Information security strategy for Smart Government in United Arab Emirates – Investigating future effectiveness, threats and vulnerabilities

استراتيجيـــة أمـــن المعلومـــات للحكومـــات الذكيـــة فـــي دولـــة الإمـــارات العربيـــة المتحـــدة – دراســـة الفعاليـــة والتهديـــدات ومواطـــن الضعـــف

by

SAEED ALKUWAITI

A dissertation submitted in fulfilment

of the requirements for the degree of

MSc IT MANAGEMENT

at

The British University in Dubai

Prof. Khaled Shaalan
May 2017

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

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 may be copied and distributed by The British University in Dubai for the purposes 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 I 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.

_____

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

Executive Summary

UAE has always aimed to be at par with the changing world, and transforming itself into a smart government was one of the steps. This transformation suggests that the governmental practices, policies and transactions are all transparent and are aligned with the latest technology. However, while the transformation is a step ahead, there is a lacking of Information security strategy in the smart government framework. Information security is an extremely important aspect of smart government as smart government heavily relies on technology- especially the internet and web; and technology is prone to malicious attacks and threats. Loopholes and vulnerabilities provide a chance for hacking and other attacks. This paper has attempted to learn in detail the information security strategy of the UAE through literature review and qualitative analysis. Based on the results, a conceptual framework has been drawn out which suggests the important factors that need to be adopted as well as discussed in order to ensure a strong and robust information security strategy for the smart government of UAE.

الملخص التنفيذي

تهدف دولة الإمارات العربية المتحدة دائما إلى أن تكون على قدم المساواة مع العالم المتغير ومواكبته، وتحويل نفسها إلى حكومة ذكية كان واحدا من الخطوات. ويشير هذا التحول إلى أن الممارسات والسياسات والمعاملات الحكومية تتسم بالشفافية وتتفق مع أحدث التقنيات. ومع ذلك، في حين أن التحول هو خطوة إلى الأمام، وهناك افتقار إلى استراتيجية أمن المعلومات في إطار الحكومة الذكية. أمن المعلومات هو جانب مهم للغاية من الحكومة الذكية والحكومة الذكية تعتمد اعتمادا كبيرا على التكنولوجيا، وخاصة الإنترنت وشبكة الإنترنت؛ والتكنولوجيا عرضة للهجمات والتهديدات الخبيثة. توفر الثغرات ومواطن الضعف فرصة للقرصنة وغيرها من الهجمات. وقد حاولت هذه الورقة التعرف بالتفصيل على استراتيجية أمن المعلومات في دولة الإمارات العربية المتحدة من خلال مراجعة الأدبيات والتحليل النوعي. واستنادا إلى النتائج، تم وضع إطار مفاهيمي يوحي بالعوامل الهامة التي يجب اعتمادها وكذلك مناقشتها من أجل ضمان استراتيجية قوية وقوية لأمن المعلومات للحكومة الذكية في دولة الإمارات العربية المتحدة.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Background

With the rapid increase of the urban population, a lot of pressure is on resources in order to meet the demands of the growing population. The UAE has been home to a large number of expatriates and number is only increasing. This has prompted the UAE government to take the smart approach and has thus been striving to become a smart government. A number of initiatives have been adopted to become a smart government as the country aims to become a smart city. The vision of smart government is very vast as it aims to manage the entire city by embedded technologies. Such governments monitor as well as integrate all of their infrastructure, people, utilities, education, health and overall management via information and communication technologies (ICT) (Ijaz et al., 2016).

ICT has proven to be a useful tool in administration as well as setting up an environment that harbours a favourable setting to establish political motions worldwide (Hirschfeld, 2012; Reddick, 2010; Serageldin, 2011). These new technologies are equally risky as they can potentially expose massive surges in power among those who wield it to form relationships that strengthen political ties as well as make strategic relationships (Beer, 2011; Nixon &Koutrakou, 2007). Smart government is a unique approach in this respect, where the government simply provides channels of its services for easy access and utilization. In a society where ICT is a mainly predominant feature, smart governments can prove to be an invaluable form of administration and governance. Through smart government, the public will not have to spend much of their money or time in order to procure the relevant information and services that they are searching for. There are numerous benefits to having a smart government in practice. They are: efficiency, improved services, better accessibility of public services, and more transparency and accountability (Atkinson & Castro, 2008).

ICT in this regard, poses as much a threat as it does a boon for communications. More businesses today are facing security threats that cause drastic business discontinuity since many of the company's main channels of function and distribution are accessed through a networking platforms as well as different shared access points. In the same vein smart services could become vulnerable to open-ended attack that can take the relevant data of the government hostage at any given point in time. Although various guidelines and manoeuvres are being implemented and discussed for the safety of the government and government related entities, there is still a notion

within government bodies that undermine the effectiveness of a security threat and the danger it can pose to the existence of the processes that these governmental organizations have put in place. Data is an organization's most valuable asset and events such as corruption, data loss and data mining can instantly overturn the reputation and the functional capacity of a smart government.

The current trend in security standards is not completely fail proof and consists of various loopholes through which attackers can cheat the system and bypass the necessary security protocols (Ijaz et al., 2016). However strong the basis of security is and despite the rules and guidelines established to assess measure of security of a company, it is still prone to an attack that can disarm a secure network should the event arise (Ijaz et al., 2016). This is why the security standard is constantly evolving and changing as rising security threats continue to occur. In the case of a smart government, as it controls more than one distribution channel, which means that there are numerous sectors and departments that are unified under one single body, the importance of having stringent security measures is of prime concern. Having different organizations linked to one another through a common platform opens the risk of one channel being affected that results in the multitude of channels interlinked to be affected as well. This research paper aims to identify these threats and discusses the standards for information security at length in order to gauge what changes are needed to ensure privacy as well as safety from threats and attacks.

1.2 Problem Statement

UAE, since the formation of the Union has undergone a number of administrative reforms. In 2013, the UAE government came up with the desire to become a smart government. This is why the nation has called upon the importance of having a smart government installed into its current method of governance (Habibur Rahman, Yousef AlRaeesi AlBalooshi and Sarker, 2015). Steps are currently being taken to ensure that there is a smooth transition of the government into a smart government, by fusing the current generation of processes into a technologically-oriented hybrid, thereby introducing new technological infrastructure to integrate all the various channels of distribution (M. Al-Khouri, 2012). IT, however progressive, still holds certain risks that can potentially harm national security, should the internal systems by compromised. This is why information security needs to be established in order to protect the citizen's information and government system as well as put down any threat that makes its way into the smart government system.

It becomes a much simpler task in identifying the threats that prevail by first analysing the key components that reside in an information system environment (Ijaz et al., 2016). How the process of transforming government into smart government can also serve as good knowledge for developing strategies for policy and effective implementation. The current literature supports this forward-thinking process, adding that acknowledgment of both technical and social issues is important in order to zero in on the security concern. With the growing development of UAE becoming a smart government, there is an imminent need for secure frameworks to establish Information Security strategy and implementation strategy for the various modules and aspects that the smart government features. Providing relevant data in the interests of the experts on the domain and policymakers, would help in advocating better norms for safety procedures as well as identify key catalysts in the building of relationships that branch from government sectors as well as private sectors. The purpose of this study is to understand this relationship between smart government and information security strategy and discuss key issues that determine the threats and vulnerabilities faced by information security within a smart government.

1.3 Research Aim and Objectives

The urban growth poses its own benefits and challenges; the UAE has seen an influx of expats from across the globe in recent years which has caused a significant evolution of demographic and social ecosystems along with adaptation of city governance according to the changing economies. The Emirate has become more 'smart', and has taken a much more rational approach in the manner services are being operated as well as delivered; aiming at a better quality and sustainable life for the residents. There are a number of definitions of smart city, but for the purpose of this research it is defined in terms of delivery of services based on information and communication technology (ICT) which is a key enabler. The systems are all interconnected and the development of the city is dependent on these systems. However, there are many risks associated with its implementation and this research's main aim is to identify these threats and risks through a consolidated framework. The aim of this research is to:

> *Develop a framework for information security strategy for UAE to benefit the future government in taking a consolidated approach to enforce security, achieve early detection of risks and threats, and enhance security at national level*

In order to do so, there are a few objectives which the research will address:

- A comprehensive review of the literature in the IS and smart government areas, with a critical analysis
- To identify the role of Information Technology in the smart city implementation and the factors that restricting the deployment of information security
- To conduct a detailed qualitative analysis on the identified factors in IS and smart government and propose a suitable strategy for IS for future government in UAE

1.4 Research Questions

2. What is the current scenario of information security strategy in UAE and on what factors are the key initiatives developed?
3. What are the factors that define the smart government mechanism leading to achievement of information security and a strong operating model?
4. How can UAE transform into a smart government with information security supporting future innovation and development?
5. What are best practices to be followed to establish information security strategy for smart city / smart services?

1.5 Dissertations structure

This thesis has been divided into 5 Chapters which are discussed below:

Chapter number	Description
Chapter 1-Introduction	Under this chapter, an introduction to the thesis, the background, problem statement, aims and objectives of research, research questions and research structure have been discussed. This chapter helps to identify the research topic and understand the research problem at length so that the literature review can be aligned to the research questions.
Chapter 2- Literature Review	This chapter provides the reader with an understanding of the literature related to the various topics related to the thesis' main

	topic which further helps to develop the conceptual framework which forms the basis of the research. The main topics within the Literature review include: ▪ Smart Government Background, which comprises of smart government / smart services – definitional analysis, smart government and services concept and its evolution, characteristics of a smart government / smart services and smart government / services (SGS) and information security ▪ Information Security comprising of a detailed bbackgrounds followed by definitional analysis of Information Security and existing literature. ▪ Information Security Management and its Standards ▪ The role of Information Security in Smart Government, covering the challenges of information security for Smart Government, identifying the threats and critical success factors in Information Security in Smart Government. ▪ Conceptual Framework
Chapter 3- Methodology	This chapter solely talks about the research methodology used for collection of data for the purpose of the present research paper. It begins with an introduction about the importance of research methodology and how it helps in the accurate and systematic collection of data, followed by brief descriptions about the various research methodologies, their benefits and what methodology has been chosen for this research paper. Finally it talks about the interview, its relevance to the study and the outcome of the interviews.
Chapter 4- Results and Discussion	This chapter begins with an introduction to the chapter, followed by an in-depth data analysis of the interview conducted. Qualitative analysis is carried out which helps in the understanding of the responses recorded and each question is discussed to understand the general consensus as well as depicts the outcomes that the researcher has reached upon analysing the data.
Chapter 5- Conclusion and Recommendations	In this chapter, the reader is presented with the research outcomes, recommendations for future studies and future research

	opportunities. Furthermore, limitations of the research are also discussed to enable future research. Thus this chapter provides a systematic outline of the entire research paper so that it is easy to navigate through the paper for the reader.

Chapter 2: Literature Review

2.1 Introduction

As UAE grows exponentially, there is a rising pressure for the need of smart government that is transparent, easily accessible, reliable, and promotes environmental concerns. Such smart governments are the need for a technologically advanced world of today and identifying this need, the UAE government too has taken initiatives to transform into a smart government. However, it is important to note that Information Technology (IT) is a major component of such a smart government and therefore the government needs to adapt them into their agenda. However, recognition of the complexity of making use of information technology and the associated risks is vital (Gil-Garcia, 2005). Therefore a number of structured tools have been developed that support the IT infrastructure and ensure information security at every point. This chapter talks in detail about what is smart government, its definition, about information security and its association with smart government, especially with respect to the UAE.

2.2 Smart Government Background

UAE has emerged as a leading country in terms of innovation, technology, infrastructure and strategic security (Efthymiopoulos, 2016). Innovation solutions are a necessity for places like the UAE to increase its productivity and to accommodate the requirements of its citizens. Finding smarter ways of operating can be rather challenging and UAE is no exception to this fact. In order to deal with this, the government has transformed itself into a smart government- a government wherein there is implementation of a set of processes and underlying technological capabilities in order to enable seamless flow of information from across governmental organizations and programs. While doing so the government becomes more intuitive in providing high quality services to the residents across all governmental organizations and programs (Rubel, 2014). Following this route, the UAE government has achieved a lot of success in becoming a smart government thanks to the introduction of eservices in all government sections. Today, those in the UAE can easily avail all the governmental services via the internet without having to make a run to the respective ministries. Although the transformation hasn't been complete, it is steadily making changes, readying the smart government for smart city initiatives and implementation.

2.2.1 Smart Government / Smart Services – Definitions

Smart government is a relatively new term, although its conception can be seen since the early 2000's. Various researchers have tried to define this concept and have linked it to smart city concept. Smart government forms one of major dimensions of smart city (Giffinger and Gudrun, 2010). Key and We (2009), relate smart government to smart ICT procedures for education, cross-agency working etc. In the same manner Rahman et al. (2012) state that a smart government is the one which makes use of ICT and is reliant on the internet. Cellary (2013), Mellouli et al. (2014) and Rubel (2014) further corroborates to this theory stating that a smart government is the one which makes extensive use of smart technology for completing and achieving governmental tasks. In the opinion of Savoldelli et al (2014), it is the next step towards an open government that makes use of innovation. Gil-Garcia et al. (2014) too agree that a smart government is all about innovations and emerging technologies. Innovative polices are used by a smart government to fulfil tasks (Dolicanin, 2014). Gil-Garcia et al. (2015) simply puts it that it is a source of is the source for smart public service delivery. Table 1 lists out these definitions for clear understanding.

Table 1: Definition analysis of Smart Government / Smart Services

Definition	Reference
A smart government is that which makes extensive use of smart technology for achieving all governmental tasks.	Cellary (2013) and Mellouli et al. (2014)
Implementation of a number of ICT based business processes which assists in the cross-government flow of information along with provision for high quality service.	Rubel (2014)
Smart ICT government procedures which includes infrastructure for educational training, cross-agency working groups for all ICT fields and establishing procurement strategies.	Key and We (2009)
Smart government is the next step for an open, e-government which makes use of innovation.	Savoldelli et al. (2014)
Smart government is the mix of innovations and emerging technologies in the public sector.	Gil-Garcia et al. (2014)

A smart government uses information and communication technology; especially the World Wide Web and the internet in order to run government activities in relation with government stakeholders	Rahman et al. (2012)
Smart government makes use of innovative policies along with business models and technology in order to address the environmental, financial and service challenges that face the public sector.	(Dolicanin, 2014)
Smart government is the source for smart public service delivery, of city administration and of public engagement.	Gil-Garcia et al. (2015)

2.2.2 Smart Government and Services- Concept and its Evolution

The smart government landscape has been evolving continuously, reflecting on how governments are trying to search for innovative digital solutions for economic, social and political issues, while in the course laying down new processes. In a narrow sense, smart government makes use of apt use of the internet for running government activities. The concept of smart governance is dependent on consolidates information systems and communication networks (Dolicanin, 2014). According to Gil-Garcia and Martinez-Moyano (2007), the evolution of smart government towards a more transactional and integrated presence of the government over the internet and the spike in technological as well as organizational sophistication that happens on the national and local level are extremely important dynamics of the evolution of smart government. Upon tracking the evolution of smart government from the electronic one in 90's to the digital by default agenda one today, Katsonis and Botros (2015) have pointed out that during the progress, there was an increase in cultural, governance and leadership challenges as well. The transformation of government to the smart government can be attributed to the evolution of technology, institutional arrangements and organizational networks. The transformation of a government to a smart government results in internal transformation as well as changes in the relationships between social and political actors and the government, via the development of the communication and information technologies in the government (Luna-Reyes & Gil-Garcia, 2014).

2.2.3 Characteristics of a Smart government / smart services

There are two dimension of a smart government; governmental administration and public service management. In the opinion of Nam and Pardo (2011), a smart government is efficient and effective in management of front as well back office management of city government operations. For a smart government to be able to be transformed into one, there are certain paradigms which need to be fulfilled. Technology plays a vital role in the evolution of a government as it strives to become more efficient and transparent, becoming more accessible to the people. It is becoming imperative for governments to take a citizen-centric approach and focus on citizen management (Anthopoulos, 2017). Furthermore, smart government is agile and responds to the demands of the citizens, administration and businesses in a technologically driven manner (Habibur Rahman, Yousef AlRaeesi AlBalooshi and Sarker, 2015). Accountability and transparency form the core of a smart government (Habibur Rahman, Yousef AlRaeesi AlBalooshi and Sarker, 2015). The core characteristics of a smart government have been detailed below in table 2.

Table 2: Core Characteristics of Smart Government

Factor	Description	Sources
Accountability	The government is accountable for all the services being provided and any discrepancies is the government's outlook.	Habibur Rahman, et al. (2015)
Transparency	All governmental transactions, fees and any other dealings are transparent in a manner that people are aware of what they are being charged and what service they will get.	M. Al-Khouri, (2012)
Use of ICT	The core of a smart government is the use of Information and communication technology (ICT) as technology plays a major role in the transformation of a government into a smart government.	Giffinger and Gudrun (2010)
Smart economy	ICT enabled smart systems in all sectors including healthcare, transportation, e-business and e-commerce etc.	(European Parliament Committee on Industry, Research and Energy., 2014)

2.3 Smart Government / Services (SGS) and Information Security

While the desired aspects of a smart government with respect to development and functioning can be fulfilled via various means, one important aspect that needs attention is the security threat in the digital world. Currently, privacy of those using the information technology is vulnerable to many security breaches; this is mainly because the security system can be penetrated via a number of applications such as programs, advertisements and also spam emails. It is obvious that it is the main internet protocols as well as network architecture that when ignored leads to vulnerabilities in the information security systems. This causes those users who are unable to identify threats or seek easy solutions at potential threat from innocent looking applications or approaches (Otero, 2015). This is why it is imperative for smart governments to acknowledge built-in security systems for the future smart city implementation. In the opinion of Lewis (2015), being a smart attacks means being advanced in mobility which lead to being more disruptive. When faced with these threats such as malware, fraud and phishing, it can cause smart government to face severe economic issues. Since internet offers a lot of flexibility, there are multiple methods of security breaches via communication technologies. As systems grow to become more complex, handling more information and becoming more interconnected, city IT ecosystems are increasingly built on public sector cloud or through infrastructure visualisation along with social and mobile computing as the primary services and applications access point. Therefore the expansion of smart city's technological as well as communication environment leads to increased vulnerabilities for attacks. According to research by Gupta and Gupta (2015), nearly 40% of fake transactions have been initiated from mobile devices. Furthermore, according to the Data Breach Investigation and Statistical Report (2015), 2,122 out of 79,790 incidents related to security took place in organizations in varied countries and confirmed data breaches. It is observed that the sectors that have been most affected by such breaches has been the public, financial and information services and thus, smart government services need to pursue sophisticated protection strategies and also develop solutions that give preference to information security as the most important consideration. It is important to note that it is not feasible to provide the same kind of protection for all the elements of a smart city ecosystem and therefore smart government will have to identify the most crucial areas that are vulnerable to attacks.

2.4 Information Security Introduction

Park and Ruighaver (2008) & Ahmad et al. (2014b) have stated that the more integrated the Information Security (IS) plan is towards the central framework planning of an organization, the more effective its security features can be. It is also an intrinsic part of an organization as it helps in eradicating threats to a company's information. IS can be acknowledged as being one of several key components that feature safety measures, with the following qualities whenever required. They are deterrence, prevention, surveillance, detection, response, deception, perimeter defence, compartmentalisation and layering. It is important for bigger business personalities to endorse the validity of having an information security system in place, especially with respect to smart government/services.

IS is an extremely vital challenge which has not been addressed fully yet in the construction of smart government (Ferraz, Sampaio and Ferraz, 2015). At the same time it is not just vital to maintain data that is trafficked but is also important to provide the city government ways in which data can be shared responsibly as well as be protected. In the opinion of Sen (2013), there are many information security issues, especially related to privacy within the sphere of smart government which need to be addressed urgently. In order to do so, a basic understanding of Information Security and its definition is important, which will be discussed in the ensuing sections.

2.4.1 Background

When there are security threats established, contingencies are set in place. Understanding contingency management helps in improving the response time to threats discovered as well as builds relevant knowledge about the organizational management as well as the technology behind the information system. IS is ingrained in the business strategy as much as any other facet of the organization, according to Sveen et al. (2009) and serves the purpose of building more resources. According to Hong et al. (2003) however, imply IS as being but a functional value of various orientation systems such as policy orientation, risk management orientation, control and auditing orientation, management systems orientation and contingency management. Sveen et al. have merely described IS but have not delved into a definition of the term. It is with their comprehensive analysis that our study can merit from their findings.

There are numerous definitions surrounding what IS really is. Sveen et al. (2009) maintain that it is but a process of business strategy, but Ahmed et al. (2014b), Hong et al. (2003) along with

Ruighaver (2008) do not share the same perspective. Beebe and Rao (2010) define IS as being a plan of action. And although many other researchers mention IS as being 'information security strategy' in their respective literary mentions, their definitions are still not as definitive or conclusive.

There are two concepts that researchers choose to underscore while describing IS. They are: (1) a static plan, described as a tool to be commonly used by stakeholders (Beebe and Rao, 2010; Von Solms and Von Solms, 2004 and Bowen et al., 2006), and (2) a dynamic process, to be followed by stakeholders concerned with protecting organisational information (Flores et al,. 2014; McFadzean et al., 2006; Sveen et al. 2009; Van Niekerk and Von Solms, 2010). An extraction of the core values that arise out of the understanding of these two concepts will help in IS research applications. While some researchers maintain IS as a static plan that is meant to link the goals, policies and action sequences of an organization, they are still fundamental features that are naturally attributed in an organization (Beebe and Rao, 2010; Baskerville and Dhillon, 2008). Process orientation involves strategy-setting while keeping the goals of the organization's security structure intact, by means of regulatory compliance. Some researchers and scholars do not acknowledge IS strategy at all but rather deconstruct it and add it to the business process somehow, under a different guise (Park and Ruighaver, 2008; Hong et al., 2003;). As mentioned through process orientation, the set up achieves the purpose of receiving the end goal by producing a business strategy or by separately conjoining the IS strategy with the business strategy as well.

2.4.2 Definition of Information Security

Information Security (IS) is broadly defined and is approached in various ways as well as implemented through numerous methods, they are all varied and do not provide a coherent definition. Information security (IS), is an important component of all those entities which make use of ICT. Therefore IS is vital for organizations, smart cities as well as smart government. Therefore the definition of this concept differs, based on the relevant entity. Park and Ruighaver (2008) describe it as the art of deciding how and what defensive IS technology to use on the incoming threats and attacks on the organization. NSTISSC (1999) provides a rather comprehensive definition stating that it is mere protection of information systems from unauthorized access or stopping the modification of data. P. Pironti (2010) goes on to state that IS protects the information and other important elements such as hardware and systems**.** Beebe and

Rao (2010), explain that it a plan which integrates the IS plans, policies and action sequences into a whole. Lastly, Felipe et al. (2015), reiterates that IS addresses attacks that are made on the interoperable systems of a smart city. Hence this section of the literature is structured based on the author's perceptions over the concept-centric perceptions that have been adopted so far.

Table 3: Varied definitions of Information Security

Definition for Information Security Strategy	Reference
IS is the pattern or plan that integrates the organisation's major IS goals, policies, and action sequences into a cohesive whole	Beebe and Rao (2010)
IS is an art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defence (sic) organisation's information infrastructure(s) against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while to be effective"	Park and Ruighaver (2008)
It is protecting the information system from unapproved access to or modifying the data whether it is in the stage of storage, processing or transit as well as against denying services to the authorized users including the measures that are essential to sense, document and counter the threats	NSTISSC (1999)
Information security addresses the attacks made on the interoperable systems of a smart city by various channels as well as looks into the unintentional compromises made by user errors, natural disasters and equipment failures.	Felipe et al. (2015)
Information security is the protection of information along with its important elements including the hardware and the systems which are used to store and transmit information.	(Whitman and Mattord, 2012)
An information security strategy of an organization provides a roadmap for information infrastructure protection with goals and objectives that make sure that the capabilities assigned are aligned to the risk profile of the organization.	(P. Pironti, 2010)

2.4.3 Analysis of Information Security

Upon analysis, actual responses to security measures and real-world experience, analysts and researchers have come up with certain remedies. While the management does acknowledge internal security threats by securing the information infrastructure, it does away with past technology-centred ideals (Colwill, 2009; Catrantzos, 2010). There is a necessary process that

needs to be undertaken that abides by the relevant rules and regulations set up by the authorities (Gerber and von Solms, 2008). It is because of these measures that the need for a proper program that incorporates training and awareness is established to protect the interests of the cyber space (McCrohan et al., 2010). On the other hand, Polónia and de Sá-Soares (2013) have, in a recent study, pointed out 26 different issues in IS management and have assigned degrees of importance to them. However, their study is more enterprise and organizational focused, hence their understanding of national and international functions on this platform are not as definitive.

As the cyber realm stretches beyond the boundaries of geographic borders, any semblance of a framework or guideline should acknowledge laws and regulations that are the same for the enterprise level as well as the national and international level of governance as it is they, who authorize the relevant protocols when responding cyber threats such as cyber warfare and cyber terrorism. Many instances have been made where the internet has now become but a reflection of our life (Jung et al., 2010) and organizations are adapting to its environment and architecture (CyLab Report, 2010; Westby, 2010). There are however, certain novelties to be found when searching for fresh approaches in dealing with cyber security and its threats (Oliver, 2009). Currently, the information infrastructure and its components are mostly acquired by the private sector even through the security level is national-level at best. The public-private partnership and its framework as well, are what define the current landscape of IS (Navare and Gemikonakli, 2010).

National security is integrated with cyber space (National Security Threats in Cyberspace, 2009) and the level of national-grade policies being implemented and structured across frameworks is also being implemented across the public domain (National Cyber Security Policy, 2011). The establishment of international standards for cyber security and its need has been fully made aware of and a number of institutes as well as bodies have come together to serve that cause (DHS, 2009; Dogrul et al., 2011; BIC, 2013; Forsyth, 2013).

In contemporary literature, the impact and the importance of new policies in the cyber domain through various initiatives has been fully addressed and acknowledged, especially on the basis of information security (Torres et al., 2009; Goel and ChengalurSmith, 2010). There is also a need for a model to be created and implemented to incorporate the security behaviour that at the same time addresses information security issues, for which the same is currently being worked upon by the relevant authorities (Liang and Xue, 2010; Knapp et al., 2009). Next Generation Networks

(NGN) is an integral part of the information security discussion currently, and forms as the basis upon which future arguments and ideas will be shared. It also consists of internet applications for business uses that operate co-dependently with other applications for the smooth running of business (CISCO, 2011). The current literature discusses the move from the technical perspective to the managerial perspective, as well as the shift in enterprise-level security to national/international levels of security. Coinciding all of these points is the unifying need for having a holistic framework that integrates the best of these modules and security solutions.

2.5 Information Security Management and its Standards

It cannot be denied that information is an important asset of a smart government, thus protecting its security becomes imperative (Susanto, Nabil Almunawar and Chee Tuan, 2011). However, there isn't a single solution that would help in information security; thus there are a set of standards or benchmarks which when adopted present with adequate amount of information security. These fall under the activities of the Information Security Management Systems (ISMS) that manages the resourced and configures the various requirements to the resources allotted. The primary objective of ISMS is to establish the security protocols as per the business standard of the organization. Application of these standards in the smart government framework will help to achieve information security while ensuring accurate use of resources. According to ISO/IEC 27001:2005 (2005) standards, ISM is an integral part of the broader management system that is related to different approaches in business risk, as well as necessitate, monitor, operate, review and implement the information security (ISO/IEC 27001:2005, 2005). The planning activities, the procedures, the policies and processes are also all governed by these protocol methods. There are essentially three methods of operating. They are: strategic (policy driven), tactical (guideline driven) and operational (measures driven) (Eloff and Eloff, 2005). Information Security Management System (ISMS) becomes a culmination of the procedures, activities and the accumulation of resources as well as their implementation by the organization in order to protect critical management assets. It is entirely dependent upon the organization's ability to face risks. By taking into account the various risks that an organization has to be aware of ISMS can only be successful in realizing the various factors that can be used and methods implemented to protect these information assets (ISO/IEC 27000:2012, 2012). According to some scholars (Eloff and Eloff, 2005; Posthumus and von Solms, 2004; Hong et al., 2003; Ma et al., 2009), some suggested

methods for framework involve addressing of issues as mentioned in the tables (Table 2). For example, Posthumus and von Solms (2004) have emphasized that the external and internal factors of implementation are the best ways for going about approaching a successful implementation of ISMS. Musa (2010) also mentions that covering standards, performance analysis as well as policy management under information security is also important. This is why there is a growing need into finding effective means as to managing information security into the various specified factors. The table (Table 3) further explains the key factors which are vital components of the previous IS framework and which help to identify those components that are required for the IS framework for the smart government of UAE.

Table 4: Key factors as identified in past IS frameworks

Source	Key factors	Highlights of the research	Focus
Musa (2010)	▪ External factors ▪ Regulatory standards ▪ Legal ▪ Best practices Various business-related issues ▪ IT infrastructure ▪ Internal factors	**INPUTS** Strategy in IT, as well as the risk assessment factors, the regulatory requirements along with processes for the baseline security **PROCESS** Information security – policies, standards and objectives as well as the implementation methods, along with policies decided, mentoring and evaluation of performance **OUTPUT** Alignment of the strategy, measuring the performance, value delivery, risk and management of resources	Information security governance framework
Ma et al. (2009)	**Five steps:** 1. Evaluation of the organization environment 2. Bring to light the various security objectives 3. Take into account the numerous requirements for security 4. Manage the controls for security 5. Apply training methods for security and management purposes.	▪ Based on four guiding principles ▪ Consisting of a specific goal to follow ▪ Converging the security goals with the business strategy ▪ Showing ISM as being dynamic as a process ▪ Showing ISM as being a multivariate system	Integrated framework for ISM

Source	Key factors	Highlights of the research	Focus
von Solms and von Solms (2006)	▪ Strategic Factors. ▪ External: external risk, regulatory as well as legal complexities. ▪ Internal – Role of the IT department, strategic vision for the company as well as convergence of IT and company's visions, competition etc. ▪ Tactical Factors: Policies on security measures, standards as well as the procedures followed. ▪ Operational factors. ▪ Guidelines prescribed by administration.	**Core principle 1** There are three distinct levels for the information security governance: Strategy, Tactical as well as Operational. **Core principle 2** Three specifc actions to follow – to direct, to execute and to control at all levels.	Information security governance model
Eloff and Eloff (2005)	▪ Various policies on security, standards as well as the procedures implemented. ▪ Security culture – awareness and harnessing through training prgrams, supervising compliance based programs at risk management at the organization and infrastructure level.	**Five requirements** 1. Have a holistic approach and culminate all aspects 2. Merge many roles to create better implementation methods 3. Have a comprehensive method for information security 4. Management of risk is integral and have a predetermined life cycle 5. Should be measurable	Information security Architecture
Posthumus and von Solms (2004)	▪ Internal Factors. ▪ Business issues / IT setup. ▪ External factors. ▪ Best practices used/ legal formalities/regulations followed.	Having adequate information security policies is a corporate responsibility	Information security governance framework

Since Information Security plays a vital role in the supporting important smart government activities, it is important to have a standard or benchmark that regulates governance over information security (Susanto, Nabil Almunawar and Chee Tuan, 2011). There are various bodies established that make benchmarks for organizations to follow according to appropriate information security methods. They also take up legal regulations so that there are adequate guidelines supported, to ensure that the organization does not misuse or mistake the policies and used in the most effective manner possible. IT governance follows many IT standards such as PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT. However, it should be noted that all these standards are not well adopted by smart governments due to a number of reasons. Therefore, instead the Big Five of ISMS Standards are used readily for information security. Below is a table that demonstrates the factors that comply with the standards of information security, based on the big five ISMS standards.

Table 5: Comparison of IS factors across big five IS standards

Factors	COBIT	ITIL	PCIDSS	BS	ISO 27001
The Information Security Policy Implementation	✓	✓	✓	✓	✓
Methods revolving around access control	✓	✓	✓	✓	✓
Management of Operations as well as communication	✓	×	✓	✓	✓
Acquisition of information systems, maintenance and further development	✓	×	✓	✓	✓
Management of assets	✓	✓	✓	✓	✓
Information security and its organizational aspects	✓	✓	✓	✓	✓
Management of incident security management				×	
Business Continuity Management methods	✓	✓	✓	✓	✓
Adequate Physical and Environmental Security	✓	×	✓	✓	✓
Compliance standards	✓	✓	✓	✓	✓
Implementation of Human Resources Security	✓	×	✓	✓	✓

From the table 5, one can see that the Big Five tick on most of the important IS concerns and addresses them in detail. This demonstrates their usefulness in smart city and smart government implementation. The fact that all five of them have compliance standards, have methods that revolve around access control, have proper management of assets take care of information security and the related organizational aspects and offer business continuity management methods clearly show their utility in smart government implementation in the UAE. Alfantookh (2009) has mentioned certain essential features which the smart government or any organization must implement. These are known as 11 Essential Controls or 11EC, which were also identified in past IS literature (Ijaz et al., 2016; Pironti, 2010; Eloff and Eloff, 2003;). As a benchmark, it is important that all ISMS standards cover this majority of these features to be termed as effective standards of information security. Multiple sources have discussed these features independently in literature. These 11 benchmark features are described in Table 6.

Table 6: 11 Essential Controls

11EC	Description of 11EC	Sources
Information Security Policy:	How institutions have to show their intent when elaborated to an information security system, the means institutions gather their information, as well as directing management and the staff towards the right implementation, information stakeholders of the primacy of the efforts towards the vision of the security of the organization.	Alfantookh (2009), Pironti, (2010)
Communications and Operations Management	A guided and assessed policy for security followed by the organization, significantly reducing risks and making sure that correct computing procedures, as well as operational procedures, controls and well-defined responsibilities are established.	Alfantookh (2009), Eloff and Eloff (2003)
Access Control	Gives power to an authority who can have access to specific areas as well as the resources required in a facility, or also on a computer-based information system.	Alfantookh (2009), (Ijaz et al., 2016)
Information System Acquisition, Development	A process that merges various protocols, establishes the boundaries and the technical information systems that begins with the acquisition, the development as well as maintenance.	Alfantookh (2009), P. Pironti, (2010)

and Maintenance		
11EC	**Description of 11EC**	**Sources**
Organization of information society	It is what the organization owns and is used to implement information security. It consists of the following: commitment and management to the information security on every level; co-ordination of the information security levels; authorization of the information security.	Alfantookh (2009), P. Pironti, (2010)
Asset Management	Considers the importance of tracking, identifying, classifying as well as assigning an ownership for the most integral assets of a company to make sure that they are properly protected and secure	Alfantookh (2009) (Ijaz et al., 2016)
Information Security Incident Management	Is a program that prepares the company for any incidents that may arise. Provides the resources and the innovation needed in identifying the problems in order to prevent future incidents from happening.	Alfantookh (2009), Eloff and Eloff (2003)
Business Continuity Management	To ensure that business continues under stressing conditions. Plans are kept in advance, should a situation present itself where BCM should be implemented.	Alfantookh (2009) (Ijaz et al., 2016)
Human Resources Security	To make sure that the employees as well as the contractors and users of sensitive data are eligible enough to match the criteria of fulfilling the job responsibilities and ensure that the relevant access to these employees is expunged should their job profiles be terminated	Alfantookh (2009) (Ijaz et al., 2016)
Physical and Environmental Security	Security measures that employ the protection of physical assets as infrastructure, systems, buildings as well as other environmental structures so that all the equipment and systems housed under them are firmly protected, which hold all the crucial information and data	Alfantookh (2009) (Ijaz et al., 2016)
Compliance	Which involves two specific areas: one which involves supporting numerous laws, regulations as well as other contractual requirements which make up an institution. The other, is the compliance of information security policies, the standards and the processes.	Alfantookh (2009)

2.6 The role of Information Security in Smart Government

The smart government in its simplistic terms is about making use of ICT to enable the general public and business partners in accessing governmental data and other essential services (M. Al-Khouri, 2012). It has still not been figured by the practitioners as to how they can exploit its full benefits. There exists an issue of equilibrium in applications related to smart government and restrictions that arrive for justifying the huge investments made in ICT for one and half decade. The expectations of public towards the administration are framed as per the capability of the government to bring an improvement in the overall life of citizens (M. Al-Khouri, 2012).

The government is further required to make sure that the policies, rules and services assist in the participation of citizens followed by addressing the needs for bringing an improvement in service delivery (Petrov, 2014). There is a need to reengineer and reshape the service delivery process so that expectations of the public can be met with respect to increased social security and life quality. The policies should be such that they are able to enable governments for bringing in radical changes in organisation such as fostering service growth; reducing costs and burden of regulations on companies; strengthening the overall training and educational system; boosting good managerial practices; fostering innovation and novel applications; nurture market scenarios followed by creating an environment where productive economy can be promoted (Petrov, 2014)

The smart government advocates have pointed out towards the prevailing opportunities for citizens by which they can play a better role in public policy (Habibur Rahman, Yousef AlRaeesi AlBalooshi and Sarker, 2015; Ambali, 2010; Navarra & Cornford, 2007). The advocates further lay emphasis on the potential to connect the citizens and deliver the governmental offerings in a quick and direct manner (absence of queues and waiting time, 24*7 service offering) (Pardo et al. 2011). Cost cutting has been regarded as the main factor that drives the decision to become online and Smart Government has a possibility to cut the overhead expenses by about 90 percent through streamlining communications and integrating the systems that have increased the level of effectiveness and convenience (Lee et al. 2014). The initiatives undertaken by the smart government can aid in reducing burdens, process time cycles as well as responsiveness (Lee et al. 2014; Bonina & Cordella, 2008). One of the benefits associated with smart government is the reduced costs; in comparison to the traditional over the counter services substantial amount of cost can be reduced by online services as there is no need for building infrastructure, appointing employees, and paying bills of electricity etc. The varied potential for development and

competition are offered by ICT in public sector areas such as client service and organizational excellence which may aid in lowering the cost of governmental services by computerisation and also increase the pressure on the firm to improve their performance standards and alter conservative attitude.

According to AlAhmad, and Al-Kaabi, (2008) ICT development and its capability to share and deliver data are bringing changes in the manner by which business is carried out by e-government system. Difficulties may arise while sharing data between governmental institutions and amongst the government, businesses, and public. The issues arise on account of the absence of trust as well as transparency in information system designing followed by the ethical and legal issues when the information system is being integrated (Mattord & Whitman, 2006). This legalizes the need for a complete security system that gives consideration to system integration parts. An information security strategy that takes into consideration the need for integration of all the government entities in order to provide a smooth and seamless experience to residents in a safe and secure environment.

2.6.1 Challenges of Information Security for Smart Government

The growth as well as the spread of electronic services has affected the efficiency of Smart Government system and thereby raised the challenges for governments in developed as well as developing nations. An additional attention will be required by government information for securing programs for avoiding any unwanted access that may affect the operations and reveal private data of the citizens (Francis et al., 2007). When talking about government information security the need is to identify varied aspects that might have an impact on the overall security of data. The security framework in the context of smart government is inclusive of three main elements being persons, procedures, and technologies (Francis et al., 2007). The present paper will focus on information security of Smart Government with respect to technical and non-technical perspectives. This is as smart government cannot be regarded as the only source of protecting the ICT assets however it can be regarded as protecting the technical and non-technical assets of governmental departments (AlAzizi, S. 2008). Hence overall security of smart government can be illustrated in the figure 1.

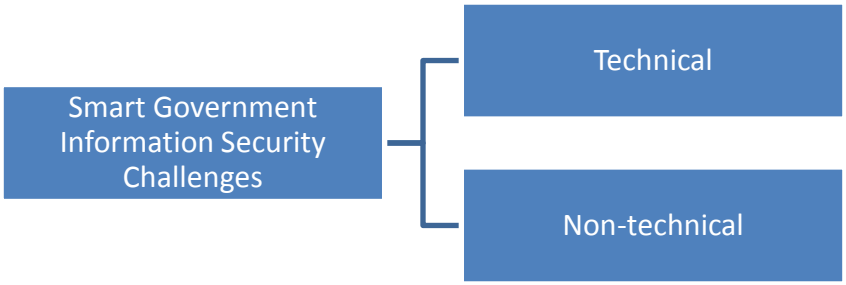


Figure 1: Classification of smart government information security challenges

Source: (AlAzizi, S. 2008)

2.6.1.1 Technical Security Challenges

There is a presence of many research studies that have given varied models for addressing security challenges as faced by Smart Government followed by measuring the C.I.A triangle (confidentiality, integrity, and availability). By exposing the security issues citizens in smart government can be convinced for accessing, sharing and exchanging the data in a secured manner (AlAzizi, 2008). There is a presence of varied kinds of technical and physical challenges that put an impact on the overall security of Smart Government data as shown in the below-mentioned table. Sharing of data between government departments is always regarded as a source of many security threats but it is essential so as to ensure towards completion of electronic service process in a secured manner. However, it is not enough to address and understand the threats from the technical viewpoint and hence challenges related to information security should be addressed from non-technical view point as well; emphasis should be given on these areas as their presence can pose risk for information security. These challenges are described in the table below.

Technical Challenges	Description of the challenge	Noted by
Network Security	The absence of internet availability; high costing especially in the developing nations; network attacks and issues related to system architecture and network topology are some of the challenges that are required to be taken care of.	Mazumdar, 2009 Polk, and Hastings, 2000
Privacy	Threats related to disclosure of confidential data as well as unwanted access to the private data of public.	Louie, 2014 Singh, and Karaulia, 2011
Identification	Securing the safety of participants with respect to unique identification.	Conklin, and White, 2006
Electronic Authentication	Success in smart government system can only take place when there is a presence of reliable identification system for public/private sectors and Government institutions.	Omura, 2000 Singh, and Karaulia, 2011
Access Control	It is the user-oriented kind which involves for identifying, authenticating and authorizing issues.	Rodgers, 2012 Mazumdar, 2009
Information Sharing	Exchanging data amongst governmental departments has always been of crucial concern.	Polk, and Hastings, 2000
Work Flow	Work flow technology is a method to manage work flow as well as data during the planning, implementation and assessment stages in Smart Government system	Khalid, et. al. 2014 Singh, and Karaulia, 2011
Data Type	Data classification is the procedure to sort out data resources on the basis of nominal values as per sensitivity (impact of laws and regulations). There is a classification of data and information sources on the basis of unauthorized access risk.	Zu'bi, and Al-Onizat, 2012 Mazumdar, 2009

Technical Challenges	Description of the challenge	Noted by
Network Infrastructure	The absence of properly installing network firewalls, the configuration of network security, issues related to internet protocol as well as dependence on the internet are the major source of challenges that has an effect on the safety of e-government.	Singh, and Karaulia, 2011 Polk, and Hastings, 2000
Interoperability	Absence of interoperability on account of semantics, absence of standards as well as different kinds of in classification system impacts the overall efficiency of e- government system	Anders, et. al. 2013 Webb, et. al. 2014
Usability	If there is a presence of high security then the usability potential is increased.	Webb, et. al. 2014 Al-fawaz, et. al. 2008
Security Policy	It is the plan that is utilized to find out essential resources of the institution followed by providing a thorough description of acceptance as well as rational behaviour from the public and stakeholders so that information security can be guaranteed.	Al-shboul, 2012 Mazumdar, 2009
Security Standards	These standards are about the security policies of the smart government as set by regulatory and governing authorities so as to ensure towards secured work atmosphere. It is inclusive of electronic voting, electronic democracy among others.	Livonen, 2011 Webb, et. al. 2014
Legal Framework	The absence of laws and policies on information security are likely to impact the trust in government in a negative manner.	Al-Azazi, 2008

Technical Challenges	Description of the challenge	Noted by
Privacy	There is a need to make usage of advanced techniques to increase the efficacy of public administration as well as enhance the confidence in privacy process by ensuring common transparency between the public and administration.	Al-fawaz, et. al. 2008 Mazumdar, 2009
Culture	Security culture showcases the major attitude towards creating a secured institution which is influenced by the regulatory and legal norms, the nation as well as institutional cultures.	UN, 2012 Al-fawaz, et. al. 2008
Awareness	Awareness about information security is required in order to understand the feasibility of security usage.	Zu'bi, and Al-Onizat, 2012
Trust	The trust in smart government is dependent on the relation that exists between smart government authorities and other institutions with respect to convincing the government infrastructure and the other government institutions.	Mazumdar, 2009 Iivonen, 2011
Political	The political issue acts as a crucial source of challenge in influencing information security with respect to smart government.	Anders, et. al. 2013 Mazumdar, 2009

2.6.1.2 Challenges of Information Security

Challenges faced by Smart government are parallel to the ones faced by information security. Both can be classified into technical as well as non-technical. As the above table lists them out, these challenges although specific to smart government, are also faced by IS. There are many resources in literature which talk about these challenges faced by IS. While culture is discussed as a non-technical challenge for smart government, it is also a factor for IS, as Mitnick & Simon, (2003) point out that human interaction is used as a device to break into security procedures. Networok security is a challenge that is common to both, outages and lack of firewalls can make it easy for threats to attack (Sen et al. 2013). Awareness is another major challenge that is faced in IS. It is

imperative that within the smart government framework, citizens as well as government entities be made aware of the security threats which loom over smart government in case of lack of IS strategy (Elmaghraby and Losavio, 2014). As mentioned earlier, there are a number of security standards which when applied to the IS strategy can help to secure the information. These standards have been formulated by organizational experts and they ensure that all sensitive information is always kept secure (Ijaz et al., 2016). Lastly, the absence of a legal framework which addresses the IS security breaches and the course of action in that area poses a major challenge for IS and its implementation (Kunzmann, 2014). The below table 7 presents a cross matrix of the challenges faced by both, Smart Government as well as Information Security.

Table 7: Mapping of Challenges of IS and SG

		Smart Government Challenges				
Information Security challenges		Network Security	Awareness	Security Standards	Legal Framework	Culture
	Network Security	X				
	Awareness		X			
	Security Standards			X		
	Legal Framework				X	
	Developing into a Culture					X

2.6.2 Identifying the Threats

As has been pointed out, smart government is built on technology and technology is prone to attacks in the absence of a good information security strategy. In order to formulate an effective information security framework, it is essential that the government be aware of the various threats that can affect the smart government initiatives in a number of ways.

Threats to Critical Infrastructures: Changing even a single process within the critical infrastructure can lead to massive losses or delays (Abouzakhar, 2013). Health care, telecommunication and industry all come under critical infrastructures. These infrastructures are implemented in smart

government on the basis of IoT and Smart Grids. Therefore any threats that could affect these two technologies should be reviewed and taken care of. Furthermore, the big data that is generated via these infrastructures need to be stored and managed in a secure manner. This falls on the critical infrastructure and therefore critical infrastructures need to be protected from malicious attacks that can lead to loss of vital information. For example, the healthcare is one of the most important critical infrastructures and a security threat to it can compromise the patient's privacy (Solanas et al., 2014).

Smart Mobility: This is another area of concern as personal information can be easily disclosed during the collection, publishing or utilizing phase. The information shared via smart mobility devices can be prone to malicious attack as there are very less safeguards. Therefore it is necessary to analyze the problem and in the domain and it requires the use of ICT technologies keeping in mind the security and privacy threats.

RFID Tags: The Radio Frequency Identification (RFID) tags are used massively within the smart government framework. While they are very beneficial, they are also prone to risks and threats (Xiwen, 2012). According to Nie and Zhong (2013), the RFID tag can give away sensitive information via unauthorized access, thus creating problems with respect to data confidentiality as well as privacy. Some of the common problems faced with RFID tags include; abuse of tag, killing of tag cloning, jamming, Denial of Service (DoS), spoofing and software attacks.

Smart Grids: These again play a core part in the smart government framework as they are related to deployment and management of energy. They consist of communicating instruments such as sensors and communication networks which aid in the communication of the data in real time (Clastres, 2011). When there is real time data sharing between power generator, service provider, resources and users, any attack targeted at any one of these process will lead to system failure. This in turn will also lead to the user being disgruntled with the government. The main threats that should be considered while deploying smart grids include; threats to the availability of network, threats to information privacy, threat to data integrity and threat to devices.

Biometrics: It is an automated recognition of a person via the unique behavioural as well as biological characteristics of the person. Physiological and behavioural are the twomain characteristics of biometrics. Both of these are acquired after the application of proper sensors and distinct features are taken in usage to catch a biometric template in the authentication process (Rathgeb and Uhl, 2011). In fact it is usually thought that there is no other substitute for biometrics

for identification which is integrated well in the security applications. Biometrics play a vital role in information security strategy in smart governments. In fact, the thousands of Dirhams worth of frauds can be solved with the implementation of biometrics (Smart Cities Council). While these are extremely resilient to malicious attack, there remains a bit of security threat and thus due diligence is important.

Smart Phone: A smart government is majorly based on smart phones as it becomes more available to the public via easy login, via their smart phones. The basis of smart government is to make governance easier and simpler for the masses and therefore many services are offered by the government which are accessible via the smart phone. However, there is very little security and there is always a risk of malicious attacks which can be carried out easily. Hackers and viruses are easily able to gain control of the smart phones and thus they fall prey to such attacks. Some of the major threats to smart phones include; malicious smart applications, spyware, bootnets, location and GPS hacking, threats via the Bluetooth, Threats from WiFi, Threats through social networks etc. In order to combat these problems there are a number of suggested solutions (Jeon, Lee and Won, 2011) such as, filters, firewalls, anti-virus, secure API, filters etc.

Thus for any smart government, identification of threats is extremely important. As mentioned above there are numerous possibilities of attacks and threats and for a successful smart government implementation, government needs to draw a framework based on the identified threats and vulnerabilities so that it can be addressed and major issues with respect to security can be avoided. Governments need to recognize the fact that an attack or threat if undetected can cause a major collapse of the governmental operations and therefore it becomes imperative that they be identified and a robust information security strategy be drawn out.

2.6.3 Critical Success Factors in Information Security in Smart Government

Varied cyber regulations are to be dealt by the smart government in fields such as electronic banking, government, healthcare and commerce among which all of them depend on how cyberspace is governed for facilitating the usage of the web as a medium for promoting global exchange without any risk factor. Assessment of the degree of security for e-government can be done by assessing the regulations, security policy as well as security measure model. It has been pointed out by (Mohammad & Hamdan, 2012) that most crucial threats faced by e-government can be classified into the one on client end; communication channel and server end threats and

what security requirements are needed for information systems and confidentiality**.** However, the study has laid focus on performance measure followed by overlooking the notion that prevention is always a better option than cure although it is always a good option to build up security metric. Identification of success factors for information security in smart government is only possible when there is a clear understanding, definition, and implementation of technical and non-technical issues for smart government in correct order (Ferraz, Sampaio and Ferraz, 2015). Measurement of smart government services in case of both quality and quantity of security may lead to enhancement and security of smart government services. The initial need is to apply the model as a checklist for identification, growth, and application of Smart Government security needs. A plan for security requirements can then be created for the Smart Government services projects before, during and after the stage of implementation. Also, security makes it necessary for Smart Government system to carry out analysis of the threats and attacks that may be faced by it which can be assimilated in secure application development by using method for modern software risk analysis (Ijaz et al., 2016). This will help in preparing the governmental institutions towards the vulnerable issue with respect to privacy, integrity as well as the presence of trustworthy and consistent information. This will ensure that government institutions are capable enough to prepare themselves in the case of any undesirable issue with respect to confidentiality as well as accessibility of constant and reliable data. Other than this, the success factors in the security of information in Smart Government is establishing a proper framework for ICT security that governs the protection of the norms and processes in the system so as to guarantee privacy, trustworthiness, and availability of information on the consistent basis (Clavell and Gemma,). The challenge is worthy of consideration by the governmental establishments so as to drive the information security in a successful manner with respect to e-Smart Government (Ijaz et al., 2016). Other than this, the need is also to gain active managerial support; awareness of staff and training them as it is the manager who would be accountable and will have the responsibility to initiate and support the project.

Information security infrastructure in the context of developing nations faces challenges with respect to the absence of security technology structures like encryption system and public key infrastructures (PKI) which put an impact on the overall quality of information (Symantec, 2015). The technologies can assist in ensuring towards authentication, access control and confidentiality of services. It is further required to be guaranteed that staff members of government institution get

information about safety teaching and training sessions on a continual basis. In the case of developing nations with respect to information security infrastructure, there is an absence of security technology structures like Public-Key Infrastructures (PKI) and satisfactory encryption structures which act as a crucial challenge thereby affecting the generation of electronic data of high quality (Liu et al., 2012). Hence it is crucial to develop security infrastructure goals for attaining IT security targets and operating surroundings. Security properties can be considered as those techniques which offer facilities for security in form of password system, firewalls as well as digital signature. These technical infrastructures can then handle the required volume and varied kinds of transactions in a secured manner so as to obtain goals related to information assurance. Other than this, access control, authenticity and integrity can also be offered for the government that is moving into the stage of electronic information (Symantec, 2015) .

With respect to the perspective of hardware/software, ICT infrastructure should be popularized by the authorities in the context of smart government. But in legal terms, there is a need to set a legitimate framework so that people can be provided with opportunities where they can be equal in front of the law. Other than this with respect to process, the smart government is required to implement security standards as well as knowledge management, providing a particular type of services followed by asserting towards its quality (Symantec, 2015). International authentication center can also be created so as to assist the user for using services by presenting their identity and the transactions will then be registered in national file management center so as to protect the electronic documents from any misuse. It is further essential to preserve the information of people so that trust towards government can be enhanced. At last in terms of user opinion, it is required that governmental officials encourage as well as provide support to employees for gaining security skills that are knowledge based. There is further a need to have high user acceptance, clear outline of user's power and responsibility and improving IT skills of users.

2.7 Conceptual Framework for Information Security in Smart government Implementation

After reviewing the literature review, it has become obvious that in the domain of smart government, information security plays a major role. However, it is also vulnerable to many threats and outside attacks which can greatly compromise the privacy of not only the government but also the people. As has been observed there are limited studies carried out on smart government and information security and the challenges faced. After critically reviewing the literature, it has been

identified by this research paper that information security in smart government implementation is an important issue which needs to be studied carefully. Therefore, this chapter presents a framework doe identification of information security strategy for smart government in the UAE, identifying the vulnerabilities and threats.

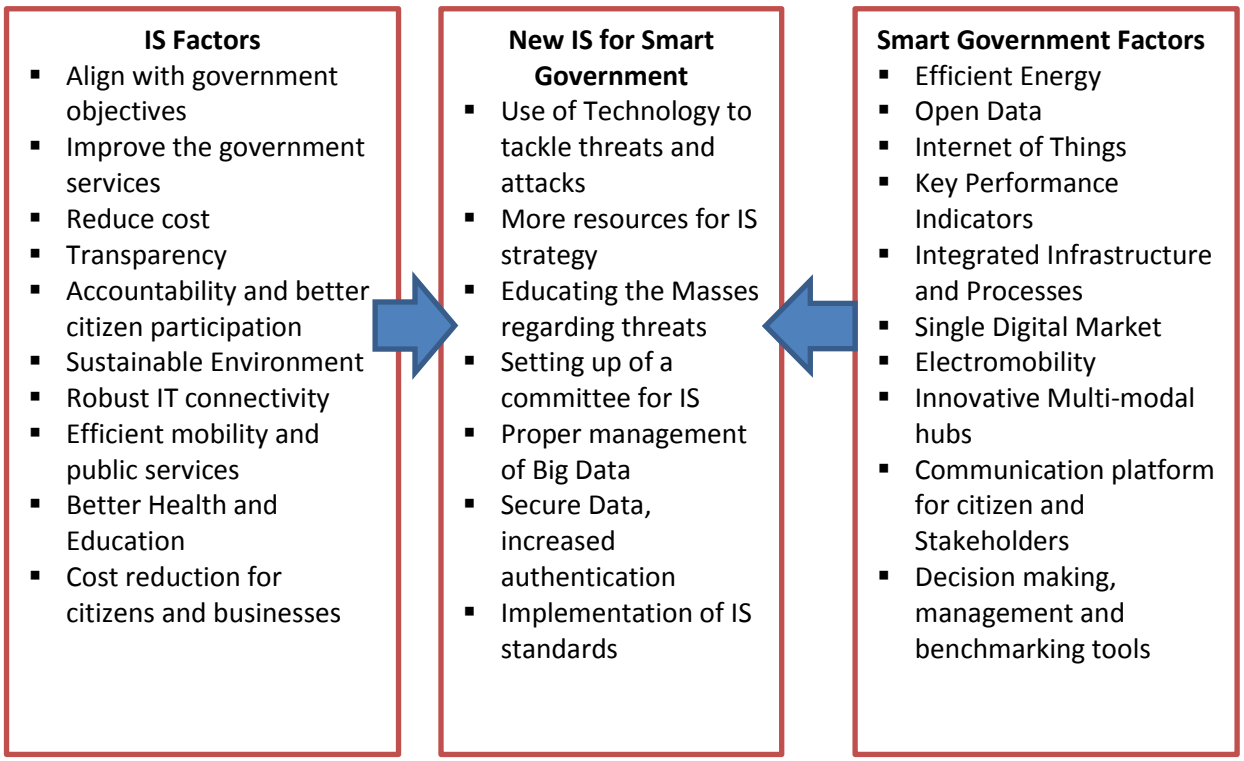


Figure 2: Conceptual Framework for New IS in Smart Government

The above figure 2 mapped out Conceptual Framework takes into consideration the factors of both, IS as well as Smart Government and proposes a new IS for Smart Government in UAE. UAE has been making a lot of advancement in the field of smart government and have also paid attention to information security strategy. Keeping this in mind, a number of key strategies, policies and standards were announced by The National Electronic Security Authority (NESA) in 2014 which aligned with the information security strategy (Khaleej Times, June 27, 2014). NESA, established by the UAE government is a federal authority that is responsible for the planning, developing, supervising and monitoring the implementation of the country's information security standards, strategies and policies (Lewis, 2014). It not just aims at safeguarding the UAE online environment but also contributes towards the achievement of national goals. Furthermore, the government initiated the National Cyber Security Programme, which was attended by senior officials from

federal as well as private entities from the entire spectrum of the smart government of the UAE. The National Cyber Security Strategy has been designed by the government that entails the various strategies and standards that must be followed by the federal entities as well as stakeholders in order to ensure information security. The telecommunication hub of the UAE-Telecommunications Regulatory Authority (TRA) also hosted the First Introductory Workshop of the Information Security Awareness Committee "ISA" in January 2017 which was attended by professionals from federal as well as private entities. The aim of the conference was to build a better and secure digital environment (Tra.gov.ae, 2017).This shows that the UAE government has taken steps in the right direction with respect to information security in a smart government. This therefore leads to our first research questions:

RQ 1: What is the current scenario of information security strategy in UAE and on what factors are the key initiatives developed?

Information and communication technology (ICT), is at the core of smart government. Internet of Things (IoT), RFID, smartphone technology, linked data, smart apps, cloud computing, biometrics and collective intelligence all form the ICT framework (Ijaz et al., 2016). Thus a smart government framework heavily relies on ICT for its success. In order to ensure that the critical services such as energy, utility, healthcare, governance are able to continue without any delays, information security needs to be fool proof (Silva Ferraz, Candido Barros Sampaio and André Guimarães Ferraz, 2015). The main factors which should be taken into consideration to be able to identify the issues in information security in a smart government are social/economic factors, governance factors and economic factors (Ijaz et al., 2016). According to most researchers, IoT is an important component of a smart city as smart government is entirely built on it (Dohler et al., 2011). Another important factor that plays an important role in the development of smart government is 'big data'. The production of large volume of important data in a smart government is inevitable which includes governmental records, resident information and other important data (Kitchen, 2014). While this big data present opportunity for the government to better their functioning, it also poses many security and privacy threats (Schmitt, 2014). Thus safeguarding the same is met with challenges such as lack of management tools for the management of big data, threats to public database, third party sharing and data leakage (Ijaz et al., 2016). It is this sphere that the

government needs to look into and find out the proper channels to avoid such security risks. This leads us to the second research question:

RQ 2: What are the factors that define the smart government mechanism leading to achievement of information security and a strong operating model?

In 2013, the ruler of UAE had expressed his desire to transform UAE into a smart government (The National Plan for UAE Smart Government Goals, 2015). This caused many changes in the manner the government operated; it caused the government entities to update their strategies and plans wherein more efforts were put to become more modernized in their capabilities. Committee were set to ensure that the goals of smart government initiative were aligned with UAE Vision 2021 (The National Plan for UAE Smart Government Goals, 2015). The vision as proposed and the framework of this vision apart from various other factors also focussed on; centralized smart government functions, promote e-lifestyle amongst residents, ensure resources for development of best ICT practices and to develop the required infrastructure for information security strategy. While the government seeks an integrated approach, there is a need to look into best policies that would help secure the systems without compromising the information of the residents or the government. In this regard the future innovations need to be protected from attacks and vulnerabilities. Intrusion prevention techniques along with robust policies for areas such as email, browser patches and network usage need to be developed along with educating the masses. Furthermore, the meters at the end-user level can be easily hacked and therefore to secure data integrity advanced metering infrastructures (AMI) and Public key infrastructures (PKI) could be used (Symantec, 2015). There is little literature available with respect to steps taken by the UAE government to develop their information security strategy and thus this leads us to the third research question as below:

RQ 3: How can UAE transform into a smart government with information security supporting future innovation and development?

As mentioned earlier there is a major threat that looms over ICT in a smart government setup. However, these can substantially be overcome if the right practices are put into place. For any

government looking to transform into a smart government, there are certain aspects of information security strategy which should be applied in order to make sure security is maintained. While RFID tags are being widely used in the smart government framework, they are prone to many security risks (Ijaz et al., 2016).To counter this, Pateriya and Sharma (2011) suggest tag sleeping wherein the tag is put to sleep when not in use. Other options include selective blocking or tag clocking (Nie and Zhong, 2013). Another major component of a smart government is the smart grids which help in the deployment of energy and its management. It is again prone to threats in the form of data integrity and information privacy. To combat that, PKI is a good solution. Smart phones are extremely important in the smart government infrastructure and is also prone to a host of vulnerabilities right from malwares, to threats via GPS systems, botnets and even spyware. There are a number of suggested solution to counter these threats such as firewalls and antiviruses, Secure API, authentication and access control and filters etc (Jeon et al., 2011). Machine to Machine (M2M) solutions are also susceptible to attacks and in order to combat them, certain standards have been set in place as discussed in the literature review. Thus the application of all these security measures into the information security strategy can be beneficial for smart government practices. This leads us to the fourth research question:

RQ 4: What are best practices to be followed to establish information security strategy for smart city / smart services?

2.7 Conclusion

This chapter has aimed to review the literature that talks about smart government and its basics while also drawing attention towards information security. Smart government and information security are both interoperable and the success of one factor depends on the other. In this chapter the researcher has attempted to draw parallels between the challenges faced in the implementation of smart government as well as information security. It can be seen that both these concepts face their own challenges which are similar and can affect the way the smart city operates. Threats and attacks on the smart government can disrupt the manner in which operations are carried out and in severe cases also compromise the privacy of the residents along with the government. In this respect it is extremely important that information security be the core foundation of a smart government. However, while the literature points out to the fact that information security is a vital

component of smart government, a case study of the smart government of the UAE has revealed that information security is not given the importance it deserves. Although the government has made it an agenda and have conducted important conferences in this regard, the implementation is little. It can be observed that the UAE government has not yet placed information security as an important part of the smart government and thus there is no smart government information security strategy in place. The literature review also aimed to answer the 4 research questions and based on which a conceptual framework was derived. This conceptual framework showed the gaps in research and thus presented opportunity for further research. This is integral for the research as it helps to identify the gaps in literature and what specific areas need to be addressed. This calls for further reviewing of the literature, seeking to find how much the government aims to change its approach towards information security. More research in this regards will shed more light and help to understand the agenda that the government has formulated for future implementation of information security.

Chapter 3: Methodology

3.1 Introduction

Carrying out research on the development of smart UAE government that is based on information security is filled with barriers due to the developmental stage of the market. However, this research stream in case of mature markets is quite well developed. The current section of the study will focus on discussing varied types of research methods that can be applied for present study followed by selecting the best methodology. Other than this, emphasis will also be given on detailed discussion about the advantages and limitations of the research methods followed by providing the justification about the selected methodology. The present section thus focuses on explaining a detailed and stepwise approach to research in order to provide a clear idea about research techniques adopted for the study.

3.2 Research Approach

Positivist studies usually focus on testing a theory so as to enhance the predictive understanding of a process. Researchers have classified information security research as positivist if there is an existence of evidence related to formal propositions, hypothesis testing, measurable variables and if inferences about the given process can be drawn from the sample for a given population (Oates, 2006; Saunders *et al*, 2007). The science philosophers have criticized that the given research paradigm has an important role to play towards conceptualizing theory/ hypothesis however constraints are put on results by usage of extremely organized research design that may not focus on important findings (Collis & Hussey, 2009). Interpretive studies aim to assess the process by the meanings that have been assigned by people. In the case of information security research, interpretive methods focus on creating an understanding of its background. It can be considered as the philosophical paradigm that has arisen after positivist in order to cover the insufficiencies of techniques that have been applied to social science, which could only be applied to natural science (Irani *et al.*, 1999).

The assumption of Interpretivism is that there is a multiple nature of social reality which is impacted by the act of investigation. It is based on the belief that social constructs in form of language, insights, awareness and shared meanings enable towards easy access to reality that can be communicated to a person or a group. In case there is non-generalisation of research findings

then interpretivism will assist the researcher in transferring as well as applying qualitative data to similar such viewpoints (Myers & Avison 2002; Ryan *et al*, 2007).

The given research study emphasizes on finding out and analyzing the factors for the strengthening of information system in smart UAE government. Hence interpretivism can be regarded as the most suitable research approach for the study as it assist the researcher in adapting wide techniques to describe, translate and come to terms with the meaning and not the frequency of occurrences of natural processes in the society. Interpretivism in tune with the inductive process will assist in arriving at generalizations (Collis & Hussey, 2009).

3.3 Research Methodologies

As per view points of Patton (1990), the very first step is to decide which approach will provide for most appropriate solutions so as to draw valid conclusions for the issues that are being investigated. Galliers (1994) feels that it is not easy to select a suitable approach for Information Systems as IS aids the research to make a choice of the method from diverse approaches as they are not linked to a sole theoretical viewpoint. On account of the above fact, the information system can utilize positivist paradigm as per the nature of knowledge about research studies which are quantifiable, objective and traditional (Myers & Avison, 2002; Saunders *et al*, 2007). Interpretive approach is the best for present research as it is in need of opinions that are based on perceptions held by respondent as well as the researcher (Harling, 2002; Creswell, 2009). While making a selection of a particular approach to research, 3 methodologies have been suggested that are inclusive of qualitative, quantitative and mixed as per figure 3.

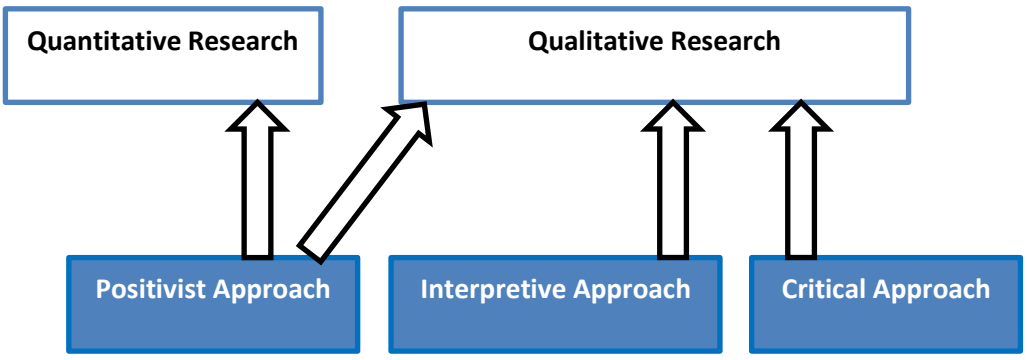


Figure 3: Approaches to Qualitative and Quantitative Research

Source: (Straub et al., 2005)

3.3.1 Quantitative Method

It has been believed that there has been an emergence of quantitative approach on account of exploring natural process hence the perception is towards the adoption of objective and scientific technique in tune with positivism as shown in figure 1. Quantitative analysis is all about interpreting numerical data patterns (ordinal, interval or ratio) which may involve techniques like correlation, regression, mean comparison and analysis through graphs and diagrams. The results are further required to be valid so as to assist in the attainment of accurate and reliable data. This clarifies as to why the quantitative approach is used in the interdisciplinary field where there is a usage of the multi-method approach of research in order to assess the human experiences. Organised as well as open research is supported by the Quantitative approach by making use of large samples which are not known to participants and utilizes tests and formal instruments (Oates, 2006; Collis & Hussey, 2009). There exists reliability of data as the focus is given on theory as well as hypothesis testing which makes it difficult to get selected.

3.3.2 Qualitative Method

Qualitative analysis can be utilized for describing numerous realities, creating in-depth understanding, building theory. It has been suggested that this approach assesses and translates the process by meanings that are assigned to people in order to produce an understanding of IS as well as the influences it causes on the environment. There is inductive nature of qualitative approach followed by the presence of specific examples to arrive at generalizations. The collected data is inclusive of written text, sounds or visuals as the meanings can be interpreted by text or images (Lee & Baskerville, 2003; Hussey & Hussey, 1997). Qualitative analysis as per the scholars is subjective as it focuses on the meanings, experience, and description. There is further a presence of an unstructured and open research strategy so as to aid in generalisation and checking the validity and reliability of findings by verifying them. The process of data collection further involves for social interactions between researcher and respondents where the results can be assessed by making use of descriptive, investigative, predictive or analytical approaches solely or in combination. There is further a requirement of interpersonal skills on part of researcher in order to assess the importance of information that is present for research methods.

Information system process for smart cities is a new one and there exists very little research on emerging nations like UAE. Hence researcher has to emphasize on literature reviews followed by

assessing the strengths and weakness of research methods (quantitative and qualitative) so that most suitable technique can be applied in effective and efficient manner. However, due to nature of data and research focus the present study will prefer using the qualitative approach. This technique is perfect for the present study as the work is inductive and there can be the use of specific examples to arrive at generalized findings. An important role will also be played by in developing the conceptual framework which is not good for the quantitative approach where the emphasis is given on testing the hypothesis. As per view point of Collis and Hussey (2003) qualitative research is aimed at looking for patterns and ideas rather than testing of hypothesis. Hence the reason behind the research was to assess the factors that can aid the researcher in utilizing research strategy followed by developing theories so that IS can be successfully implemented in the government of UAE.

3.4 Research Strategy

It can be defined as an action plan for providing direction to the efforts of the researcher and enable him or her to conduct research in an organized way in comparison to haphazard manner (Saunders *et al*, 2009). It is essential to find out suitable research strategy as it directs the efforts of researcher including the process by which the study is being carried out. It further provides the researcher with a general plan for answering the research questions or finding out the orientation of conducting the study (Remenyi *et al*, 2003; Bryman, 2008). Denscombe (2003) has briefed 4 types of strategies being case study; survey research, historical research; & experimental study (Yin, 1994; Klein & Myers, 1999). Case study is the total of all the details derived from multiple sources about a particular process in the real world setting where the boundaries between the processes are not clear. The given research study utilizes contextual analysis of the individual, group or event so as to explore the principles, followed by relying on many evidential sources (Yin, 2009).

Historical research is about the technique of assessing the past event followed by interpreting the recapturing of nuances and ideas that impact the events. Historical research is thus about researching the events that have occurred in past or to communicate the understanding of them. This type of research is advantageous as past patterns can be displayed and they can help in understanding there the source of occurrence and solutions that were used to resolve them. Overall it can be said that historical research is about assessing the past and present events in an organized manner so as to discern there meanings in the best possible manner (Leedy, 1997). Survey research

is that technique of sociological investigation which utilizes questionnaire sets or statistical survey for collecting data on what people think and how they act. This research plays a key role in creating a document for present community conditions, features of population and their opinion. The technique has been considered as a crucial one so as to ask the question to the respondents (Lemanski & Overton, 2011).

The experimental study entails for using experiments carried out in the laboratory as well as fields. The research activity in this context is applied under controlled conditions so as to explain the cause and effect. Laboratory experiments are carried in controlled conditions where specialized treatment is given to different groups so as to contrast the relations that are present between the variables. While the field experiments are carried out in real life situation as the object of the study can be under direct supervision of the researcher (Leedy, 1997; Klein & Myers, 1999; Walliman, 2001). Overall it can be said that experiment study has a responsibility towards the research scenario throughout the study and is based on assumption that few of the input variables are the cause of changes that occur in the investigation process.

3.4.1 Justification

While selecting the research strategy certain conditions have been applied as recommend by Yin (2003) which are based on the question that is required to be addressed as discussed in the 1st chapter as well as the research context which is UAE's smart government. It has further been found that making a choice for research approach is a difficult task for the research study on IS due to its multi-disciplinary nature. However, the objectives, as well as data type, have a relation with the conceptual framework for the evaluation of IS in the case of smart government hence the researcher is focusing on highlighting the factors that put an influence on implementing information system and identifying the role of key activities. As very limited research has been carried out in this area and seeing the need for subjective aspect the refereed strategy is the case study. In addition to this, case study research has been regarded as a valid one for managing the IS and also as an evaluative tool that has the ability to adapt to the availability of diverse evidence followed by assessing the outcomes as well as testing casual and rival theories. Case study research has been used by researchers over a long span of time and across varied disciplines. The research process is interpretive in nature and is aimed at producing a consideration towards the background

of IS. The case study is one of the most important types of research approach as it aims to address the questions being;

1. What is the current scenario of information security strategy in UAE and on what factors are the key initiatives developed?
2. What are the factors that define the smart government mechanism leading to achievement of information security and a strong operating model?
3. How can UAE transform into a smart government with information security supporting future innovation and development?

The strategy adopted for the present research is of the case study about a smart government of UAE, as the research purpose inculcates reviewing current scenario; identifying key factors that impact IS as well as developing and authenticating the conceptual framework.

3.5 Research Design

Suitable research design has been used by the researcher for collating data so as to address the issues as found in the research problem. The usage of research design has been supported by scholars and the design is regarded as the organized set of making rational decisions as well as creating guidelines for producing valid/reliable results. This is followed by ensuring that the information has been gathered by an objective procedure and the design is relevant to the research problem. The research design is about making the problem to become researchable by setting a study in such a manner so as to generate answers to particular research questions (Straub *et al*, 2001; Hamed, 2009: Alhujran, 2009; Cavana *et al*, 2001). In the context of current research, the research issue focuses on the factors that impact the proper implementation of IS in emerging nation such as UAE by making use of case study approach. On the basis of literature review and identified gaps the research will be able to create and define the questions which are;

1. What is the current scenario of information security strategy in UAE and on what factors are the key initiatives developed?
2. What are the factors that define the smart government mechanism leading to achievement of information security and a strong operating model?
3. How can UAE transform into a smart government with information security supporting future innovation and development?

4. What are best practices to be followed to establish information security strategy for smart city / smart services?

As discussed in section 3.2, the interpretive approach was selected by the researcher as it aids in adopting a wide range of methods. It is inductive in nature so as to enable findings and particular instances to arrive so as to reach generalized conclusions. On the basis of this, the qualitative analytical method has been utilized by the researcher so as to assist in developing an in-depth understanding and building of theory. A crucial role will thus be played by qualitative analysis in developing the conceptual framework. The research was further able to assess and develop research methods followed by collecting data by document analysis and case study research. The illustration for the research design is presented in the figure 4.

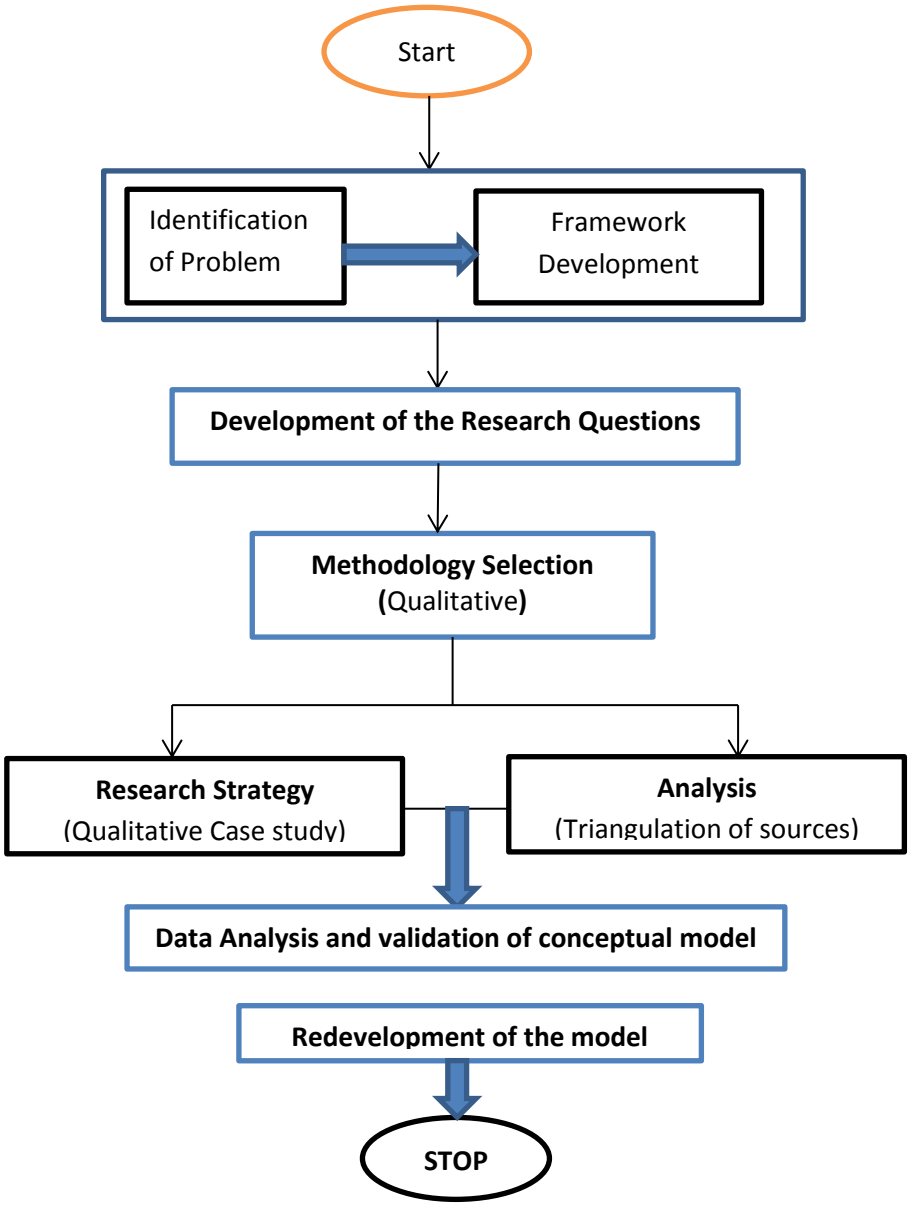


Figure 4: Research Design model

3.6 Data Collection

It is an essential part of any research and is linked with the methodology that has been chosen for the study. In the present study, there is a choice of inductive and qualitative technique whereas research philosophy is the ground theory. For this research, the data will be collected in two ways- making use of primary as well as secondary sources. Although primary data is more effective as well as reliable than secondary data, it is vital to make use of secondary data also in order to support

the analysis made by the primary data. Using secondary data will act as a basis for making a roadmap, measuring change and operating model development. Secondary data will be used to substantiate the argument that is formed through primary data and a conclusion will be reached combining both the data. The analysis for the paper will be qualitative based on the interviews conducted which will be then cross-referenced with the literature review to draw conclusions.

3.6.1 Interview

In order to collect in-depth data, interviews are the most common methodology for qualitative research purposes. According to Mann (2011), if the research requires exploring the beliefs, experiences or identities of the participants, then interviewing is an apt approach for qualitative research. Venkatesh, Brown, & Bala (2013) states that interviews can be conducted in conjunction with other methods for mixed-method projects or can also be conducted independently, as is the case with the present research. For research purposes there are 3 main types of interviews which can be employed, as discussed by Denzin and Lincoln (2011);

- Structured Interviews: This is a pre-planned interview wherein the questions are provided by the researcher to the participant before conducting the interview. It is an apt format to maintain the focus on target topic (Bryman, 2008).
- Semi-Structured Interviews: In this format, although the questions are pre-decided, the interviewee is not provided the questions in advance and the questions and open-ended ones (Alsaawi, 2014).
- Unstructured: This kind of interview is informal in nature where the questions have not prepared beforehand which leads a conversation kind of interview which is guided by the interviewer.

In the present research, the researcher has made use of the structured interview process, wherein the researcher conducted the interview with stakeholders who are involved in the Information Security firms and projects. It included professionals such as IT engineers, IT directors, Strategists, IS experts and system architects. All the participated personnel were based in the UAE and were involved in various smart city projects that are to be implemented in the UAE. The interviews were conducted over a span of 3 months and includes a sample size of 25 participants. It was vital to include experts in Information Technology for the interviews in order to understand the views of various stakeholders within the area of expertise. All these stake holders play important roles with

respect to information technology and thus are aware of the implementation process. Interviewing these stakeholders provides a clear understanding of the process and the barriers and challenges faced with respect to information technology in smart city implementation.

For this research, open-ended as well as close-ended questions were probed. In the opinion of Creswell (2012), for grounded theory methodology, 20-30 interviews should be conducted while for phenomenology, 5-20 are sufficient. Keeping this in mind in the present research a total of 30 people were approached out of which 5 refused to give an interview while 25 participated in the interview. All the participants were involved in smart city implementation, either currently or previously and therefore he data collected is relevant to the study.

3.6.2 Secondary data

The collection of secondary data is done by reviewing of previous research studies, academic resource, websites, publications, indices as well as articles in the selected field of research. In the context of the present study, secondary data plays a key role in providing a good source of evidence for analysing the present situation of information security strategies used in UAE, identification of factors to attain IS followed by the development of a model for its successful implementation.

As per the view point of Howell (2013) secondary data is a very powerful source but less reliable on account of the information provided by it. Secondary data is usually factual and the information can be strengthened by utilizing high-quality data sources like publications, research article, and studies in the selected research area which is required to be reviewed. The below-given table 6 provides a summary of the research methods and outcomes for study followed by explaining the data sources and outcomes along with aim, objectives, techniques and activities carried out for the study.

Table 8: Techniques for the research design

Aim and Objectives	Research Approach	Techniques	Sources	Link
Review the literature on smart government and information security	Qualitative	Secondary data	Journals, Books, Government reports, Websites	Chapter 2 – literature review

Aim and Objectives	Research Approach	Techniques	Sources	Link
Develop the conceptual framework	Qualitative	Secondary data	Journals, Books, Government reports, Websites	Chapter 2 – literature review
Investigate the factors affecting IS in smart government, focussing on UAE	Qualitative	Interviews / Secondary data	IS Stakeholders, Journals, Books, Government reports, Websites	Chapter 4 – Data Analysis and Discussion
Development of the implementation framework for successful IS strategy for smart government of UAE	Qualitative	Interviews / Secondary data	IS Stakeholders, Journals, Books, Government reports, Websites	Chapter 4 – Data Analysis and Discussion

3.7 Data Analysis

The final part of empirical research methodology is the analysis of data. There are a number of approaches for qualitative data analysis which can be used for the research. Data analysis itself is a complex task wherein textual data is involved. Since the data collected in this research is qualitative, the analysis is non-mathematical. After the data is collected, general themes were identified and interpretation of the given responses was done. Furthermore, as mentioned by Seidman (2012) to interpret the interviews accurately, the researcher highlighted the most important and categorized the responses. In addition to the interviews, the secondary data collection was reviewed and the responses from the interview were analysed with respect to the collected secondary data so as it come to definite conclusions.

3.8 Research Protocol

In the present study, the information security strategy of UAE's smart government has been studied to identify any threats, risks and vulnerabilities. The smart government model is at a risk of security breaches and this research has attempted to highlight those and what views the stakeholders present

regarding the same has been elaborated. To understand the view of stakeholders, a sample size of 25 participants will be chosen, all belonging to the IT and IS sphere, holding senior positions. It is important that the participants have knowledge about Information security and have worked in this area of specialization in order to gauge their point of view and to find out what threats and risks are prevalent. The questions posed will be both, open-ended as well as close ended so that the participants are able to view their opinions freely, without being limited to a certain outlook. The interview protocol will be implemented in a span of 3 months and all the necessary information regarding the interview will be relayed to the participants before the start of the interview. There are no immediate risks or benefits to the participants through this research.

3.8.1 Questions Addressed

According to Yin (2009), it is important to develop and maintain a set of questions which reflect the collected data. The questions that were developed were for the knowledge of the researcher and not the interviewees in order to remind the researcher the objective of the research and to collect relevant literature for analysis. It is essential to collect the data in order to identify the stakeholders, factors that affect information security strategy and how the smart government initiative in the UAE required a more comprehensive outlook from the point of view of information security. These protocol questions are the key questions for the researcher in order to focus on what questions should be asked to the interviewee (Yin, 2009).

3.9 Research Ethics

Ethics in research is extremely important since it addresses the privacy of the participants. Researcher should inform the participants about the research procedures as well as associated risks (if any) prior to gathering data. Participants should also be made aware that the gathered data will be used for the purpose of the study but the details will remain confidential. Under no circumstances should their identity be compromised. It is essential that the participants be informed that their identity will remain confidential throughout. All participants have a right to privacy and this should not be compromised in any manner at any point. Only if the participants agree to the interview and give consent to the usage of the shared information should the researcher go ahead and include it in the data analysis. There are set standards in ethics which should be followed by researchers in order to maintain the privacy of the participants. In no way should the

right of the participants be side-lined or overlooked. Furthermore, researcher should inform the participants that they can choose to end the interview anytime they deem fit or not answer certain questions. In the present study, participants were informed and consent was obtained prior to the beginning of the interview.

3.10 Conclusion

The aim of this chapter was to justify the chosen research methodology for the present thesis. This thesis has deployed a research strategy with the intention of theory building. The researcher has justified the use of interpretive stance for the research along with making use of the qualitative research methodology in this chapter. The reason for making these choices are dependent on the aim and objectives of the study which deals with learning the information security strategy of the smart government of UAE and building of a conceptual framework doe information security strategy. Furthermore, the research strategy used for this study was also discussed as well as justified in this chapter. The strategy was a case study to investigate the smart government initiatives taken by the UAE keeping in mind the information security challenges that are a part of a smart government. A case study of the UAE's smart government has provided enough information to carry out the research. Furthermore the use of research methods was outlined and the reasons for the use of particular methods were provided. Consequently, data collection was done via interviews, and literature review. Finally, research protocol, questions addressed and research ethics was discussed at length. Thus, the presented work in this thesis will provide a better understanding of information security strategy of UAE's smart government and provide other researchers an essential tool for further studies in this sphere.

Chapter 4: Results and Discussions

4.1 Introduction

In order to reach a conclusion of the present research, primary data analysis is extremely important. The primary data for this research has been collected in the form of interviews. Out of the 30 senior IT and IS related professionals, 25 of them responded and they provided an outlook about information security in smart city implementation. The questions developed were close as well as open ended so that the personnel could formulate their own opinions. An analysis of the responses from the 25 participants are analysed below.

4.2 Data Analysis

In spite of a number of studies and protocols with respect to information security, there has been an increase in number of vulnerabilities in the connected applications. To understand the role of information security in smart cities, 25 personnel were interviewed in total.

4.2.1 Demographic Overview

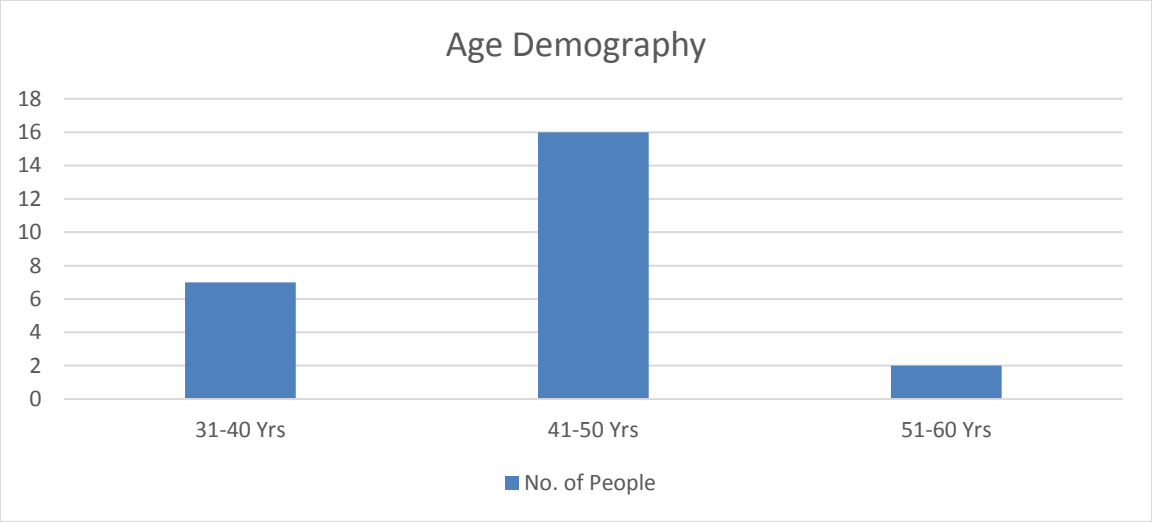


Figure 5: Demographics by Age

Out of the total 25 professionals interviewed, 19 were males and 6 were females. 16 belonged to the age group of 41-50 years while 7 belonged to 31-40 years and only two belonged to 51-60 years age group (Table 5). Total years of experience of 14 people was 15 years and above, of 3 people it was 12 years and above while of 5 people it was 10 years and above. With respect to qualifications, 16 out of 25 held Master's degree while 9 were PhD holders.

4.2.2 Stakeholders Outlook

In the second part of the interview, respondents were asked close ended questions which were to be answered in Yes or No [see figure 6]. Amongst a choice of 10 factors, stakeholders had to identify if the factors mentioned were important to them and their stakeholders with respect to Smart government implementation. Amongst the list of area of specialization, 15 agreed for Efficient Energy, 20 agreed for Open Data, all 25 agreed for Internet of Things, all agreed for Key Performance Indicators, all agreed for Integrated Infrastructure and Processes, 16 agreed for Single Digital Market, 18 agreed for Electromobility, 21 agreed for Innovative Multi-modal hubs, 24 agreed for Communication platform for citizen and Stakeholders, 23 agreed for Decision making, management and benchmarking tools. This corroborates to the fact that was mentioned by Ijaz et al., (2016), stating it becomes a much simpler task in identifying the threats that prevail by first analysing the key components that reside in an information system environment.

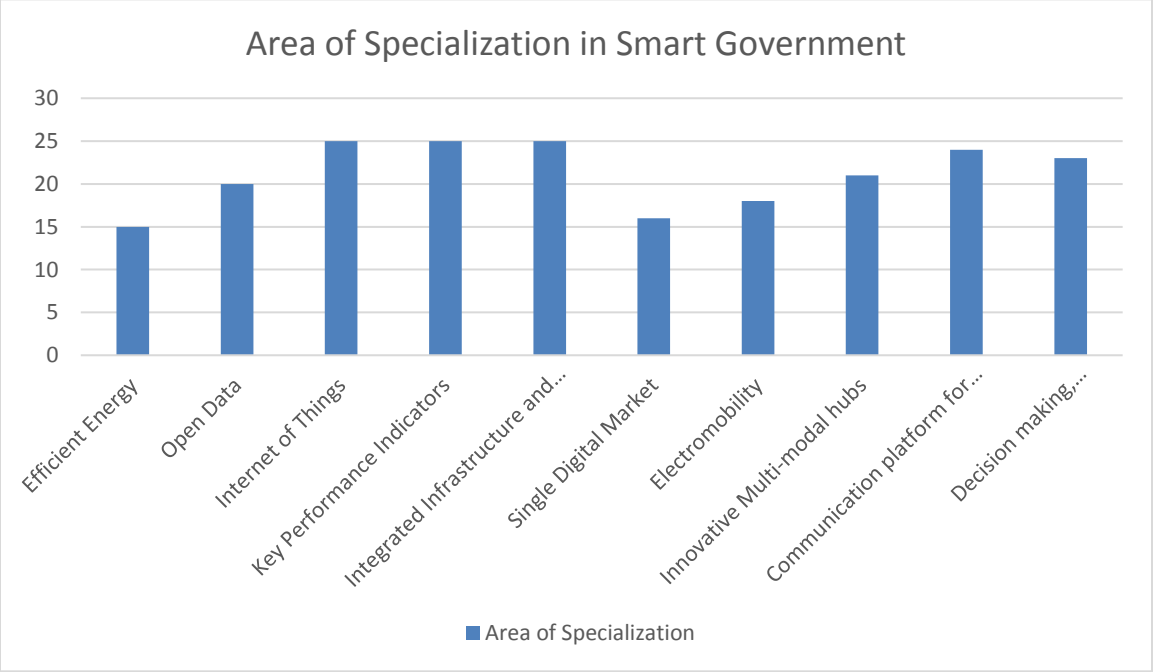


Figure 6: Demographics by specialization

The next question was again a close ended one where the respondents were asked to select from the list regarding what were the views of the stakeholders from the smart government. 20 respondents chose Align with government objectives, 21 chose Improve the government services, 25 chose Reduce cost, 25 chose Transparency, 21 chose Accountability and better citizen participation, 20 chose Sustainable Environment, 25 chose Robust IT connectivity, 23 chose

Efficient mobility and public services, 22 chose Better Health and Education, 20 respondents chose Cost reduction for citizens and businesses. These results are indication that stakeholders consider IT connectivity and security that benefits the masses as an important part of smart city implementation [See figure 7]. Gil-Garcia and Martinez-Moyano (2007), had pointed out the fact that for the evolution of smart government towards a more transactional and integrated presence of the government over the internet and the spike in technological as well as organizational sophistication that happens on the national and local level are extremely important dynamics of the evolution of smart government. The above choices made by the participants further reinforced the fact mentioned by Gil-Garcia and Martinez-Moyano (2007), that the government needs to become more technological in its approach and inculcate the characteristics of smart government such as accountability (Habibur Rahman, Yousef AlRaeesi AlBalooshi and Sarker, 2015) and transparency (M. Al-Khouri, 2012).

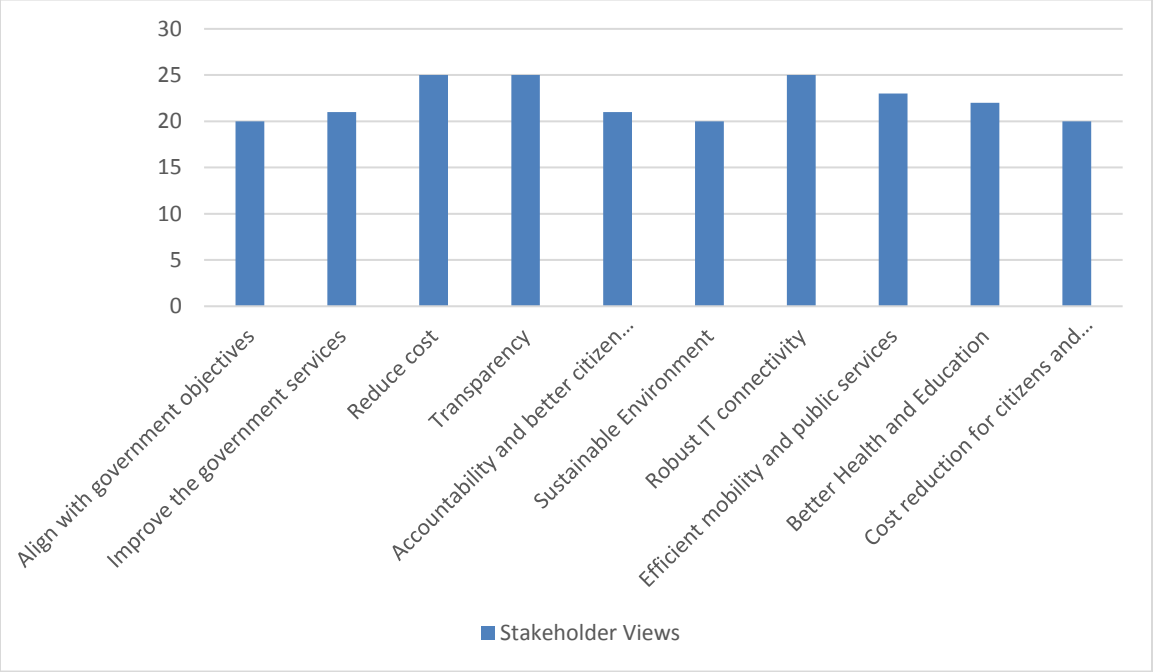


Figure 7: Stakeholder Views

In the next set of questions, stakeholders had to present answers to various questions in Yes or No and provide with a justification to their answers [Figure 8]. When asked if the technologies chosen for smart city had proper security measures in place, all 25 participants responded positively. When inquired whether the chosen products were evaluated for security posture, 23 replied positively

while 2 replied negatively with the justification that the chosen technologies were from trusted vendors who had strict quality measures in place. Upon inquiring whether proper engineering practices such as threat modelling established for understanding the unique risks were undertaken, 17 replied positively while 8 replied negatively and justified that the vendors did the checking before selling the product. Asked if risk management is carried out to define security requirements, 16 replied positively while 5 replied negatively stating that they did not possess the necessary tools to carry out risk management while 4 remained non-committal. When asked if the smart city solutions comply with basic security requirements such as authorization and authentication capabilities, strong cryptography, anti-tampering capabilities etc. 23 responded positively while 2 were not sure if all the standards were met, although these respondents justified that quite of standards were covered. Lastly when asked if vendors made any Service Level Agreements, 21 answered positively while 4 did not answer this question. From the above data, it can be concluded that stakeholders in the UAE give a lot of importance to information security and take all the necessary steps to ensure that there are no vulnerabilities that could affect the smart city implementation with respect to information technology and its security.

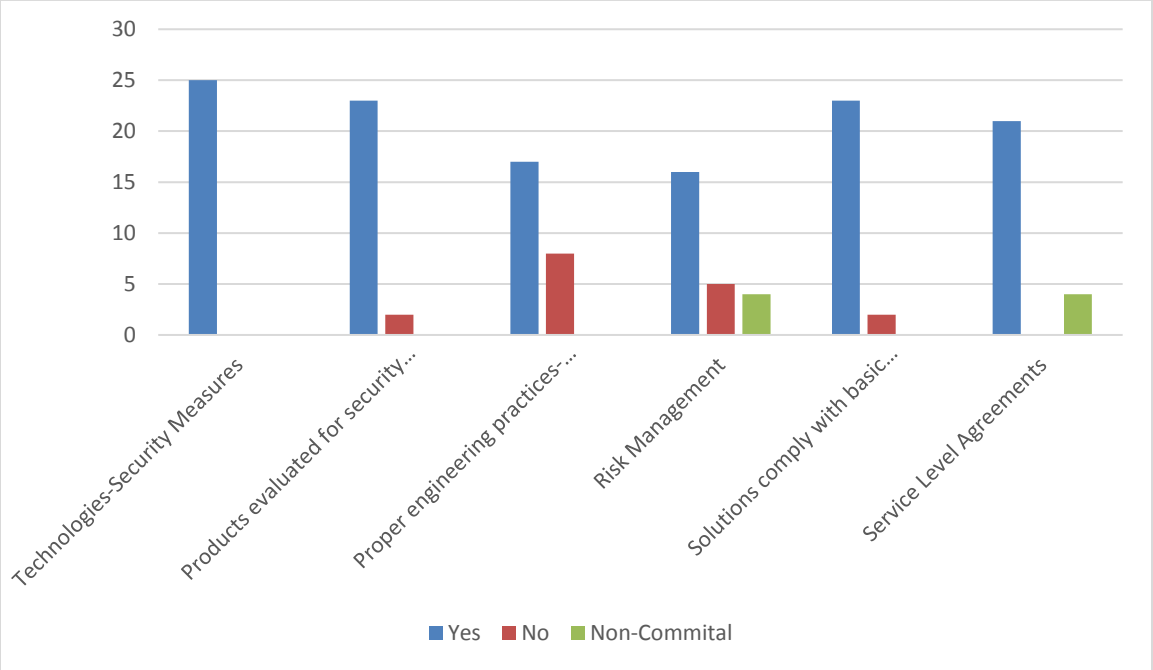


Figure 8: Technologies chosen for smart city with proper security measures

In the next part, participants were asked open ended questions which would help to gauge the how stakeholders have readied themselves to align their roles with smart city implementation and with

smart government and how much emphasis is laid on information security during the implementation phase.

Firstly, they were asked that during the implementation of new smart government initiative, who is involved in the implementation process, respondents noted that during the initial phases the stakeholders play a major role as they are the ones who will help in planning of the framework for smart government. Furthermore, vendors of various technologies would be the other faction who play a major role since, after the planning stage, in terms of implementation, their products would ready the framework and put it to practical use.

Next, they were asked about the phases of smart government implementation and the respondents pointed out that the first step to smart government is digitization (technology in government), which included access to government information is electronic formats, development and operation of government websites, technological infrastructure for smart government. The next is transformation stage wherein there takes place organizational change as well as management of change; portfolio and project management, sharing and collaborating on information. The technological and IT security phase is the next step as it is important the information that is shared and disseminated through various channels is protected in order to ensure privacy. The next step according to most of the stake holders is engagement phase wherein one sees increasing participation and adoption of technology by residents and also building of trust. Lastly, it is the contextualization phase wherein smart government is taken in national and sectorial contexts and also the smart government addresses the policy-relevant problems along with the vulnerabilities.

When specifically asked about how difficult the technological and information security phase's implementation was, there was a unanimous agreement amongst the participants that the phase proved to be challenging since the implementation of this phase required co-operation of a number of channels as well as the government's agreement to keep everything transparent. Furthermore, to be able to implement this phase, the right infrastructure was needed which lacked in the initial timeframe. This is corroborated by Sen (2013) when he stated that there are a number of challenges in the implementation of IS within the smart government framework.

The next question aimed at understanding what role the stakeholder's department played with respect to the IT department and its working. As mentioned previously, all the respondents hold positions within the IT and security departments and therefore all of their positions and departments played an important role in conjunction with the IT department as the core of smart

government is IT infrastructure. Following up on the previous question, when inquired how important IT infrastructure was for the implementation of both smart city as well as smart government, the participants were quick to point out that it was extremely important and the core component of both smart city as well as smart government implementation. This was because the basis of smart government is the ability to go digital and be available to everyone at any time, via the internet and the World Wide Web. As pointed out by Habibur Rahman, Yousef AlRaeesi AlBalooshi and Sarker (2015), smart government is agile and responds to the demands of the citizens, administration and businesses in a technologically driven manner. Furthermore, according to the definition of smart government by Gil-Garcia et al. (2014), it is the mix of innovations and emerging technologies in the public sector.

Participants were then asked regarding the importance given to security and privacy in the implementation of the smart city initiative. It was observed that participants insisted that during the implementation process as well as after the implementation, security and privacy remained the top most concern. Furthermore, they went on to elaborate that during the implementation process, due diligence is carried out to ensure that no loopholes are present to give a chance for threat to enter. The researcher aimed to learn more on the topic and therefore asked the participants whether after the implementation of a new smart government service, is it followed up to ensure no information security loopholes are present. Through the responses it was observed that not a lot follow-up was done as most participants said that they relied on the word of the vendor and that due to long business relationships, there did not seem any need to follow-up for loopholes or checks. This is a major point of concern as it shows that the senior level management was not giving due importance to the possible threats that could jeopardize the functioning of the smart government and could breach data.

4.2.3 Current State and Followed Practices

In this section of the interview, the questions were open-ended and the answers helped to gauge the practices that were being followed by the stakeholders. The first question was regarding the roles and responsibilities that the participants played at their respective positions. From the responses received it was observed that all the personnel held high positions at their respective jobs. As mentioned earlier they all belonged to the IT and IS sphere and therefore their duties included safeguarding the computer networks and systems of the organization, lookout for

vulnerabilities, monitor and investigate security breaches, install and manage operating systems as well as system management tools, maintain the availability of systems and infrastructure. All these roles and responsibilities work closely with smart government implementation and are therefore extremely important. The next questioned inquired whether they had any defined strategy for governments to transform into smart governments and if so, what were the components of the strategy. Participants responded that their companies had the strategy chalked out for the smart government and smart city implementation. The strategies included important components such as IT readiness, implementation plan, phases of implementation and also feedback. While the components were well structured, its implementation was not aligned with the strategy. The answers received for this questioned helped to reach the conclusion that in the UAE, there is still a lot of scope to merge the literature about strategy for smart government into actual action plans. This can be attributed to the fact that the infrastructure is yet developing and therefore there are still some gaps when it comes to strategy and implementation of smart government. Therefore, there is a need for a model to be created and implemented to incorporate the security behaviour that at the same time addresses information security issues, for which the same is currently being worked upon by the relevant authorities (Liang and Xue, 2010; Knapp et al., 2009). Following up on the above question, respondents were asked if security was a part of the strategy, and if so, to what extend it has been considered and established. Respondents pointed out that when in the UAE the plan for smart government was rolled out in 2013, the emphasis on security was less since the vulnerabilities were unknown. However participants stressed that now security was the top-most priority of the government and therefore vendors, stake holders and government personnel are always instructed to give critical importance to security, not just during the planning phase, but even during implementation and thereafter. Ferraz, Sampaio and Ferraz, (2015) had pointed out that IS is an extremely vital component which is not fully addressed.

4.2.4 Information Security Implementation Issues

The first question under this sub-section inquired about the major challenges that were faced by them or their organization. When asked what the challenges were that their organizations faced on smart government prospective which affected the Information Security, the reasonable lack of understanding of protocols was cited as a major concern.

In similar vein, when asked what were the challenges in deployment of information security on smart government initiatives; it was pointed out by respondents that it was the lack of infrastructure from all vendors that posed an issue in the implementation of smart government services. Furthermore, since the nationalities differed and everyone had different technical knowledge, getting everyone on page proved to be difficult. Participants were quick to attribute lack of information security standards and tools. Without these being in place, the implementation seemed difficult.

Participants were then asked to list out the barriers that they faced in the deployment of information security for smart government initiatives. Firstly, the cost factor was a major barrier as implementation of up-to-date security standards can prove to be very costly, thus innovative funding was being sought after. Secondly, technology readiness was another barrier as the government needs to be adept with changing technology to be able to implement the sophisticated information security strategies. Lastly, the lack of assessment tools make it difficult to implement information security strategy uniformly.

4.2.5 Strategies and Suggestions

Participants were asked to give strategic actions that needs to be adopted before planning for smart government, during implementations and post implementations in terms of information security. Participants said that in order to implement a safe and smart government that is technologically driven, important protocols and standards need to be identified and applied prior to becoming a smart government in order to ensure there is no breach of information.

The participants were then asked what were the best practices that should be followed and considered to overcome of the challenges and barriers of smart government initiatives in terms of information security. The participants said that in order to overcome the barriers, it was best to first address them and acknowledge them at the planning stage itself. When identified at the planning stage, it becomes easier to overcome them during them during the implementation stage. Participants also pointed out that it was vital smart government build the necessary infrastructure that is required for the implementation of information security strategy.

Lastly, participants were asked for their own recommendations for the application of a successful information security strategy for smart city and there were a number of recommendations that came to the fore. Respondents of the study suggested making the services more citizen-centric

while also using cloud computing, privacy enhancing technologies and transparency enhancing technologies to ensure better privacy. Furthermore, necessary standards that have been set should be followed as well as applied stringently by the smart government to ensure there is no breach of privacy and all vulnerabilities are addressed.

4.3 Discussion

From the above responses received and the data analysis made, it is certain that there is a major risk faced by smart government of UAE with respect to information security threats. While going smart makes it a more citizen-centric approach, there is no denying about the threats that the government can face. The interviews presented the fact that smart government is heavily reliant on smart technology i.e. Internet and the web portal for its effective functioning (Rahman et al. , 2012). The definition of smart government presented by various researchers discussed previously corroborate this fact (Rubel, 2014; Savoldelli et al., 2014). However, these gateways are prone to malicious attacks and security threats which can compromise the security of the government and the people. This fact was not only noted in the literature review done in the previous chapter wherein Otero, (2015) mentioned, those users who are unable to identify threats or seek easy solutions are at potential threat from innocent looking applications or approaches but also confirmed by participants of the conducted interview which consisted of senior level IS and IT personnel. The participants were well adept with information security and had been in the responsible positions, working closely with the government in the smart government implementation. Upon asking open-ended questions in relation to the information security strategy of the UAE it was observed that while most of them agreed that the UAE's vision to transform into a smart government was taking shape since 2013 (The National Plan for UAE Smart Government Goals, 2015), information security was an area that was not given enough attention (M. Al-Khouri, 2012). This was attributed to the fact that while the UAE spent a good amount on the infrastructure, information security was a neglected field. Another major component for this neglect was the cost factor. In order to make sure that the information security strategy is in place, government will have to not only hire professionals or the required tools but also develop an entire unit that would address the information security strategy for smart government. In the literature review it was suggested that RFID Tags, Smart Grids, advanced metering infrastructures (AMI), Public key infrastructures (PKI) etc. should be used for establishing information security. These

suggestions were also given by a number of researchers such as Xiwen, (2012), Clastres, (2011) and Rathgeb and Uhl, (2011) In the similar vein, professionals suggested investing in these technologies as they will enable to secure the information and data that is being exchanged continuously. Furthermore, as mentioned in the literature review, there are certain standards and protocols known as ISMS whose application helps organizations remain secure and avoid any outside threats and attacks or security breaches (Susanto, Nabil Almunawar and Chee Tuan, 2011). Echoing the same thought, participants suggested making use of these standards to help secure the data that is being exchanged. Not only public data, but even the publically available government data can be at risk and therefore there is an immediate need to safeguard these domains.

The interviews helped to shed light on the fact that while the UAE was technologically ready to become a complete smart city and the government has evolved to become a true smart government, information security strategy is largely neglected which poses a threat to the public as well as the government. There is therefore an immediate need on the part of the government to develop and implement smart government information security strategy which addresses the various vulnerabilities and formulates a strong security plan.

4.4 Conclusion

This chapter has successfully aligned the literature review from the previous chapters with the results and findings from the interviews conducted which corroborate the fact that while UAE is truly a smart city with a smart government, what it lacks is the information security strategy. While the government has addressed the issues in their conferences, little has been done in this sphere. The collaborating vendors and stakeholders too have not put information security at the helm of necessities and therefore there needs to be more thought, planning and implementation needs to be done in this sphere.

Chapter 5: Conclusion and Recommendations

5.1 Introduction

This chapter summarizes the findings of the study and also offers recommendations regarding information security strategy for smart governments which will ensure that the government of the UAE is up-to-date with respect to information security so that it can avoid any attacks, threats and vulnerabilities which could compromise the privacy of the government as well as the people. Information security is one of the basis of smart government since smart government is made up of technological components, all which are vulnerable to attacks and threats. Whether it is a simple smart phone or complex smart grids for energy deployment, all face the risk of being attacked by malicious hackers or other components looking to compromise the security of the smart government framework. This study was therefore aimed at gauging how ready the smart government of the UAE is with respect to information security and whether any steps were being taken to inculcate it into the smart government framework.

5.2 Key Findings

Countries across the globe are looking to transform into smart governments and smart cities. This is because of the technological advancements and the penetration of technology into everyday lives. Governments are looking to become more transparent, more efficient and more accessible to their people. Smart government embodies all these aspects and thus it is being adopted by places such as Korea, Seoul etc. Another country to have transformed into a smart government is the UAE which has embraced smart government initiative since2013 and have implemented it successfully over the years. The government has slowly transformed into a smart government by making all their services available online, thus increasing transparency, replacing cash with cashless transactions and making services available to the residents in quick time thanks to the internet.

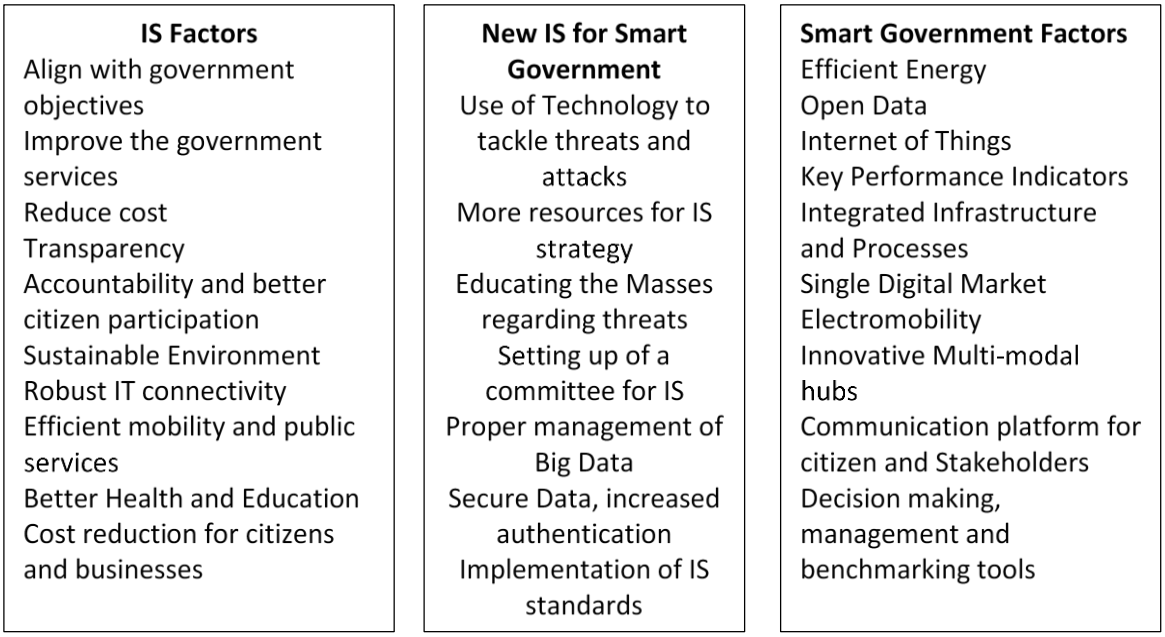
While smart government is the forward way to lead, one important detail which should be acknowledged is the need for information security. Where there is technology, internet and web, there is a threat of being attacked with security breaches, malicious attacks etc. These attacks can greatly compromise the sensitive private information of the people as well as the government. Hackers have successfully hacked information and caused a lot of problems for the people and the government. Thus it is extremely important that the government gives importance to information

security and has a strategy in place that will be able to combat such attacks and not compromise the privacy. While the UAE has implemented the smart government initiative successfully, it has not taken into account the information security. Although in recent years, there are more conferences and meetings held between government and private entities regarding the information security strategy, there is still little implementation and literature available to corroborate the same. Key IS and IT personnel were of the opinion that the lack of information security strategy can be attributed to the lack of resources as well as understanding the gravity and therefore there is an urgent need to look into the same. Defining the information security strategy and acknowledging the threats will help the government become a smart government in all manners.

5.3 Recommendations

Firstly the government should conduct more research in this sphere to get a better understanding of the problem and how it can affect the functioning of the smart government. Secondly, the government should lookup other model smart government nations and dwell into their information security strategy which can be modelled in the UAE. This will help to ensure that the proposed strategy has been tested and is effective and therefore apt for the country. More personnel should be hired with specialization in information security and information technology who would draw out the next plan forward and also sketch the security framework for the UAE. Such professionals, who have extensive knowledge in information security will be able to gauge the loopholes and accordingly they will come up with an effective plan that will ensure that the government is secured throughout and so are the people. Furthermore, the government also needs to educate the masses regarding the threats and attacks so that security practices are followed by people. This will help to make the government more secure and robust. All these recommendations have been made based on the conceptual framework, interviews and literature review and therefore there is always more scope for review.

The factors from both, Smart government and Information security have been studied and a new IS strategy for Smart Government of UAE has been mapped out which addresses the gaps and recommends those factors which have not been considered in order to formulate a stronger IS strategy.



Conceptual Framework for New IS in Smart Government

5.4 Research Limitations

While an extensive research was carried out for this study, certain aspects were not taken into consideration and thus could present an opportunity for future research. The interviews conducted had a sample size of 25 personnel only and therefore, the results cannot be considered conclusive. The research has looked only into the information security aspect of the smart government and not the smart city framework and therefore there might be loopholes with respect to UAE having an information security strategy for smart city in place which can be extended to smart government. The resources available for review were limited and therefore a more thorough investigation should be conducted.

References

1. Abouzakhar, N. (2013) *Critical infrastructure cybersecurity: A review of recent threats and violations*.
2. Al-Khouri, M. A. (2012). eGovernment Strategies The Case of the United Arab Emirates (UAE). *European Journal of ePractice*, pp.126-150.
3. Anthopoulos, L. (2017). *Understanding smart cities: A Tool for Smart Government or an Industrial Trick?*. 1st ed. Springer.
4. Cellary, W. (2013). Smart Governance for Smart Industries. In *Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance (ICEGOV '13)* (October 22-25 2013, Seoul, Republic of Korea), 91-93.
5. Clastres, C. (2011) Smart grids: Another step towards competition, energy security and climate change objectives, *Energy Policy*, 39(9) pp. 5399–5408.
6. *Data Breach Investigation and Statistical Report* (2015), Verizon Enterprise Solutions.
7. Dohler, I. M., Vilajosana, X., Vilajosana, and LLosa, J. (2011) *Smart cities: An action plan, in Barcelona Smart Cities Congress*.
8. Dolicanin, C. (2014). *Handbook of research on democratic strategies and citizen-centered e-government services*.
9. Efthymiopoulos, M. (2016). Cyber-security in smart cities: the case of Dubai. *Journal of Innovation and Entrepreneurship*, 5(1).
10. Elmaghraby, A. S. and Losavio, M. M. (2014) Cyber security challenges in smart cities: Safety, security and privacy, *Journal of Advanced Research*, 5(4) pp. 491–497.
11. *European Parliament Committee on Industry, Research and Energy*. (2014). Mapping Smart Cities in the EU.
12. Giffinger, R. and Gudrun, H. (2010). Smart Cities Ranking: An Effective Instrument for the Positioning of Cities? *ACE: Architecture, City and Environment*, 4(12), 7-25
13. Gil-Garcia, J., & Martinez-Moyano, I. (2007). Understanding the Evolution of e-Government: The Influence of Systems of Rules on Public Sector Dynamics. *Government Information Quarterly*, 24(2), 266–290. doi:10.1016/j.giq.2006.04.005
14. Gil-Garcia, J.R., Helbig, N. and Ojo, A. (2014). Being smart: Emerging technologies and innovation in the public sector. *Government Information Quarterly*, 31 (S1), I1-I8

15. Gil-Garcia, J.R., Pardo, T.A. and Nam, T. (2015). What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization. *Information Polity*, 20(1), 61-87
16. Habibur-Rahman, M., AlBalooshi, S. Y., and Sarker, A. (2015). The UAE Model of Smart Government: An Exploratory Analysis. In: *Public service innovation and the delivery of effective public services conference.* National University of Public Service.
17. *How connectivity and biometrics are making cities safer*, (2015) Accessed fromhttp://smartcitiescouncil.com/article/how-connectivity-and-biometricsare-making-cities-safer on 2017-05-31.
18. Ijaz, S., Ali, M., Khan, A. and Ahmed, M. (2016). Smart Cities: A Survey on Security Concerns. *International Journal of Advanced Computer Science and Applications*, 7(2), pp.612-625.
19. Jeon, W., Kim, J., Lee, Y. and Won, D. (2011) A practical analysis of smartphone security, in *Human Interface and the Management of Information*. Interacting with Information. *Springer*, 2011, pp. 311– 320.
20. Katsonis, M., & Botros, A. (2015). Digital Government: A Primer and Professional Perspectives. Australian Journal of Public Administration, 74(1), 42–52. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84923875583&partnerID=tZOtx3y1
21. Key, T. and We, C. (2009). Smart IT. *IEEE IT Pro*, 20–23.
22. Khaleej Times (2014). *Federal e-security body outlines new strategies*. [online] Available at: http://www.khaleejtimes.com/nation/government/federal-e-security-body-outlines-new-strategies [Accessed 30 Apr. 2017].
23. Kitchin, R. (2014) The real-time city? big data and smart urbanism, *GeoJourna*l, 79(1), pp. 1–14.
24. Kunzmann, K. R. (2014) Smart cities: A new paradigm of urban development, *Crios*, 4(1), pp. 9–20.
25. Lewis, Dave. (2015). *IoT securing smart city.* RSA Conference Abu Dhabi [online]. Abu Dhabi.
26. Lewis, J. A. (2014). Cybersecurity and Stability in the Gulf. *Center for Strategic and International Studies.* Washington, DC.

27. Liu, J., Xiao, Y., Li, S., Liang, W. and Chen, C. (2012) Cyber security and privacy issues in smart grids, Communications Surveys & Tutorials, *IEEE*, 14(4), pp. 981–997.
28. Luna-Reyes, L. F., & Gil-Garcia, J. R. (2014). Digital government transformation and internet portals: The co-evolution of technology, organizations, and institutions. *Government Information Quarterly*, 31(4), 545–555. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84922402495&partnerID=tZOtx3y1
29. Mellouli, S., Luna-Reyes, L.F. and Zhang, J. (2014). Smart government, citizen participation and open data. *Information Polity*, 19, 1-4.
30. Mitnick, K. and Simon, W. (2003). *The art of deception*. 1st ed. New York: Wiley.
31. Nam, T., & Pardo, T. A. (2011, June). Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times* (pp. 282–291). ACM.
32. Nie, X. and Zhong, X. (2013) Security in the internet of things based on rfid: Issues and current countermeasures, in *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering*. Atlantis Press.
33. Otero, Angel R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems.* 18(1), pp.26-45.
34. P. K. Gupta, Sanjeev Gupta, (2015) Corporate frauds in India – perceptions and emerging issues, *Journal of Financial* Crime, 22(1), pp.79-103, doi: 10.1108/JFC-07-2013-0045
35. P. Pironti, J. (2010). Developing an Information Security and Risk Management Strategy. *ISACA Journal,* 2.
36. Pateriya, R., and Sharma, S. (2011) The evolution of rfid security and privacy: a research survey, in Communication Systems and Network Technologies (CSNT), *International Conference on. IEEE*, 2011, pp. 115–119.
37. Petrov, O. (2014). Open Data as a Key Enabler of Smart Government. In: *17th National Conference on e-Governance*.
38. Pironti, J. (2010). Developing an Information Security and Risk Management Strategy. *ISACA Journal,* 2.

39. Rahman, M.H., Low, K.C.P., Almunawar, M.N., Mohiddin, F. and Sik-Leong, A. (2012). Egovernment policy implementation in Brunei: lessons learnt from Singapore. In Manoharan, A. and Holzer, M. (eds) *Active Citizen Participation in E-Government: A Global Perspective*, Hershey, USA: IGI Global, 359-377.
40. Rathgeb, C. and Uhl, A. (2011) A survey on biometric cryptosystems and cancelable biometrics, *EURASIP Journal on Information Security*, 2011(1), pp. 1–25, 2011.
41. Rubel, T. (2014). *Smart government: creating more effective information and services*. Retrieved from http://www.govdelivery.com/pdfs/IDC_govt_insights_Thom _Rubel.pdf on 1 May 2017,
42. Savoldelli, A., Codagnone, C. and Misuraca, G. (2014). Understanding the e-government paradox: Learning from literature and practice on barriers to adoption. *Government Information Quarterly*, 31, S63-S71.
43. Schmitt, C. (2014) *Security and privacy in the era of big data*.
44. Sen, M., Dutt, A., Agarwal, S., and Nath, A. (2013) Issues of Privacy and Security in the Role of Software in Smart Cities, *International conference of Communication system and network technology*., pp. 518–523.
45. Silva Ferraz, F., Candido Barros Sampaio, C. and André Guimarães Ferraz, C. (2015). Towards A Smart-City Security Architecture. In: SOFTENG 2015: The First International Conference on Advances and Trends in Software Engineering. *IARIA*.
46. Solanas, A., Patsakis, C., Conti, M., Vlachos, I., Ramos, V., Falcone, F., Postolache, O., P´erez-Mart´ınez, P. A., Di Pietro, R., and Perrea, D. N. (2014) Smart health: a context-aware health paradigm within smart cities, *IEEE Communications Magazine*, 58(8), pp. 74–81.
47. Susanto, H., Nabil Almunawar, M. and Chee Tuan, Y. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences*, 11(5), pp.23-29.
48. Symantec (2015). *Transformational 'smart cities': cyber security and resilience*. Executive Report: Smart Cities.
49. Tra.gov.ae. (2017). *TRA Hosts the First Introductory Workshop of the UAE Information Security Awareness Committee 'ISA' - Press Releases - Media Hub - Telecommunications Regulatory Authority (TRA).* [online] Available at: https://www.tra.gov.ae/en/media-

hub/press-releases/2017/1/15/tra-hosts-the-first-introductory-workshop-of-the-uae-information-security-awareness-committee-isa.aspx [Accessed 1 May 2017].

50. Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *Management Information Systems Quarterly*, 37(1), (pp. 21–54).
51. Whitman, M. and Mattord, H. (2012). *Principles of information security*. Boston, MA: Course Technology.
52. Xiwen, S. (2012) Study on security issue of internet of things based on rfid, in Computational and Information Sciences (ICCIS), *2012 Fourth International Conference on. IEEE*, 2012, pp. 566–569.
53. Yin, R. K. (2009). *Case study research: Design and methods*, Sage Publications, Incorporated.

Appendix: Interview Questions:

Part 1: Demographical Information

Name (optional)		
Current Position		
Gender	□ Male	□ Female
Age	□ 20-30 □ 31-40 □ 41-50 □ 51-60 □ 60 and above	
Total years of experience		
Years of experience in current position		
Total years of experience in Information Technology		
Total years of experience working in government		
Qualifications level	□ High School □ Diploma □ Bachelor □ Master □ PhD	

Part 2: Stakeholder Outlook

1. Please select in Yes or No if the following areas are important to you and your stakeholders with respect to Smart Government implementation.

Area of Specialization	***Yes***	***No***
Efficient Energy	□	□
Open Data	□	□
Internet of Things	□	□
Key Performance Indicators	□	□
Integrated Infrastructure and Processes	□	□
Single Digital Market	□	□
Electromobility	□	□
Innovative Multi-modal hubs	□	□
Communication platform for citizen and Stakeholders	□	□
Decision making, management and benchmarking tools	□	□

2. What are the views of the stakeholders from the smart government? Please select from the following table and add if others not listed

Stakeholders view	**Select**
Align with government objectives	□
Improve the government services	□
Reduce cost	□
Transparency	□
Accountability and better citizen participation	□
Sustainable Environment	□
Robust IT connectivity	□
Efficient mobility and public services	□
Better Health and Education	□
Cost reduction for citizens and businesses	
Others, please specify	□

3. The following table has general questions with respect to Information Security in Smart government Implementation.

SR#	***Question***	***Yes***	***No***	***Justifications***
1	Technology Selection- Are technologies chosen with proper cyber security controls as well as protections?	□	□	25
2	Are the products that are acquired for smart government solution evaluated for security posture?	□	□	
3	Are proper engineering practices such as threat modelling established for understanding the unique risks?	□	□	
4	Is risk management carried out to define security requirements?	□	□	
5	Do the smart government solutions comply with basic security requirements such as authorization and authentication capabilities, strong cryptography, anti-tampering capabilities etc.	□	□	
6	Are commitments made by vendors with respect to certain Service Level Agreements?	□	□	

4. Information Security and Identifying Stakeholders

SR#	***Question***	***Response***
1	When implementing a new smart government initiative, who is involved in the implementation process	
2	What are the phases for implementation of smart government initiative?	
3	How complicated is the technological and IT security phase.	
4	What is the value of the relationship between your department and the IT department?	
5	How important is the IT infrastructure to implement smart government initiatives?	
6	How much importance is given to security and privacy in the implementation of the smart city and smart government initiative?	
7	After the implementation of a new smart service, is it followed up to ensure no information security loopholes are present?	

2 *Part 3: the current state and followed practices*

1. Can you describe your roles and responsibility on the smart government initiative?

---

2. Do you have a defined strategy for government transformations to smart government? If yes how long it has been established, how often it's been reviewed and what is the strategy and its components?

---

3. Is the information security part of the strategy? If yes, to what extend it has been considered and established

---

---

4. What are the main challenges facing you or your organizations smart government?

---

5. What are challenges facing you organizations on smart government prospective and affecting the Information Security?

---

6. What are the challenges facing you on Information Security deployment on smart government initiatives?

---

7. What are the barriers facing you on Information Security deployment on smart government initiatives?

Part 5: Strategies, Suggestions, feedback and comments

8. What are the strategic actions to be adopted before planning for smart government, during implementations and post implementations in terms of information security?

---

9. What are the best practices to be followed and considered to overcome of the challenges and barriers of smart government initiatives in terms of information security?

---

10. Based on your experience, what are your recommendations for successful information security strategy for smart governments?

Part 6: Feedback and Suggestions

Please mention if you have any further suggestions, feedback and comments.
