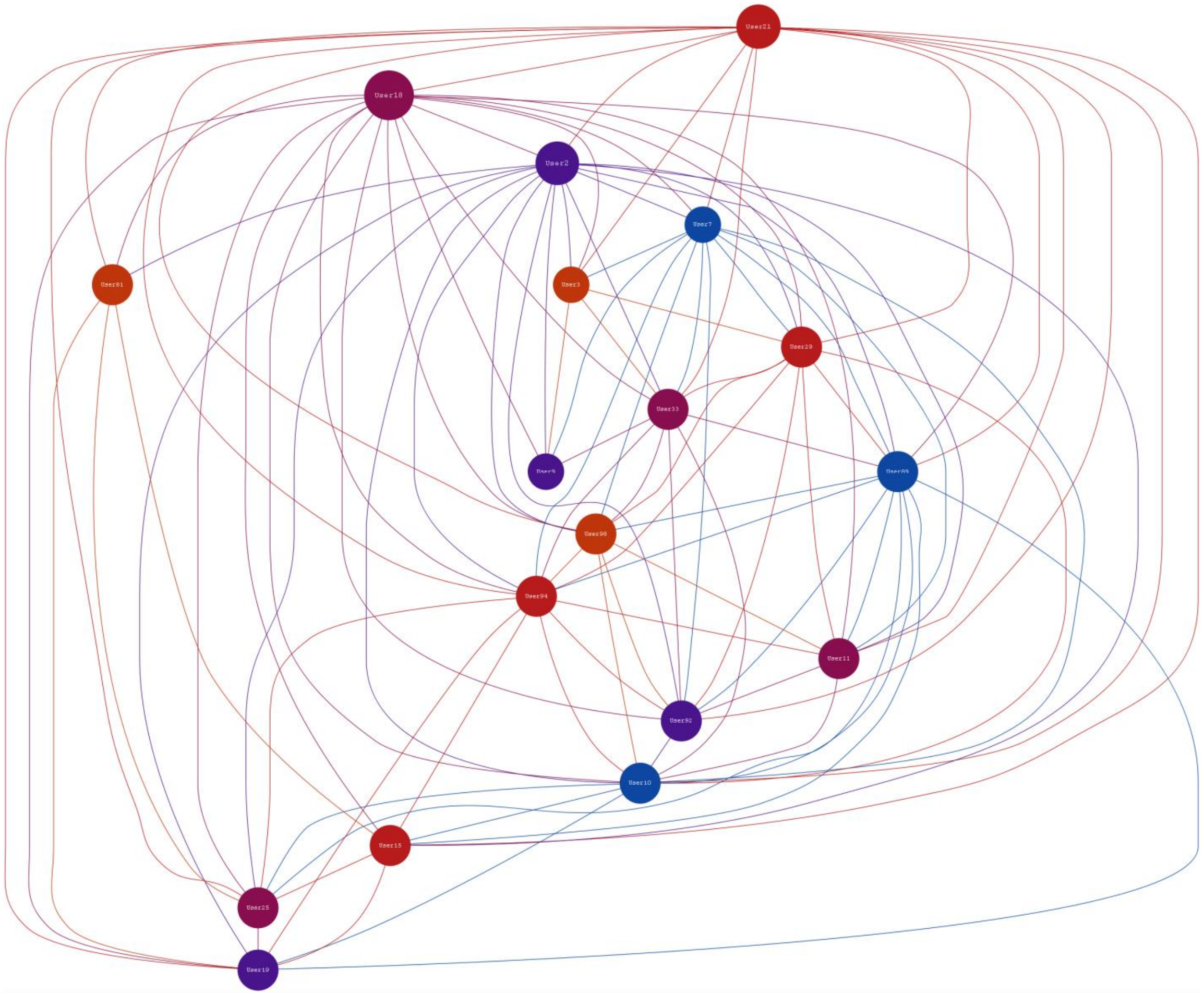


Figure APP-2: Betweenness Centrality Event and Magnitude.

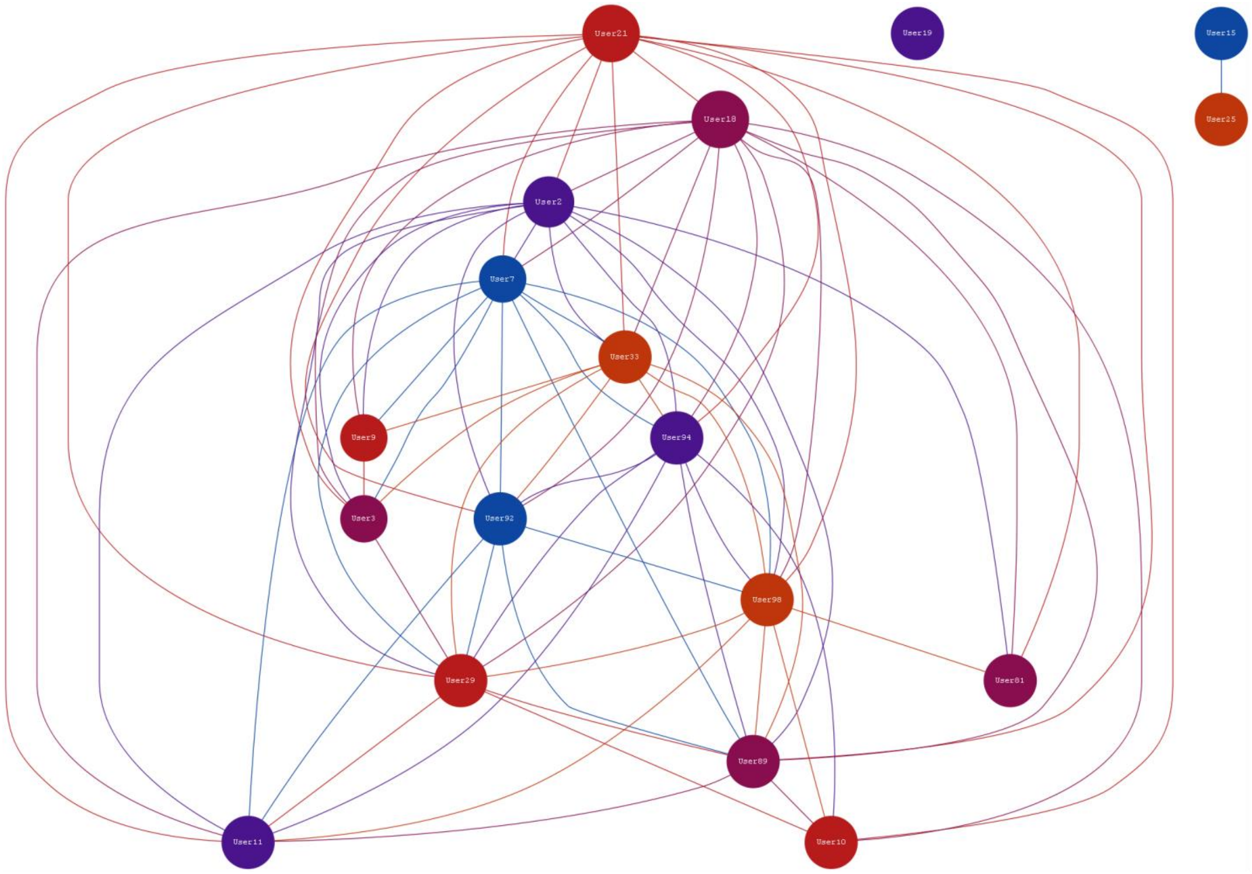


Figure APP-3: Betweenness Centrality Hour and Event.

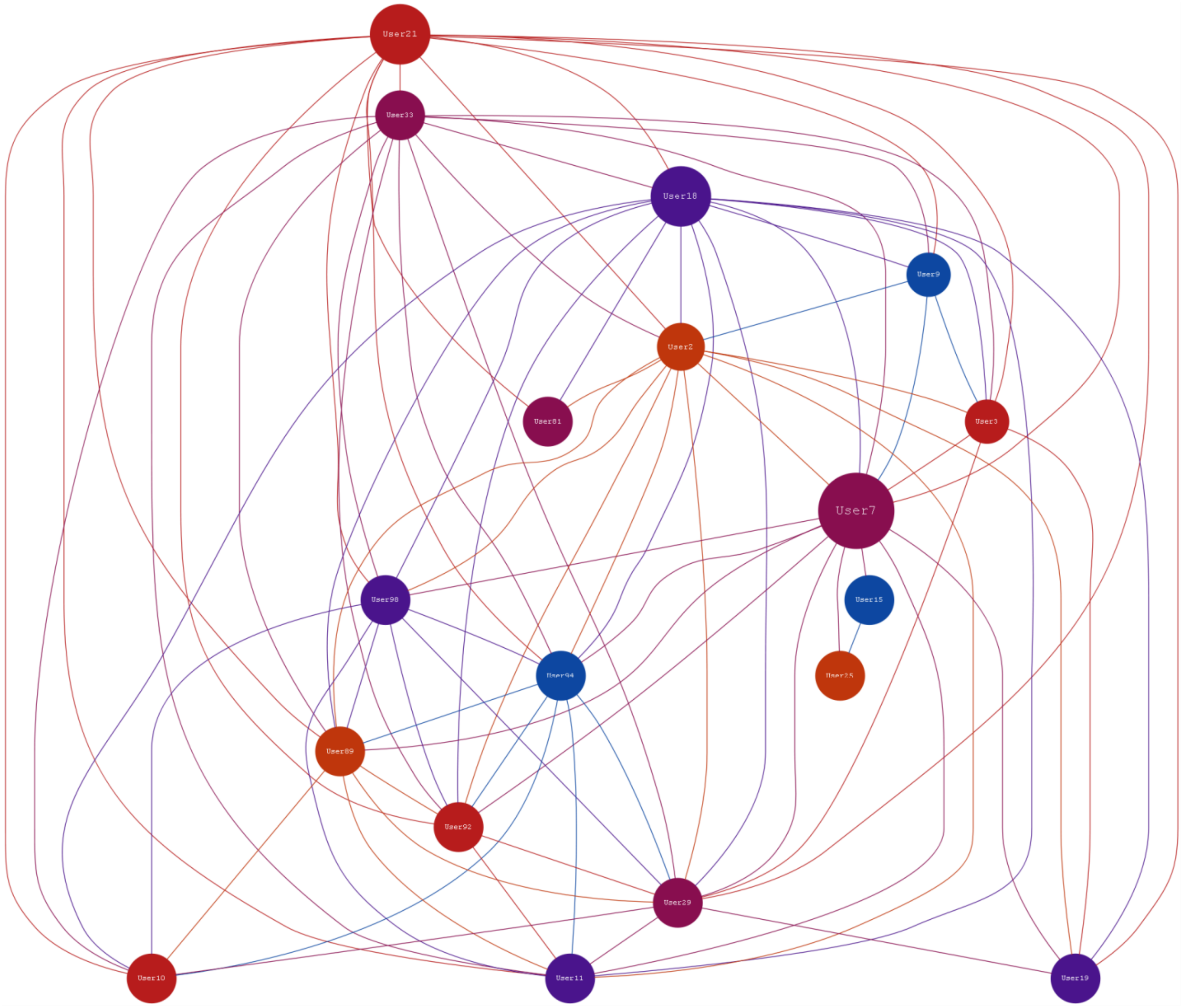


Figure APP-4: Betweenness Centrality Hour and Magnitude.

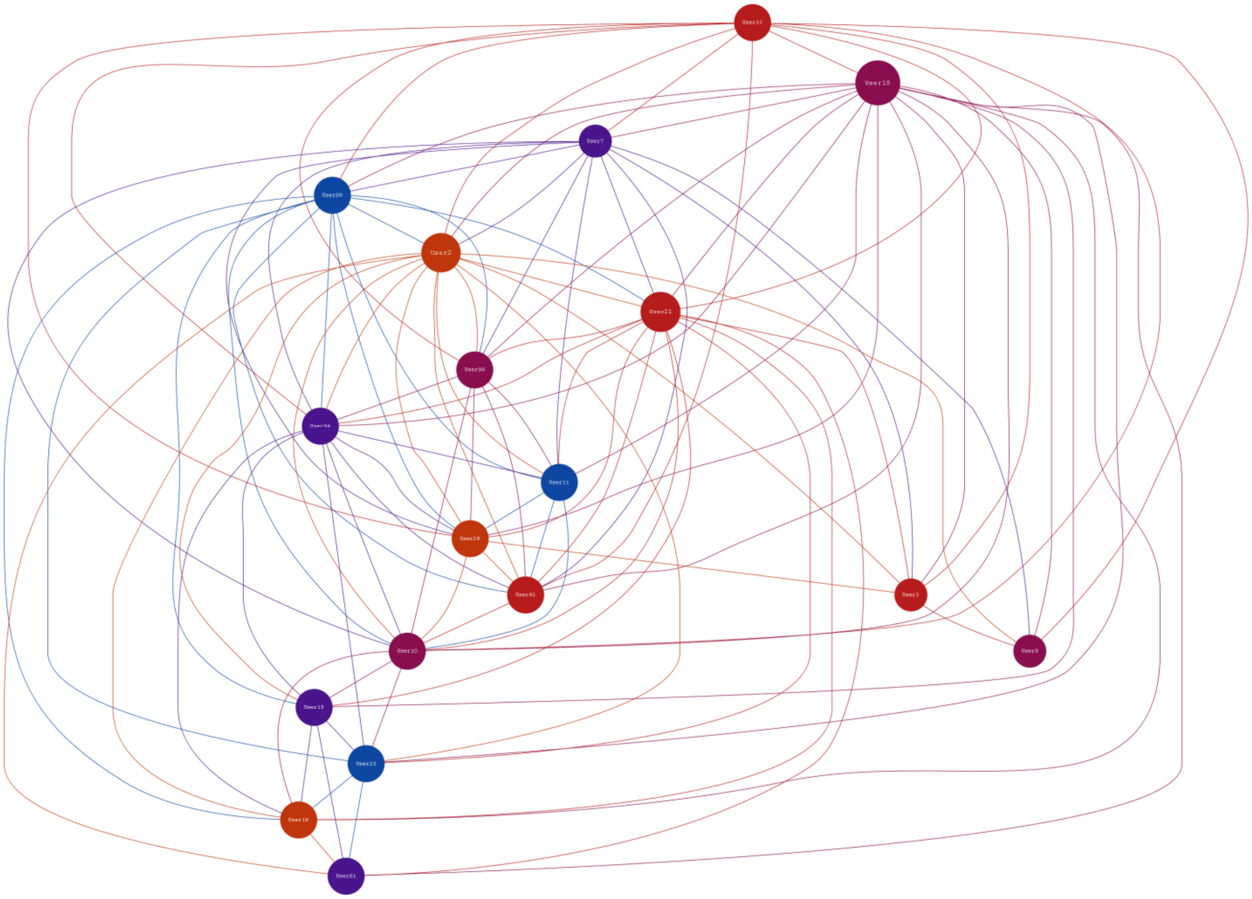


Figure APP-5: Betweenness Centrality Magnitude and Event.

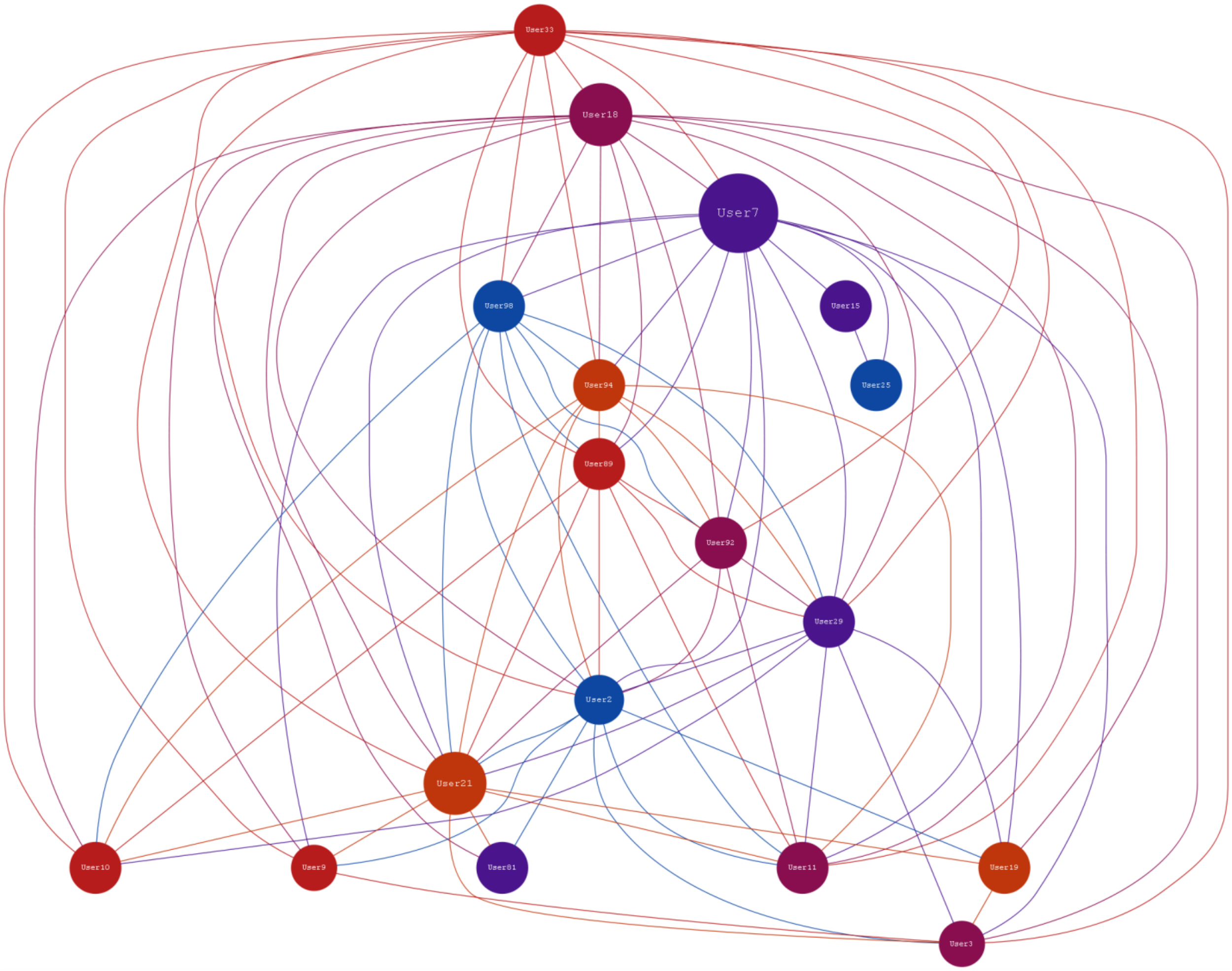


Figure APP-6: Betweenness Centrality Magnitude and Hour.

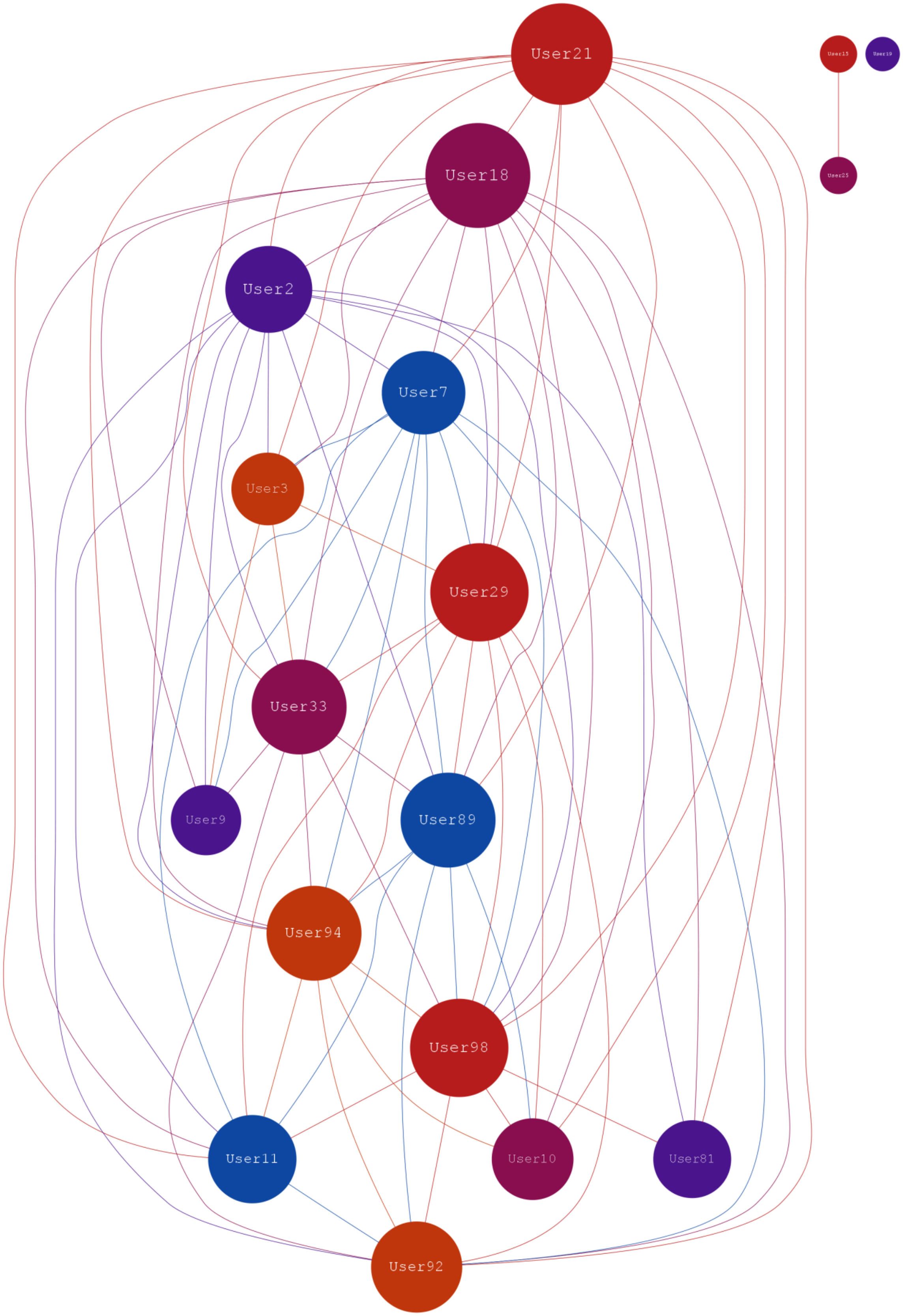


Figure APP-7:Closeness Centrality Event and Hour.

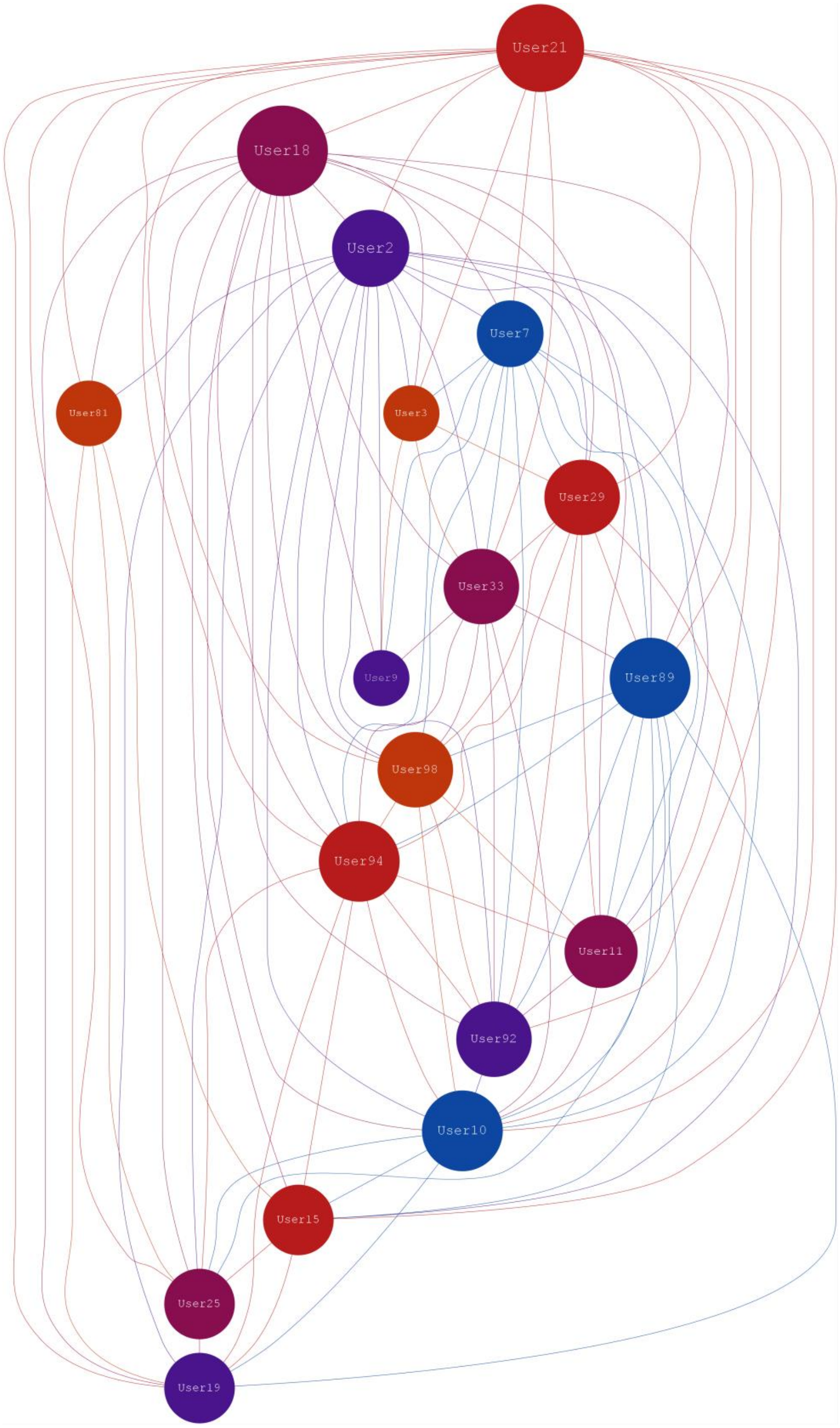


Figure APP-8: Closeness Centrality Event and Magnitude.

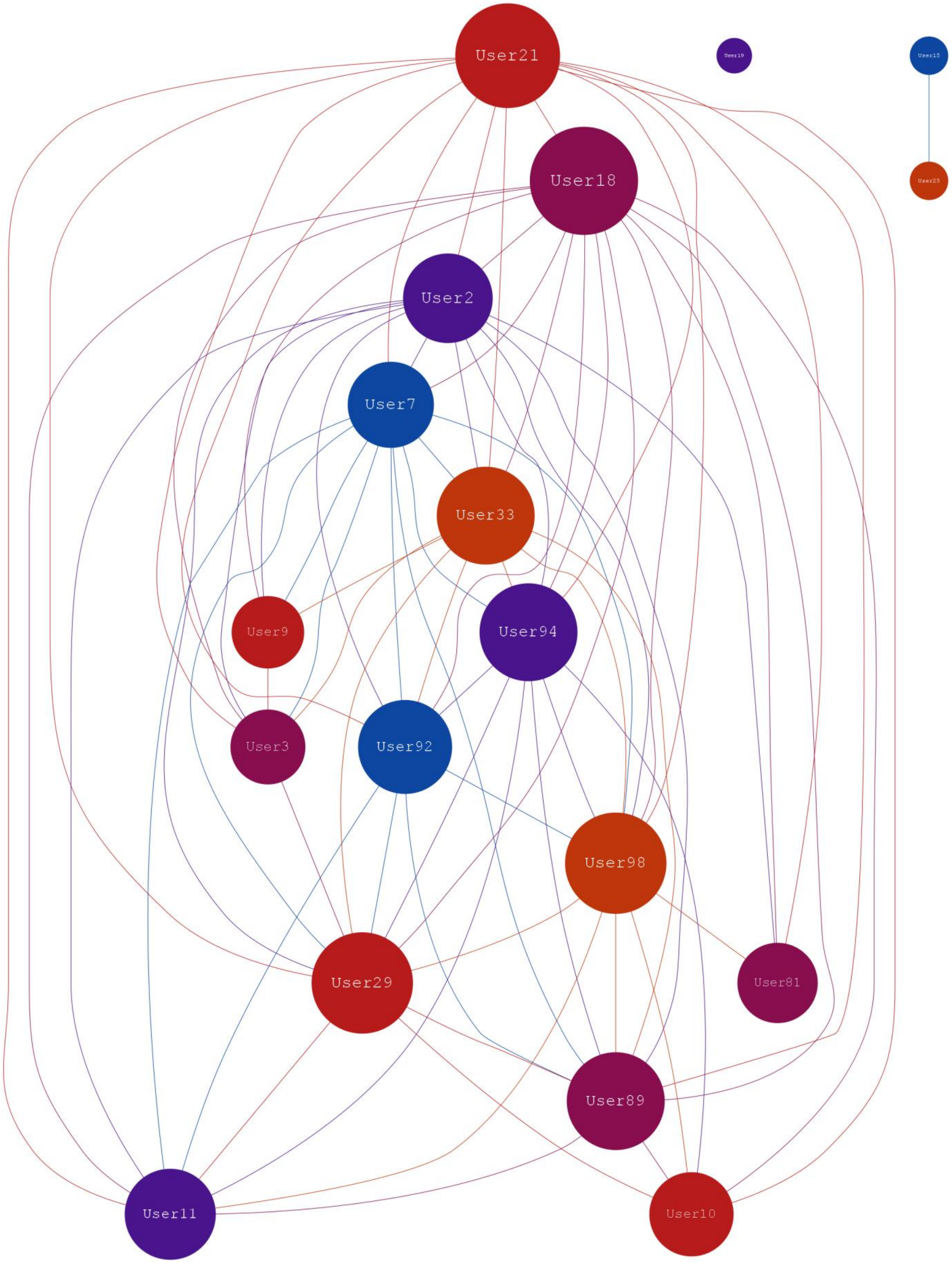


Figure APP-9: Closeness Centrality Hour and Event.

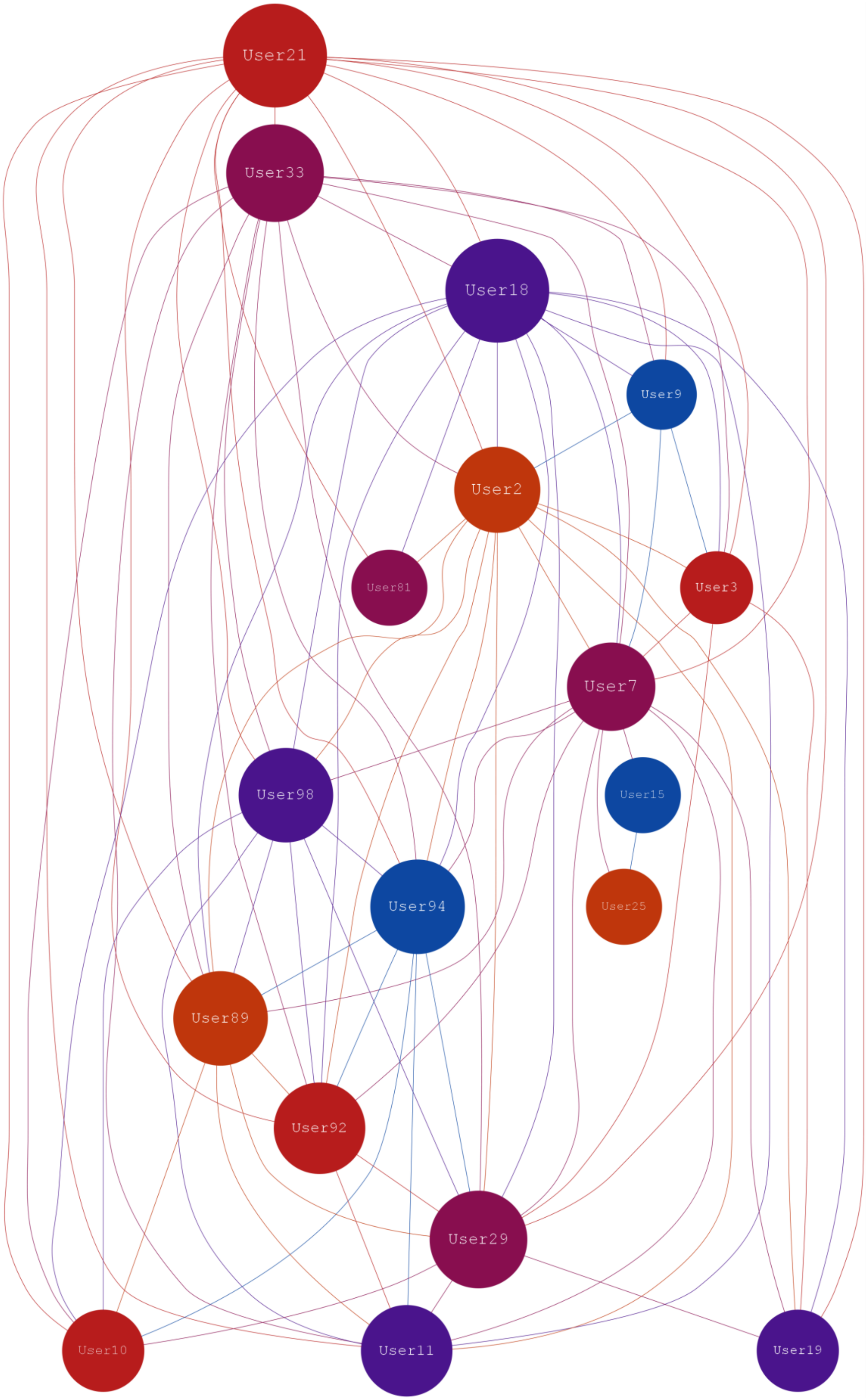


Figure APP-10: Closeness Centrality Hour and Magnitude.

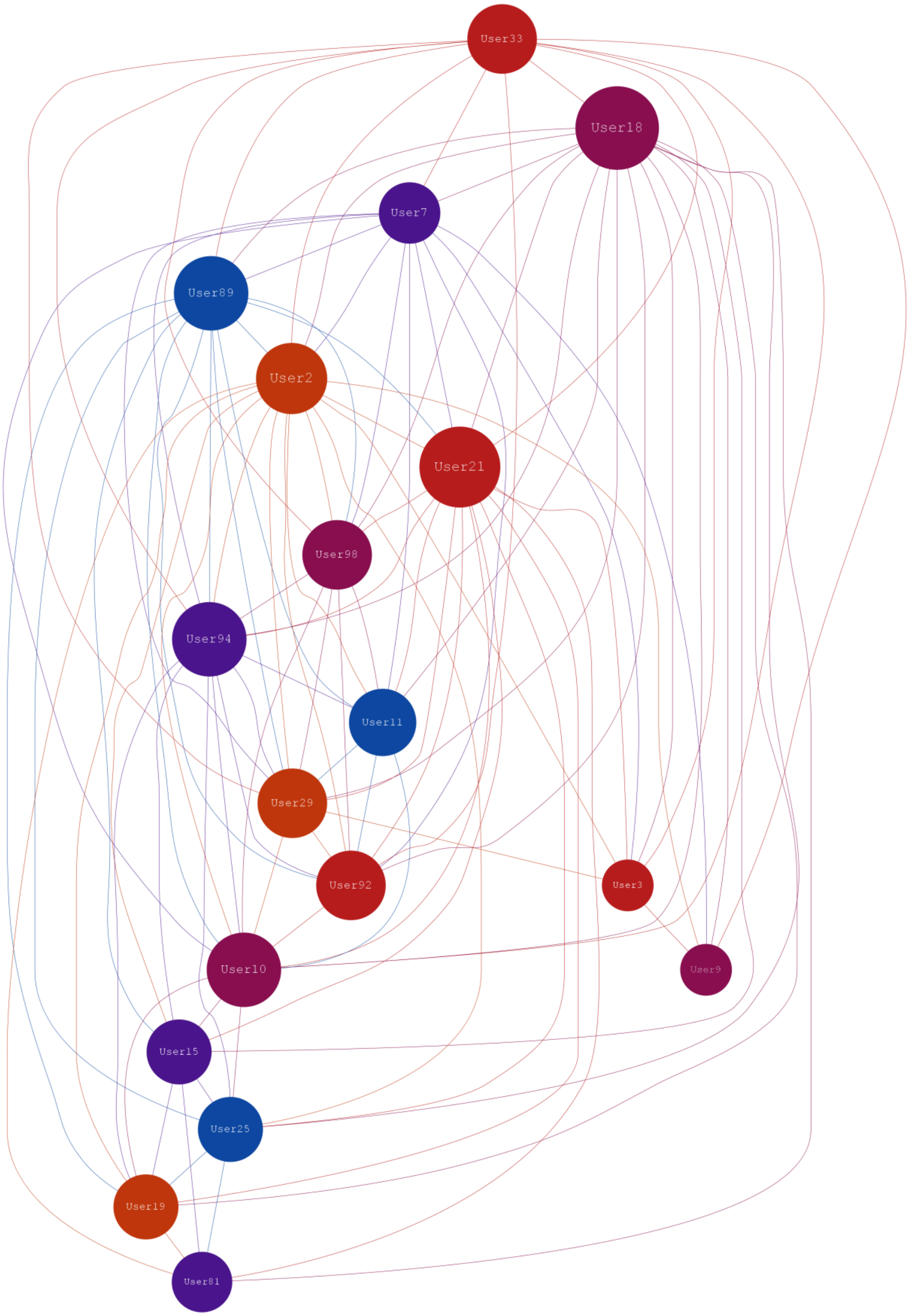


Figure APP-11: Closeness Centrality Magnitude and Event.

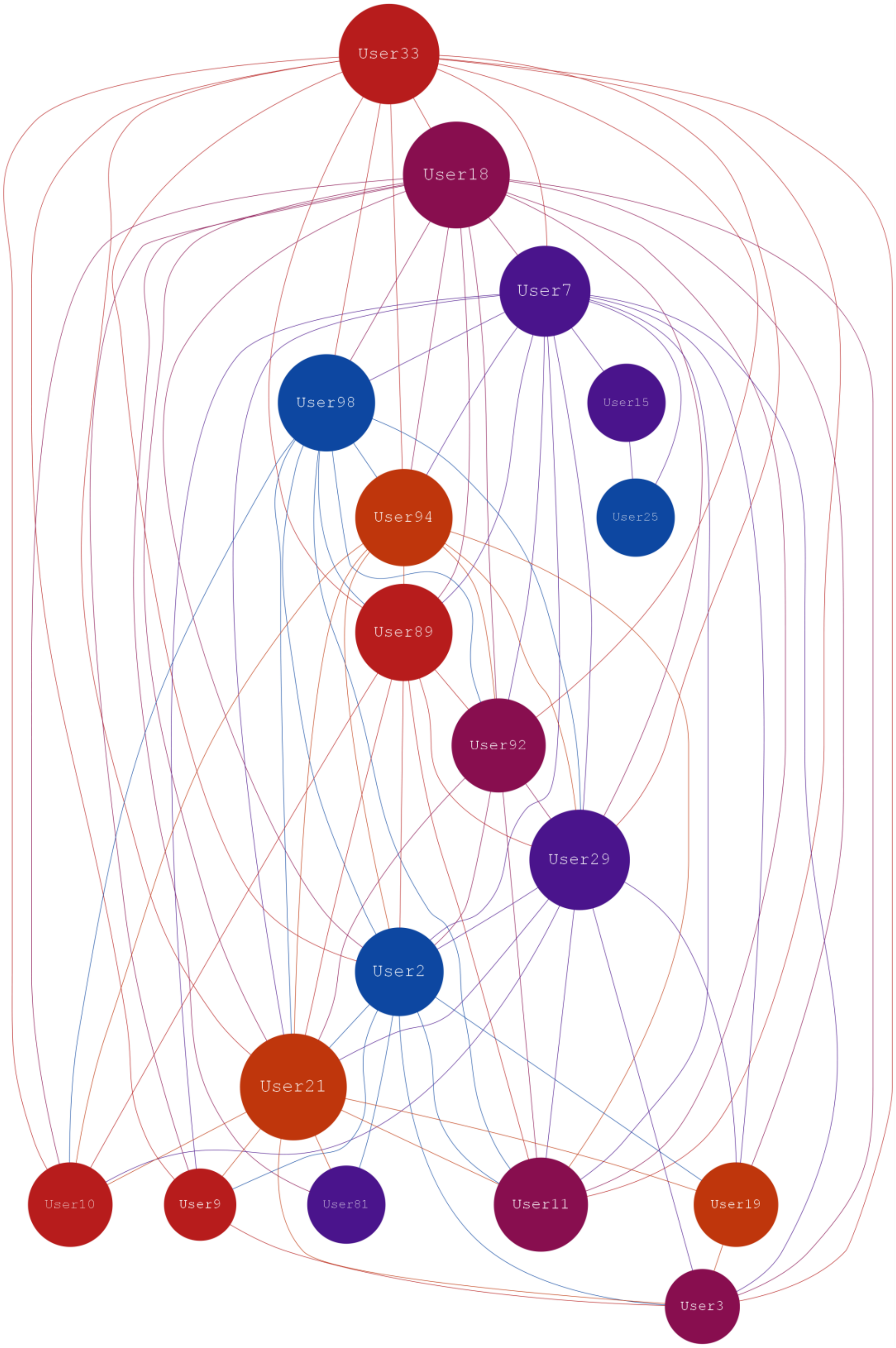


Figure APP-12: Closeness Centrality Magnitude and Hour.

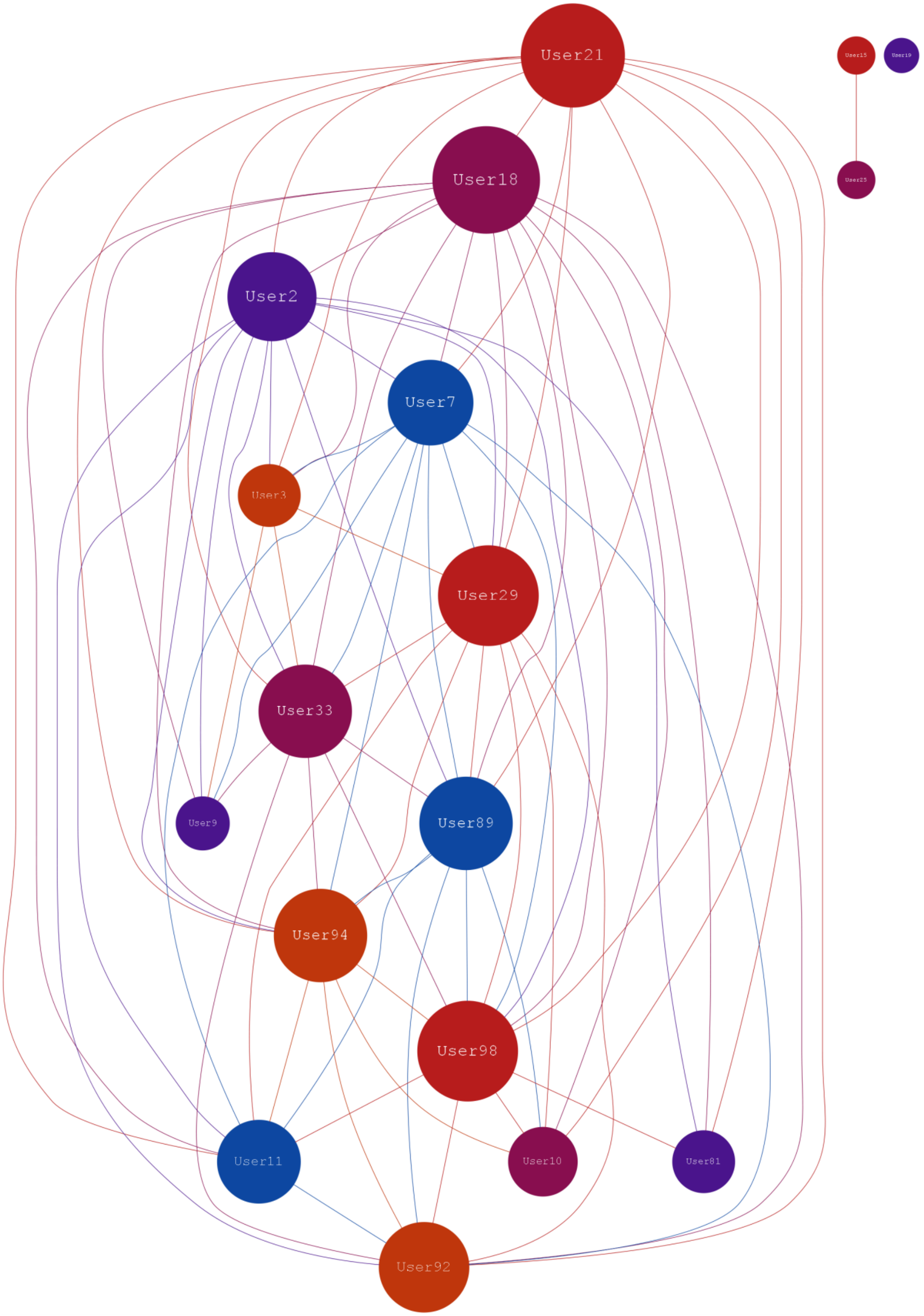


Figure APP-13: Degree of centrality Event and Hour.

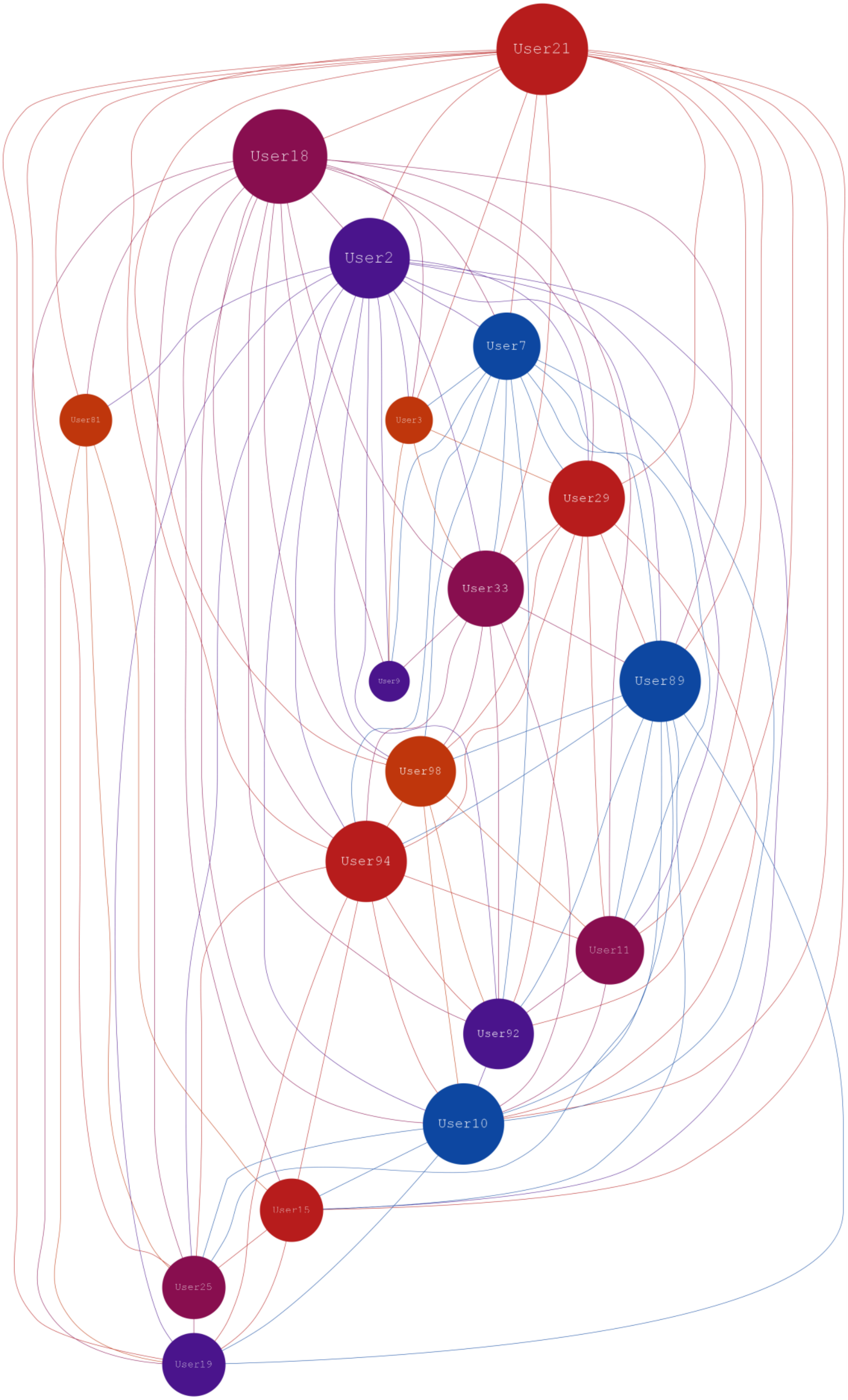


Figure APP-14: Degree of centrality Event and Magnitude.

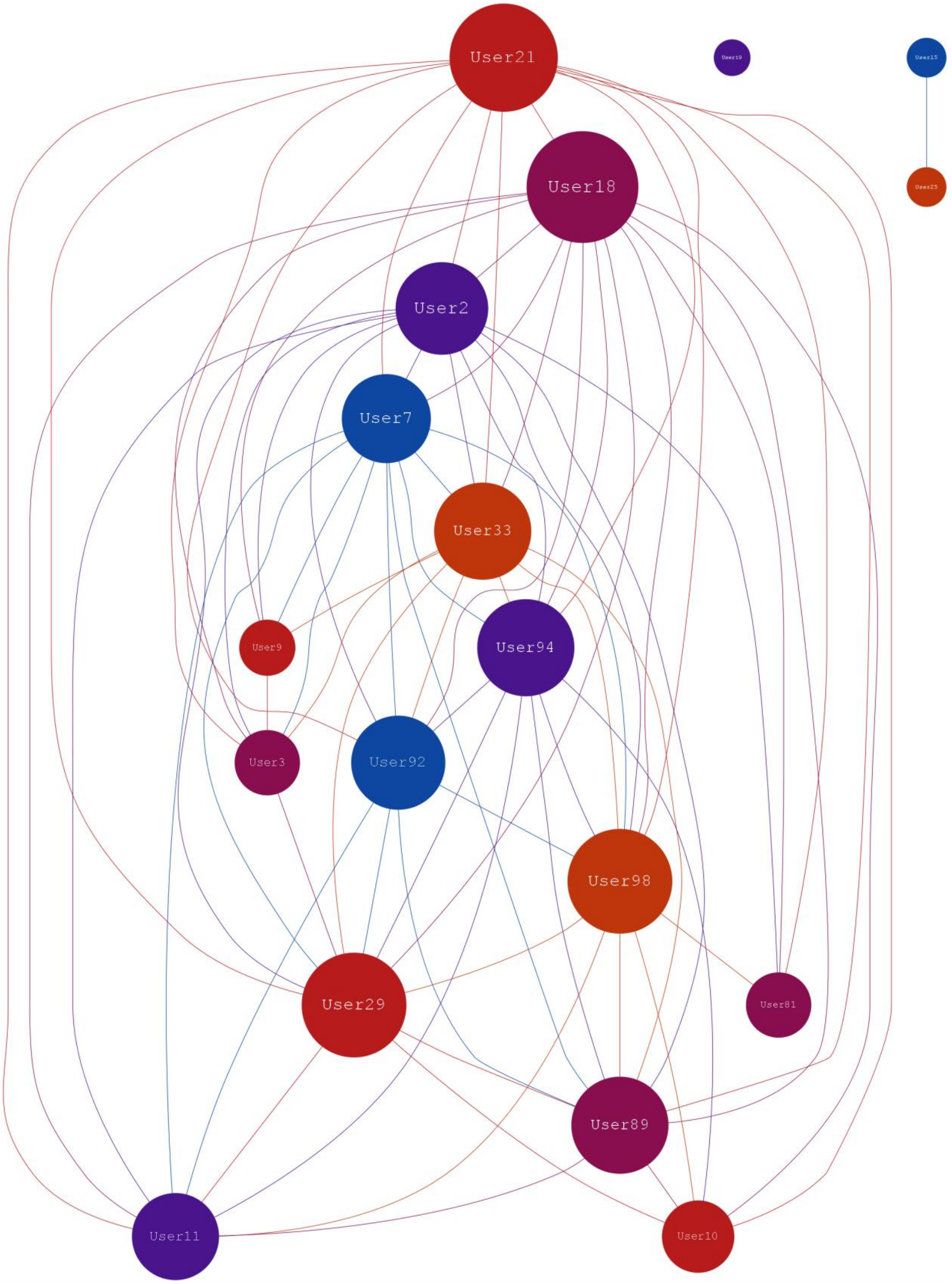


Figure APP-15: Degree of centrality Hour and Event.

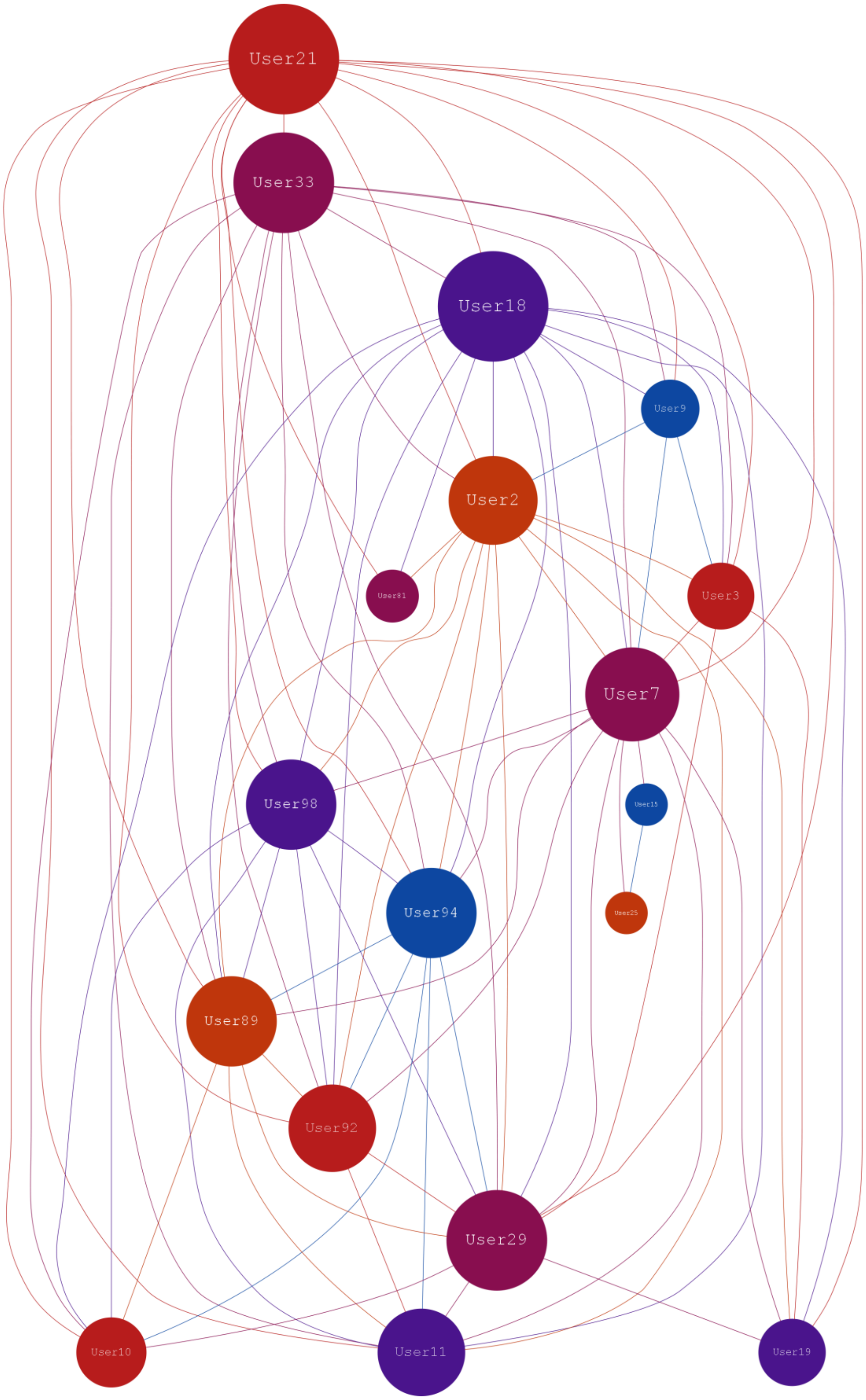


Figure APP-16: Degree of centrality Hour and Magnitude.

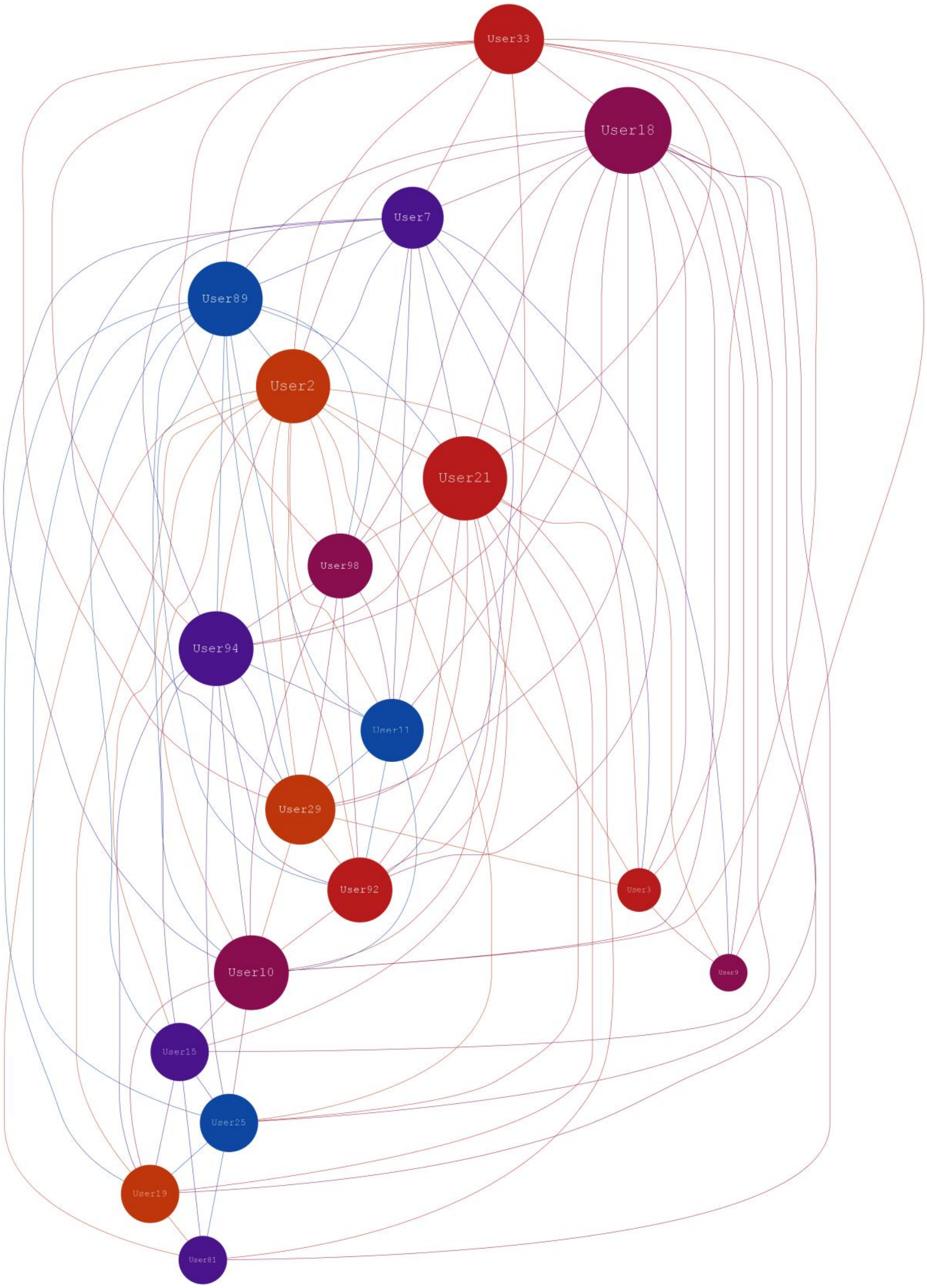


Figure APP-17: Degree of centrality Magnitude and Event.

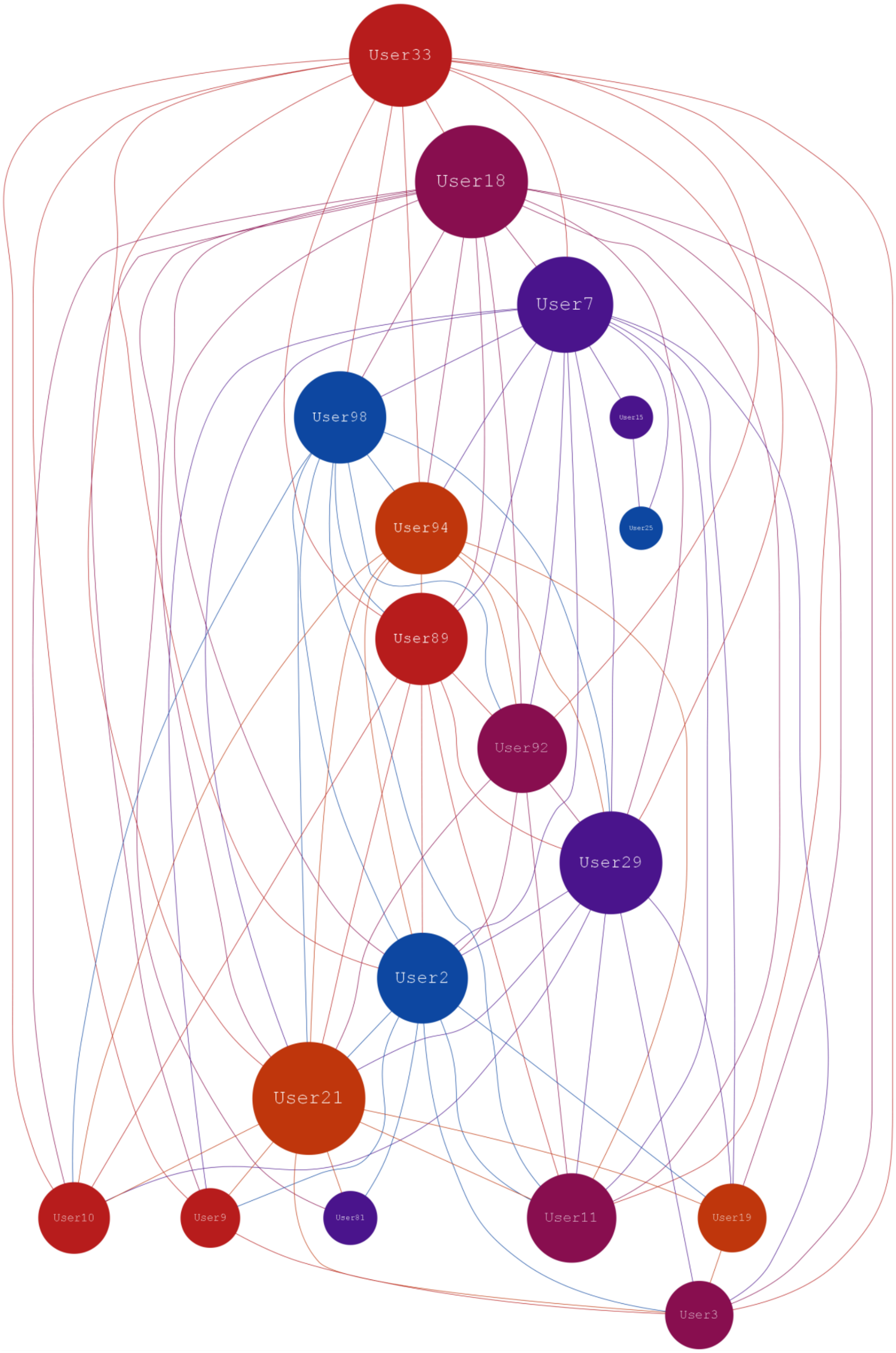


Figure APP-18: Degree of centrality Magnitude and Hour.