

**A Decision Modelling Approach for Security Modules
of Delegation Methods in Mobile Cloud Computing
using Probabilistic Interval Neutrosophic Hesitant
Fuzzy Set**

نهج نمذجة القرار للوحدات الأمنية في طرق التفويض في الحوسبة السحابية
المتنقلة باستخدام المجموعة النيوتروسوفية الضبابية المترددة الاحتمالية
والفاصلة

by

SENDEYAH SALEM RASHID ALHANTOOBI

**A thesis submitted in partial fulfilment
of the requirements for the degree of
DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE
at**

The British University in Dubai

March 2023

**A Decision Modelling Approach for Security Modules of Delegation Methods
in Mobile Cloud Computing using Probabilistic Interval Neutrosophic
Hesitant Fuzzy Set**

نهج نمذجة القرار للوحدات الأمنية في طرق التفويض في الحوسبة السحابية المتنقلة باستخدام
المجموعة النيوتروسوفية الضبابية المترددة الاحتمالية والفاصلة

by

SENDEYAH SALEM RASHID ALHANTOABI

**A thesis submitted to the Faculty of Engineering and IT
In partial fulfilment of the requirements for the degree of
DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE
at
The British University in Dubai**

**Main Supervisor: Dr.Aos Alaa Zahidan
Second Supervisor: Prof. Dr.Khaled Shaalan**

March 2023

Approved for award:

Name
Designation

Name
Designation

Date: _____

Approved for award:

Name
Designation

Name
Designation

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that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.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

A handwritten signature in black ink, appearing to read 'Sindhu', written in a cursive style.

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

The author whose copyright is declared on the title page of the work has granted to the British University in Dubai the right to lend his/her research work to users of its library and to make partial or single copies for educational and research use.

The author has also granted permission to the University to keep or make a digital copy for similar use and for the purpose of preservation of the work digitally.

Multiple copying of this work for scholarly purposes may be granted by either the author, the Registrar or the Dean only.

Copying for financial gain shall only be allowed with the author's express permission.

Any use of this work in whole or in part shall respect the moral rights of the author to be acknowledged and to reflect in good faith and without detriment the meaning of the content, and the original authorship.

ABSTRACT

Mobile Cloud Computing (MCC) has become a pervasive technology that offers on-demand, flexible, and scalable computing resources to mobile devices. However, the security issues associated with MCC have become a major concern for users and organizations, leading to the development of various Security Modules. These modules typically use delegation methods that involve the transfer of data or operations from mobile devices to the cloud to perform the task at the best performance and security levels.

Despite extensive attempts to design secure security modules of delegation in Mobile Cloud Computing (MCC), none of the existing modules possess all the necessary development attributes. Our analysis indicates that previous studies have not used security development attributes as evaluation criteria to compare and assess the available Security modules of delegation methods in MCC. However, Modeling these modules is critical and poses significant challenges in selecting the most secure security module. du to multicriteria, importance of data and data variation. To address this issue, this study proposes a Decision Modelling Approach for Security Modules of Delegation Methods in Mobile Cloud Computing using multi-criteria decision-making (MCDM) methods. The proposed approach involves the integration of Evaluation based on Distance from Average Solution (EDAS) method with fuzzy weighted with zero inconsistency (FWZIC) under Probabilistic Interval Neutrosophic Hesitant Fuzzy Set (PINHFS) environment. .

The framework presented in this study involves two primary stages : the construction of decision matrices for Security Modules of delegation methods in MCC and the application of the PINHFS-FWZIC method to determine the weight of the security evaluation criteria. The EDAS method is then employed to modeling the Security Modules of delegation methods in MCC

based on the formulated decision matrices and criteria weight. The validation and evaluation of the proposed framework were conducted through model validation and decision evaluation procedures. Model validation involved sensitivity analysis and systematic ranking procedures . The benchmarking checklist was used to compare the results of the proposed framework with the existing approaches.

Based on the findings, it can be concluded that the proposed framework can efficiently weight the security criteria and successfully rank Security Modules of delegation methods in MCC. The PINHFS-FWZIC method effectively handled the uncertainty and hesitancy of the decision-makers in assigning weights to the evaluation criteria. Overall, the proposed framework provides a useful benchmark for evaluating other Security Modules of delegation methods in MCC. It can aid decision-makers in selecting the most secure MCC delegation method system by providing a comprehensive evaluation and Modeling of the available Security Modules.

الخلاصة

أصبحت الحوسبة السحابية للأجهزة المحمولة (MCC) تقنية منتشرة توفر موارد حوسبة مرنة وقابلة للتطوير عند الطلب للأجهزة المحمولة. ومع ذلك ، أصبحت القضايا الأمنية المرتبطة بـ MCC مصدر قلق كبير للمستخدمين والمؤسسات ، مما أدى إلى تطوير نماذج أمان مختلفة. تستخدم هذه النماذج عادةً طرق التفويض التي تتضمن نقل البيانات أو العمليات من الأجهزة المحمولة إلى السحابة لأداء المهمة بأفضل مستويات الأداء والأمان.

على الرغم من المحاولات المكثفة لتصميم أنظمة أسلوب التفويض الأمان للحوسبة السحابية المتنقلة (MCC) ، لا يمتلك أي من الأنظمة الحالية جميع سمات التطوير الضرورية. يشير تحليلنا إلى أن الدراسات السابقة لم تستخدم سمات تطوير الأمان كمعايير تقييم لمقارنة وتقييم أنظمة أساليب تفويض MCC المتاحة. ومع ذلك، فإن قياس أداء هذه الأنظمة أمر بالغ الأهمية وي طرح تحديات كبيرة في اختيار النظام الأكثر أمانًا. لمعالجة هذه المشكلة، تقترح هذه الدراسة نهجًا قائمًا على القرار لتقييم وقياس أنظمة أسلوب تفويض MCC باستخدام طرق صنع القرار متعددة المعايير (MCDM). يتضمن النهج المقترح تكامل التقييم على أساس المسافة من طريقة الحل المتوسط (EDAS) ومجموعة ضبابية متذبذبة للفترات الاحتمالية (PINHFS) مرجحة مع عدم تناسق (PINHFS-FWZIC) لترتيب الأنظمة.

يشتمل إطار العمل المقدم في هذه الدراسة على مرحلتين أساسيتين: بناء مصفوفات القرار لأنظمة أسلوب تفويض MCC وتطبيق طريقة PINHFS-FWZIC لتحديد وزن معايير التقييم الأمني. ثم يتم استخدام طريقة EDAS لقياس أنظمة أسلوب تفويض MCC بناءً على مصفوفات القرارات المصاغة ووزن المعايير. تم التحقق من صحة الإطار المقترح وتقييمه من خلال إجراءات التحقق من صحة النموذج وتقييم القرار. تضمن التحقق من صحة النموذج تحليل الحساسية وإجراءات التصنيف المنهجية. تم استخدام قائمة مرجعية معيارية لمقارنة نتائج الإطار المقترح مع النهج الحالية لتقييم القرار.

بناءً على النتائج ، يمكن استنتاج أن إطار العمل المقترح يمكن أن يرفع معايير الأمان بكفاءة ويصنف أنظمة أسلوب تفويض MCC بنجاح. تعاملت طريقة PINHFS-FWZIC بشكل فعال مع عدم اليقين والتردد لدى صانعي القرار في تعيين أوزان لمعايير التقييم. بشكل عام ، يوفر الإطار المقترح معيارًا مفيدًا لتقييم الأنظمة الأخرى في مجال نماذج أمان الحوسبة السحابية المتنقلة. يمكن أن يساعد صانعي القرار في اختيار نظام أسلوب تفويض MCC الأكثر أمانًا من خلال توفير تقييم شامل وترتيب للأنظمة المتاحة

DEDICATION

This thesis is dedicated to the individuals who have given me unwavering support and belief throughout my life, including my late parents, siblings, and dear friend Aseilah Al Hamoudi.

ACKNOWLEDGEMENT

With immense gratitude and appreciation, I extend my sincerest thanks to the Allah (the God) , the Lord of the Worlds, for granting me the knowledge, wisdom, and perseverance to embark upon this journey of discovery and learning.

I would like to express my utmost appreciation to the distinguished Dr. Aws for his exceptional guidance, unwavering support, and insightful knowledge that were instrumental in achieving this significant milestone. His mentorship and teachings have been invaluable, and I will forever be grateful for the immense impact he has had on my academic career.

I would also like to acknowledge and extend my heartfelt thanks to my late parents, who laid the foundation for my upbringing and education, and my siblings, whose unwavering support and encouragement have been an endless source of motivation throughout my academic journey.

Finally, I would like to express my deepest appreciation to my dear friend “Aseila”, whose unwavering friendship and encouragement have been a constant source of strength and comfort throughout my PhD and academic endeavors.

I extend my gratitude and thanks to all those who have supported and encouraged me along the way. All praise and thanks be to God, the Lord of the worlds.

TABLE OF CONTENTS

TABLE OF CONTENTS	<i>i</i>
LIST OF FIGURES	<i>v</i>
LIST OF TABLES.....	<i>vi</i>
LIST OF APPREVIATION	<i>vii</i>
CHAPTER 1: INTRODUCTION	<i>1</i>
1.1. Background	<i>1</i>
1.2. Problem Statement.....	<i>4</i>
1.3. Research Questions.....	<i>10</i>
1.4. Research Objectives.....	<i>11</i>
1.5. Connection among Research Objectives, Questions and Problem	<i>12</i>
1.6. Scope of the Study.....	<i>13</i>
1.7. Significant of the Study	<i>14</i>
1.8. Main Terminology	<i>16</i>
1.9. Structure of Thesis.....	<i>16</i>
1.10. Chapter Summary	<i>18</i>
CHAPTER 2: LITERATURE REVIEW.....	<i>19</i>
2.1. Introduction.....	<i>19</i>
2.2. Taxonomy of Literature Review on Security Modules of Delegation Methods in Mobile Cloud Computing and its related Development security attributes.	<i>21</i>
2.2.1. Delegation Methods in Mobile Cloud Computing	<i>22</i>
2.2.2. Development Security attributes	<i>23</i>
2.3. Critical Review of Security Modules of Delegation Methods in MCC.....	<i>24</i>

2.4.	Challenges of Security Modules.....	31
2.4.1.	Multi Evaluation Criteria issue	32
2.4.2.	Criteria importance issue	33
2.4.3.	Data Variation issue.....	34
2.5.	Theoretical Background of Multicriteria Analysis in Security and Cloud Computing	35
2.6.	Multicriteria Decision Making Methods.....	37
2.7.	EDAS Method.....	43
2.8.	FWZIC Method.....	49
2.8.1.1.	Probabilistic Interval Neutrosophic Hesitant Fuzzy (PINHFS)	52
2.9.	Perspectives on Dataset Generation across Various Case Studies in Decision Making.	54
2.10.	A Comprehensive Review of Validation and Evaluation Procedures in Decision Science	57
2.10.1.	Sensitivity Analysis Procedure.....	58
2.10.2.	Systematic Ranking Procedure.....	60
2.10.3.	Comparative Analysis Utilizing Benchmarking Checklist Approach.....	61
2.11.	Chapter Summary	63
CHAPTER 3: RESEARCH METHODOLOGY		65
3.1.	Introduction.....	65
3.2.	Investigation phase.....	66
3.3.	Proposed Modeling decision-based approach for the delegation method of MCC	67

3.3.1.	Decision matrix identification phase	67
3.3.2.	Formulation and Development phase	68
3.4.	Validation and Evaluation phase.....	68
3.4.1.	Sensitivity analysis	69
3.4.2.	Systematic Ranking	70
3.4.3.	Benchmarking Checklist	71
3.5.	Chapter Summary	74
CHAPTER 4: DECISION MODELLING APPROACH FOR THE SECURITY MODULES OF DELEGATION METHODS IN MOBILE CLOUD COMPUTING		75
4.1.	Introduction.....	75
4.2.	Identification of Decision matrix	77
4.2.1.	Security Evaluation Criteria identification	77
4.2.2.	Security Modules of Delegation Methods in MCC identification	81
4.2.3.	Decision Matric formulation	82
4.3.	Formulation and Development phase	84
4.3.1.	PINHFS- FWZIC method	84
4.3.2.	Utilizing EDAS method	92
4.4.	Chapter Summary	96
CHAPTER 5: FINDINGS AND DISCUSSION.....		97
5.1.	Introduction.....	97
5.2.	Benchmarking framework result	98
5.2.1.	Decision Matrix Results.....	98

5.2.2.	Determining Criteria Weight Result Using PINHFS -FWZIC.....	99
5.2.3.	Ranking Result of Security Modules of Delegation Methods in MCC using EDAS ...	103
5.3.	Validation and Evaluation Results	108
5.3.1.	Sensitivity Analysis Result	108
5.3.2.	Systematic Ranking Result.....	116
5.3.3.	Benchmarking Checklist Result	119
5.4.	Conclusion and Future Review	122
5.4.1.	Objectives Achieving	122
5.4.2.	Research Contributions.....	125
5.4.3.	Practical Contributions	127
5.4.4.	Limitation	129
5.4.5.	Future Work.....	130
5.5.	Chapter Summary	131
REFERENCES		132
APPENDIXES.....		147
Appendix A : Security Evaluation Criteria		147
Appendix B : Decision Matrix Results		149

LIST OF FIGURES

Figure 1: Problem Statement.....	10
Figure 2: Connection among Research Objectives, Questions and Problem	12
Figure 3: Scope of the Study	14
Figure 4: Significant of the Study	15
Figure 5: Structure of Thesis	17
Figure 6: Literature Review Structure.....	20
Figure 7: Taxonomy of LR on MCC Security Modules delegation methods and its related security issues.....	22
Figure 8: Evaluation and Benchmarking issues of MCC Security Modules delegations methods	31
Figure 9: Multi Evaluation Criteria issue	32
Figure 10: Criteria importance issue	33
Figure 11: Data Variation issue.....	34
Figure 12: MCDM approaches.....	38
Figure 13: EDAS Integrations samples	46
Figure 14: New EDAS Versions	48
Figure 15: New versions of FWZIC under different fuzzy sets	51
Figure 16: History of PINHFZ	53
Figure 17: Validation and Evaluation Procedures.....	58
Figure 18: Research Methodology	65
Figure 19: Modeling decision-based approach for delegation method of MCC.....	76
Figure 20: Number of system in each MCC delegation methods	82
Figure 21: PINHFS-FWZIC weighting method.....	84
Figure 22: Benchmarking Framework Results for MCC delegation method systems: An Overview	97
Figure 23 : Sensitivity Analysis of Layering Delegation Method Alternatives Benchmarking in nine scenarios	110
Figure 24 : Sensitivity Analysis of Encryption Delegation Method Alternatives Benchmarking in nine scenarios	111
Figure 25 : Sensitivity Analysis of Dynamic Offloading Delegation Method Alternatives Benchmarking in nine scenarios	112
Figure 26 : Sensitivity Analysis of Authentication Delegation Method Alternatives Benchmarking in nine scenarios	113
Figure 27: Layering Delegation method Correlation result	114
Figure 28: Encryption Delegation method Correlation result	115
Figure 29: Dynamic Offloading Delegation method Correlation result	115
Figure 30: Authentication Delegation method Correlation result	116
Figure 31: Research Contributions and Novelty Mapping.....	126

LIST OF TABLES

Table 1: Security Modules in Layering Delegation Method	25
Table 2: Security Modules in Encryption Delegation Method	27
Table 3: Security Modules in Dynamic Offloading Delegation Method	28
Table 4: Security Modules of Authentication Delegation Method	29
Table 5: Mathematical approach most common used methods	38
Table 6 : Human Approach most common used methods	41
Table 7: Exploring the Application of Root Article Method in Diverse Case Studies	55
Table 8: A Review of Sensitivity Analysis Evaluations across Diverse Case Studies	59
Table 9: Systematic Ranking Procedure in Various Case Studies	60
Table 10: A Comparative Study of Benchmarking Checklist Procedures in Various Case Studies	62
Table 11: Comparison Points definition.....	72
Table 12: Decision Matric formulation for all MCC delegation methods	83
Table 13: Linguistic Expressions and Corresponding Numerical Scales	86
Table 14: Expert decision matrix (EDM).....	87
Table 15: Layering Delegation Method Decision matrix.....	99
Table 16: Expert Preference for Delegation Methods in MCC Systems Security Evaluation Criteria.....	100
Table 17: EDM of MCC delegations method systems.....	100
Table 18: Corresponding (PINHFN) for Each Linguistic Term	101
Table 19: Security evaluation Criteria's weight	103
Table 20: layering delegation method alternatives result based on EDAS method	104
Table 21: : Encryption delegation method alternatives result based on EDAS method	105
Table 22: : Dynamic Offloading delegation method alternatives result based on EDAS method	106
Table 23: : Authentication delegation method alternatives result based on EDAS method ...	107
Table 24: Criteria Weighting for MCC Security evaluation criteria in nine Scenarios	109
Table 25: Ranking Results Segregation for Each Delegation Method.....	117
Table 26: Group Distribution Validation Results	117
Table 27: Comparing the Proposed Study to the Benchmark Study: Key Points of Comparison.	120
Table 28: Encryption Delegation Method Decision matrix	149
Table 29: Dynamic Offloading Delegation Method Decision matrix.....	150
Table 30: Authentication Delegation Method Decision matrix	150

LIST OF APPREVIATION

Appreviation	Meaning
MCDM	Multi Criteria Decision Making
MCC	Mobile Cloud Computing
EDAS	Evaluation based on Distance from Average Solution
PINHFS	Probabilistic Interval Neutrosophic Hesitant Fuzzy Set
FWZIC	Fuzzy-Weighted Zero-Inconsistency
EDM	Expert decision matrix
MINDPRES	Mobile- Cloud Intrusion Detection and Prevention System
UL	User Layer
APE	Attribute Based Encryption
PDA	Positive Distance Average
NDA	Negative Distance from Average
PDHL	Probabilistic Double Hierarchy Linguistic
AI	Artificial Intellegence
DCSI	Data Centre Security Index
TOPSIS	"Technique for Order of Preference by Similarity to Ideal Solution "
AHP	Analytic hierarchy process
ANP	Analytic Network Process
BWM	Best–worst method

PROMETHEE	Preference Ranking Organization Method for Enrichment Evaluations
GRA	Grey Relation Analysis
GWP	Global warming potential
WEPLPA	Weighted extended probabilistic linguistic power average
CPT	Cumulative prospect theory
PDHL	Probabilistic Double Hierarchy Linguistic
MAGDM	Multiple Attribute Group Decision Making
SEJ	Structured expert judgment
BES	Bald Eagle Search
IOT	Interned Of Things
DH-FWZIC	Dual hesitant fuzzy weighted zero inconsistency
DH-FDOSM	Dual hesitant fuzzy decision by opinion score method
ROFWZIC	rung orthopair fuzzy-weighted zero-inconsistency
SCC	Spearman's correlation coefficient
SPOF	Single point of failure
PINHFWA	Probabilistic Interval Neutrosophic Hesitant Fuzzy Weighted Averaging
SP	Positive weighted distance
SN	Negative weighted distance
NSP	Normalized Positive weighted distance
NSN	Normalized Negative weighted distance

AS	Appraisal score
AV	Average Solution

CHAPTER 1: INTRODUCTION

1.1. Background

The rapid progress in technology has led to an increase in reliance on cloud computing, as companies and institutions strive to make their applications available on computing to ensure seamless and flexible services to users to support their rapid digital transformation journey. The latest report from Gartner on the extent of spending on the use of public cloud computing stated that expenditures for the benefit of cloud computing are constantly increasing and are expected to reach approximately \$600 million in 2023, compared to roughly \$490 million in 2022 (Gartner, 2022).

According to the report, the most significant increase in spending is Cloud Application Infrastructure Services (PaaS) and Cloud Application Services (SaaS). Gartner also reported that more than 80% of companies will move to cloud computing and close their on-premises data centers by 2025. All these statistics and reports indicate that the use of cloud computing as a service, whether at the level of individuals or organizations, is constantly increasing and non-stop, as the use includes Various services provided on the cloud, including Application, Mobile, Storage, Database, Servers, ...etc. Mobile Cloud Computing (MCC) is one of the most used services currently at level of people. MCC is the ability to use mobile devices to run existing applications or access applications on cloud computing over wireless networks (Seada Abdu Wakene et al. 2021). It is also defined as running applications on remote servers so that the mobile device acts as a client device on the remote server (the cloud) (Gnana Jeevan & Maluk Mohamed 2020).

Nowadays, many of the applications that are used via smartphones are conducting their processing on the cloud (Özkan, Erdem & Özceylan 2022) , meaning that the processing takes place in massive

data centers owned by major local or global companies, such as Amazon, Microsoft, Google, and other companies provide these services. Despite the popularity of these applications and their frequent use, there is a great issue behind this use, which is the security of cloud computing (Chen & Lin 2022) . Cloud computing security is one of the biggest challenges facing cloud service providers. Studies are constantly seeking to propose and implement solutions that mitigate the risks of using cloud services.

Recently, many studies have presented Security Modules for avoiding MCC security issues. These Security Modules are designed to security the so-called delegation method, which means delegating operations from the mobile to the cloud to perform the task at the best performance. This explains the importance of the Security Modules of delegation methods. There are various delegation methods, such as Layering, Authentication, Dynamic Offloading, and Encryption. Firstly, For **layering**, (Ogwara et al. 2021) proposed a model called MINDPRES (Mobile- Cloud Intrusion Detection and Prevention System) to enhance the security of the User Layer (UL) in the Mobile Cloud Computing environment. In addition (Lawal et al. 2021) propose a three-level layer of security to help with the privacy concerns for MCC. Also (Huang et al. 2010) developed a conceptual framework known as MobiCloud, which proposes a three-layers architecture for mobile cloud computing (MCC). Each layer comprises several components that function as service vendors and intermediaries. Secondly, for **authentication**, Sridhar & Smys (2020) established remote services access through a cloud network that improves encryption and decryption processes in the cloud-computing environment. (Wilczynski, Kolodziej & Grzonka 2021) proposed a model for authentication based on blockchain technology. Furthermore, (Khan et al. 2013) introduced the concept of safeguarding user identities in mobile-cloud computing, by developing an automatic and dynamic credential identification system for mobile devices through the utilization of cloud

computing capabilities.. Thirdly, For **Dynamic Offloading**, (A. Almusaylim & Jhanjhi 2020) established a model that offloads sensitive user location-based data to the cloud, and with (Derhab et al. 2020) offloading architecture is proposed for the application of two-factor mutual authentication. And lastly, many studies proposed many models for **Encryption**, such as Madhurya et al. (2021) offered a CP-ABE (Attribute-Based Encryption) to make it fit for versatile cloud environments. It achieves this by changing the structure of the access control tree to make it sufficient for multipurpose cloud environments. Further, (Bhatia, Verma & Sharma 2020) propose a pairing-free incremental proxy re-encryption scheme (without certificates) that addresses the resource overheads from the requirement that mobile nodes in MCC encrypt and recalculate the hash value for any adjustment to uploaded records.

In the current scenario, (AlAhmad et al. 2021) have surveyed and reviewed the Security Modules of delegation methods in MCC and they noted that the security issues derived from the security modules of delegation method. An example of security issues are privacy, Authentication (cloud-to-client authentication, Client to cloud authentication, and Multi-factor Authentication), Data Security, Encryption key, single failure points, security threats, communication channels issues, Un proper access control, authorization issues and anonymity. According to systematic review done for the previous studies of Security Modules issues in MCC from 2008 to 2022, a unified security module with all the desired properties that can overcome security issues has not yet been presented. The focus was on identifying issues only, individually overcoming them, and developing new MCC model with specific delegation method. However, there was no comparison for the security modules criteria (security issues) and their evaluation while it is necessary to evaluate based on multiple criteria. More than 50 Security Modules and 13 development attributes for MCC were analyzed in this study. It was noted that each criterion has its specificity and differs according

to the type of delegation method from the mobile to the cloud. Furthermore, the assessment process in itself is intricate owing to the divergent and heterogeneous nature of the data being evaluated (Security Modules of delegation methods in MCC) . A Decision Modelling Approach for Security Modules of Delegation Methods in Mobile Cloud Computing need to be developed to select the secured Security modules of delegation methods in MCC.

1.2. Problem Statement

Problem statement of this research driven from tow gaps which are research gap and theoretical gap. Many researchers have developed Security Modules to avoid security issues while delegating the device's operations to the cloud such as Madhurya et al. (2021) , Sridhar & Smys (2020) , (Ogwara et al. 2021), (A. Almusaylim & Jhanjhi 2020) , Kołodziej & Jaatun (2021) , (Bhatia, Verma & Sharma 2020) and (Seada Abdu Wakene et al. 2021) but according to (AlAhmad et al. 2021), some Security Modules ignored some security development attribute when choosing the delegation method. In contrast, some modules considered most of these attributes to reach a secure security module. The security development attribute varied between privacy, Authentication, Data Security, Encryption key, single failure points, security threats, communication channels issues, Un proper access control, authorization issues and anonymity. Despite all the efforts made in designing Security Modules of delegation methods in MCC, none of the modules took all security development attributes into account, so the trade-off between which is more secure is the most complex and challenging. As mentioned before, the various security development attributes were not considered as security evaluation criteria for evaluating and modeling an appropriate Security Modules of delegation methods in MCC. However, evaluating Security Modules of delegation methods in MCC and modeling the most secure one through comparative analysis is both important and arduous. This is due to the intricate and diverse combinations of security criteria that are

present in such systems. Consequently, it becomes difficult to conduct a fair modeling of these systems from a specific perspective, given the unique variations that exist between them. This issue is affecting the MCC service providers, as they benefit from the research conducted in this field. Therefore, this problem exists at the organizational level.

To overcome the noted research gap, three fundamental issues necessitate resolution when benchmarking mobile cloud computing (MCC) models., which are **First , multiple evaluation criteria**, as the process of evaluating and modeling Security Modules of delegation methods in MCC is complicated by the presence of various evaluation criteria (Shao et al. 2018) . Taking in to account these criteria into the modeling process is essential in discerning the most secure module (Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023) . Each security moudle is associated with 13 distinct security issues, including privacy, authentication (e.g., cloud-to-client, client-to-cloud, and multi-factor authentication), data security, encryption keys, single failure points, security threats, communication channel issues, improper access control, authorization issues, and anonymity. **Second, the importance of criteria**, the significance of security criteria may differ depending on their intended objectives. Nonetheless, to evaluate and model Security Modules of delegation methods in MCC , adequately integrating the relative importance of these criteria is imperative, as it poses a challenging task. (Albahri, Albahri, et al. 2022a) . **Third and last issue is data variation**, Decision-makers face significant challenges when attempting to compare alternatives to the Security Modules of delegation methods in MCC due to differences in data availability across various criteria. The criteria available in one security module for layering delegation methods may vary significantly from those in another system within the same delegation method (Alsalem et al. 2021a) .

To overcome the mentioned issues, MCDM is dealing with evaluating a set of alternatives with multiple and often conflicting criteria to provide the most appropriate, accurate, and correct choice and to arrange the alternatives according to preference (Duarte Alonso et al. 2018). Many types of research specialized in MCDM research related to security issues and cloud computing. Still, none of them are specialized in the security issues in the delegation methods and which delegation method's system is the best which is considered as a **research gap** (Özkan, Erdem & Özceylan 2022), (Chen & Lin 2022), (Kumar Tiwari & Kumar 2022), (Kumar, Kumari & Kumar 2021), (Torbacki 2021), (Turskis et al. 2019), (Paul et al. 2018). **Up to date**, Several multi-criteria decision-making (MCDM) techniques have been devised and employed across diverse domains, proffered as suitable remedies to support decision-makers in tackling complex challenges encountered in practice (Asadabadi, Chang & Saberi 2019) (Khaira & Dwivedi 2018) (Salih, Zaidan & Zaidan 2020) (Moslem et al. 2020) (Youssef 2020).

Evaluation based on Distance from Average Solution (EDAS) is one of the MCDM mathematical method (Alinezhad & Khalili 2019). It's used for calculating every alternative's distance from the average value to help decision makers to find the best solution (Huang, Lin & Chen 2021). EDAS is calculating the distance from the Positive Distance Average (PDA) and the Negative Distance from Average (NDA), which is the lowest alternative from the best value (Ghorabae et al. 2015) and for that it can be used to overcome the mathematical approach issues which is related to distance measurement. Various academic researchers use EDAS as a mathematical method in their MCDM research because of its efficient (Fan, Li & Wu 2019), (Tanwar, Mehrotra & Nagpal 2020), (Dr. A Sahaya Sudha 2019), (Mayssara A. Abo Hassanin Supervised et al. 2019), (Mitra 2020). According to (Sharma & Sharma 2020), with EDAS, calculating the data with the mean-wise technique along with dealing with outliers was the best performer.

Thus, the EDAS method is a viable approach to evaluate and rank the performance of MCC delegation mehtod's systems. However, a notable limitation of this method is its inability to assign weight to criteria, which are crucial factors that directly impact the ultimate decision outcome in MCDM. Consequently, an external method must be employed to address this crucial aspect in order to to realize the complete capability of the EDAS method. Because of that , New versions of EDAS are proposed which are integrated with MCDM human methods in order to weight the criteria. (Zavadskas et al. 2019) use EDAS with CRITIC to evaluate and rank the autonomous vehicles , (No et al. 2021) use interval EDAS to evaluating and ranking some Irani's banks according to some economic criteria, and (Fan LEI, Guiwu WEI, Weijie SHEN 2022) integrate EDAS with PDHL (Probabilistic Double Hierarchy Linguistic) to evaluate and rank 3D printers. However, there are still some challenges with human approaches lie in Inconsistency, time consumption in pairwise comparisons, and unnatural comparisons (Alamoodi, Mohammed, et al. 2022a) , (Alsalem et al. 2021a) , (Albahri, Zaidan, et al. 2022a) , (Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023).

FWZIC can be deemed as the optimal solution to mitigate human multi-criteria decision-making (MCDM) issues, as it can weigh attributes without any inconsistencies, irrespective of the number of criteria involved. Expert preferences can be utilized in multi-criteria decision-making (MCDM) to calculate the significance of each criterion level through the application of FWZIC (Krishnan et al. 2021). The initial iteration of FWZIC was established utilizing triangular fuzzy sets (TFNs) as its foundation, which have some constraints such as difficulty of directly defining the membership value and Data uncertainties (Albahri, Zaidan, et al. 2022b). New versions of FWZIC were proposed with new fuzzy sets to overcome the constraints raised. Recently many researchers user FWZIC with new fuzzy sets such as (Qahtan, Yatim, et al. 2022) use spherical FSs , (Alamoodi,

Albahri, et al. 2022) use Cubic Pythagorean FSs, (Anor et al. 2022) , (Al-Humairi et al. 2022) use linear Diophantine fuzzy rough sets (LDFRSs) and (Al-Humairi et al. 2022) use dual hesitant FSs . **Recently** , (Qahtan, Alsattar, et al. 2022) use probabilistic hesitant fuzzy set and (Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023) use Pythagorean probabilistic hesitant fuzzy sets as Probability theory is often regarded as a means of representing knowledge. Within the domain of fuzzy decision-making problems, elevating the probability value can be a viable approach. (Shao et al. 2018) . Furthermore, the theory of neutrosophic fuzzy sets has received extensive attention and practical applications (Shao et al. 2018).

Based on what was analyzed above and a collection of the limitations mentioned earlier and constraints, the integration of EDAS with FWZIC under Probabilistic Interval Neutrosophic Hesitant Fuzzy Set was not addressed which can be considered a **theoretical gap** as the integration may lead to more accurate results in choosing the best Security Module of Delegation Methods in Mobile Cloud Computing.

The integration of EDAS with FWZIC can be justified for the many reasons: Firstly, EDAS and FWZIC can complement each other by addressing the limitations of other mathematical methods commonly used in Multi-Criteria Decision Making (MCDM) such as TOPSIS, VIKOR, SAW, HAW, and WSM. These limitations include issues related to normalization, distance calculations, the need for subjective weighting from a human approach, and dealing with vague data. Secondly, EDAS has been successfully integrated with several MCDM human approaches, demonstrating highly accurate ranking results. It is also the only method that evaluates the intangibility of average solutions considering decision-maker uncertainties. By integrating EDAS with FWZIC, the accuracy and reliability of the decision-making process can be further enhanced. Thirdly, EDAS calculates the distance from the Positive Distance from Average (PDA) and the Negative Distance

from Average (NDA), allowing for a comprehensive assessment of alternatives based on their proximity to the best value. This distance-based evaluation aligns well with the analytical nature of FWZIC, which aims to determine the weight attributes without inconsistencies using techniques such as AHP, ANP, and BWM. Finally, FWZIC has the capability to overcome several limitations of specific MCDM methods like BWM, AHP, and ANP. It addresses inconsistency issues in pairwise comparisons, accounts for ordinary consistency, and evaluates the reliability of results by addressing the deficiency of consistency threshold values. By integrating FWZIC with EDAS, these limitations can be effectively addressed, resulting in more robust and reliable decision-making outcomes.

Briefly, the integration of EDAS with FWZIC offers a synergistic approach to MCDM by combining accurate ranking results, consideration of intangibility and uncertainties, distance-based evaluations, and overcoming limitations of other methods. This integration can lead to improved decision-making processes and more reliable outcomes in complex decision scenarios. It can be concluded that the proposed Decision Modelling Approach for Security Modules of Delegation Methods in Mobile Cloud Computing will introduce novel weighting techniques for security criteria and a novel evaluation and benchmarking framework for modeling alternatives. The specific problem statements are depicted in detail in Figure 1.

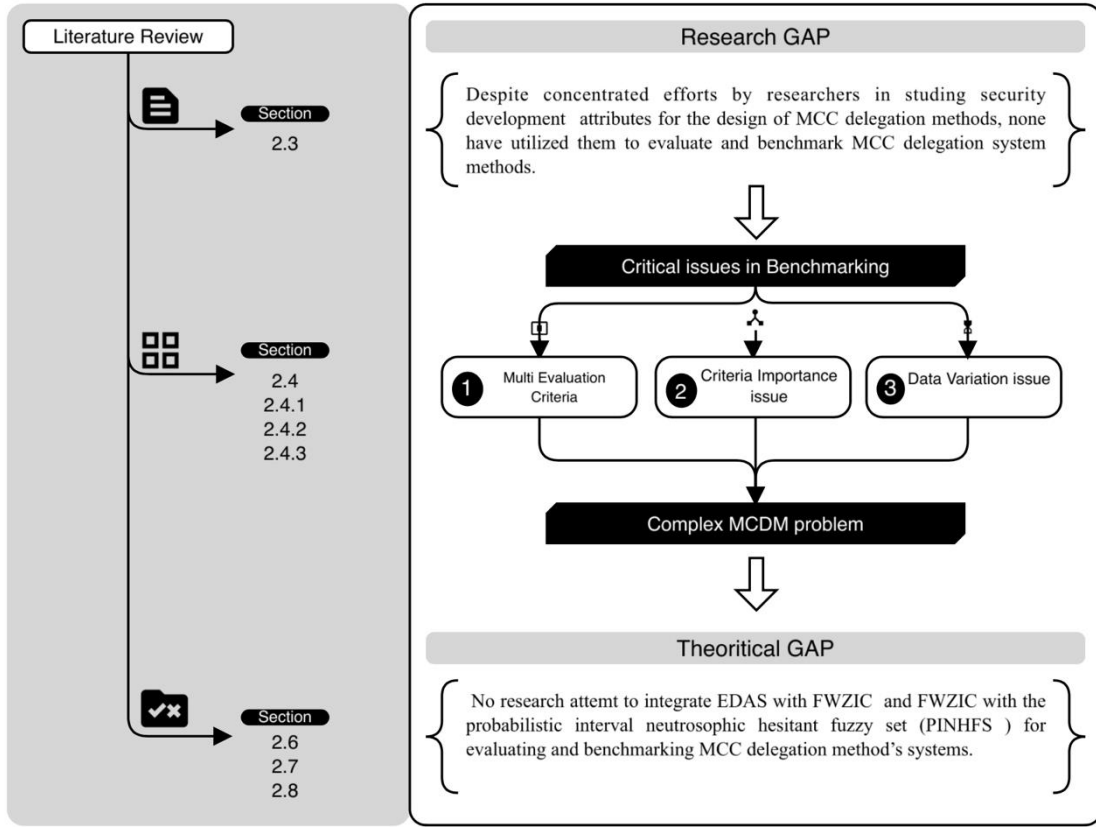


Figure 1: Problem Statement

1.3. Research Questions

The present investigation aims to resolve the research problem by providing answers to the following research problem:

- RQ_01: What evaluation techniques are available for evaluation security modules of delegation methods in MCC?
- RQ_02: What is the requirement for creating A Decision Modelling -based approach for Security Modules of delegation methods in Mobile Cloud Computing?
- RQ_03: What are the criteria that can be used to evaluate and rank security modules of delegation methods in MCC?

- RQ_04: Is there any integrated A Decision Modelling -based approach containing “security evaluation criteria” and “Security modules of delegation methods in MCC security models”?
- RQ_05: What are the suitable techniques that can be used to develop a A Decision Modelling -based approach for Security Modules of delegation methods of Mobile Cloud Computing to surmount the recognized difficulties and obstacles?
- RQ_06: How the results of the proposed modelling approach can be validated?
- RQ_07: How the proposed modelling approach can be evaluated?

1.4. Research Objectives

The aim of this study is to develop a Modelling decision-based approach for delegation method of Mobile Cloud Computing. Consequently, following the objectives to achieve this aim:

- To demonstrates the existing evaluation techniques for Security modules of delegation methods of MCC and drawing attention to the evaluation drawbacks.
- To articulate the decision matrices based on the intersection of Security Modules of delegation method for MCC with the security evaluation criteria.
- To formulate and develop an extension of FWZIC method under a Probabilistic Interval Neutrosophic Hesitant Fuzzy Set called (PINHFS).
- To develop a A Decision Modelling Approach for Security Modules of Delegation Methods in Mobile Cloud Computing using the formulated decision matrices and the integration of EDAS and new extension of FWZIC under PINHFS..
- To assess and verify the outcomes of the suggested modelling approach, by utilizing sensitivity analysis, systematic ranking, and benchmarking checklist (Evaluation and Validation process).

1.5. Connection among Research Objectives, Questions and Problem

The delineation of the research questions in this investigation serves to establish the structure and trajectory of the inquiry, whereas the research objectives function as solutions to these research inquiries. Every objective is affiliated with one or two inquiries. Moreover, the distinct and extensive issues are associated with several research objectives and inquiries. Figure 2 portrays the correlation between the research inquiries, research objectives, and the research problem.

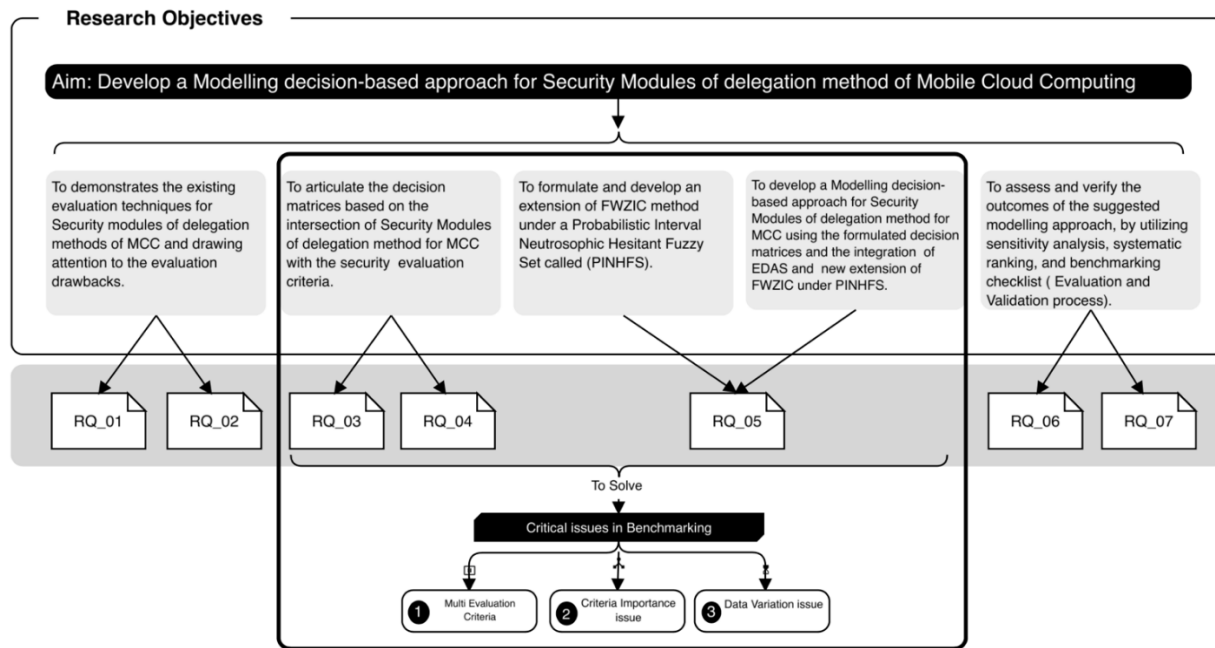


Figure 2: Connection among Research Objectives, Questions and Problem

It is clear that the answer to the first and second questions achieved the first goal. At the same time, the third objective is achieved by answering the third and fourth questions. As for the fifth question, the answer achieves the third and fourth objectives. The last two questions, the sixth and seventh, serve the last goal of verifying the results' validity and effectiveness. It is also noted that the fundamental research problem is solved by answering the third, fourth, and fifth questions.

1.6. Scope of the Study

As mentioned above that the main aim is to develop A Decision Modelling Approach for Security Modules of Delegation Methods in Mobile Cloud Computing, accordingly, below is the scope of this research:

- This research effort focus on the development of A Decision Modelling Approach for Security Modules of Delegation Methods in Mobile Cloud Computing on the basis of MCDM.
- This research emphasizes proposing decision matrices that are planned to evaluate the Security Modules of Delegation Methods in Mobile Cloud Computing.
- This study is not concerned with developing a secure security module of delegation method in MCC; instead, it is used as a POC for the proposed Decision Modelling Approach.
- This study does not imply that the evaluation of Security Modules depends only on security criteria, as there are several criteria for the effectiveness of use, the extent of sustainability, the speed of delegation, the delegation operational processes that take place, or the extent of use, but this is outside the scope of this research.

Figure 3 generally shows the research method, scope, and type. Whereas the desired final output of this research is the Modelling decision-making approach, which includes several steps that improve the process of evaluation delegation methods used in MCC Security Modules. The second output consists of a comprehensive guide to evaluating and benchmarking the Security Modules of Delegation Methods in Mobile Cloud Computing.

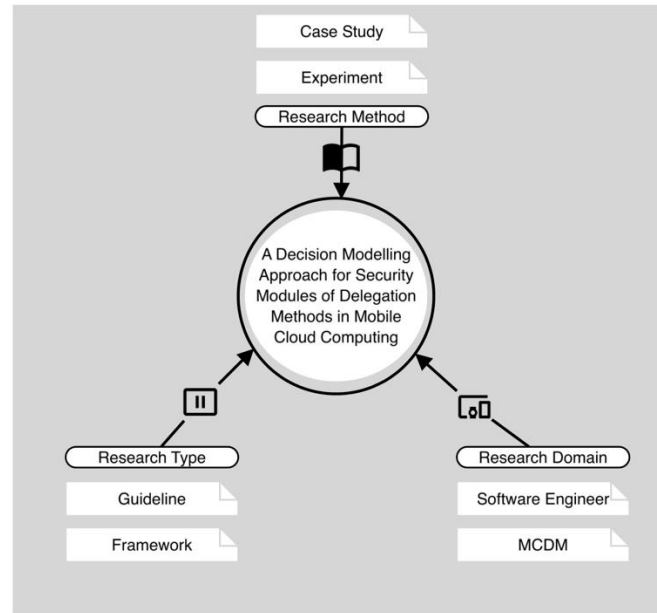


Figure 3: Scope of the Study

1.7. Significant of the Study

The eyes of significant technology companies, developers, and service providers are turning to the growing mobile cloud computing market in the current era to get a share of this market by providing secure and reliable solutions to manage data in MCC (AlAhmad et al. 2021) . Therefore, specialized research on the security of mobile cloud computing is considered a significant supporter of innovation and development in this field, as developers and service providers compete to design an architecture for mobile cloud computing that is free of security issues and ensures the security, confidentiality, and privacy of the user at the same time (Kumar Tiwari & Kumar 2022) . The importance of this research lies in its extensively evaluated delegation methods of mobile cloud computing Security Modules, as it can consider a starting point for all developers to choose the best and most secure Security module of delegation method in MCC (Lopez-Arboleda, Sarmiento & Cardenas 2019). In addition, it helps the researchers as a future recommendation to develop the

current evaluations of Security modules of delegation methods in MCC Modules. Figure 4 below illustrates the main area of research significant.

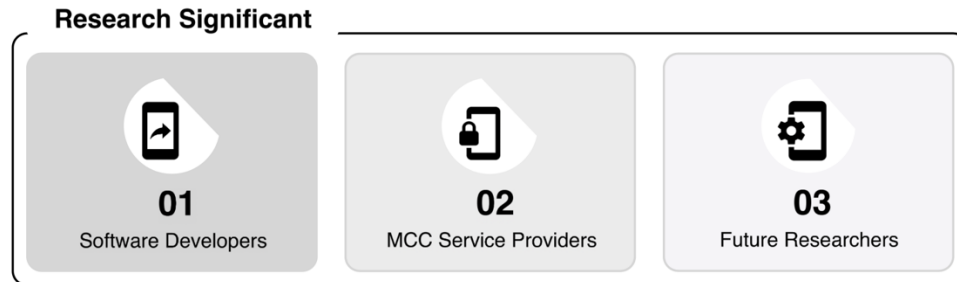


Figure 4: Significant of the Study

A Decision Modelling Approach for Security Modules of Delegation Methods in Mobile Cloud Computing can have a significant impact on both individuals and corporations. By providing a structured and systematic method for evaluating security risks in MCC, For individuals, mobile cloud computing offers the convenience of accessing applications, data, and services from any device and location. However, this convenience also comes with security risks, as sensitive information may be stored on remote servers and transmitted over public networks. To address these risks, a decision modelling approach can provide a framework for evaluating the security risks associated with different delegation methods, such as task delegation, data delegation, and authentication delegation. This approach can help individuals make informed decisions about which cloud services to use and how to delegate their tasks securely.

For corporations, mobile cloud computing can provide cost savings, scalability, and agility. However, it also introduces new security challenges, such as data privacy, compliance, and governance. A decision modelling approach can help corporations to design and implement secure delegation mechanisms that minimize these risks and ensure compliance with industry standards and regulations. This approach can also help to identify potential security breaches, detect them early, and respond to them effectively. In Addition this approach can help in designing and

implementing secure delegation mechanisms that minimize security risks and ensure compliance with industry standards and regulations.

Overall, a decision modelling approach for security modules of delegation methods in mobile cloud computing can benefit both individuals and corporations by enhancing the security and reliability of mobile cloud computing.

1.8. Main Terminology

Two basic terms in this study and the details are as follows:

- **Modeling** process, which included comparing several Security Modules of different delegation methods on Mobile Cloud Computing and verifying their validity through several verification processes.
- **MCDM** is the scientific method that helps individuals and groups make sound decisions in scientific ways, away from any other influences.

1.9. Structure of Thesis

This thesis comprises five chapters which provide a comprehensive overview of the research on Security Modules of Delegation methods in MCC. The first chapter of this research provides an overview of the study's context and importance, along with defining the research objectives and questions. It also establishes the connection between the research objectives, questions, and problem, and delineates the scope of the study. Chapter 2 presents a taxonomy of literature review on MCC, critical review, challenges of Security Modules, theoretical background, FWZIC method, EDAS method, and validation and evaluation procedures. Chapter 3 explains the investigation phase, proposed Decision Modelling Approach for Security Modules of Delegation Methods in Mobile Cloud Computing, decision matrix identification phase, formulation and development phase, and validation and evaluation phase. Chapter 4 discusses the identification of decision

matrix, security evaluation, criteria , Security Modules and delegation methods identification, decision matrix formulation, PINHFS-FWZIC method, and utilizing EDAS method. Chapter 5 provides the Modeling result, validation and evaluation result, discussion, recommendation, and future review of the study. The study contributes to the body of knowledge in the field of Security Modules of different delegation methods on Mobile Cloud Computing and provides insights for future research. Figure 5 presents the structure of the thesis in details.

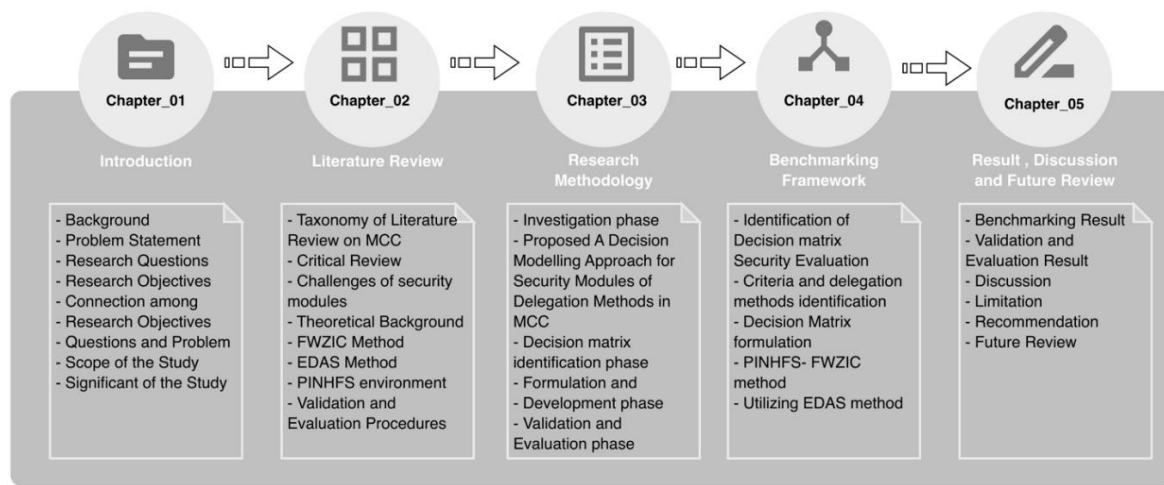


Figure 5: Structure of Thesis

1.10. Chapter Summary

Chapter 1 serves as an introductory chapter to the Decision Modelling Approach for Security Modules of Delegation Methods in Mobile. It comprises several sections, including a background on MCC delegation methods and MCDM methods, a problem statement that identifies the research gap and theory, research questions that investigate seven different aspects of the approach, such as MCDM methods for weighting and Modeling, and contribution, research objectives that articulate the primary aim of creating a Decision Modelling Approach for Security Modules of Delegation Methods in Mobile via the integration of EDAS and PINHFZ-FWZIC. Additionally, the chapter outlines the connection between the research objectives, questions, and problem, specifies the scope of the study, highlights the significance of the study, and provides definitions of the main terminology. Finally, the chapter concludes with a summary of its contents, which offer a comprehensive overview of the essential concepts and components of the decision-based approach for delegation method of Mobile Cloud Computing.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

The present chapter in the research elucidates on the specifics of the literature review's structure as shown in Figure 6. Section 2.1 briefly introduces this chapter. The taxonomy of Literature Reviews on Security Modules of delegation methods in Mobile Cloud Computing and related security development attributes was presented in Section 2.2. Section 2.3 presents, the Critical Review of the Security Modules of delegation methods in MCC. Section 2.4 addresses three fundamental issues that need resolution when Modeling Security Modules of delegation methods in MCC, to bridge the existing research gap. Additionally, Section 2.5 of this chapter delves into the theoretical basis of multi-criteria analysis in the context of security and cloud computing. In addition, Section 2.6 of this study presents an exposition on Multicriteria Decision Making Methods, followed by details about EDAS in section 2.7 , and then FWZIC method with Fuzzy set environment are presented in in Sections 2.8. Section 2.10 of this research provides an in-depth analysis of validation and evaluation techniques employed in decision science, specifically focusing on the Sensitivity Analysis Procedure, Systematic Ranking Procedure, and Comparative Study Based on Benchmarking Checklist Procedure, to gauge the efficiency and efficacy of the suggested Decision Modelling Approach.

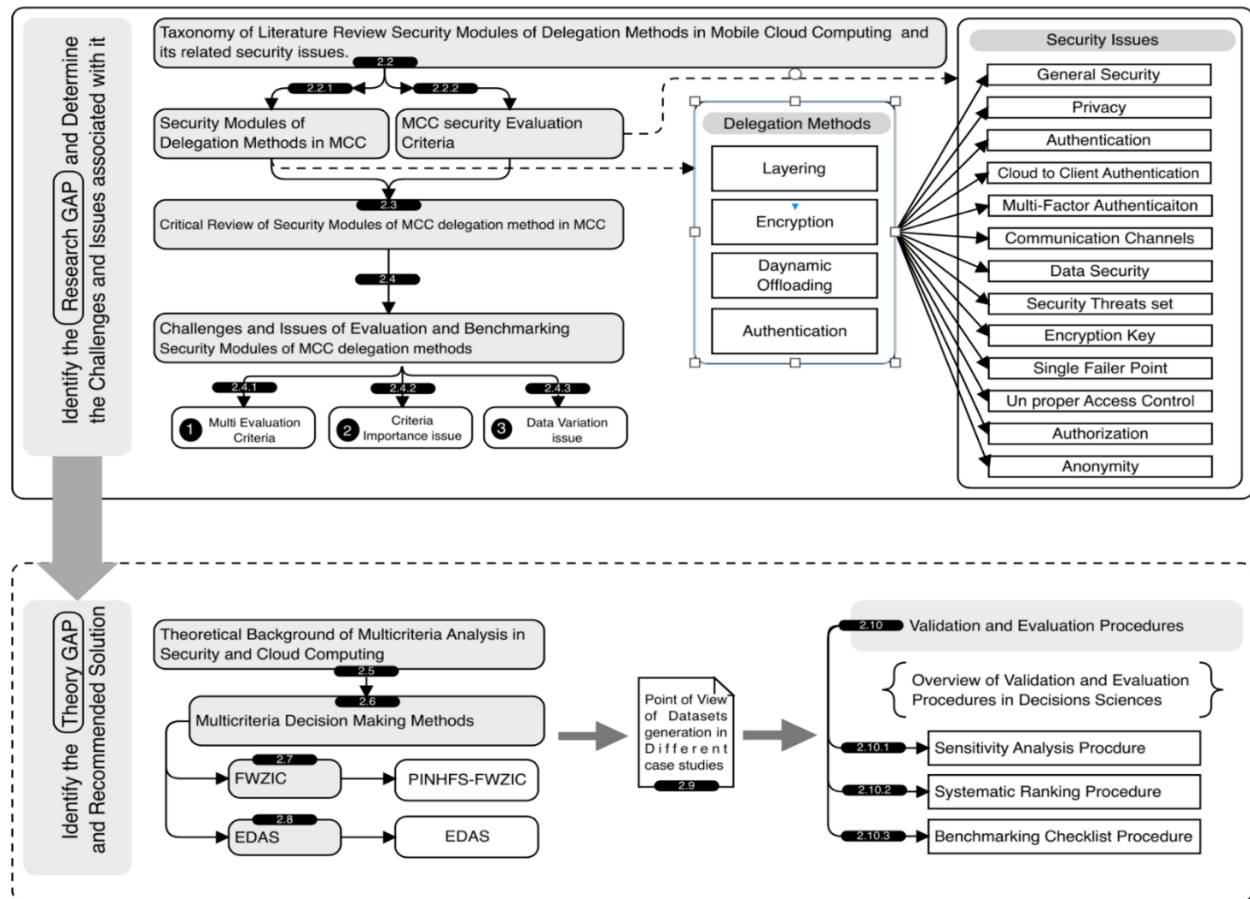


Figure 6: Literature Review Structure

2.2. Taxonomy of Literature Review on Security Modules of Delegation Methods in Mobile Cloud Computing and its related Development security attributes.

The literature review of this research includes a detailed explanation of Security Modules of Delegation Methods in Mobile Cloud Computing and related development security attributes. Sixty research papers as an outcome were used as the primary reference for the data in this research. Several databases were relied upon to search for the subject of Mobile Cloud computing security issues, especially in Security Modules of Delegation Methods in Mobile Cloud Computing . The search strategy started using keywords that included "Mobile cloud computing" OR "MCC," combined with AND operator with "Security issues" and “ Security Modules “ . From 2008 till 2022, The initial outcome was approximately (n= 13,000) research papers distributed among several databases (ACM Digital, Google Scholar, IEEE, IGI Global, Science Direct, and Scopus). After removing duplication, applying inclusion/ exclusion Criteria (Must be for an Security Modules of Delegation Methods in Mobile Cloud Computing security issues, Must be in English langue, Removing papers that are not published in journal or conference, Removing papers with outdated information and papers that are not addressed the subject exactly) and the last step is abstract screening to ensure that the paper is addressing the topic exactly (n = 60) papers were selected.

The scope of this study analyzed the selected papers based on two aspects which are (i) Security Modules of Delegation Methods in Mobile Cloud Computing (ii) Development security attributes. Figure 7 shows the Taxonomy of Literature Review on Security Modules of Delegation Methods in Mobile Cloud Computing and related development security attributes.

As a proof of concept, the study benchmarking process evaluated a total of 50 alternatives, with specific emphasis placed on four delegation methods, including the Encryption delegation method

(n=23), the Authentication delegation method (n=12), the Layering delegation method (n=9), and the Dynamic Offloading delegation method (n=6). Moreover, the present study examined the security development characteristics incorporated in the design of Security Modules of Delegation Methods in Mobile Cloud Computing, as reported in 50 articles. Thirteen distinct development security attributes were identified, including privacy, cloud-to-client authentication, client-to-cloud authentication, multi-factor authentication, data security, encryption key management, mitigation of single failure points, security threat management, communication channel security, access control, authorization management, and anonymity.

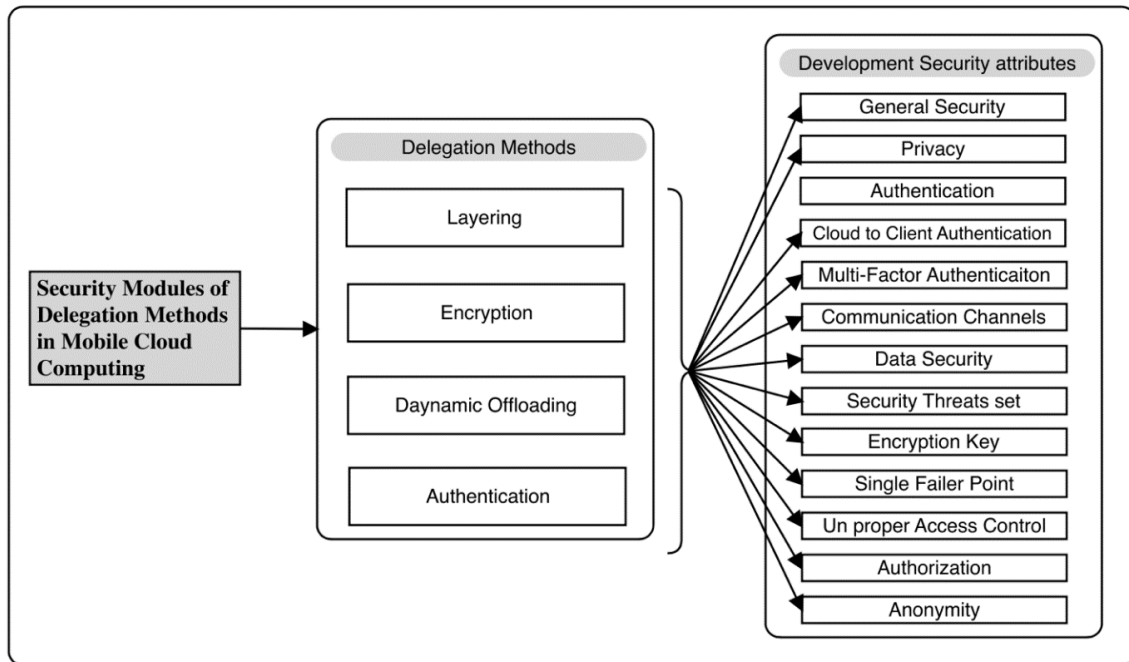


Figure 7: Taxonomy of LR on MCC Security Modules delegation methods and its related security issues

2.2.1. Delegation Methods in Mobile Cloud Computing

Despite these advantages and the massive use of cloud-based applications and services, data security, resources, and communications have become a critical issue in current MCC Models. The essential security-related aspects are confidentiality, authentication, and integrity. Many academic

researchers such as (AlAhmad et al. 2021) have surveyed and reviewed the security issues in Security Modules of Delegation Methods in MCC, which mainly result from the delegation method between mobile devices and cloud computing. The concept of delegation refers to delegating operations from the mobile to the cloud to do the task at the best performance due to the limited resources and capabilities of the mobile. Here, privileges are granted to the cloud temporarily to use mobile resources to complete the required operations (Ahmad et al. 2020) . There are many **delegation methods**, including Layering, Authentication, Mirroring, Encryption, User third party, Dynamic offloading Virtualization and AI Prediction models . The most common from these delegation method and analyzing in this research are **Layering** which is adding layers with security components that act as a barrier between the connection and the cloud to avoid and address security issues (Huang et al. 2010). **Authentication** is the most used delegation method which means verifying the user's identity and the device to allow tasks to be performed between the mobile and the cloud. The authentication can be done reciprocally from the transmitter to the cloud and vice versa (Chow et al. 2010). **Encryption** encrypts data so that only authorized users who can decipher the agreed-upon code can read it. (Zhou & Huang 2012) delegated the encryption between the clients and clouds, where the complex one was commissioned to the cloud and the simple encryption for the client. **Dynamic offloading** is the dynamic delegation of tasks or processes partially or entirely to the cloud to save energy and effort on the mobile device (Mavromoustakis et al. 2015).

2.2.2. Development Security attributes

According to (AlAhmad et al. 2021) and as per our analysis and the proposed categorization framework (as presented in Section 2.2 and Figure 2.2), the scholarly literature has identified thirteen distinct development security attributes across all Security Modules of Delegation Methods

in Mobile Cloud Computing , namely , privacy, Authentication (cloud to client authentication, Client to cloud authentication, and Multi-factor Authentication), Data Security, Encryption key, single failure point, security threats, communication channels issues, Un proper access control, authorization issues and anonymity.

2.3. Critical Review of Security Modules of Delegation Methods in MCC

The researchers focused their efforts on developing several Security Modules to avoid the security issues caused by the delegation methods in MCC. The tables below provide information on how each security module intersects with delegation methods and which development security attributes are taken into account or excluded during the security module's design. As mentioned previously, nearly 50 security modules, as an outcome to determine the scope of the research, presented in four delegation methods and 13 development security attributes.

A total of nine security modules are present in the layering delegation method as shown in Table 1 where YES/NO approach indicate whether the development security attribute are included or not in a given security module. Two of security modules (SM_06 and SM_07) of which (92%) addressed all development security attributes and took them into account during the designing phase, except for one common development security attribute that was not discussed at all modules in scope which is Cloud to a Client Authentication. Three security modules (SM_01, SM_08, and SM_09) of which (85%) addressed all development security attributes except two, while only one security module (SM_03) ignored three development security attributes (77%). As for the rest of the modules, Two security modules (SM_02 and SM_04) of which (69%) addressed nine development security attributes out of 13, and only one security module (SM_05) of which (31%) dealt with only four development security attributes, ignoring the remaining nine. Furthermore, all security modules employed in the layering delegation method in MCC included General security, Improper access control,

and Anonymity development security attributes, with a presence rate of 100%. In contrast, the Cloud to Client Authentication issue is absent in all security modules (0%). Authentication, Encryption key, Single failure point, and Authorization had existence rates of 89%, while communication channels and Data security issues were present in 56% of the modules. Privacy and Multi-factor authentication development security attributes had a presence rate of 78%, while the Security threats set development security attribute was present in 67% of the security modules.

Table 1: Security Modules in Layering Delegation Method

Delegation Method	Security Modules	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity	Issues Covered
Layering	SM_01: (Ogwara et al. 2021)	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	85%
	SM_02: (Lawal et al. 2021)	YES	YES	YES	NO	YES	YES	NO	NO	YES	YES	YES	NO	YES	69%
	SM_03: (Huang et al. 2010)	YES	YES	YES	NO	NO	YES	NO	YES	YES	YES	YES	YES	YES	77%
	SM_04: (Chen & Wang 2011)	YES	NO	YES	NO	YES	NO	YES	NO	YES	YES	YES	YES	YES	69%
	SM_05: Sumter (2021)	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	YES	YES	31%
	SM_06: (Qiu, Liu & Zhao 2011)	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	92%
	SM_07: (Abdellaoui, Laksantini & Chaoui 2016)	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	92%
	SM_08: Yadav (2018)	YES	YES	YES	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	85%
	SM_09: (A & Arockiam 2018)	YES	YES	YES	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	85%
Total		100%	78%	89%	0%	78%	56%	56%	67%	89%	89%	100%	89%	100%	

For the Encryption delegation method, a total of 23 security modules classified under the Encryption delegation method. One security module (SM_23) addressed all development security attributes except for the Authentication development security attribute, representing a percentage of 92%. Thirteen security modules (SM_10 to SM_22) considered all development security

attributes, ignoring only two development security attributes. This group of security modules represented a percentage of 85%. Six security modules (SM_04, SM_05, SM_06, SM_07, SM_08, SM_09) addressed ten development security attributes and ignored three development security attributes, representing a percentage of 77%. Only one security module (SM_03) addressed nine development security attributes, which accounted for 69% of the development security attributes and missed the other four. Similarly, only one security module (SM_02) ignored five development security attributes and considered the other eight development security attributes, representing a percentage of 62%. The last security module under the Encryption delegation method, SM_01, addressed only four development security attributes, ignoring the remaining nine attributes, accounting for a percentage of 31%. Conversely, the Anonymity development security attribute was present in all security modules in Encryption delegation methods, representing a percentage of 100%. In contrast, the Cloud to Client Authentication development security attribute was ignored in all security modules except for one. General security and Single Failure point were considered in all security modules, except for two security modules, with a current rate of 96%. However, three development security attributes, Multi-factor Authentication, Improper Access Control, and Authorization, were ignored in two security modules, representing a percentage of 91%. Further, 87% of the security modules considered the Privacy development security attribute, while Authentication and communication channel had a presence rate of 83% in the security modules. Furthermore, six security modules, representing a percentage of 74%, did not include an Encryption Key development security attribute. Lastly, Data Security and Security Threats set were addressed only in 15 security modules, accounting for a percentage of 65%.

Table 2: Security Modules in Encryption Delegation Method

Delegation Method	Security Modules	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity	Issues Covered
Encryption	SM_01: Madhurya et al. (2021)	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	YES	YES	77%
	SM_02: (Bhatia, Verma & Sharma 2019)	YES	YES	NO	NO	YES	YES	NO	YES	NO	YES	YES	NO	YES	77%
	SM_03: (Seada Abdu Wakene et al. 2021)	YES	NO	YES	NO	YES	YES	NO	NO	YES	YES	YES	YES	YES	62%
	SM_04: (Sukumaran & Misbahuddin 2021)	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	NO	YES	YES	77%
	SM_05: (Swetha & Latha 2021)	YES	YES	YES	NO	YES	YES	NO	YES	NO	YES	YES	YES	YES	77%
	SM_06: (Abidin et al. 2022)	YES	YES	YES	NO	YES	YES	NO	YES	NO	YES	YES	YES	YES	85%
	SM_07: (Khedr et al. 2020)	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	NO	YES	YES	92%
	SM_08: (Qayyum & Ejaz 2020)	YES	YES	NO	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	69%
	SM_09: (Shabbir et al. 2021)	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	77%
	SM_10: (Khan, Kiah, et al. 2014)	YES	YES	YES	NO	YES	YES	YES	YES	NO	YES	YES	YES	YES	31%
	SM_11: (Khan, Othman, et al. 2015)	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	92%
	SM_12: (Khan, Mat Kiah, et al. 2015)	YES	YES	YES	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	85%
	SM_13: (Zhou & Huang 2012)	YES	YES	YES	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	85%
	SM_14: (Jia et al. 2011)	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	85%
	SM_15: (Baharon, Shi & Llewellyn-Jones 2015)	YES	YES	YES	NO	YES	YES	YES	YES	NO	YES	YES	YES	YES	85%
	SM_16: (Banerjee et al. 2017)	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO	YES	85%
	SM_17: (Sulami & Muhammad Mostafa Monowar 2015)	YES	YES	YES	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	85%
	SM_18: (Lin et al. 2017)	YES	YES	YES	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	85%
	SM_19: (Bhatia, Verma & Sharma 2019)	YES	YES	YES	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	77%
	SM_20: (Tsai & Lo 2015)	YES	YES	YES	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	85%
	SM_21: (Irshad et al. 2019)	YES	YES	YES	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	85%
	SM_22: Audithan (2017)	YES	YES	YES	NO	NO	YES	YES	YES	YES	YES	YES	YES	YES	85%
	SM_23: (Roy et al. 2017)	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	85%
Total		96%	87%	83%	4%	91%	83%	65%	65%	74%	96%	91%	91%	100%	

According to Dynamic Offloading Delegation method that appears in Table 3 where Six security modules are classified under it. Two security modules (SM_02 and SM_03) addressed all development security attributes except for the Security Threats set, representing a percentage of 92%. One security module (SM_01) ignored three development security attributes, accounting for a percentage of 77%, while the remaining security modules (SM_04 to SM_06) missed only two development security attributes: Cloud to Client Authentication and Data Security. Moreover, all six security modules considered eight development security attributes fully when designing the security modules under the Dynamic Offloading Delegation method, representing a percentage of 100%. Single Failure point and Privacy had a presence rate of 83% in all six security modules. For the remaining attributes, Security Threats set had a presence rate of 67%, while Data Security had a presence rate of 50%. The Cloud to Client Authentication development security attribute had the lowest presence rate of 33%.

Table 3: Security Modules in Dynamic Offloading Delegation Method

Delegation Method	Security Modules	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity	Issues Covered
Dynamic offloading	SM_01: (A. Almusaylim & Jhanjhi 2020)	YES	NO	YES	NO	YES	YES	YES	YES	NO	YES	YES	YES	YES	77%
	SM_02: (Saber & Azmi 2020)	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES	YES	92%
	SM_03: (Derhab et al. 2020)	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES	YES	92%
	SM_04: (Mavromoustakis et al. 2015)	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	85%
	SM_05: (Gai et al. 2016)	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	85%
	SM_06: Kaur and Sohal (2017)	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	85%
Total		100%	83%	100%	33%	100%	100%	50%	67%	83%	100%	100%	100%	100%	

Twelve security modules under the Authentication delegation method are analyzed as shown in Table 4. Eight security modules (SM_05 to SM_12) addressed nine out of thirteen development security attributes, representing a percentage of 85%, while four security modules (SM_01 to SM_04) addressed eight out of thirteen development security attributes, accounting for a percentage of 67%. Cloud to Client Authentication was missing in all security modules, while General Security, Multi-factor Authentication, Encryption Key, Improper Access Control, and Anonymity existed in all security modules, with a presence rate of 100%. Privacy, Communication channel, and Single Failure point had a presence rate of 92% in all security modules of the Authentication delegation method. Authorization had a presence rate of 83%, while Security Threats set and Data Security had a presence rate of 75% and 67%, respectively.

Table 4: Security Modules of Authentication Delegation Method

Delegation Method	MCC Modules	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity	Issues Covered
Authentication	SM_01: Sridhar & Smys (2020)	YES	YES	NO	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	77 %
	SM_02: Irshad et al. (2020)	YES	YES	YES	NO	YES	YES	NO	NO	YES	YES	YES	YES	YES	85 %
	SM_03: (Yadav & Namdeo 2020)	YES	NO	YES	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	85 %
	SM_04: (Ikram et al. 2021)	YES	YES	YES	NO	YES	NO	NO	YES	YES	YES	YES	YES	YES	77 %
	SM_05: (Wilczynski, Kolodziej & Grzonka 2021)	YES	YES	NO	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	85 %
	SM_06: (Salami et al. 2021)	YES	YES	NO	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	85 %
	SM_07: (Chow et al. 2010)	YES	YES	YES	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	85 %

Delegation Method	MCC Modules	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity	Issues Covered
	SM_08: (Khan et al. 2013)	YES	YES	NO	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	77 %
	SM_09: (Khan, Othman, et al. 2014)	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO	YES	85 %
	SM_10: (Wu et al. 2017)	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES	92 %
	2 SM_11: (Alhassan & Bayor 2021)	YES	YES	YES	NO	YES	YES	YES	YES	YES		YES	YES	YES	85 %
	4 SM_12: (Elwakil, Ibrahim & Hefny 2015)	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO	YES	77 %
Total		100 %	92 %	67 %	0%	100 %	92 %	67 %	75 %	100 %	92 %	100 %	83 %	100 %	

Overall, from the 50 security modules analyzed above, the Anonymity development security attribute was present in all Security modules of delegation methods (100%). In contrast, Cloud to Client Authentication was considered the lowest development security attribute presented in the security modules, with (6%). Despite this, the remaining development security attributes (General Security issues, Privacy, Authentication, Multi-factor authentication, Communication channel issues, Data Security, Security Threats set, Encryption Key, un proper Access Control, and Authorization issues) had existence rates of 98%,86%,82%,92%,82%,62%,68%,84%,94%,96%, and 90%, respectively.

Despite commendable efforts to create a MCC Security Modules that is both secure and private, none of the security modules were found to satisfy the thirteen required development security attributes. Instead, a significant variance was observed in the development of numerous security modules, thereby presenting a considerable challenge to Security Modules of delegation methods

in MCC providers in determining the most secure, suitable, advanced, and effective system. Additionally, while researchers have focused on these development security attributes to propose solutions, they have not employed them to evaluate and benchmark Security Modules of Delegation Methods in MCC, which represents a **research gap** and challenge.

2.4. Challenges of Security Modules

As previously discussed in this chapter, numerous scholars have endeavored to create Security modules of delegation methods in MCC by integrating with 13 development attributes. However, none of them have employed these development security attributes as evaluation criteria to assess and benchmark Security modules of delegation methods in MCC. Furthermore, evaluating and benchmarking Security modules of delegation methods in MCC to determine the most desirable module is not without its challenges, particularly given the diverse combinations of evaluation criteria present in Security modules of delegation methods in MCC. As such, it is unreasonable to compare existing security modules from a single perspective.

To address the research gap identified, three key issues must be considered in the benchmarking process which are multiple evaluation criteria , criteria importance, and data variation as shown in Figur 8 (Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023) (Alsalem et al. 2021a; Alamoodi, Mohammed, et al. 2022a; Albahri, Albahri, et al. 2022b; Albahri, Zaidan, et al. 2022b; Ibrahim et al. 2023).

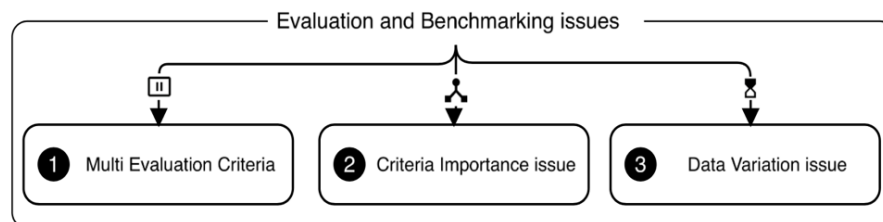


Figure 8: Evaluation and Benchmarking issues of MCC Security Modules delegations methods

2.4.1. Multi Evaluation Criteria issue

Multi-criteria have been considered to compare each Security Module of Delegation Method in MCC, which are privacy, Authentication (cloud to client authentication, Client to cloud authentication, and Multi-factor Authentication), Data Security, Encryption key, single failure point, security threats, communication channels issues, Un proper access control, authorization issues and anonymity (AlAhmad et al. 2021) . Each criterion has its specificity and differs according to the type of delegation method from the mobile to the cloud. That is, there is a massive variance in the criteria, and thus this is an indication of the complex issue in multi-criteria decision-making when benchmarking need to be establish as integrated platform (Shao et al. 2018; Alsalem et al. 2021a; Alamoodi, Mohammed, et al. 2022a; Albahri, Albahri, et al. 2022a; Albahri, Zaidan, et al. 2022a; Qahtan, Alsattar, et al. 2022).

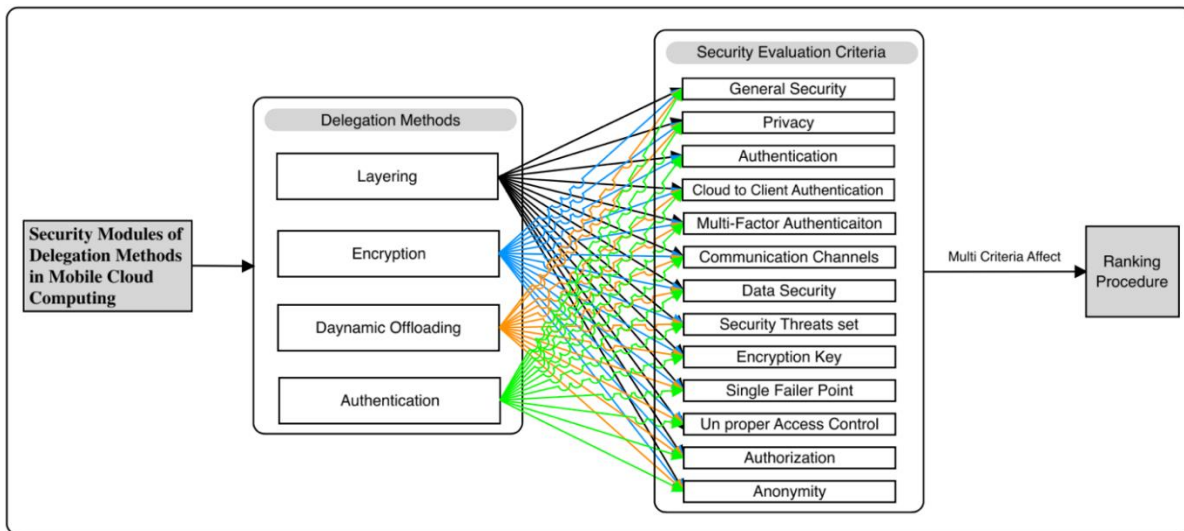


Figure 9: Multi Evaluation Criteria issue

Figure 9 demonstrates the impact of respective criteria on the benchmarking of Security Modules of Delegation Method in MCC. In the present scenario, determining the most secure security module is a challenging task. As per Table 1 in Section 2.3 where may be SM_01 under the Layering delegation method can ranks highest on the user authentication criterion, whereas may be SM_07 ranks highest on the data security criterion. Consequently, it raises the question of which system to prioritize. Hence, ranking the

Security Modules of Delegation Method in MCC based on a single criterion is considered unfair, and it is recommended to consider multiple evaluation criteria instead.

2.4.2. Criteria importance issue

Numerous security evaluation criteria have been utilized in the scholarly works to facilitate the development of Security Modules of Delegation Method in MCC . The significance of these security evaluation criteria differs based on their respective objectives. Nonetheless, it is crucial to adequately consider the comparative importance of these criteria, which has been identified as a challenge in evaluating and benchmarking Security Modules of Delegation Methods in MCC. In Multi-Criteria Decision Making (MCDM), determining the relative importance of the criteria is a critical issue. The ultimate decision is influenced by the relative importance of the criteria, and if the criteria are not weighted properly, the decision may not be optimal. In addition, Criteria are not of the same importance and weight, and each criterion has functional specifications that distinguish it from others, so none of the criteria can be preferred over the other (Alsalem et al. 2021a; Albahri, Albahri, et al. 2022b; Albahri, Zaidan, et al. 2022b; Ibrahim et al. 2023) .

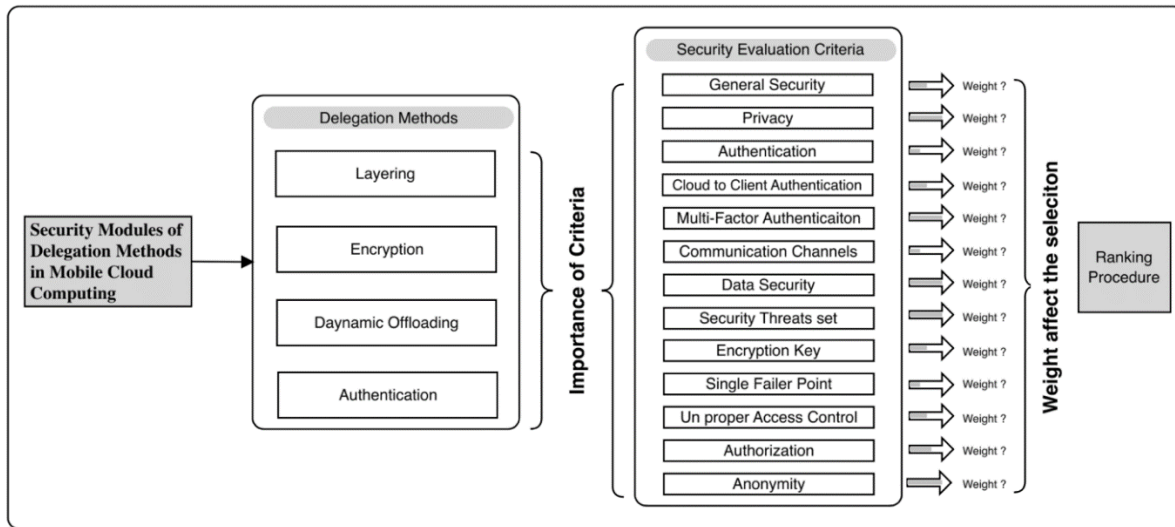


Figure 10: Criteria importance issue

In the present study, all Security Modules of Delegation Methods in MCC possess identical developed security attributes, and it is indeterminable whether Privacy or Authentication is the superior criterion, and

a comparison can be performed based on them. It is imperative to devise an apt resolution to address the problem of prioritizing specific security criteria over others (Alamoodi, Mohammed, et al. 2022a). Figure 10 provides a framework for evaluating each set of criteria to determine their relative importance in comparison to the others, thereby aiding in resolving the issue of criteria prioritization. Consequently, in the context of evaluating Security Modules of Delegation Methods in MCC, each criterion's relative significance should be assigned a weight to determine its importance (Albahri, Albahri, et al. 2022b).

2.4.3. Data Variation issue

The availability of these criteria varies from one system to another for example Layering delegation method that studied by (Ogwara et al. 2021) , (Ogwara et al. 2021) and (Huang et al. 2010) ignore Cloud to Client Authentication and Data security issues while take in to consideration Communication channel , encryption key and Single Failure point security properties when building the model. In encryption delegation methods, we can't choose between Security Modules proposed from (Sukumaran & Misbahuddin 2021) and (Sukumaran & Misbahuddin 2021) despite both of their Security Modules tackling ten development security attributes and ignoring three issues. As one criterion may affect the other criteria, data variance is considered as issues and must be taken into consideration.

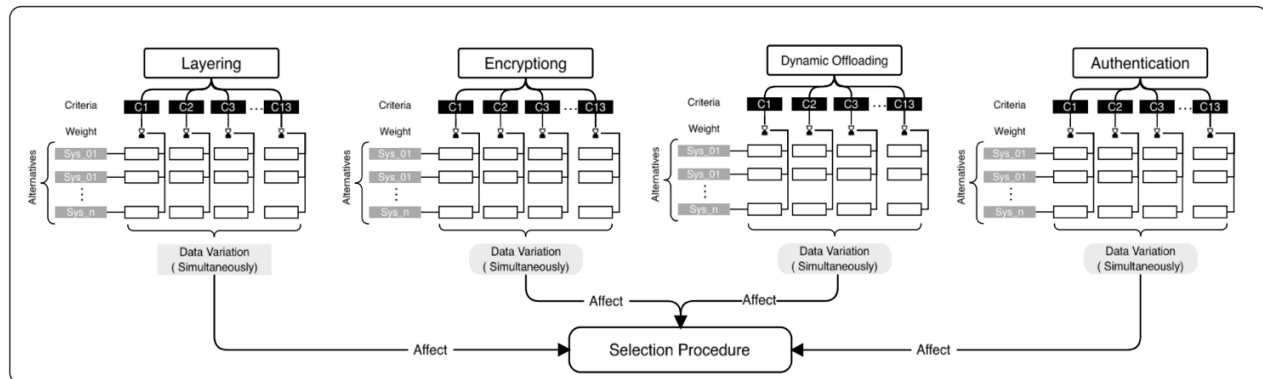


Figure 11: Data Variation issue

As the variability of data increases, the complexity of benchmarking tasks for Security Modules of Delegation Methods in Mobile Cloud Computing also increases. Comparing alternatives among decision-makers becomes challenging due to varying data across different criteria. Thus, resolving this issue is imperative as it streamlines the benchmarking procedure while handling substantial amounts of data (Albahri, Albahri, et al. 2022b; Albahri, Zaidan, et al. 2022a; Ibrahim et al. 2023). Figure 11 illustrates that data variability may arise if the maximization measures of criteria influence the data of the alternatives , ensuring an enhanced benchmarking process.

The findings from Section 2.4.1, Section 2.4.2, and Section 2.4.3 indicate that the selection of a suitable Security Model of Delegation Method in MCC is a challenging task. Despite this, the matter of assessing and comparing these systems based on several security evaluation criteria concurrently remains unsettled. As such, further research is necessary to address these outstanding concerns and advance the current understanding of security in the Security Modules of Delegation Methods in Mobile Cloud Computing.

2.5. Theoretical Background of Multicriteria Analysis in Security and Cloud Computing

Numerous research articles have been published on various case studies in the fields of security and cloud computing, exploring the topic of decision-making and evaluating the efficacy of various options. (Özkan, Erdem & Özceylan 2022) assessed and compared the risk profiles of countries in the Asia Pacific Accreditation and Cooperation (APAC) that influence the effectiveness of data centers. Specifically, they developed a systematic evaluation methodology by leveraging Mulity Criteria Decision Making (MCDM) methods. Data obtained from the Data Centre Security Index (DCSI) was used to rank countries. According to the results, the top three countries were Singapore, Hong Kong, and New Zealand, and the most important risk factors were the availability of secure internet servers and access to electrical energy.

In other research by (Chen & Lin 2022) , The authors set out to develop fuzzy sub-judgment asymmetric matrices and decompose a fuzzy judgment matrix. Specifically, they proposed a fuzzy geometric mean decomposition-based fuzzy technique for choosing appropriate technologies for supporting mobile health care services. The inclusion of the fuzzy geometric mean was aimed at decomposing a matrix into fuzzy sub-judgment matrices, which might exhibit asymmetry. The proposed method was applied to the problem of choosing health applications from a group of technologies. Based on the experimental results, the method was able to rank and recommend the optimal technology based on the patient need and viewpoints. In addition to eliminating the need for decision-makers in establishing the weights of fuzzy sub-judgment matrices, the proposed method is flexible. It also produces decomposed matrices that align with the linguistic variables established at the start of the exercise.

The selection of cloud service providers is an MCDM problem as it entails choosing the best provider based on several metrics. Accordingly, (Kumar Tiwari & Kumar 2022) developed integrated MCDM methods to rank cloud providers. The final result performed showed that the proposed framework is stable even when cloud service providers are added or removed from the system. It is also robust to rank reversal phenomenon. Overall, the framework is recommended for cloud service selection owing to its efficiency and robustness. In addition , (Kumar, Kumari & Kumar 2021) developed a novel framework for comparing cloud services based on quality-of-service criteria. Other research by (Torbacki 2021) presented an integrated MCDM model for assessing cybersecurity Based on the findings, this method identified the most important security assessment criteria, the most essential dimensions of cybersecurity, and the most significant group of security measures.

(Turskis et al. 2019) developed a hybrid approach for assessing information security risk of critical infrastructure by integrating MCDM methods for ranking and weighting . Based on the experimental findings, the proposed approach is superior to conventional methods as it can make group decisions in two environments. In addition to identifying the main criteria of information security, it ranked the various risks. Overall, the model was recommended as a suitable technique for establishing the probability and impact of risks. Moreover , The objective of study created by (Paul et al. 2018) was to enhance the reliability, security, and quality of service of Delay Tolerant Networks through the creation of a framework that also exploited the features and functionality of mobile devices in a hostile networking setting. It introduced a novel unified next-hop carrier selection framework for Delay Tolerant Networks based on trust and an MCDM technique. Based on the simulations and evaluations done, the framework was found to be effective, efficient, and usable.

The aforementioned studies provide evidence that MCDM has been extensively applied to address security-related concerns, specifically in resolving intricate multicriteria decision-making problems. This underscores the significance and impactful function of MCDM in facilitating the selection of optimal alternatives.

2.6. Multicriteria Decision Making Methods

The development of MCDM methods not only solves real-life problems but also develops a basis for decision-making using technologies (Khaira & Dwivedi 2018) . There are three stages in MCDM: defining criteria and alternatives, transforming the importance of criteria to alternatives to numerical measures. The last stage is processing these numerical measures to determine the priority and ranking of alternatives (Panos M. Pardalos 2000) . (Ghorabae et al. 2016) observe that the theory of multi-criteria decision making is effective in solving problems with distinct

peculiarities. MCDM is divided into two approaches as shown in Figure 12: a mathematical approach and a human approach where mathematical approach provide ranking for the alternatives and human approach provides criteria weighting (Salih, Zaidan & Zaidan 2020).

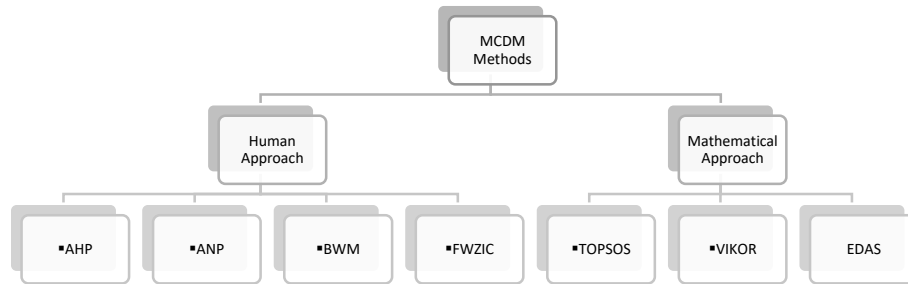


Figure 12: MCDM approaches

As for mathematical methods, Table 5 presents the most common mathematical based approach methods used and brief about them.

Table 5: Mathematical approach most common used methods

Method	Brief
Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) (Nădăban, Dzitac & Dzitac 2016)	TOPSIS is a popular technique for selecting the optimal alternative, which relies on the premise that the preferred alternative should be positioned in close proximity to the ideal positive point and the farthest distance away from the negative point. Despite its widespread use, TOPSIS faces several common issues, which are as follows: - Normalization produce different metrics that change the behavior of the data and the final decision

	- TOPSIS has limited sensitivity to small values, which results in a comparatively diminutive distance between the positive and negative solutions when using the Euclidean distance metric as its primary mechanism.
VIKOR (Mardani et al. 2016)	A method developed for multi-criteria optimization of complex systems in which median and weight stability intervals are determined to reach the closest solution. This method relies on arranging and choosing between various alternatives in the presence of conflicting criteria. For the issue of VIKOR , it requires an external weighting method to provide weighting for criteria
Evaluation based on Distance from Average Solution (EDAS) (Ghorabae et al. 2015)	EDAS used for calculating every alternative's distance from the average value to help decision makers to find the best solution. EDAS emerged as the only method that that appraised the intangibility of average solutions with regard to decision makers and considering the uncertainties in the decision-making environment to obtain aggregated results.

Based on the table presented above, it is evident that none of the methods that were discussed have been utilized to rank the Security Modules of Delegation Methods in MCC. Furthermore, it is apparent that the employment of the mathematical approach is impeded by certain obstacles. **First**, normalization, and **Second** issues related to the distance between the ideal solution and the alternatives, as it is not sensitive to some small values. Therefore, this affects the Euclidean distance on which it works mainly, leading to a relatively small distance between the positive and negative

solutions. The **third** challenge is related to the Criteria weighting since the mathematical approach must reflect the preferences of the criteria-based decision before proceeding with the rest of the steps such as VIKOR method requires an external weighting method to provide weighting for criteria (Salih, Zaidan & Zaidan 2020) . **The fourth** challenge also mentioned by Salih is the vagueness in the data, as experts have linguistic terms that cannot be weighed with real numbers and cannot be resolved, thus affecting the final result of the alternatives.

Evaluation based on Distance from Average Solution (EDAS) is one of the mathematical approaches used in multi-criteria decision making. EDAS is one of the effective methods of MCDM , as it is the only method that that appraised the intangibility of average solutions with regard to decision makers and considering the uncertainties in the decision-making environment to obtain aggregated results (Zhang et al. 2019). Despite the prevalence of EDAS, The EDAS method exhibits a deficiency in its inability to assign relative weights to attributes for the purpose of determining their respective levels of significance. As a result, numerous studies have been conducted to incorporate human-based MCDM approaches for weight determination.

For the MCDM human approach methods, Table 6 represent the most popular MCDM methods for human based approach including definition, strength and issues. (Asadabadi, Chang & Saberi 2019) (Khaira & Dwivedi 2018) (Salih, Zaidan & Zaidan 2020) (Moslem et al. 2020) (Youssef 2020).

Table 6 : Human Approach most common used methods

Method	Brief
Analytic hierarchy process (AHP) (Asadabadi, Chang & Saberi 2019)	It is a simple, flexible, practical, and multi-parameter decision-making method that uses pairwise comparison to rank alternatives. it is proposed by the American operational researcher Professor Thomas L. Saaty in the early 1970s. As a strength points it is Popular and Adaptive and doesn't include complex mathematics. On the other hand it raised the Inconsistency issue which is resulting from the following: Expressing the pairwise comparison matrix on a number scale entered by the DM's based on their experience incredibly leads to complexity when determining weights. Increasing the number of criteria lead to increase the number of comparisons, and then pairwise comparisons raise inconsistency Not all problems related to decision-making can be structured hierarchically when it requires the interaction of all components to make an appropriate decision.
Analytic Network Process (ANP) (Asadabadi, Chang & Saberi 2019)	It is a method very similar to AHP but with additional steps where interrelationships between the same group elements are considered here regardless of hierarchy. Criteria and sub criteria are treated equally as nodes in the network. The most common issues in it is : Different results resulting from different structures between attributes are complex for experts.

Method	Brief
	The number of pairwise comparisons matrix in ANP is higher than in AHP, which generates inconsistency that can be more easily identifiable than in AHP.
Best–worst method (BWM) (Pamučar et al. 2020)	The BMW method developed by Rezaei is based on deriving weights with fewer consistent comparisons. This method can be combined with other multi-criteria decision-making methods as it does not derive weights independently. It Overcome the inconsistency issue in pairwise comparisons. The mose common issues of it is as following: The difficulty of determining the best and worst criteria from other criteria and the level of importance for each of them. The process of determining the best and worst criterion to other criteria requires several times and comparing unrelated criteria, which is not an easy process to achieve, nor is it a natural process.
Fuzzy-Weighted Zero-Inconsistency (FWZIC) (Albahri, Albahri, et al. 2022b)	(FWZIC) used to solve this issue and weight attributes without any inconsistencies regardless the number of criteria is. The importance of each criterion level can be computed using FWZIC in MCDM based on expert preferences .

As per (Asadabadi, Chang & Saberi 2019) (Khaira & Dwivedi 2018) (Salih, Zaidan & Zaidan 2020) (Moslem et al. 2020) (Youssef 2020) The challenges in the human approach lie in the Inconsistency in pairwise comparisons. For example in Analytic hierarchy process (AHP) inconsistency issue resulting from expressing the pairwise comparison matrix on a number scale entered by the DM's based on their experience incredibly leads to complexity when determining weights. In addition, increasing the number of criteria lead to increase the number of comparisons, and then pairwise comparisons raise inconsistency. In Analytic Network Process (ANP) the number of pairwise comparisons matrix is higher than in AHP, which generates inconsistency that can be more easily identifiable than in AHP. In addition, Several pairwise comparisons lead to time-consuming as well as unnatural comparisons as in Best–worst method (BWM) the process of determining the best and worst criterion to other criteria requires several times and comparing unrelated criteria, which is not an easy process to achieve, nor is it a natural process. For FWZIC, despite the basic version of it, which was developed based on TFN, it is considered the best method for the human approach as it can solve a lot of limitations for some MCDM Methods (BWM, AHP, and ANP).

2.7. EDAS Method

EDAS is one of the effective methods of multi-criteria decision making MCDM. It was developed by Keshavarz Ghorabae, Zavadskas, Olfat, and Turskis in 2015 (Ghorabae et al. 2015) . (Alinezhad & Khalili 2019) agree that the method was informed by the need develop a practical solution to conditions with peculiar characteristics. EDAS applied in Multi-Attribute Decision Making (MADM) for independent attributes. It's used for calculating every alternative's distance from the average value to help decision makers to find the best solution (Huang, Lin & Chen 2021). EDAS is calculating the distance from the Positive Distance Average (PDA) and the Negative

Distance from Average (NDA), which is the lowest alternative from the best value (Zhang et al. 2019). Before the development of EDAS, scholars had investigated the effectiveness of other multi-criteria decision making approaches, including Elimination and Choice Expressing the Reality (ELECTRE), Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), Preference Ranking Organization Method for Enrichment Evaluations (PROMETHEE), Grey Relation Analysis (GRA), and Interactive Multi-Criteria Decision Making (TODIM), and found glaring ineffectiveness when developing alternative solutions to problems (Zhang et al. 2019). EDAS emerged as the only method that appraised the intangibility of average solutions about decision makers and considering the uncertainties in the decision-making environment to obtain aggregated results. EDAS is considered one of the mathematical approaches in MCDM that must reflect the preferences of the criteria-based decision before proceeding with the rest of the steps, so it must be integrated with another MCDM weighting technique to prioritize and determine the weights of a set of identified criteria.

Numerous research using EDAS showed its importance and efficiency. (Fan, Li & Wu 2019) use EDAS to find the best way to select industrial robots. In this research, they discovered that EDAS is more apparent when compared to DEA (data envelopment analysis), which is used to study the problems of choosing appropriate techniques without a set of weights for aggregating and determining the ultimate cross-Aefficiency scores. In addition, EDAS help to identify the most reliable technology in networking to provide security and connectivity within the network (Tanwar, Mehrotra & Nagpal 2020). In other research by (Dr. A Sahaya Sudha 2019) , EDAS was used to choose the appropriate agricultural situation or the appropriate crop to consume less water as well as benefit and higher income for the farmer. The method proved that it is also possible to choose the proper time for harvest, which increases the accuracy of selection, reduces water consumption,

and raises the level of farmers' income. One of the most important engineering problems is select the robots in manufacturing organizations where (Mayssara A. Abo Hassanin Supervised et al. 2019) raised this issue. According to this research the problem was solved and the appropriate robots were selected in factories using the EDAS method, as it was considered a viable and proper method for accurately determining robots according to the Spearman correlation coefficient analysis when compared with other MCDM methods. The appropriate cotton fabric was selected using the EDAS method to achieve optimal thermal comfort properties (Mitra 2020) , which proved the effectiveness and strength of the proposed approach. EDAS underwent three stages to confirm the accuracy: sensitivity testing, changing the dynamic conditions by changing the matrix elements, and it was compared with other MCDM methods.

As previously mentioned, EDAS has been integrated with several MCDM human approaches to generate the weights of the criteria. As shown in Figure 13, EDAS integrated with a lot of methods. For example, In research by (Asante et al. 2020), EDAS integrated with the traditional **MULTIMOORA** method to improve it, which was used to fuse the ranking outputs of the three parts of the MULTIMOORA method, which led to an accurate result. (Behzad et al. 2020) Use EDAS integrated with **BWM** (BWM-EDAS) to evaluate the assessment of solid waste management performance in Nordic countries. EDAS was used to assess the final performance considering the criteria weights and BWM results. According to the Spearman correlation coefficient with which the results were examined, the results obtained by EDAS are reliable, as the study recommended the application of the proposed model resulting from integrating EDAS with BWM. In another integration, (Poongavanam et al. 2021) integrated EDAS with **TOPSIS** and **MOORA** to select the Low GWP (global warming potential) for Automobile Air Conditioning Refrigerant and the results came to approve that there were no significant differences in the results

for each method, but the EDAS method came with the best effect; as the alternative refrigerant with the maximum values of PDA and lesser values of NDA is the best selection. Further, (Abdel-Basset et al. 2021) proposed MCDM model consisting of **AHP**, **COPRAS**, and EDAS to evaluate and select the most sustainable hydrogen production system. According to Pearson correlation coefficient, proposed methods showed that the selection accuracy was 0.96 compared to the other MCDM methods, such as AHP and BWM-TOPSIS approaches. There are more integrations in which EDAS has proven its ability to select with high accuracy, for instance, integration with Credal networks (**CNs**) (Hou et al. 2021) and integration with WEPLPA (weighted extended probabilistic linguistic power average) and **CPT** (cumulative prospect theory) (Zhang et al. 2022).

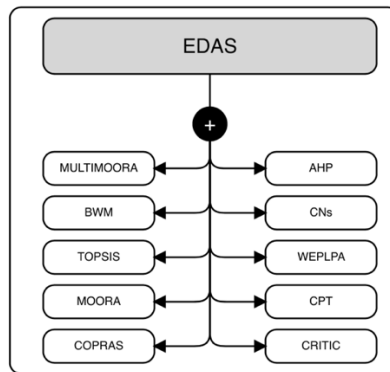


Figure 13: EDAS Integrations samples

As shown in Figure 14, there are some new versions of EDAS. Starting with **EDAS-M**, as per (Zavadskas et al. 2019), Unlike the classical EDAS, EDAS-M includes a modified extension of evaluating alternatives. In EDAS, focus is placed on the average to determine the distance of the solutions. The optimal solution, derived from average solution of Positive Distance Average (PDA) and the Negative Distance from Average (NDA) determine the highest and lowest values. The average results have been found to be less accurate than the criteria values obtained through Criteria Importance Through Intercriteria Correlation that is integrated into EDAS-M. EDAS-M

contributes to the development of EDAS by integrating the CRITIC method to address MCDM issues. Since the CRITIC method introduces objective weights for evaluating MCDM problems, it helps in deriving a standard deviation of different measurements from the average and, hence, a high correlation. Additionally, the obtained values during ranking are based on criteria rather than average results, which helps to improve the accuracy of EDAS. (No et al. 2021) came with new version of EDAS which is **EDAS Multi-Criteria Solution Approach**. As per (No et al. 2021) , the limitation was that the classical method obtained crisp values for average solutions which may lead to wrong ranking. The new extension of EDAS enables solutions to be proposed and converted to equivalent interval forms. The intervals include, definition of alternatives, normalization of the decision matrix, calculation of averages solution for the explored criteria, calculation of interval values for both positive and negative distances evaluated from the average and determining the weighted sum of the positive and negative distances for the proposed alternatives. This is followed by calculating the weighted sum of the distances and evaluating the interval value to appraise the scores for each alternative. A comparison of the appraised interval scores helps to determine the integrated priority for each alternative. EDAS Multi-Criteria Solution Approach is an extension of the classical EDAS. It develops the classical EDAS by integrating expert opinions as an exogenous method of determining the importance of criteria weights. By calculating the interval values obtained from expert opinions, the method provides a more accurate values for positive and negative distances.

Other version of EDAS is **CPT-EDAS** , as according to (Huang, Lin & Chen 2021) Classical EDAS was developed to simulate decision makers' psychological characteristics. The value function, or the marginal impact of change, in classical EDAS can only be calculated through the probability of loss avoidance (Huang et al., 2021). Hence, it is weakened by the limits of random

possession. The enhancement EDAS method based on Prospect Theory was introduced to bridge the gap by calculating the value function using the cumulative probability distribution function. Enhancement EDAS develops EDAS by integrating Prospect and Cumulative Prospect Theory in analyzing rationality of decision making. When compared with TODIM, enhancement EDAS has been found to be more effective in decision making. Last version of EDAS proposed by (Fan LEI, Guiwu WEI, Weijie SHEN 2022) which is **PDHL-EDAS**. PDHL-EDAS develops EDAS by extending its integration to Multiple Attribute Group Decision Making (MAGDM). As a single standard, EDAS has a limited objective weight. However, the integration of a probabilistic double hierarchy improves the quality of selection. Instead of exclusively using linguistic explanations that have a limited scope due to generalization and use of fixed classifications, PDHL-EDAS allows the use of numbers that are more specific and distinct for each selection.

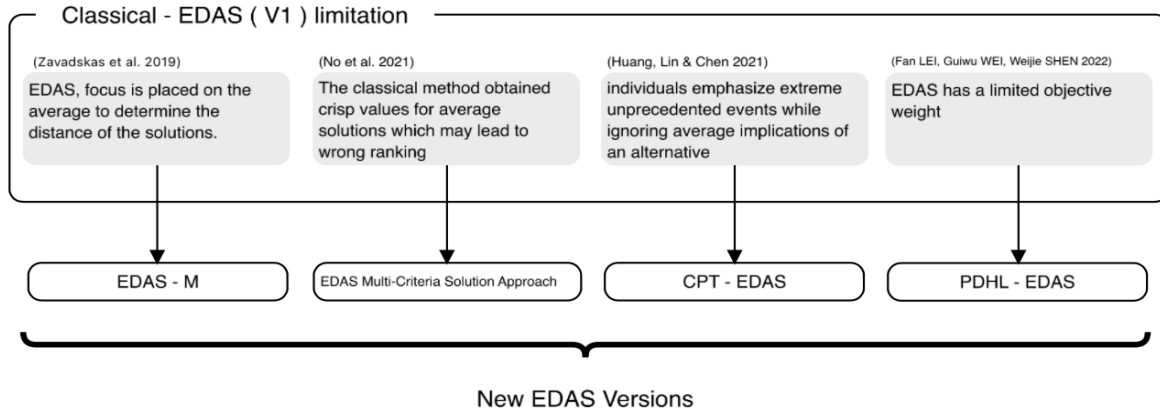


Figure 14: New EDAS Versions

EDAS models mentioned above provides a framework for improvement by authors who customize it to solve specific problems in different industries. In the provided literatures, EDAS-M method for decision making, EDAS Multi-Criteria Solution Approach , enhancement EDAS method based on Prospect Theory (PT), Probabilistic Double Hierarchy Linguistic EDAS (PDHL-EDAS) have been discussed as improved versions of classical EDAS and they build on its limitations.

Based on the literature, it can be inferred that while various MCDM human approach methods have been integrated with EDAS, FWZIC, which is considered the most effective MCDM human approach method, has yet to be integrated with EDAS and this is a **theory gap** that will be solved in this study.

2.8. FWZIC Method

Fuzzy-Weighted Zero-Inconsistency (FWZIC) used to weight attributes without any inconsistencies irrespective of the quantity of criteria. The computation of the criterion's level of significance in decision making using FWZIC is dependent on the distinct preferences of experts for each criterion (Alamoodi, Mohammed, et al. 2022b) (Krishnan et al. 2021) . As per (Krishnan et al. 2021) The FWZIC technique has the capability to overcome several limitations of certain MCDM methods including BWM, AHP, and ANP. These limitations include (i) addressing inconsistency issues with pairwise comparisons, (ii) accounting for ordinary consistency, and (iii) evaluating the reliability of results by addressing the deficiency of consistency threshold values. FWZIC method requires five basic steps that begin with identifying specific criteria and sub-criteria groups. The second step is to identify and select structured expert judgment (SEJ) panelists. Expert decision matrix (EDM) creation is the third step. The fourth step is the application of the fuzzy membership function. Lastly, the values of the final weight coefficients are computed in the fifth phase.

According to (Krishnan et al. 2021), the basic version of FWZIC was developed based on triangular fuzzy sets (TFNs), which have some constraints as for each input, the membership grade is a crisp value, which raises the difficulty of directly defining the membership value. Data uncertainties are the other constraints of TFNs, as its incapability of directly modeling and minimizing their effect. Interval type-2 trapezoidal has easy computational operations and can model the issue raised in

TNFs and Data uncertainties. In addition, it defined the exact membership function, and all these advantages led to the new development of FWZIC versions using trapezoidal fuzzy numbers. In MCDM, uncertainty and vagueness affect the final score in choosing the correct alternative (Albahri, Zaidan, et al. 2022b) . Because of that, many fuzzy sets were introduced to solve these issues.

Recently, New versions of FWZIC developed under different fuzzy sets as shown in Figure 15 . For instance, **spherical FSs** by (Qahtan, Yatim, et al. 2022), where MCDM was applied to choose the best blockchain-based IOT Healthcare system. To weigh the security and privacy features of the systems, a novel edition of FWZIC, referred to as spherical FWZIC (s-FWZIC), was employed. Additionally, GRA-TOPSIS and Bald Eagle Search (BES) techniques were utilized to rank the systems. **Cubic Pythagorean FSs** introduced also by (Alamoodi, Albahri, et al. 2022) to select the best system for sign language recognition, with the integration with two MCDM method extensions, CP-FWZIC for criteria evaluation weights and CP-FDOSM for ranking alternatives. Another research in this field was by (Anor et al. 2022) , where the aim was to select the best international oil companies to build a sustainable transportation system using **linear Diophantine fuzzy rough sets (LDFRSs)** with FWZIC. The new development of the integration of these two MCDM methods was LDFRS-FWZIC which is considered the new extension for FWZIC. In another study on the best paving strategies used to achieve sustainable transport initiated by (Al-Humairi et al. 2022) , MCDM methods were used to solve this issue where the multi-layer **dual hesitant fuzzy weighted zero inconsistency (DH-FWZIC)** was used to assign the weight, as well as the dual hesitant fuzzy decision by opinion score method (DH-FDOSM) to choose the best strategic option in paving.

Further , The COVID-19 disease is considered one of the most potent diseases that invaded the world recently and had a significant impact on all levels, political, social, economic, educational, and others. Several vaccines appeared to mitigate the damage of this disease. A clear strategy was required to distribute these vaccines to guarantee fair distribution and mitigation of damage and distributed according to specific priorities and criteria. Therefore, in research conducted by (Albahri, Albahri, et al. 2022b), the MCDM strategy was applied to solve this issue. An extension of the FWZIC called the **q-rung orthopair fuzzy-weighted zero-inconsistency (q-ROFWZIC)** was used for weighting, and the q-rung orthopair fuzzy decision by opinion score method (q-ROFDOSM) was used for selection. Another evaluation using MCDM methods to evaluate the sign language recognition systems has been conducted by (Albahri, AlSattar, et al. 2022). A new fuzzy set called the *m*-polar fuzzy set combined with a Pythagorean fuzzy set (PFS) was used. A further extension of **FWZIC (Pm-PFWZIC)** and FDOSM (Pm-PFDOSM) is coming where weight is assigned by the former, and the ranking of alternatives is based on the latter.

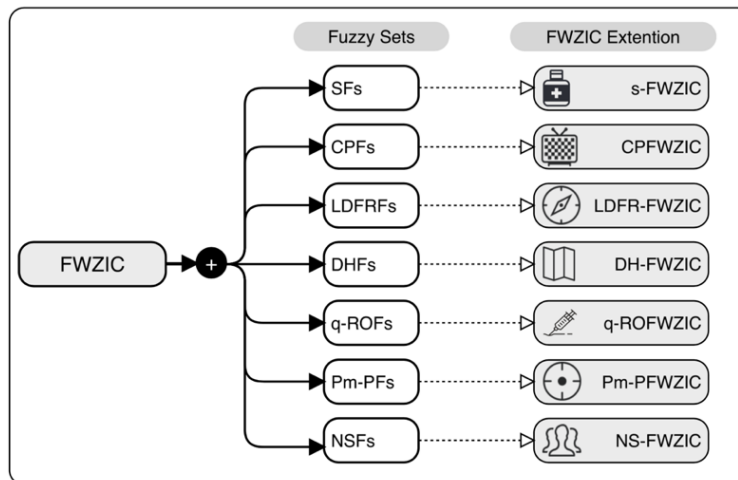


Figure 15: New versions of FWZIC under different fuzzy sets

In addition , A new paper in the year 2022 developed by (Alamoodi, Mohammed, et al. 2022b) demonstrates the importance of using MCDC methods to solve issues related to decision-making.

The research was conducted to evaluate e-tourism applications using new type of fuzzy set called the **neutrosophic fuzzy set**, as this proved its high ability to deal with ambiguity. The weight for each attribute in this research was calculated using **FWZIC (NS-FWZIC)**, and then the alternatives were evaluated using FDOSM (NS-FDOSM). (Alamoodi, Mohammed, et al. 2022a; Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023) have demonstrated the effectiveness of neutrosophic and probabilistic fuzzy sets, respectively, when utilized in conjunction with FWZIC. Consequently, this study intends to employ Probabilistic Interval Neutrosophic Hesitant Fuzzy (PINHFS), given its advantageous characteristics as highlighted in (Shao et al. 2018). However, to date, no research has been conducted on the integration between PINHFS and FWZIC, indicating a **theory gap** in this area.

2.8.1.1. Probabilistic Interval Neutrosophic Hesitant Fuzzy (PINHFS)

As previously stated, various fuzzy set theories have been integrated with fuzzy logic based on the FWZIC model. One of these integrations involves the integration of neutrosophic fuzzy sets. This study aims to further expand upon this integration by introducing a novel type of neutrosophic fuzzy set called Probabilistic Interval Neutrosophic Hesitant Fuzzy Set (PINHFS). According to (Shao et al. 2018) Uncertainty is a common problem in real-world decision-making scenarios, and fuzzy set theory has been introduced as a mathematical model to address this issue. Several other fuzzy set theories have also been developed over time. In practical applications, statistical uncertainty is a significant consideration, and the fusion of fuzzy set theory with probability theory has been explored. Diverse approaches have been devised to tackle with fuzzy decision-making problems, such as using probability theory to represent knowledge and generating fuzzy values by

integrating stochastic simulation with nonlinear programming. The concept of probabilistic fuzzy linguistic term set, hesitant probabilistic fuzzy sets, and probabilistic dual hesitant fuzzy set have also been proposed to solve uncertain risk evaluation issues.

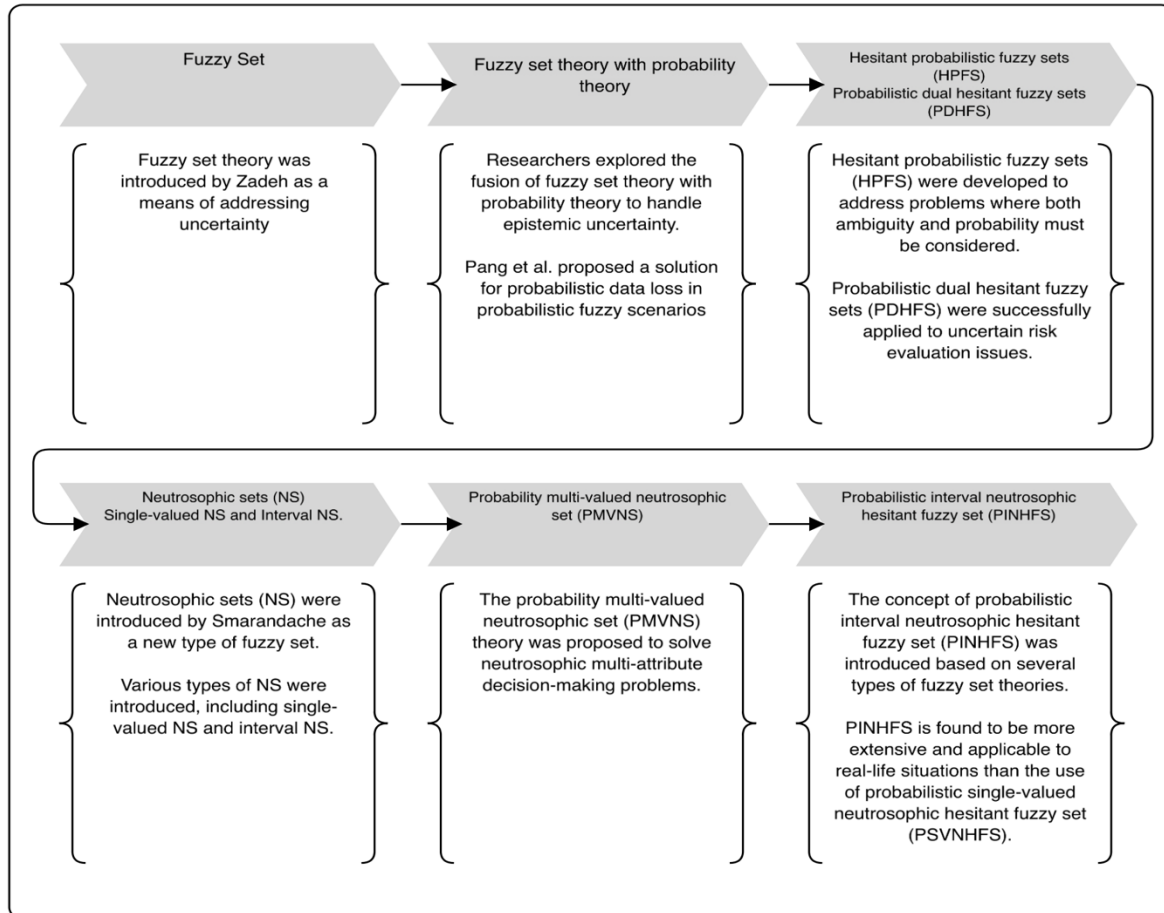


Figure 16: History of PINHFS

The concept of neutrosophic sets, which encompass truth membership, indeterminacy membership, and falsity membership, has been presented as a novel kind of fuzzy set. Subsequently, the neutrosophic fuzzy set theory has been extensively studied and put into practice, and new types of neutrosophic sets have been developed. The probability multi-valued neutrosophic set theory has been proposed to solve multi-criteria group decision-making problems without losing information. Finally, the concept of probabilistic SVNHFS and PINHFS has been introduced to solve MADM

problems under probabilistic interval neutrosophic hesitant fuzzy circumstances. Figure 16 illustrates the history of PINHFZ.

The concept of handling the ranging part in **Neutrosophic** can be described using a general form such as $x + y = 3$. This represents an advancement over **Intuitionistic**, which can only handle like $x + 1 = 1$. The use of Neutrosophic allows for more flexibility and space in the representation of uncertainty. Additionally, Neutrosophic introduces the notion of intervals with upper and lower bounds, as well as probabilistic elements, which further expand the available representation space. This is why the choice of PINHFS becomes relevant in this context (Khan et al. 2021) .

2.9. Perspectives on Dataset Generation across Various Case Studies in Decision Making.

Obtaining actual, reliable data in research has become difficult due to the difficulty of receiving information from its sources, the inaccuracy of the data, or the lack of trust in the sources providing the data. In addition, obtaining high quality data and high privacy has become one of the problems facing researchers recently. Therefore, many researchers have resorted to using synthetic data, as it is generated by the researcher and not collected from a source, and is almost of higher quality than real data (Figueira & Vaz 2022) . There are several studies that used synthetic data including those researches that used synthetic data to simulate the symptoms of corona for patients to suggest the appropriate solution (Alsalem et al. 2021b; Mohammed et al. 2021; Albahri, Albahri, et al. 2022b; Albahri, Zaidan, et al. 2022a).

In addition to that, another method is called root articles; many researchers adopted it to obtain high-quality and private data. The root article can be defined as a knowledge container that summarizes previous studies in the same field based on certain factors, criteria, or attributes. Table 7 displays a selection of prior investigations that have utilized root article techniques.

Table 7: Exploring the Application of Root Article Method in Diverse Case Studies

References	Case study	The root article	Number of prior studies/alternatives	Number of categories	Number of development factors or attributes	Data type	Data size (partial or full)
(Qahtan, Yatim, et al. 2023)	Healthcare industry 4.0 application based blockchain	(Hussien et al. 2021)	52	2	6,7	Binary based	Full
(Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023)	Fuel Supply System for Electric Vehicles	(Lopez-Arboleda, Sarmiento & Cardenas 2019)	33	2	2	Categorical based	Full
(Alamoodi, Albahri, et al. 2022)	Sign language recognition system	(Al-Samarraay et al. 2022a)	30	2	11	Categorical based	Full

As per above table , The study by (Qahtan, Yatim, et al. 2023) utilized the foundational research by (Hussien et al. 2021) to assess the application-based blockchain in the healthcare industry, with a focus on Industry 4.0, using multi-criteria decision-making (MCDM) methods. The authors collected data from a full binary dataset, as detailed in the root article, which encompassed 52 healthcare systems divided into two categories, and evaluated based on six and seven attributes. (Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023) employed the foundational article by (Lopez-Arboleda, Sarmiento & Cardenas 2019) to benchmark and evaluate 33 Fuel Supply System for Electric Vehicles, with data from 11 alternatives within two primary criteria. Finally, (Alamoodi, Albahri, et al. 2022) utilized data from the root article by (Al-Samarraay et al. 2022a) to evaluate 30 sign language recognition systems, categorized into two groups and assessed based on 11 attributes.

According to (Qahtan, Yatim, et al. 2023) research , (Alamoodi, Mohammed, et al. 2022b) and (Krishnan et al. 2021) use the entire data from the original article put forward by (Hamid, Albahri, Alwan, et al. 2021), whereas the latter analyses 65 systems and classifies them into five categories and evaluates each system based on 12 attributes. The data type in Hamdi's root article is based on a binary set where a "yes" response signifies the presence of attributes in the system. Other full data were used from (Albahri et al. 2020) and (Sarah et al. 2022). (Albahri et al. 2020) use the full data of (Bai et al. 2020) from research about "COVID-19 Presumed Asymptomatic Carrier Transmission" where Five patients from one family were examined with respiratory symptoms and fever, with one from same family without symptoms. The examination was based on eight biological laboratory test features. (Sarah et al. 2022) conducted research regarding choosing the best sustainable transportation system for international oil companies using the root article initiated by (Trivyza et al. 2022), which has 62 sustainable transportation systems with ten evaluation attributes. In addition, At the level of data that was partially taken from the root article , (U.S.Mahmoud et al. 2022) and (Salem et al. 2022) use partial data from the root article initiated by (Talal et al. 2020). They selected 14 out 39 systems suggested by (Talal et al. 2020).

It is clear from the above that using the root article to take data and use it in other research is a scientific method adopted by many researchers, whether the use of data in whole or in part. These research came either to complement previous research, to develop a new study based on what was presented or recommended, or to take advantage of the data in making scientific decisions by using them in scientific ways. In this research we used the same approach and depends on root article proposed by (AlAhmad et al. 2021) by using partial binary based data

as this research focus only on four delegation methods in MCC Security Modules which are Layering , Authentication , Encryption and Dynamic offloading.

2.10. A Comprehensive Review of Validation and Evaluation Procedures in Decision Science

In MCDM, validation and evaluation refer to the process of assessing the quality and performance of the decision-making model and the outcomes generated by it. According to (Alsalem et al. 2021b, 2022; Albahri, Zaidan, et al. 2022a), there are various procedures used to validate and evaluate methods in decision science. As shown in Figure17, This process can be divided into two main steps: model validation and decision evaluation. **Model validation:** This step involves checking the consistency, completeness, and accuracy of the model, as well as its ability to generate results that are consistent with the problem definition and data. **Sensitivity analysis** is one technique used in this phase, which assesses the robustness of the model by analyzing the effect of variations in the input data and model assumptions, and benchmarking, which compares the model's performance against other models or real-world data (Alamoodi, Albahri, et al. 2022) , (Anor et al. 2022). **Systematic ranking** is other techniques used which is a method used to rank a set of alternatives based on a set of criteria. It involves assigning a score or a weight to each alternative for each criterion and then combining these scores to determine the overall ranking of the alternatives (Qahtan, Yatim, et al. 2023) , (Albahri, Zaidan, et al. 2022a) , (Krishnan et al. 2021).

The second step in this phase is the **Decision evaluation:** This step involves assessing the quality of the decision outcomes generated by the model, by evaluating the performance of the selected alternative against the objectives and criteria. This step can include techniques such as **Benchmarking checklist** (Al-Samarraay et al. 2022b)..

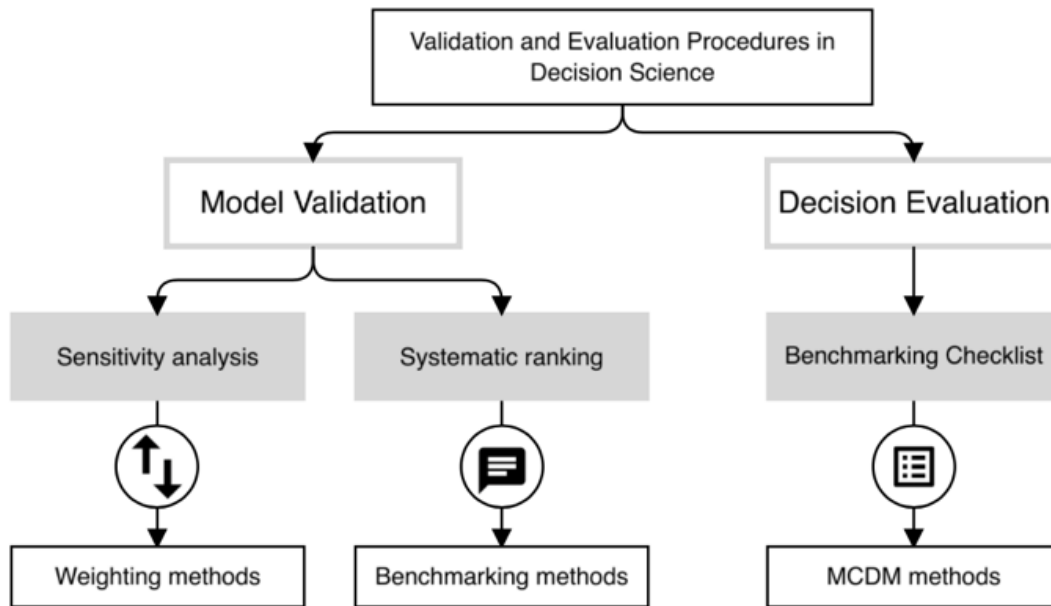


Figure 17: Validation and Evaluation Procedures

2.10.1. Sensitivity Analysis Procedure

Sensitivity analysis is employed to investigate how variations in an independent variable impact a dependent variable under a particular set of assumptions (Lee & Chang 2018) . Different studies are using sensitivity analysis procedures to validate weighting methods. The Table 8 below presents various case studies using sensitivity analysis.

According to Table 8, various case studies used the same sensitivity type, elasticity coefficient () with different scenarios and criteria for evaluation. (Qahtan, Yatim, et al. 2023) Use nine scenarios with seven criteria, while (Alamoodi, Albahri, et al. 2022) and (Anor et al. 2022) use the same number of scenarios and criteria, which are nine and eleven, respectively. Additionally, the Spearman's correlation coefficient (SCC) was utilized to evaluate the association between the outcomes of diverse scenarios and the suggested solution in all the case studies outlined in the table. As per above, other weighing methods are used, such as S-FWZIC,

CP-FWZIC, and LDFRS-FWZIC with different fuzzy sets, Spherical FSs, Cubic Pythagorean FSs, and linear Diophantine fuzzy rough sets.

Table 8: A Review of Sensitivity Analysis Evaluations across Diverse Case Studies

References	Case study	Weighting method	Fuzzy set	Number of scenarios	Number of criteria	Sensitivity Type	Correlation Type
(Qahtan, Yatim, et al. 2023)	Healthcare industry 4.0 application based blockchain	S-FWZIC	Spherical FSs	5	7	elasticity coefficient (α_c)	Spearman correlation coefficient (SCC)
(Alamoodi, Albahri, et al. 2022)	Sign language recognition system	CP-FWZIC	Cubic Pythagorean FSs	9	11	(α_c)	(SCC)
(Anor et al. 2022)	select the best international oil companies to build a sustainable transportation system	LDFRS-FWZIC	linear Diophantine fuzzy rough sets	9	2 criteria 9 sub-criteria	(α_c)	(SCC)

According to (Qahtan, Yatim, et al. 2023) research, a lot of researchers such as (Albahri, Zaidan, et al. 2022a), (Albahri, Albahri, et al. 2022b), (Krishnan et al. 2021) and (Alsalem et al. 2021b) used the same sensitivity type which is () and the same correlation type with the different number of scenarios and criteria. They are using other waiting methods, which are PFWZIC, ROFWZIC, IT2TR-FWZIC, and T-SFWZIC with various fuzzy sets, which are Pythagorean fuzzy set, q-rung orthopair fuzzy set, Interval type 2 trapezoidal-fuzzy set and T-spherical fuzzy

set. From the foregoing, it becomes clear the importance of applying the sensitivity analysis for validation weight methods.

2.10.2. Systematic Ranking Procedure

The systematic ranking procedure is utilized to validate the benchmarking method. As depicted in Table 9 below, this procedure is adopted by numerous scholars:

Table 9: Systematic Ranking Procedure in Various Case Studies

References	Case study	Total number of alternatives	Number of groups	Number of alternatives per group	Matrix based on raw, normalized, or weighted data
(Qahtan, Yatim, et al. 2023)	Healthcare systems – TMIS	11	3	4,4,3	Row
	Healthcare systems – RPMSs	16	3	5,5,5	
	Healthcare systems – EHRs	16	3	5,5,6	
	Healthcare systems – EMRs	6	2	3,3	
	Healthcare systems – PHRs	4	2	2,2	

Based on the aforementioned table, a recent study by (Qahtan, Yatim, et al. 2023) was subjected to a systematic ranking process. The study involved a matrix consisting of 52 alternatives categorized into five groups, with each group containing a varying number of alternatives distributed across two or three subgroups. For instance, the TIMS systems were classified into three subgroups, with each subgroup containing four, four, and three systems, respectively, based on raw data

According to (Qahtan, Yatim, et al. 2023) research three references dealt with the same topic, the Covid-19 vaccine dose, with the same matrix based, raw, each has its number of alternatives. (Albahri, Zaidan, et al. 2022a) and (Albahri, Albahri, et al. 2022b) participated in the same number of alternatives and groups 300-6, respectively. In contrast, (Alsalem et al. 2021b) used 150 alternatives distributed in six groups. The same paper of (Qahtan, Yatim, et al. 2023) as well illustrates that (Krishnan et al. 2021) has matrix based on raw and normalized data in case study about Smart e-tourism. Krishnan's group of alternatives numbered 65, distributed over five case studies. They all have the same number of three groups, with a difference in the number of alternatives in each group, as shown in the table. In addition, (Hamid, Albahri, Albahri, et al. 2021) with case study about Telemedicine has the same matrix based of (Krishnan et al. 2021) with 500 alternatives classified in three groups and 166 alternative under each group. Last reference in this systematic ranking procedure is the (Salih et al. 2021) where case study is about Network congestion control and the number of alternatives is six, divided into two groups equally.

2.10.3. Comparative Analysis Utilizing Benchmarking Checklist Approach

The benchmarking framework requires validation via a comparative study employing benchmarking checklist procedures. Table 10 below highlights a few studies that have utilized comparative study for this purpose.

Table 10: A Comparative Study of Benchmarking Checklist Procedures in Various Case Studies

References	Case study	Challenges and issues listed	Score points followed	Theory- or application- based	Number of benchmarking points
(Qahtan, Yatim, et al. 2023)	The Implementation of Blockchain Technology in Healthcare Industry 4.0	A Benchmarking Analysis of Blockchain Technology in Healthcare Industry 4.0 : - Multiple Evaluation criteria - Importance of Criteria - Variations in data	NA	Theory	17
(Sarah Qahtan et al. 2022)	A Modelling Approach for the Fuel Supply System of Electric Vehicles	A Benchmarking Analysis of Alternatives for Fuel Supply System Modeling Approaches (FSSMA): - Multiple evaluation criteria - Balancing of criteria trade-offs - Variations in data	NA	Theory/ Application	21
(Ibrahim et al. 2023)	The Implementation of Sustainable Practices in the Palm Oil Industry	A Benchmarking Analysis of the Most Sustainable Practices in the Palm Oil Industry: - Multiple evaluation criteria - Criteria importance - Criteria confliction.	Applied	Theory/ Application	16

According to table above, three recent case studies are presented in the above table through which the Comparative study is applied. Two of them are based on theory and application (Sarah Qahtan et al. 2022), (Al-Samarraay et al. 2022b) and the first one based on theory only (Qahtan, Yatim, et al. 2023) . The only one who based on theory is (Qahtan, Yatim, et al. 2023). (Al-Samarraay et al. 2022b) applied score point only as appeared in the table. The main

common issues for all studies are Multiple evaluation criteria, Data variation, and the importance of criteria. Regarding the number of benchmarking points , it was 17,20,16 respectively for (Qahtan, Yatim, et al. 2023), (Sarah Qahtan et al. 2022) , (Al-Samarraay et al. 2022b).

As per (Qahtan, Yatim, et al. 2023) a lot of researchers use the benchmarking checklist in order to decision evaluatin. (Qahtan, H.A.Alsattar, et al. 2022a) and (Hamid, Albahri, Albahri, et al. 2021) which are based on theory and application , they raised the same issues of MCDM which is data variation , criteria importance and multible evaluation criteria and they both applied the score points. Inconstruct (Krishnan et al. 2021) have more two MCDM issues which are Fuzziness and Imprecision. In the regard to the number of benchmarking points , it was 17,5,16 for (Qahtan, H.A.Alsattar, et al. 2022a) , (Krishnan et al. 2021) and (Hamid, Albahri, Albahri, et al. 2021) respectively.

2.11. Chapter Summary

Section 2.2 provides a classification of literature reviews is presented with regard to the development attributes of Security Modules of Delegation Methods in MCC. A critical review of Security Modules of Delegation Methods in MCC is carried out in Section 2.3 to identify a research gap. **As the research gap** arises from the fact that while researchers have proposed solutions and focused on the development security attributes, they have not utilized these attributes to evaluate and benchmark Security Modules of Delegation Methods in MCC. This indicates a lack of research in assessing the effectiveness and performance of these modules based on the required security attributes.

Section 2.4 examines the difficulties and unresolved issues linked to multi-criteria benchmarking, highlighting three main issues: (i) the use of multiple evaluation criteria, (ii) the

issue of criteria importance, and (iii) Variation on Data. Sections 2.5, 2.6, 2.7, and 2.8 present a summary of the theoretical framework underpinning multi-criteria analysis in Security and Cloud computing and MCDM methods. However, there is still a **theoretical gap** in the research, as no previous studies have attempted to integrate the EDAS and FWZIC in PINHFS environment to evaluate and benchmark Security Modules of Delegation Methods in MCC.

In Section 2.9, various case studies are presented where a "root article" was used to create a dataset when actual data was unavailable. Finally , Section 2.10 discusses the validation and evaluation processes of MCDM methods, which include the systematic ranking procedure, sensitivity analysis procedure, and comparative study based on benchmarking checklist procedure.

CHAPTER 3: RESEARCH METHODOLOGY

3.1. Introduction

This chapter explains the research methodology that leads to achieving the desired objectives. It consists of four main phases to develop a Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing. Each phase is linked with specific research objectives and has a clear, detailed plan, as shown in the Figure 18.

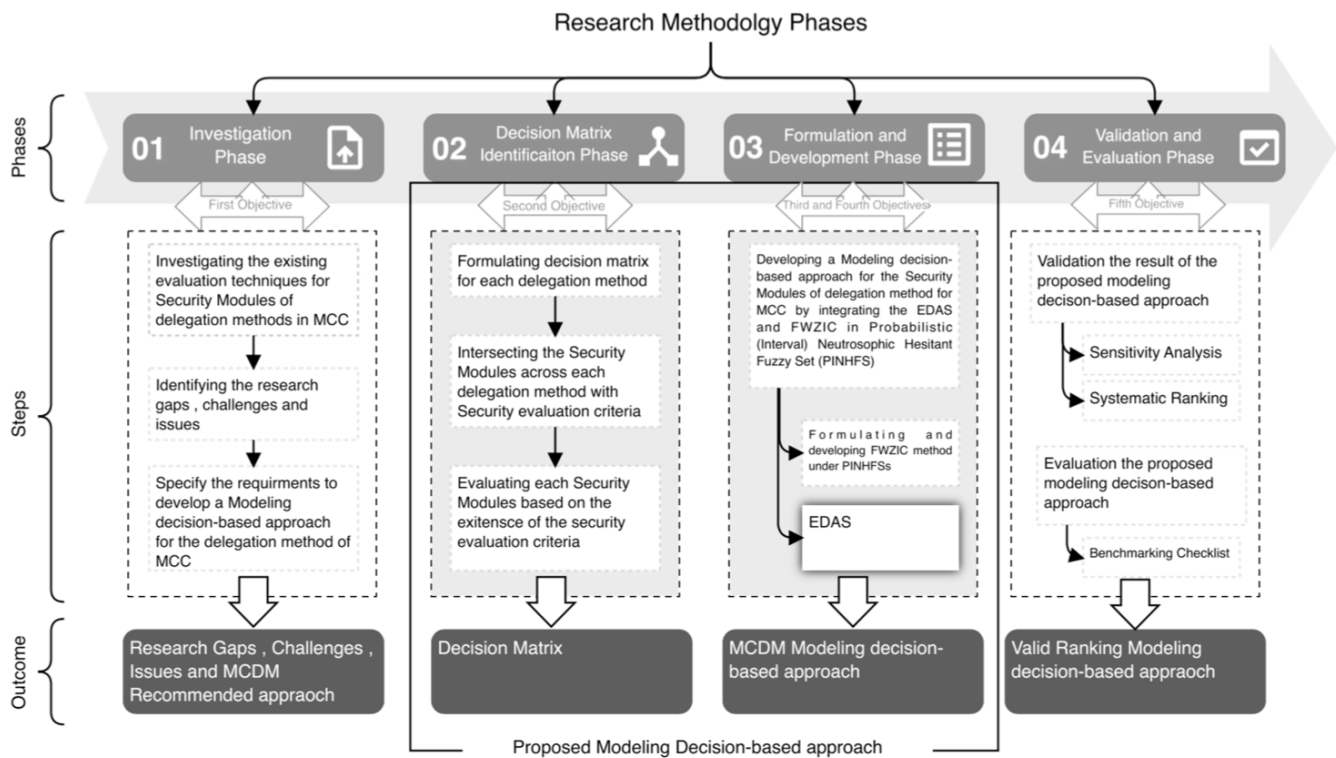


Figure 18: Research Methodology

The investigation phase presented in section 3.2 is the first phase which consists of research and theory gaps with the recommended MCDM solution. Section 3.3 illustrates the details of the second and third phases. The second phase (**decision matrix identification phase**), presented in section 3.3.1, presents the formulation of a decision matrix based on the identified delegation methods and security evaluation criteria. While section 3.3.2 offers the third phase (**formulation and**

development), which details the formulation and development of a Modelling decision-based approach for the delegation method of MCC based on integrating the EDAS and FWZIC with Probabilistic Interval Neutrosophic Hesitant Fuzzy Set (PINHFS). **The validation and evaluation phase** is the methodology's fourth and last phase, where the proposed modeling decision-based approach will be validated using sensitivity analysis and systematic ranking and evaluated using benchmarking checklist.

3.2. Investigation phase

To achieve the first objective and primary aim of this investigation “To demonstrates the existing evaluation techniques for Security modules of delegation methods in MCC and drawing attention to the evaluation drawbacks.” and before conducting an in-depth analysis of Security Modules of Delegation Methods in MCC, a preliminary study is necessary to evaluate the existing evaluation techniques and identify their limitations. In the taxonomy of the literature review of this research, the most critical research that dealt with the field of security modules in cloud computing was reviewed, and no study was found that directly addressed the topic of the study, as (AlAhmad et al. 2021) worked on reviewing all security modules of delegation methods in MCC and What security issues are included and ignored. A critical review of the Security modules of delegation methods in MCC was also conducted to determine the **research gap**. The most pressing challenges and issues facing specialized research in comparing modules and choosing the best ones were also reviewed, represented in Multi evaluation criteria, Criteria importance issues, and Data variation issues.

The literature review section also covered the theoretical foundations of multicriteria analysis in security and cloud computing to identify potential gaps in the theory and propose potential solutions to overcome this gap, and the MCDM methods that can be used. Furthermore, the data

set, how to obtain it, and the essential studies that used the same approach in determining their data were reviewed at this phase of the research. In addition, the Validation and Evaluation procedures in decision sciences were examined to ensure the validity of what was followed.

3.3. Proposed Modeling decision-based approach for the delegation method of MCC

As shown in Figure 18 the proposed modeling decision-based approach can be achieved in two phases as below:

3.3.1. Decision matrix identification phase

In this phase, the second objective, “To articulate the decision matrices based on the intersection of Security Modules of delegation method in MCC with the security evaluation criteria.” will be achieved. The second phase of utilizing a decision matrix to assess and compare various alternatives or options is known as the identification phase. During this phase, the options or alternatives that will be evaluated (Security Modules of delegation method in MCC) will be identifies, as well as the criteria or factors (Security issues) that will be used to evaluate them. The Intersecting of alternatives across each Security Modulesw with evaluation criteria will be included in this phase. The identification phase also includes the process of defining and prioritizing the criteria, as well as determining the relative importance of each criterion. This phase is important for ensuring that all relevant options and criteria are considered in the decision-making process and that the decision matrix is properly structured to accurately evaluate and compare the options.

In decision science, a lack of real data can present a challenge when trying to make accurate predictions or decisions. Without sufficient data, it may be difficult to train a model or make inferences about a particular situation. In these cases, researchers may need to rely on synthetic data, use a smaller dataset, or gather more data through additional research. Additionally, another method used which is root article that summarizes previous studies in the same field based on

certain factors, criteria, or attributes. In this research, the root article is the research conducted by (AlAhmad et al. 2021) which lists all Security Modules of delegation method in MCC and the security issues that are ignored and included in each module used in this research as evaluation criteria to benchmark the Security Modules of delegation method in MCC.

Accordingly, the articulation of the decision matrices will be included in detail in chapter 4 and the result of decision matrix will be presented in chapter 5.

3.3.2. Formulation and Development phase

In this phase, the third and fourth objectives of this research will be achieved, which are “To formulate and develop an extension of FWZIC method under a Probabilistic Interval Neutrosophic Hesitant Fuzzy Set called (PINHFS)” and “To develop a Modelling decision-based approach for Security Modules of delegation method for MCC using the formulated decision matrices and the integration of EDAS and new extension of FWZIC under PINHFS.” respectively. The **First step** in this phase is to develop and formulate FWZIC under PINHFS to assign weight to the security evaluation criteria by several steps presented in Chapter 4. The **second and final step** is utilizing the EDAS method for benchmarking the Security Modules of delegation method in MCC by several steps, as well as in Chapter 4.

Finally, the new framework, which is an integration of EDAS with a new extension of FWZIC, which is PINHFS -FWZIC- will be considered the basis of the Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing.

3.4. Validation and Evaluation phase

In this phase the fifth objective which is “To assess and verify the outcomes of the suggested modelling approach, by utilizing sensitivity analysis, systematic ranking, and benchmarking

checklist (Evaluation and Validation process).” will be achieved. Below sections details each validation and evaluation approaches.

3.4.1. Sensitivity analysis

Sensitivity analysis, as mentioned in section 2.10 in this research, is a method used to evaluate the robustness of the final decision by assessing how the decision changes in response to changes in the input data. The primary objective of conducting sensitivity analysis is to pinpoint the criteria that wield the greatest influence on the ultimate decision outcome and to evaluate the robustness of the decision by varying the input data so, this research aims to analyze the impact of variations in criteria weights on the outcomes of the suggested decision-based approach model (EDAS with PINHFS-FWZIC). Hence, the validation of the proposed method will be carried out by conducting a sensitivity analysis on the ranking of Security Modules of Delegation Methods in MCC. The weight values of the security evaluation criteria are modified in accordance with Kirkwood and Kahraman’s recommendations (Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023) . The analysis will involve making modifications to the criteria weights and following the steps outlined below.

- I. Identifying the most significant criterion using the PINHFS-FWZIC method
- II. Examining the effects of adjusting the criterion weights by producing nine scenarios based on the similar criterion weights using the following formula:

$$w_c = (1 - w_s) \times (w_c^o / W_c^0) = w_c^o - \Delta x \alpha_c$$

Where

- The weight of the most important criterion is defined by w_s .
- The weight values calculated by the PINHFS-FWZIC method initially are denoted by w_c^o .

- The sum of the original weight values for the diverse criterion weights is denoted by W_c^0 .
 - The range of modifications applied to the security and privacy criteria weights, which are the upper and lower bounds of the most crucial criterion, is indicated by Δx .
- III. Calculate the elasticity coefficient (α_c) for each criterion to assess the degree of deviation of the primary criteria.
 - IV. Perform a comparison between the rankings obtained by modifying the criterion weights in the produced scenarios and the initial ranking

The result of sensitivity analysis will be presented in Chapter 5.

3.4.2. Systematic Ranking

The aim of Systematic Ranking is to provide a transparent and structured way of validating the benchmarking methods. Below is the step that will be taken in this regard:

- I. Combine all the matrices of opinions to generate a consolidated opinion matrix.
- II. Rank the alternatives in the unified opinion matrix according to the EDAS outcomes.
- III. Divide the systems in each delegation method into groups and there is no affect for the number of systems in each group.
- IV. Apply the subsequent formula to determine the average of each group:

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

- V. Contrast the averages of each group since the decision-makers allocated the minimum linguistic terms to the optimal solution of each criterion. Therefore, the minimum average values of each cluster would yield accurate outcomes.

3.4.3. Benchmarking Checklist

The proposed benchmarking framework undergoes an evaluation process via a comparative study that employs a checklist benchmarking process. To attain validation of the proposed framework, it is subjected to a detailed comparison with other paper utilizing several predetermined comparison points from the benchmarking checklist. The benchmark study focuses on the assessment of various Agriculture-Food 4.0 supply chain approaches through the application of a Fermatean probabilistic hesitant-fuzzy sets-based decision-making model.

The evaluation is conducted from two different angles, namely theoretical and application. With regard to the theoretical aspect, the comparison is carried out in relation to the methods of weighing and ranking. Specifically, the PINHFZ-FWZIC method is compared to the benchmark study's' weighting technique, while the EDAS technique utilized in this study is evaluated against the ranking methodologies employed in the benchmark study. In contrast, the application aspect of the comparison concentrates on examining the issues pertaining to the MCDM method. The subsequent Table 11 displays the comparison criteria, which were sourced from various references such as (Hamid, Albahri, Albahri, et al. 2021; Al-Samarraay et al. 2022b; Sarah Qahtan et al. 2022; Ibrahim et al. 2023; Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Ding 2023) to align with the current investigation.

Table 11: Comparison Points definition

Points #	Comparison Points	Description
Theoretical Aspects		
Weighting perspective		
1	Use the weighting method to address inconsistencies.	This enables us to ascertain whether the weighting methodology implemented in the comparative analysis of our proposed research approach and the benchmark studies effectively resolved the problem arising from the conduct of pairwise comparisons.
2	Ensure that the criteria are not interdependent.	This aspect pertains to the capacity of the compared weighting methods to undertake reiterations of pairwise comparisons upon the introduction or exclusion of a criterion.
3	The weighting method is not overly time-consuming.	This point pertains to the time requirements associated with the implementation of the compared weighting methods.
4	The weighting method does not involve complex mathematical operations.	This point pertains to the mathematical complexity associated with the implementation of the compared weighting methods, specifically in terms of the number of mathematical operations required.
5	Gathering input from experts is a simple process	This point pertains to the extent to which the compared weighting methods can efficiently obtain expert feedback.
Vagueness, hesitancy, and uncertainty		
6	The weighting method is more dependable when it comes to solving imprecision and ambiguity in practical situations	This point is to assess if the utilized weighting technique provides increased dependability in handling vagueness and uncertainty experienced in practical situations.
7	The weighting approach can handle cases where the decision-maker's rejection is crucial to the evaluation process.	This point aims to evaluate the extent to which the weighting method is capable of effectively handling decision-making scenarios in which the refusal of the decision maker significantly impacts the judgment process.

8	The weighting method preserves probability data.	This point aim to check if the weighting method have the capability to retain probabilistic data.
9	The weighting method provides a wider variety of choices to decision-makers compared to other fuzzy sets.	This point aims to determine whether the employed weighting method offers a more extensive range of alternatives to decision-makers as compared to other fuzzy sets.
10	The weighting method is more effective and efficient in handling vagueness, hesitancy, and uncertainty than other fuzzy sets.	This point seeks to determine the relative effectiveness and efficiency of the weighting method as compared to other fuzzy sets in managing vagueness, hesitancy, and uncertainty.
Ranking perspective		
11	Assign weights to criteria.	This point relates to if the compared ranking methods can assign weights or not.
12	Integrated with Fuzzy environment	This point seeks to determine whether the ranking methodology employed in the research being compared has the capability to assign weights to the evaluated criteria.
13	Not computationally demanding.	This point pertains to the mathematical complexity associated with the implementation of the compared ranking methods, specifically in terms of the extent of calculations required.
14	Take into account the significance of the distances.	This point objective is to determine if the ranking techniques take in to account the relative importance of distances.
15	Incorporate positive and negative ideal solutions into decision matrices.	This point pertains to the extent to which the compared ranking methods consider both (PI) and (NI) solutions.
16	Calculates utility degrees based on proximity to ideal solutions.	The goal of this point is to evaluate the capability of the ranking techniques to determine the level of usefulness that is most similar to the positive ideal (PI) and negative ideal (NI) solutions.
17	Calculate utility functions.	This point aims to assess the extent to which the compared ranking methods possess the capability to compute the utility functions.

18	Remains stable even with a large number of alternatives and criteria.	This point pertains to the stability of the compared ranking methods when dealing with a vast set of alternatives and criteria.
19	Can perform multiple tasks simultaneously.	This point aims to assess the multifunctionality of the compared ranking methods
Application Aspects		
20	The evaluation process involves considering several different criteria.	This point aims to determine if other cases utilized in the benchmarking studies are capable of resolving the identified issue.
21	Prioritization of the criteria is determined based on their relative importance.	This point aims to evaluate whether the utilized applications in the compared studies have the capacity to allocate priority to criteria based on their level of importance.
22	The proposed method takes into account variations in the data.	This point seeks to determine whether the utilized application in the compared research was affected by the problem of data variation.

3.5. Chapter Summary

Chapter 3 provides a detailed account of the research methodology employed to investigate the Security Modules of delegation methods in MCC. The chapter begins by introducing the research design and describing the investigation phase, which outlines the research objectives and questions. The proposed Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing is then presented, which includes the decision matrix identification phase and the formulation and development phase. Subsequently, the validation and evaluation phase is described, which involves the implementation of sensitivity analysis, systematic ranking, and benchmarking checklist procedures to evaluate the proposed model. The chapter concludes with a summary of the key methodological components and procedures.

CHAPTER 4: DECISION MODELLING APPROACH FOR THE SECURITY MODULES OF DELEGATION METHODS IN MOBILE CLOUD COMPUTING

4.1. Introduction

In this chapter the proposal of Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing will be presented. It is divided into two key components: the identification phase of decision matrices and the formulation and development phase. The first phase of this chapter (**Section 4.2**) delves into the formation of decision matrices for Security Modules of Delegation Methods in MCC, using security evaluation criteria. These decision matrices, which serve as a dataset in the study, are then utilized in the second section of the chapter, the formulation and development phase. The second phase of the chapter (**Section 4.3**) is comprised of two sub-sections: the PINHFS -FWZIC method and the EDAS method. In the first sub-section (Section 4.3.1), the process of allocating weights to the security evaluation criteria of MCC delegation method systems using the FWZIC and PINHFS method is thoroughly discussed. The second sub-section (Section 4.3.2) deals with the development and formulation of the EDAS method, which benchmarks these systems based on the constructed decision matrices and the weighted criteria. A visual representation of the Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing can be seen in Figure 19 .

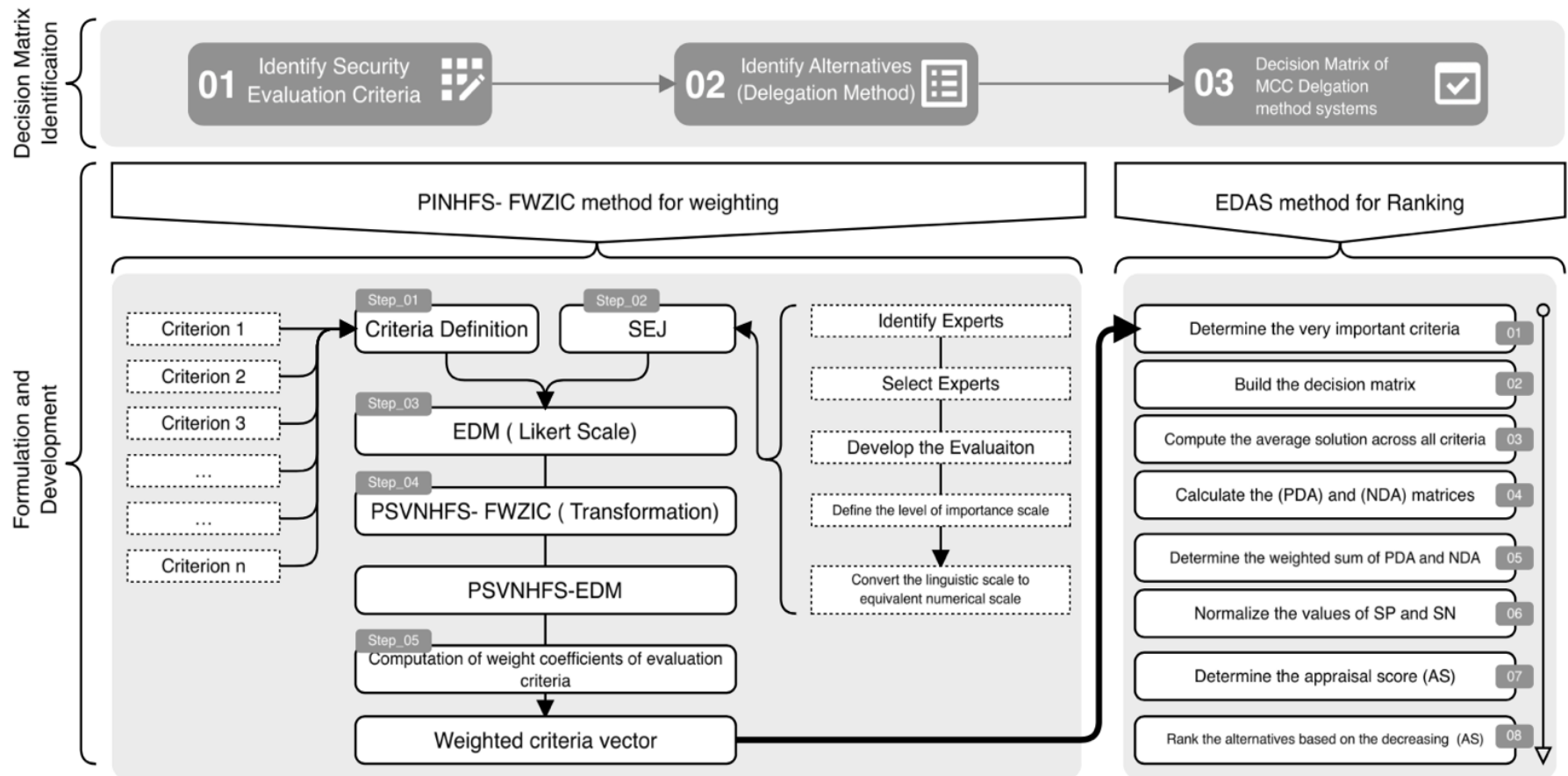


Figure 19: Modeling decision-based approach for delegation method of MCC

4.2. Identification of Decision matrix

Formulation of the Decision Matrix phase involves identifying the security evaluation criteria relevant to the decision problem and the possible alternatives being considered, then constructing a decision matrix to represent these criteria and their relationships. The following sections include the details for this process where (Section 4.2.1) details the identification of security evaluation criteria, (Section 4.2.2) presents the MCC delegation methods system, and the formulation of decision matrices will be in (Section 4.2.3).

4.2.1. Security Evaluation Criteria identification

The expression "criteria" pertains to standards or factors used to judge, evaluate or compare a set of options or alternatives. In decision-making and evaluation, criteria provide a basis for comparing and selecting the best choice based on specific objectives or goals. Based on the proposed taxonomy (Figure 7 in Chapter 2), the Security Modules of Delegation Methods in MCC were evaluated using 13 security attributes (General security issues, Privacy, Authentication (cloud to client authentication, Client to cloud authentication, and Multi-Factor Authentication), Data Security, Encryption key, single failure point, security threats, communication channels issues, Un proper access control, authorization issues and anonymity). This research employed these developmental attributes as criteria for evaluation to evaluate and benchmark delegation method systems. The following is the definition of each attribute.

As per (AlAhmad et al. 2021) , **general security** can include integrity , confidentiality and malware attach issues. Alnajrani et al. (2020) define **privacy** as the information of the known person or data subject. However, they argue that privacy has myriad perspectives that people define natively depending on their culture and other jurisdictional variables. For example, Krishnan (2017) defines

privacy jurisdictionally as a person's right to have their information protected to ensure confidentiality, appropriateness, unanimity, non-traceability, non-linkability, and non-observability. Mobile cloud technology incorporates a myriad of non-uniform resources that supplement the computational capabilities of the surfeit of resource-limited mobile devices. Accessing and utilizing cloud-based computational resources ignites numerous security and privacy concerns, such as user authentication.

Authentication is a process used to validate the identity of a mobile user, ensuring legitimacy in access to mobile cloud computing resources (Seada Abdu Wakene et al. 2021). On the other hand, Irshad et al. (2020) refer to authentication as the process of verifying rightful access to mobile cloud computing resources to ensure that they are available to genuine users. The two studies concur that authentication is a critical element of security and privacy preservation in mobile cloud technology. **Multi-factor authentication issue** is an authentication issue but the best analogy for a multifactor authentication mechanism is a door with several locks with successive dependencies. Unlike conventional logins that rely on a correct combination of the identifier and password, multifactor authentication introduces an additional layer of security such as text messages to linked cell phones, email, or authentication applications (Nawrocki et al. 2022). According to Seada Abdu Wakene et al. (2021), the additional layers improve the overall security of the mobile cloud computing environment, despite that they cause friction to the client's experience.

Cloud to client authentication is also called cloud-side authentication. In mobile cloud computing, cloud-to-client authentication is where most of the authentication steps are executed in the cloud server (Himadri & Seema 2020). Himadri & Seema (2020) observes that cloud-to-client authentication methods are more flexible and resource-efficient because they use unlimited resources of the cloud server. Even with these benefits, cloud-to-client authentication methods raise

significant privacy and information security issues, especially the exposure of users' private authentication data, such as biometrics and passwords. Aldmour, Yousef, Baker, & Benkhelifa (2021) refer to cloud-side authentication methods as those that do not need client libraries and are transparent to the user. On the other hand, **Client-to-cloud** or user-side authentication methods are those that rely on the user identity to authenticate a session (Sukumaran & Misbahuddin 2021). The goal of mobile cloud computing is to transfer resource overheads from the mobile client to the cloud. According to Jannath & S (2021), user-side authentication methods contravene this critical objective. This contradiction makes them less efficient and insecure for cloud-based mobile applications compared to cloud-to-client authentication mechanisms.

Other challenge in the MCC Security Modules is the protection of data. **Data protection** in the cloud is synonymous with securing data in traditional data centers. Data security in mobile cloud computing has the same dimensions, such as authentication and identity verification, access control mechanisms, encryption strategies, safe deletion, integrity validation, and information masking, as with traditional data centres (Bhatia, Verma & Sharma 2020). Correctly implemented data security mechanisms demonstrate due diligence concerning user privacy and information security requirements in a mobile cloud computing environment (Madhurya et al. 2021). Data security reduces the risk of exposure and malicious access and use of private information.

Security issues resulting from encryption are many and cannot be limited or limited to a specific time or period. **Encryption** is a type of information protection that transforms files into unreadable cyphers. An encryption key is a random string of bits made purposely for ciphering and deciphering information (Kruthika & Valarmathi 2018). Insecure mobile cloud computing, the longer the key, the harder it is to unscramble, meaning the underlying data is more secure. Symmetric encryption mechanisms use a single key to encrypt and decrypt data, but face one major drawback of the link

getting stolen; hence, it requires frequent change of the key (Kołodziej & Jaatun 2021b). A public encryption system implements different scrambling and unscrambling encryption keys. Because the key is not shared, this asymmetric form of security is believed to be more efficient.

A single point of failure (SPOF) is a non-redundant part of a system that will make the whole system to be dysfunctional if it fails. A single failure point represents a significant flaw in the design of the system because if a single malfunction renders the entire system dysfunctional (Abd Ali et al. 2019). A SPOF obscures the goal of high availability in mobile cloud computing because of the interdependencies that could be implicated in a single failure (A. Almusaylim & Jhanjhi 2020). Such parts are undesirable to systems that require high availability like cloud computing to ensure reliability. In addition to that, **Security threats** are a major security issue.

Security threats exist in many forms, including software attacks, denial of service attacks, theft of critical information such as intellectual property, identity theft, stealing of physical information and information systems, sabotage, or information coercion (Ogwara et al. 2021). Information systems, including mobile cloud computing environments, face constant threats that can cause different types of damage to persons and institutions (Joyner & Lotrionte 2017). Common effects include loss of confidentiality and integrity of the data and system unavailability. The saying that effective communication is not what but how it is said still anchors information sharing in mobile cloud computation. Efficiency in **communication channels** is even more relevant in the cloud environment where people access organizational resources anytime and anywhere (Irshad et al. 2020), and companies rely on effective communication to succeed in their operations (Sridhar & Smys 2020). Communication channel issues refer to barriers to information sharing and data transfers between different entities of a system. Common issues include poor or lack of feedback, system overhead, overall lack of communication, and device chaos (Zheng et al. 2019).

Furthermore, **Unproper access control** considered one of the security issues in delegation methods in MCC. It is Techniques for controlling access to resources in a computing environment from allowing access and use of these resources through authentication and authorization. When access control becomes a security issue, it means unauthorized access and use of resources in the mobile cloud computing environment. **Authorization** is granting permissions to the user to access resources. In mobile cloud computing, the security issue lies in accessing unauthorized resources. This issue is considered one of the most critical issues that many studies are working on solving and developing models to avoid this security problem(Carchiolo et al. 2019). The last MCC security issue is **Anonymity** which is the process of using resources by an anonymous person without a username or identity, and this is one of the most serious issues in cybersecurity, as it is possible to identify what this anonymous person is doing, but his identity cannot be identified, which is unlike privacy, which is likely to know the identity of the hacker, but not Can predict what he does(Yang, Huang & Liu 2016).

4.2.2. Security Modules of Delegation Methods in MCC identification

According to Figure 20 , fifty security modules were evaluated under four delegation methods. Each module was classified under its delegation method, and there were no subcategories. Nine security modules were evaluated under the Layering delegation method, twenty-three security modules under the Encryption delegation method, six security modules under Dynamic offloading, and twelve security modules under the Authentication method. It is essential to mention that the number of security modules evaluated does not impact the validity of the proposed evaluation method, as it serves only as a demonstration of its feasibility. According to (AlAhmad et al. 2021), there are other delegation methods such as Mirroring, Virtualization, and Third-Party Usage, but

these were not included in this study because the focus was on methods that have received a significant amount of attention in academic research.

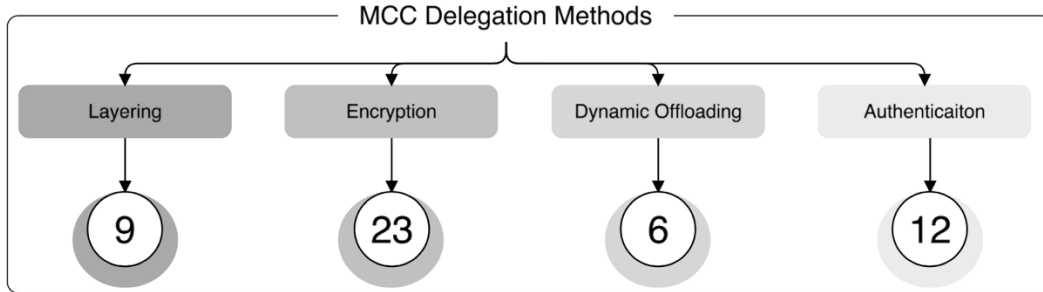


Figure 20: Number of system in each MCC delegation methods

4.2.3. Decision Matric formulation

In the proposed Modelling decision-based approach, four decision matrices serve as the main element to evaluate Security Modules of Delegation Methods in MCC. These matrices are created by intersecting 13 security evaluation criteria (General security issues, Privacy, Authentication (cloud to client authentication, Client to cloud authentication, and Multi-Factor Authentication), Data Security, Encryption key, single failure point, security threats, communication channels issues, Un proper access control, authorization issues and anonymity) with each security module of delegation methods in MCC. The representation of the decision matrices for category is shown in Table 12.

Table 12: Decision Matric formulation for all MCC delegation methods

Category (Delegation Method)	Alternatives (Security Modules)	Criteria				
		C1	C2	C3	...	C13
Layering	SM_01	C1/SM_01	C2/SM_01	C3/SM_01	...	C13/SM_01
	SM_02	C1/SM_02	C2/SM_02	C3/SM_02	...	C13/SM_02
	SM_03	C1/SM_03	C2/SM_03	C3/SM_03	...	C13/SM_03
	...	...	...	...	...	...
	SM_N	C1/SM N	C2/SM N	C3/SM N	...	C13/SM N
Encryption	SM_01	C1/SM_01	C2/SM_01	C3/SM_01	...	C13/SM_01
	SM_02	C1/SM_02	C2/SM_02	C3/SM_02	...	C13/SM_02
	SM_03	C1/SM_03	C2/SM_03	C3/SM_03	...	C13/SM_03
	...	...	...	...	...	...
	SM_N	C1/SM N	C2/SM N	C3/SM N	...	C13/SM N
Dynamic Offloading	SM_01	C1/SM_01	C2/SM_01	C3/SM_01	...	C13/SM_01
	SM_02	C1/SM_02	C2/SM_02	C3/SM_02	...	C13/SM_02
	SM_03	C1/SM_03	C2/SM_03	C3/SM_03	...	C13/SM_03
	...	...	...	...	...	...
	SM_N	C1/SM N	C2/SM N	C3/SM N	...	C13/SM N
Authentication	SM_01	C1/SM_01	C2/SM_01	C3/SM_01	...	C13/SM_01
	SM_02	C1/SM_02	C2/SM_02	C3/SM_02	...	C13/SM_02
	SM_03	C1/SM_03	C2/SM_03	C3/SM_03	...	C13/SM_03
	...	...	...	...	...	...
	SM_N	C1/SM N	C2/SM N	C3/SM N	...	C13/SM N
C1= General Security , C2= Privacy , C3=Authentication , C4=Cloud to Client Authentication , C5=Multi-factor authentication , C6=Communication channel, C7=Data Security, C8=Security Threats set, C9=Encryption Key , C10=Single Failure point, C11=un proper Access Control , C12=Authorization, C13=Anonymity						

The Security Modules in the above four delegation methods are evaluated objectively using a binary yes/no approach to indicate whether the criteria are included or not in a given system. The findings of this evaluation are discussed in Chapter 5. As stated in Chapter 1 and 2, three key challenges (multiple evaluation criteria, criteria importance, and data variation) must be addressed through the development of a decision-making solution. The solution proposed considers the significance of each criterion and benchmarks delegation method systems for each category. This will be discussed in the next section.

4.3. Formulation and Development phase

This phase includes two steps, as mentioned in Chapter 3, section 3.3.2. The First step is to develop and formulate FWZIC with PINHFS to assign weight to the security evaluation criteria. The second step is utilizing the EDAS method for Ranking the Security Modules of Delegation Methods in MCC. The result of this formulation and development is discussed in chapter 5, and this chapter represents the implementation of the below subsections.

4.3.1. PINHFS- FWZIC method

Determining criteria weights accurately can be challenging due to uncertainties. Real-life MCDM scenarios often involve working with ambiguous, imprecise, incomplete, or uncertain data. The FWZIC method as described in chapter 2, is a good way to find the criteria weights without inconsistencies. By incorporating the FWZIC method into the PINHFS environment, uncertainties and inaccuracies can be effectively addressed. The present study details the procedure for assigning weights to the predetermined security criteria of the Security Modules of Delegation Methods in MCC using the developed PINHFS-FWZIC method as shown in Figure21.

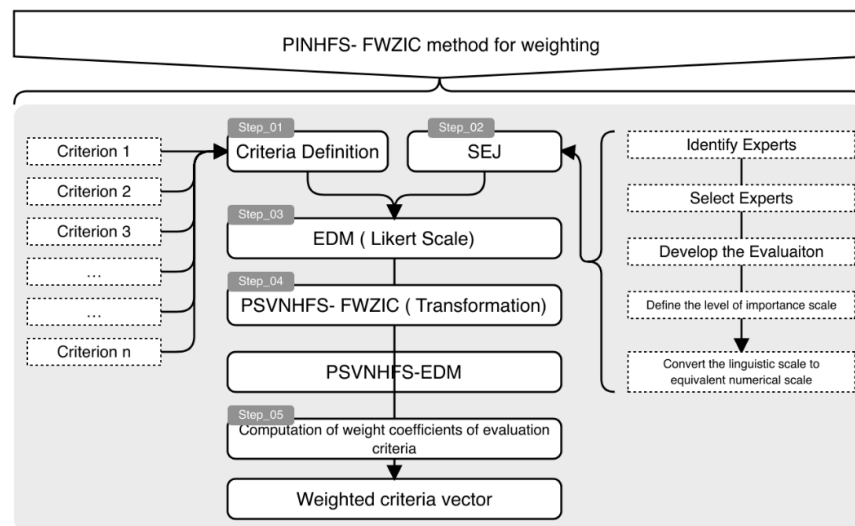


Figure 21: PINHFS-FWZIC weighting method

Step 01: Criteria Definition

In this step the exploration of the predefined security evaluation criteria for evaluating and benchmarking the MCC delegation method.

Step 02: Structured Expert Judgment (SEJ)

The present phase entails the identification and curation of subject matter experts hailing from the same academic domain, tasked with evaluating and ascertaining the significance of security evaluation criteria concerning MCC delegation methods systems. The preliminary phase involves exploring and cataloging potential experts, followed by a selection and nomination procedure, culminating in the formation of a SEJ panel. Subsequently, an evaluation form is developed to collate the opinions of all SEJ panel members concerning each criterion, and the translation of linguistic expressions into their corresponding numerical scales. The sub-steps of this process are expounded upon in greater detail below.

- I. At least three decision-makers with prior experience in security modules of delegation methods are identified and selected to construct a structured expert judgment (SEJ). In addition, an assessment form is designed and endorsed by the decision-makers in this step. The assessment form used in this study is provided in Appendix A. Choosing three experts offers practical advantages, including the avoidance of potential delays in the decision-making process. When involving a larger number of experts, the coordination and communication required among them can become increasingly time-consuming. The process of gathering input, sharing opinions, and reaching a consensus can be significantly delayed when multiple experts are involved. By limiting the number of experts to three, the decision-making process can be streamlined, enabling quicker responses and

reducing the potential for bottlenecks or communication challenges that may arise when engaging a larger group.

- II. Establish the importance scale. Three experts will appraise the importance of each security criterion using the five-point Likert scale as shown in Table13. This scale is preferred due to its ability to provide reliable quantitative data that can be easily analyzed and has a low potential for bias.
- III. Translate the linguistic expressions into equivalent numerical scores

Table 13: Linguistic Expressions and Corresponding Numerical Scales

Linguistic expressions	Numerical scoring scale
Very Important (VI)	1
Medium Important (MI)	2
Important (I)	3
Un Important (UI)	4
Very Un Important (VUI)	5

The employment of a Likert scale in the assessment of security evaluation criteria for MCC delegation methods involves the identification of discrete levels of importance that must be communicated by an individual expert. This process of assigning the degree of significance is facilitated through the use of a linguistic expressions scale that streamlines the evaluation criteria. According to (Qahtan, Alsattar, Zaidan, Deveci, Pamucar & Martinez 2023) , Experts preferred collecting data using a five-point Likert scale due to its simplicity and reduced complexity compared to higher scales, such as seven- and ten-point Likert scales. The wider range of these higher scales introduces difficulty and complexity in the comparison process. In contrast, the uncertainty associated with a five-point scale is limited to variations in expert opinions. The use of seven- or ten-point scales increases uncertainty by introducing two factors: diversity in expert opinions and the challenge of differentiating linguistic expressions. However, situations that

require differentiation between closely similar preferences or demand a high level of precision may benefit from the use of larger scales.

The aforementioned importance levels are demarcated by linguistic expressions that span a continuum ranging from "**very important**" to "**very unimportant**." Nonetheless, it may be difficult to extract relevant information from linguistic expressions while analyzing the scores provided by experts, unless they are converted into numerical values that can undergo necessary mathematical processing. Therefore, to facilitate the assessment of the degree of significance of the security evaluation criteria for Security Modules of Delegation Methods in MCC, each linguistic term has been assigned a corresponding numerical value.

Step 03: Building Expert Decision Matrix (EDM)

At this stage, the set of security evaluation criteria is matched with the inputs of the three decision-makers to create an Expert Decision Matrix (EDM). This EDM displays the assigned importance of all the criteria, as demonstrated in Table 14 below.

Table 14: Expert decision matrix (EDM)

Experts	Criteria				
	C1	C2	C3	...	C13
E1	Imp(E1/C1)	Imp(E1/C2)	Imp(E1/C3)	...	Imp(E1/C13)
E2	Imp(E2/C1)	Imp(E2/C2)	Imp(E2/C3)	...	Imp(E2/C13)
E3	Imp(E3/C1)	Imp(E3/C2)	Imp(E3/C3)	...	Imp(E3/C13)

Step 04: Utilize the PINHFS

The outcome of this step is to come up with the PINHFS-EDM. The Probabilistic Interval Neutrosophic Hesitant Fuzzy Set (PINHFS) is presented by (Shao et al. 2018) and expressed in the Equation 1:

$$N = \{ \langle x, M(x)|P^M(x), V(x)|P^V(x), N(x)|P^N(x) \rangle \mid x \in X \} \quad (1)$$

The tricomponent model proposed by (Shao et al. 2018) encompasses three distinct sets of potential elements, namely $(M(x)|P^M(x), V(x)|P^V(x) \text{ and } N(x)|P^N(x))$. These sets are composed of interval values between 0 and 1 within the unit interval, represent the feasible levels of membership hesitation, indeterminacy-membership hesitation, and falsity hesitation of an element $x \in X$ regarding the set N . The probabilities $P^M(x)$, $P^V(x)$, and $P^N(x)$ are associated with these three types of hesitation and provide additional information in a probabilistic format. Below is:

$$\tilde{\alpha} = [\alpha^L, \alpha^U] \subseteq [0, 1], \tilde{\beta} = [\beta^L, \beta^U] \subseteq [0, 1], \tilde{\gamma} = [\gamma^L, \gamma^U] \subseteq [0, 1];$$

$$0 \leq \sup \tilde{\alpha} + \sup \tilde{\beta} + \sup \tilde{\gamma} \leq 3;$$

$$P_a^M \in [0, 1], P_b^V \in [0, 1], P_c^N \in [0, 1], \sum_{a=1}^{\#M} P_a^M = 1, \sum_{b=1}^{\#V} P_b^V = 1, \sum_{c=1}^{\#N} P_c^N = 1;$$

$$\text{Where } \tilde{\alpha} \in M(x), \tilde{\beta} \in V(x) \text{ and } \tilde{\gamma} \in N(x). \tilde{\alpha}^+ = U_{\tilde{\alpha} \in M_A(x)} \max\{\tilde{\alpha}\}, \tilde{\beta}^+ =$$

$$U_{\tilde{\beta} \in V_A(x)} \max\{\tilde{\beta}\}, \tilde{\gamma}^+ = U_{\tilde{\gamma} \in N_A(x)} \max\{\tilde{\gamma}\}. P_a^M \in P^M, P_b^V \in P^V, P_c^N \in P^N$$

The symbols $\#M$, $\#V$ and $\#$ denote the total quantities of elements in the constituent

$$(M(x)|P^M(x), V(x)|P^V(x) \text{ and } N(x)|P^N(x)), \text{ respectively.}$$

Step 05: Final Value Calculation of Weight Coefficients for Security Evaluation Criteria

In this stage, the determination of the ultimate weights allocated to every security evaluation criterion in the delegation approach will be computed through the utilization of the PINHFS-EDM from the preceding phase. The following outlines the procedure.

- I. Utilize the “Probabilistic Interval Neutrosophic Hesitant Fuzzy Weighted Averaging” (PINHFWA) operator that presented in Equation 2 to aggregate the PINHFS for each criterion from the PINHFS-EDM of the three decision makers (Shao et al. 2018) .

$$\text{PINHFWA}(n_1, n_2, \dots, n_X) = \bigoplus_{j=1}^X w_j(n_j)$$

(2)

The following aggregation outcome can be attained through the utilization of PINHFWA

$$\begin{aligned} \text{PINHFWA}(n_1, n_2, \dots, n_X) = & U\{[1 - \prod_{j=1}^X (1 - \alpha_j^L)^{w_j}, 1 - \prod_{j=1}^X (1 - \alpha_j^U)^{w_j}] \\ & | \prod_{j=1}^X P_j^{M_j}\}, \{[\prod_{j=1}^X (\beta_j^L)^{w_j}, \prod_{j=1}^X (\beta_j^U)^{w_j}] | \prod_{j=1}^X P_j^{P_j}\}, \\ & \{[\prod_{j=1}^X (\gamma_j^L)^{w_j}, \prod_{j=1}^X (\gamma_j^U)^{w_j}] | \prod_{j=1}^X P_j^{N_j}\} \} \end{aligned}$$

Where $[\alpha_j^L, \alpha_j^U] = \tilde{\alpha}_j \in M_j$, $[\beta_j^L, \beta_j^U] = \tilde{\beta}_j \in P_j$, $[\gamma_j^L, \gamma_j^U] = \tilde{\gamma}_j \in N_j$,

$P_j^{M_j}$, $P_j^{P_j}$ and $P_j^{N_j}$ are corresponding hesitant probabilities of $\tilde{\alpha}_j \in M_j$, $\tilde{\beta}_j \in P_j$, $\tilde{\gamma}_j \in N_j$

$$j = 1, 2, \dots, X, w_j \text{ is the weight of } n_j \text{ and } \sum_{j=1}^X w_j = 1$$

- II. The fuzzy weights are defuzzied and transformed into crisp weights using the PINHFS score function, as described in Equation 3 (Shao et al. 2018)

For a PINHFN n , where $a = 1, 2, \dots, \#M$, $b = 1, 2, \dots, \#V$, $c = 1, 2, \dots, \#N$, the score function $s(n)$ is defined as:

$$s(\mathfrak{N}) = \frac{\sum_{a=1}^{\#M} (\alpha_a^L + \alpha_a^U) P_a^M + \sum_{b=1}^{\#V} (2 - (\beta_b^L + \beta_b^U)) P_b^V + \sum_{c=1}^{\#N} (2 - (\gamma_c^L + \gamma_c^U)) P_c^N}{6}$$

(3)

Where, The symbols ($\#M$, $\#V$ and $\#N$) represent the entire quantities of elements in the parts $M(x)|P^M(x)$, $V(x)|P^V(x)$, $N(x)|P^N(x)$ respectively.

III. The total weight of the primary criteria and every level of criteria must amount to 1, If this requirement is not fulfilled, Equation 4 is utilized to rescale the weights.

$$w_j = s(\mathfrak{N}) / \sum_{j=1}^J s(\mathfrak{N})$$

(4)

Here, $s(\mathfrak{N})$ denotes the weight allocated to each criterion

The five steps that were outlined earlier are executed autonomously for both the primary criterion and all criteria levels. This approach, as noted in (Qahtan, H.A.Alsattar, et al. 2022b), can result in more reasonable outcomes as it takes into account the actual weight of each criterion. The calculated weights are then input into EDAS to evaluate the MCC delegation methods. This process explained in the next section. The pseudocode for the PINHFS -FWZIC weighting method is presented in Algorithm below.

Step 1: Criteria Definition:	
identify $C[i]$	<i>// C is the set of criteria that have been identified</i>
Step 2: Structured Expert judgment (SEJ):	
Define $E[i]$	<i>// E refers to a group of individuals who are identified as potential expert panellists.</i>
Define EF, Imp	<i>// An evaluation form(EF) with an importance scale is created for the criteria in this step</i>
$m \leftarrow \text{length}(E)$	<i>// The evaluation form is allocated to the chosen</i>
For i in $\{1..m\}$	<i>experts who have agreed to participate</i>
if $E(i)$ is true then $E(i) \leftarrow EF(i)$	
endif	
endfor	
Step 3: Building Expert Decision Matrix (EDM):	

```

Initialize  $EDM[i, j] \leftarrow E \cup C$  // The EDM matrix is constructed by combining the
J  $\leftarrow$  length (C) // selected expert panellists and the criteria MCC
m  $\leftarrow$  length (E) // delegation methods using a crossover process.
For j in {1..J}
  For i in {1..m}
     $EDM[i, j] \leftarrow \text{Imp}(E_{ij}/C_{ij})$  // The score of importance assigned by the selected
  endfor // expert for each criterion is included in EDM.
endfor

```

Step 4: Utilize the PINHFS:

```

For j in {1..J}
  For i in {1..m}
     $\tilde{EDM}[i, j] \leftarrow EDM[i, j]$  // The EDM's linguistic term is converted into a
  endfor // PINHFS-EDM ((EDM) ~) by applying a
endfor // probabilistic interval neutrosophic hesitant fuzzy
// method as per Equation (1).

```

Step 5: Final Value Calculation of Weight Coefficients for Security Evaluation Criteria:

Step 5.1: Use (PINHFWA) to aggregate the PINHFS for each criterion

```

For j in {1..J}
   $\tilde{C}_j = \sum_{i=1}^m \text{Imp}(\tilde{E}_{ij}/\tilde{C}_{ij})$  // To compute the aggregation of the fuzzification
endfor // data, Equation (2) is utilized

```

Step 5.2: Convert the fuzzy weights into crisp weights using the PINHFS score function

```

For j in {1..J}
  s(J) // The fuzzy weights are converted into
  
$$= \frac{\sum_{a=1}^{\#M} (\alpha_a^L + \alpha_a^U) P_a^M + \sum_{b=1}^{\#V} (2 - (\beta_b^L + \beta_b^U)) P_b^V + \sum_{c=1}^{\#N} (2 - (\gamma_b^L + \gamma_b^U)) P_c^N}{6}$$
 // crisp weights using the PINHFS score
  endfor // function specified in Equation 3

```

Step 5.3: Compute the ultimate weight.

```

For j in {1..J}
   $w[j] \leftarrow s[j] / \sum_{j=1}^J s[j]$  // The computation of the final weight
  // for each criterion is performed using
  // Equation 4

```

endfor

4.3.2. Utilizing EDAS method

This section illustrates the approach of benchmarking the MCC delegation methods using EDAS methods. PINHFS -FWZIC provides the weight for each criterion, which will feed the EDAS for this benchmarking approach. Below are the steps of integrating PINHFS -FWZIC with EDAS (Ghorabae et al. 2015).

- **Step 01:** Build the decision matrix $\mathbf{X}$ as below:

$$X = [X_{ij}]_{n \times m} = \begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1m} \\ X_{21} & X_{22} & \cdots & X_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ X_{n1} & X_{n2} & \cdots & X_{nm} \end{bmatrix},$$

The value of alternative i^{th} performance on criterion j^{th} is designated as X_{ij} which all details in the next chapter. Section 4.2.3 presented the design matrixes of this research .

- **Step 02:** Compute the average solution across all criteria by using the below Equation 5:

$$AV = [AV_j]_{1 \times m} \quad (5)$$

$$\text{where } AV_j = \frac{\sum_{i=1}^n X_{ij}}{n}$$

- **Step 03:** Calculate the (PDA) and (NDA) matrices according to criteria type by using Equations 6 and 7

$$PDA = [PDA_{ij}]_{n \times m} \text{ where } PDA_{ij} = \frac{\max(0, (X_{ij} - AV_j))}{AV_j} \quad (6)$$

$$NDA = [NDA_{ij}]_{n \times m} \text{ where } NDA_{ij} = \frac{\max(0, (AV_j - X_{ij}))}{AV_j}$$

(7)

- **Step 04:** Calculate the combined weighted sum of PDA and NDA for every alternative by using Equations 8 and 9

$$SP_i = \sum_{j=1}^m w_j PDA_{ij}$$

(8)

$$SN_i = \sum_{j=1}^m w_j NDA_{ij}$$

(9)

Where w_j is the criterion weight resulted from PINHFS -FWZIC

- **Step 05:** Normalize the SP and SN values for each alternative by using Equations 10 and 11

$$NSP_i = \frac{SP_i}{\max_i(SP_i)}$$

(10)

$$NSN_i = 1 - \frac{SN_i}{\max_i(SN_i)}$$

(11)

- **Step 06:** Determine the appraisal score (AS) for all alternatives by using the Equation 12

$$AS_i = \frac{1}{2} (NSP_i + NSN_i)$$

(12) Where $0 \leq AS_i \leq 1$

- **Step 07:** Arrange the options in descending order of their appraisal score (AS), and select the alternative with the highest AS as the best choice among the options available

The pseudocode for the EDAS method is shown in Algorithm below.

input:

- matrix_a of size $i \times j$ representing the evaluation of i alternatives with j criteria.
- weight_vector of size j representing the importance of each criterion.

output:

- ranking of the alternatives based on their relative closeness values
-

Step 1: Calculate the average solution

$$AV = \text{sum}(X, \text{axis}=0) / n$$

Step 2: Calculate the PDA and NDA matrices based on the criteria type

```
for i = 1 to n do
  for j = 1 to m do
    if  $X[i, j] \geq AV[j]$  then
       $PDA[i, j] = (X[i, j] - AV[j]) / AV[j]$ 
       $NDA[i, j] = 0$ 
    else
       $PDA[i, j] = 0$ 
       $NDA[i, j] = (AV[j] - X[i, j]) / AV[j]$ 
    end if
  end for
end for
```

Step 3: Determine the weighted sum of PDA and NDA for all alternatives

```
for i = 1 to n do
   $SP[i] = 0$ 
   $SN[i] = 0$ 
  for j = 1 to m do
     $SP[i] = SP[i] + w[j] * PDA[i, j]$ 
     $SN[i] = SN[i] + w[j] * NDA[i, j]$ 
  end for
end for
```

Step 4: Normalize the values of SP and SN for all alternatives

$$\text{max_SP} = \text{max}(SP)$$

$$\text{max_SN} = \text{max}(SN)$$

```

for i = 1 to n do
    NSP[i] = SP[i] / max_SP
    NSN[i] = 1 - SN[i] / max_SN
end for

```

Step 5: Determine the appraisal score (AS) for all alternatives

```

for i = 1 to n do
    AS[i] = 0.5 * (NSP[i] + NSN[i])
end for

```

Step 6: Rank the alternatives based on the decreasing values of the appraisal score

```

for i = 1 to n do
    ranking[i] = i
end for
for i = 1 to n - 1 do
    for j = i + 1 to n do
        if AS[rating[i]] < AS[rating[j]] then
            temp = ranking[i]
            ranking[i] = ranking[j]
            ranking[j] = temp
        end if
    end for
end for

```

Step 7: Return the appraisal scores and the ranking of alternatives based on decreasing values of AS. The optimal choice is the one with the highest AS value.

```

return AS, ranking

```

4.4.Chapter Summary

Chapter 4 provides an in-depth exploration of the Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing. The chapter begins with an introduction, followed by the identification of the decision matrix, which involves the evaluation of security criteria and the identification of Security Modules of Delegation Methods in MCC. The decision matrix formulation is then presented, leading to the formulation and development phase, which includes the PINHFS-FWZIC method and the utilization of EDAS method. Finally, the chapter concludes with a summary of the key points discussed.

CHAPTER 5: FINDINGS AND DISCUSSION

5.1.Introduction

The result of a proposed methodology, the Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing, are presented in this chapter. The outcomes are organized into three segments, wherein decision matrices for four delegation methods are depicted in Section 5.2.1. The outcome of the PINHFS-FWZIC method, which allocate the weight of security evaluation criteria, are expounded upon in Section 5.2.2. Meanwhile, Section 5.2.3 showcases the rankings of each securitymodules utilizing the EDAS method across delegation categories. The validation and evaluation techniques are analyzed in Section 5.3, which includes a sensitivity analysis in Section 5.3.1, a systematic ranking in Section 5.3.2, and a benchmarking checklist validation in Section 5.3.3. This chapter concludes with a comprehensive summary in Section 5.5 and an overview of the methodology outcomes in Figure 22.

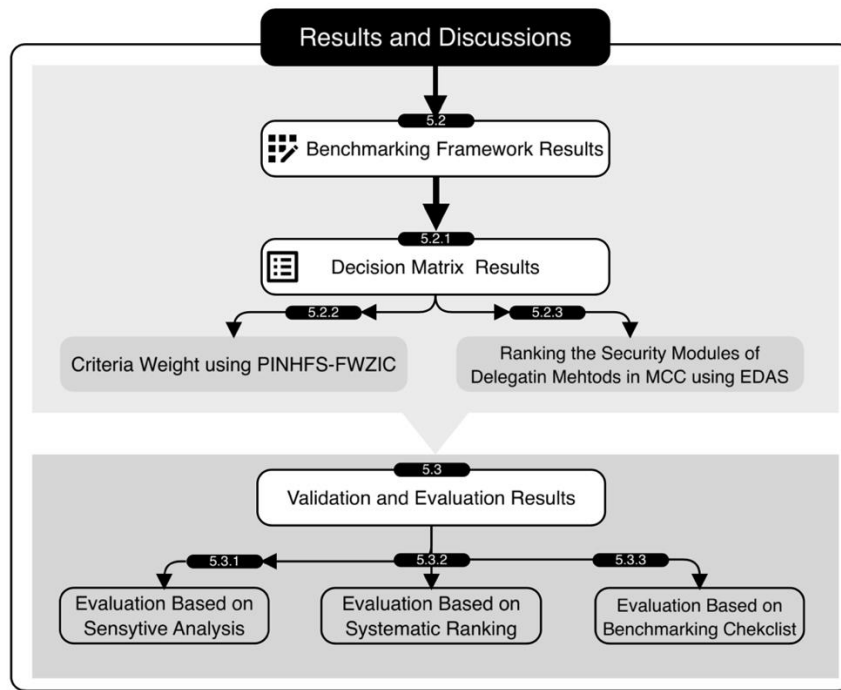


Figure 22: Benchmarking Framework Results for MCC delegation method systems: An Overview

5.2.Benchmarking framework result

This section is structured into three sub-sections, with the presentation of decision matrices for four distinct delegation methods in Section 5.2.1. The outcomes of the PINHFS-FWZIC methodology, which assign the weighting of security evaluation criteria, are thoroughly discussed in Section 5.2.2. Additionally, Section 5.2.3 displays the evaluation of each alternative through the EDAS methodology, providing rankings across the delegation categories.

5.2.1. Decision Matrix Results

In this section, the decision matrices for Security Modules of Delegation Methods in MCC, as formulated in Chapter 4, Section 4.2, are presented. Four decision matrices for Security Modules of Delegation Methods in MCC were constructed by intersecting 50 Security modules of four delegation methods with 13 security evaluation criteria. The Layering delegation method decision matrix is presented in Table 15, while the decision matrices for the remaining delegation methods, namely Encryption, Dynamic offloading, and Authentication, are presented in Appendix B in Tables 27, Table 28 and Table 29 respectively.

Table 15: Layering Delegation Method Decision matrix

Delegation Method	MCC Modules	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity
Layering	SM_01	1	1	1	0	1	1	0	1	1	1	1	1	1
	SM_02	1	1	1	0	1	1	0	0	1	1	1	0	1
	SM_03	1	1	1	0	0	1	0	1	1	1	1	1	1
	SM_04	1	0	1	0	1	0	1	0	1	1	1	1	1
	SM_05	1	0	0	0	0	0	0	0	0	0	1	1	1
	SM_06	1	0	1	0	1	1	1	1	1	1	1	1	1
	SM_07	1	1	1	0	1	1	1	1	1	1	1	1	1
	SM_08	1	1	1	0	1	0	1	1	1	1	1	1	1
	SM_09	1	1	1	0	1	0	1	1	1	1	1	1	1

The table above and those found in Appendix B represents the decision matrices that are the basis for benchmarking Security Modules of Delegation Methods in MCC. These tables showcase the scores assigned to each evaluated system based on the predefined criteria. The presence or absence of security evaluation criteria was recorded as 'Yes' or 'No', and these values were converted into binary values of '1' and '0' for the purpose of this research. As discussed previously, following the creation of the decision matrices, three significant concerns (multiple evaluation criteria, importance of criteria, and data variation) were addressed through the development of a Multi-Criteria Decision Making (MCDM) solution, which is the (integrated EDAS with PINHFS-FWZIC), which is presented in Chapter 4. The results and discussions of the overall outcome are shown in the following section.

5.2.2. Determining Criteria Weight Result Using PINHFS -FWZIC

This section presents the weighted outcomes of the security evaluation criteria used to benchmark Security Modules of Delegation Methods in MCC, as developed in Chapter 4, Section 4.3.1. The

PINHFS-FWZIC approach was used to form these results. Upon completing the necessary steps, the PINHFS -FWZIC method produced aggregated consistent weights. Table 16 shows the preference of experts for the MCC delegation methods systems security evaluation criteria.

Table 16: Expert Preference for Delegation Methods in MCC Systems Security Evaluation Criteria

Experts	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity
Expert 1	VUI	MI	VI	MI	UI	UI	VI	UI	I	VUI	I	I	UI
Expert 2	VUI	MI	MI	MI	UI	UI	VI	VUI	I	VUI	I	I	UI
Expert 3	VUI	I	VI	MI	UI	VUI	VI	VUI	MI	UI	UI	I	I
(VI) = Very Important, (MI) = Medium Important, (I) = Important , (UI) = Un Important, (VUI) = Very Un Important													

In the next step as shown in Table 17, the linguistic expressions of preferences are converted into numerical values, as illustrated in Chapter 4 , Table 13 .

Table 17: EDM of MCC delegations method systems

Experts	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity
Expert 1	5	2	1	2	4	4	1	4	3	5	3	3	4
Expert 2	5	2	2	2	4	4	1	5	3	5	3	3	4
Expert 3	5	3	1	2	4	5	1	5	2	4	4	3	3

According to Chapter 4, Section 4.3.1 in step 4, **Equation 1**, the PINHFS membership function is used to transform numerical scale to equivalent fuzzy numbers as shown in Table 18. It's worth to mention that Neutrosophic theory is characterized by its three essential components, namely, membership (M), non-membership (V), and hesitation (N). Given that it belongs to the family of fuzzy sets, specifically to the type of hesitant fuzzy set, each element in the set has more than one value. For instance, for membership, there are two values M1 and M2, for non-membership, two values V1 and V2, and for hesitation, two values N1 and N2. Additionally, because it is a type of interval fuzzy set, there exists an upper and lower limit for each value, namely, M1, M2, V1, V2, N1, and N2. Furthermore, since it is a fuzzy set, it is probabilistic, and therefore, each value, such as M1, M2, V1, V2, N1, and N2, is assigned a probability value, such as P1 for M1, P2 for M2, and so forth for non-membership and hesitation values.

Table 18: Corresponding (PINHFN) for Each Linguistic Term

Linguistic expressions	Membership						Non-Membership						Hesitant					
	M						V						N					
	M1			M2			V1			V2			N1			N2		
	M1 L	M1 U	P1	M2 L	M2 U	P2	V1 L	V1 U	P1	V2 L	V2 U	P2	N1 L	N1 U	P1	N2 L	N2 U	P2
VI	0.95	1	0.8	0.9	0.95	0.2	0	0.05	0.8	0.05	0.1	0.2	0	0.05	0.8	0.05	0.1	0.2
MI	0.75	0.8	0.7	0.7	0.75	0.3	0.2	0.25	0.7	0.25	0.3	0.3	0.2	0.25	0.7	0.25	0.3	0.3
I	0.55	0.6	0.5	0.5	0.55	0.5	0.4	0.45	0.5	0.45	0.5	0.5	0.4	0.45	0.5	0.45	0.5	0.5
UI	0.35	0.4	0.7	0.25	0.35	0.3	0.6	0.65	0.7	0.65	0.75	0.3	0.6	0.65	0.7	0.65	0.75	0.3
VUI	0.15	0.2	0.8	0.1	0.15	0.2	0.8	0.85	0.8	0.85	0.9	0.2	0.8	0.85	0.8	0.85	0.9	0.2

As per Chapter 4, Section 4.3.1, after aggregating the PINHFS using the PINHFWA operator, as demonstrated in **Equation 2**, the fuzzy weights are converted into crisp weights using the PINHFS score function presented in **Equation 3**, which involves defuzzification. The criteria weight is then

determined by weighting the primary criteria and each criterion level in a way that results in a total weight of 1 and **Equation 4** implemented for rescaling if this condition is not met.

As a result, from Chapter 4 section 4.3.1, Table 19 lists the criteria weights for evaluating delegation methods systems. The weight for each criterion is given as a decimal value, which represents the relative importance of each criterion in the evaluation of Security Modules of Delegation Methods in MCC. The higher the weight, the more important the criterion is considered in the evaluation process. The highest weight as per table is 0.2512357 for the criterion "Data Security ," which indicates that it is considered as the most important criterion in the evaluation process. The lowest weight in the table is 0.013898136 for the criterion "General Security," which indicates that it is considered as the least important criterion in the evaluation process. As for the rest of the criteria, they are arranged from most important to least as follows: (Authentication ,Cloud to Client Authentication , Privacy , Encryption Key , Authorization , un proper Access Control , Anonymity , Multi-factor authentication , Communication channel, Single Failure point , Security Threats set).

Table 19: Security evaluation Criteria's weight

Security Evaluation Criteria	Weight
Data Security	0.2512356546
Authentication	0.2371791082
Cloud to Client Authentication	0.0958342328
Privacy	0.0836359227
Encryption Key	0.0708239452
Authorization	0.0573672327
un proper Access Control	0.0493412264
Anonymity	0.0410871264
Multi-factor authentication	0.0325984486
Communication channel	0.0264880674
Single Failure point	0.0202554496
Security Threats set	0.0202554496
General Security	0.0138981356

Each weight in the table represents the relative importance of a particular criterion in the evaluation process, and the sum of all the weights should equal 1, indicating that all criteria are considered in the evaluation and none are omitted. For example, the weight of 0.083635923 for "Privacy" indicates that it is considered as an important criterion, but not as significant as "Authentication." The weight of 0.095834233 for "Cloud to Client Authentication" indicates that it is considered as a slightly more important criterion compared to "Privacy."

5.2.3. Ranking Result of Security Modules of Delegation Methods in MCC using EDAS

The EDAS methodology, as described in Chapter 4, Section 4.3.2, was employed to benchmark the various Security Modules of Delegation Methods in MCC. The extracted weights of the evaluation criteria that generated from PINHFS-FWZIC were utilized as input for the EDAS method with four various decision matrices. This served as a means of benchmarking the Security Modules of Delegation Methods in MCC.

After defining the decision matrix with the assigned weight for each security evaluation criterion, computing the average solution (AV) for each criterion in the EDAS method is calculated using Equation 5 then PDA (Positive Distance from Average) and NDA (Negative Distance from Average) were calculated using Equations 6 and 7 respectively where this is the third step. In the fourth step, the summation of PDA (SP_i) and NDA (SN_i) for all alternatives need to be calculated by using Equations 8 and 9 respectively then the result of this step will be normalized by calculating SP and SN using (Equation 10 and 11 respectively which normalize some of the positive distances and negative distances in step five. After that, step six will take the average of (NSP_i) and (NSN_i) to rank the alternatives using Equation 12 to calculate the appraisal score (AS_i), where the one with the highest AS is the optimal choice.

Table 20: layering delegation method alternatives result based on EDAS method

MCC Layering delegation method systems	EDAS					Rank
	SP	SN	NSP	NSN	AS	
SM_01	0.13065299	0.34706989	0.19586354	0.58598677	0.19586354	6
SM_02	0.11335436	0.42469257	0.16993094	0.49339212	0.16993094	8
SM_03	0.12133915	0.37966834	0.18190104	0.54710069	0.18190104	7
SM_04	0.25850558	0.22621367	0.38752896	0.73015391	0.38752896	5
SM_05	0.0071709	0.83830628	0.01074999	0	0.01074999	9
SM_06	0.62524358	0.08363467	0.93731048	0.90023376	0.93731048	2
SM_07	0.66706133	0	1	1	1	1
SM_08	0.31045106	0.1223223	0.46540108	0.854084	0.46540108	3
SM_09	0.31045106	0.1223223	0.46540108	0.854084	0.46540108	3

Table 20 displays the results of the EDAS evaluation method for assessing the performance of different Security Modules for **layering delegation method**. SM_07 came out on top, securing first place with an average score of 1. In second place is SM_06, which had an average score of 0.9. The third-ranked modules were SM_08 and SM_09, which both had an average score of 0.4. SM_04 came in fourth, followed by SM_01, System_03, SM_02, and finally SM_05, which was

ranked last with an average score of 0.01 and it was lower compared to the other security modules in the ranking. This security module may not be considered as one of the option among the MCC layering delegation methods when compared to the others. This ranking order can be used as a reference for choosing the most suitable security modules among the MCC layering delegation method.

Table 21: : Encryption delegation method alternatives result based on EDAS method

MCC Encryption delegation method systems	EDAS					Rank
	SP	SN	NSP	NSN	AS	
SM_01	0.10745325	0.39641111	0.04662625	0.4435868	0.04662625	17
SM_02	0.08715572	0.41789383	0.03781872	0.41343309	0.03781872	20
SM_03	0.03175973	0.71244017	0.01378122	0	0.01378122	23
SM_04	0.08715572	0.41789383	0.03781872	0.41343309	0.03781872	20
SM_05	0.10745325	0.39641111	0.04662625	0.4435868	0.04662625	17
SM_06	0.22114807	0.16665818	0.09596086	0.76607414	0.09596086	13
SM_07	2.30456544	0.23717911	1	0.66708909	1	1
SM_08	0.09532533	0.45096126	0.04136369	0.36701877	0.04136369	19
SM_09	0.06221997	0.584249	0.02699857	0.17993255	0.02699857	22
SM_10	0.14415506	0.60096876	0.06255195	0.15646424	0.06255195	15
SM_11	0.24614476	0.09583423	0.10680745	0.86548452	0.10680745	2
SM_12	0.237283	0.11608968	0.10296215	0.83705343	0.10296215	8
SM_13	0.24056832	0.1223223	0.10438772	0.82830516	0.10438772	5
SM_14	0.11215241	0.34706989	0.04866532	0.51284346	0.04866532	16
SM_15	0.22114807	0.16665818	0.09596086	0.76607414	0.09596086	13
SM_16	0.24068121	0.15320147	0.1044367	0.78496234	0.1044367	4
SM_17	0.237283	0.11608968	0.10296215	0.83705343	0.10296215	8
SM_18	0.237283	0.11608968	0.10296215	0.83705343	0.10296215	8
SM_19	0.24056832	0.1223223	0.10438772	0.82830516	0.10438772	5
SM_20	0.237283	0.11608968	0.10296215	0.83705343	0.10296215	8
SM_21	0.24056832	0.1223223	0.10438772	0.82830516	0.10438772	5
SM_22	0.237283	0.11608968	0.10296215	0.83705343	0.10296215	8
SM_23	0.24304015	0.12843268	0.10546029	0.81972847	0.10546029	3

The **Encryption** technique as a means of delegation is a widely utilized method within the realm of MCC and has been subject to substantial investigation by researchers. The present study, as depicted in Table 21 analyzed 23 security modules utilizing the EDAS method for ranking purposes. Upon application of the EDAS method, SM_07 was determined to be the most advantageous, with an AV value of 1, thereby providing the greatest probability of selection. Conversely, SM_03 was found to be the lowest ranked, with an AV of 0.01, thus rendering it the least likely option for consideration.

Table 22: : Dynamic Offloading delegation method alternatives result based on EDAS method

MCC Dynamic offloading delegation method systems	EDAS					Rank
	SP	SN	NSP	NSN	AS	
SM_01	0.2613634	0.2502941	0.5516368	0.2788366	0.5516368	3
SM_02	0.4737961	0.0202554	1	0.9416387	1	1
SM_03	0.4737961	0.0202554	1	0.9416387	1	1
SM_04	0.0410197	0.3470699	0.0865767	0	0.0865767	4
SM_05	0.0410197	0.3470699	0.0865767	0	0.0865767	4
SM_06	0.0410197	0.3470699	0.0865767	0	0.0865767	4

In regards to the **dynamic offloading delegation technique**, this study analyzed six security modules and applied the EDAS method for ranking purposes as shown in Table 22. The results of the analysis revealed that SM_02 and SM_03 emerged as the top ranking, each with an AV value of 1. Subsequently, SM_01 was ranked second with an AV of 0.5. Lastly, the remaining security modules, SM_04, SM_05, and SM_06, were found to have an average score of 0.08 and thus may be deemed unsuitable for selection.

Finally, Table 23 displays the results of the analysis of the **Authentication delegation method**, where 12 security modules were evaluated and arranged according to the EDAS Method. The results indicate that SM_02 and SM_03 emerged as the top ranking, each with an AV value of 1, rendering them the most trustworthy and secure options for selection. Conversely, SM_01 was ranked last with an AV of 0.04, making it a less favorable option in terms of safety and reliability.

The remaining security modules were situated between the highest and lowest ranked security modules, with average scores ranging from 0.4 to 0.2.

Table 23: : Authentication delegation method alternatives result based on EDAS method

MCC Authentication delegation method systems	EDAS					Rank
	SP	SN	NSP	NSN	AS	
SM_01	0.03007794	0.584249	0.04737676	0	0.04737676	12
SM_02	0.63486693	0.23717911	1	0.59404447	1	1
SM_03	0.63486693	0.23717911	1	0.59404447	1	1
SM_04	0.14191568	0.36732534	0.2235361	0.37128632	0.2235361	11
SM_05	0.2675335	0.11608968	0.42140091	0.80130101	0.42140091	4
SM_06	0.15569577	0.33301334	0.24524158	0.4300147	0.24524158	8
SM_07	0.26281187	0.15320147	0.41396372	0.73778052	0.41396372	5
SM_08	0.25993024	0.19972561	0.40942476	0.65814985	0.40942476	7
SM_09	0.14866749	0.34706989	0.23417111	0.40595553	0.23417111	9
SM_10	0.27244392	0.11608968	0.42913547	0.80130101	0.42913547	3
SM_11	0.26281187	0.15320147	0.41396372	0.73778052	0.41396372	5
SM_12	0.14625949	0.37355795	0.23037818	0.36061858	0.23037818	10

It is noteworthy that the significance of criteria weights plays a crucial role in system ranking, as exemplified by the layering delegation method employed in SM_08 and SM_01. SM_08 considered 11 criteria but excluded "Cloud to Client Authentication" and "Communication Channel Issues" in its assessment, while SM_01 ignored "Cloud to Client Authentication" and "Data Security Issues". Despite these discrepancies, SM_08 ranked third, whereas SM_01 ranked sixth, indicating the critical role of criteria weights in changing rankings. The weights of the security criteria excluded from both security modules were as follows: "Cloud to Client Authentication" ($W=0.095834$), "Communication Channel Issues" ($W=0.032598$), and "Data Security Issues" ($W=0.2512356$). The absence of "Data Security Issues," with its high weight, significantly impacted System_01's ranking.

5.3.Validation and Evaluation Results

This section will present the results of the model validation through systematic analysis and ranking. Additionally, the results of the decision evaluation validation will be displayed using a benchmarking checklist.

5.3.1. Sensitivity Analysis Result

The objective of sensitivity analysis is to modify the criteria that exert the most significant influence on the ultimate decision and to assess the stability of the decision by altering the input data. In this study, the impact of modifying the criteria weights on the results of the proposed Modeling Decision-Based Approach (EDAs with PINHFS-FWZIC) will be analyzed. Consequently, the relative weights of each criterion were calculated utilizing Equation in section 3.4.1 leading to the creation of nine scenarios of modified criteria weights in all security modules of delegation methods (Layering , Encryption , Dynamic Offloading and Authentication). Moreover, the elasticity coefficient (α_c) was calculated for all the criteria Security Modules of Delegation Methods in MCC , as depicted in Table 24.

Table 24: Criteria Weighting for MCC Security evaluation criteria in nine Scenarios

	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity
Initial Weight	0.01389 8	0.08363 6	0.23717 9	0.09583 4	0.03259 8	0.02648 8	0.25123 6	0.02025 5	0.07082 4	0.02025 5	0.04934 1	0.05736 7	0.04108 7
S1	0.01856 1	0.11169 9	0.31676 1	0.12799 1	0.04353 6	0.03537 6	0.00E+0 0	0.02705 2	0.09458 8	0.02705 2	0.06589 7	0.07661 6	0.05487 3
S2	0.01624 1	0.09773 6	0.27716 6	0.11199 1	0.03809 4	0.03095 4	0.125 0	0.02367 2	0.08276 4	0.02367 2	0.05766 7	0.06703 9	0.04801 4
S3	0.01392 1	0.08377 4	0.23757 1	0.09599 2	0.03265 2	0.02653 2	0.25 0	0.02028 9	0.07094 1	0.02028 9	0.04942 3	0.05746 2	0.04115 5
S4	0.01160 1	0.06981 2	0.19797 5	0.07999 4	0.02721 8	0.02211 8	0.375 0	0.01690 7	0.05911 7	0.01690 7	0.04118 6	0.04788 5	0.03429 6
S5	0.00928 1	0.05584 9	0.15838 5	0.06399 5	0.02176 8	0.01768 8	0.5 0	0.01352 6	0.04729 4	0.01352 6	0.03294 8	0.03830 8	0.02743 7
S6	0.00696 1	0.04188 7	0.11878 5	0.04799 6	0.01632 6	0.01326 6	0.625 0	0.01014 4	0.03547 7	0.01014 4	0.02471 1	0.02873 1	0.02057 7
S7	0.00464 1	0.02792 5	0.07919 5	0.03199 7	0.01088 4	0.00884 4	0.75 0	0.00676 3	0.02364 7	0.00676 3	0.01647 4	0.01915 4	0.01371 8
S8	0.00232 1	0.01396 2	0.03959 5	0.01599 9	0.00544 2	0.00442 2	0.875 0	0.00338 1	0.01182 3	0.00338 1	0.00823 7	0.00957 7	0.00685 9
S9	1.00E-05	1.00E-05	1.00E-05	1.00E-05	1.00E-05	1.00E-05	0.99988	1.00E-05	1.00E-05	1.00E-05	1.00E-05	1.00E-05	1.00E-05
alpha	0.01856 1	0.11169 9	0.31676 1	0.12799 1	0.04353 6	0.03537 6	0.33553 4	0.02705 2	0.09458 8	0.02705 2	0.06589 7	0.07661 6	0.05487 3

The comparative analysis of the nine **Security Modules of Layering delegation method** was performed using varying (α) values, as illustrated in the visual representation provided in Figure 23. Irrespective of the (α) value or scenario, a consistent benchmark for eight security modules was observed same as PINHFS-FWZIC expect SM_01(Ogwara et al. 2021). As shown in Figure 23 the ranking of four security modules in first scenario S1 varied from their previous arrangement. SM_01 rose from the 6th place to the 3rd, while SM_02 moved from 8th to 5th. As for the third and fourth security modules, they were ranked 7th and 5th respectively by PINHFS- FWZIC, but according to S1, they both came in at 4th and 5th. On the other hand, the remaining security modules from the 5th to the 9th retained their original rankings for all α values. As for the rest of the scenarios, the evaluation of the security moduels is equal to what was stated in PINHFZ-FWZIC

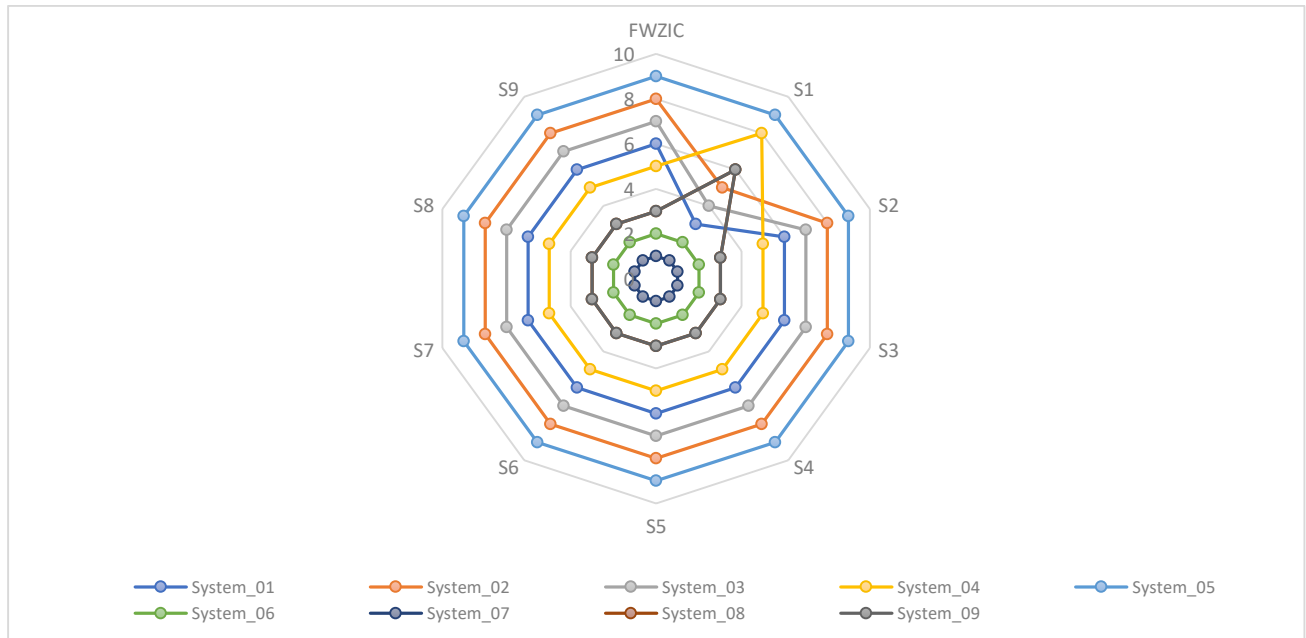


Figure 23 : Sensitivity Analysis of Layering Delegation Method Alternatives Benchmarking in nine scenarios

The order of the **Security Modules of Encryption delegation method** is different based on the first, second, and ninth scenarios. In the **(S1)**, the ranking was different for all options except for SM_07 which remained unchanged and was first in all scenarios. Figure 24 shows that eight Security modules improved their ranking, such as SM_01 and SM_05 which rose from 17th to 5th and SM_02 and SM_05 which rose from 20th to 17th. SM_03 increased by one place from 23rd to 22nd, while SM_08 rose from 19th to 16th and SM_09 rose from 22nd to 21st. SM_14 showed a significant improvement and became second after previously being ranked 16th. On the other hand, the rest of the 14 security modules saw a decline in their rankings. SM_06 fell from 13th to 19th and SM_10 dropped from 15th to the last place at 23rd. SM_11 fell one rank from second to third. Five security modules, SM_12, SM_17, SM_18, SM_20 and SM_22, dropped from 5th to 11th, while SM_13, SM_19 and SM_21 went from 5th to 8th. Lastly, SM_15, SM_16 and SM_23 dropped from 13th, 4th and 3rd to 19th, 7th and 4th respectively. In the second scenario **(S2)**, there was a change for seven security modules, with six of them showing an improvement in their

ranking and only one declining. SM_01 and SM_05 only moved up one spot, from 17th to 16th, while SM_02 and SM_04 rose from 20th to 19th. Additionally, SM_08 moved from 19th to 18th and SM_14 increased from 16th to 15th by only one place. Conversely, SM_10 experienced a significant drop, falling from 15th to 21st. The rest of the security modules did not see any change and remained in the same order of PINHFZ-FWZIC. Regarding the final (S9) scenario, it is worth noting that there were certain security modules whose hierarchical position exhibited a notable ascension. Specifically, both SM_06 and SM_15, previously situated at the 13th rank, elevated to the 8th rank, whereas SM_09, originally positioned at the 22nd rank, progressed to the 19th rank. Conversely, other security modules experienced a slight decline, exemplified by SM_08 that descended from the 19th to the 22nd rank. Additionally, SMs 12, 17, 18, 20, and 22, hitherto occupying the 8th rank, experienced a decrement in rank, all dropping two positions to the 10th rank.

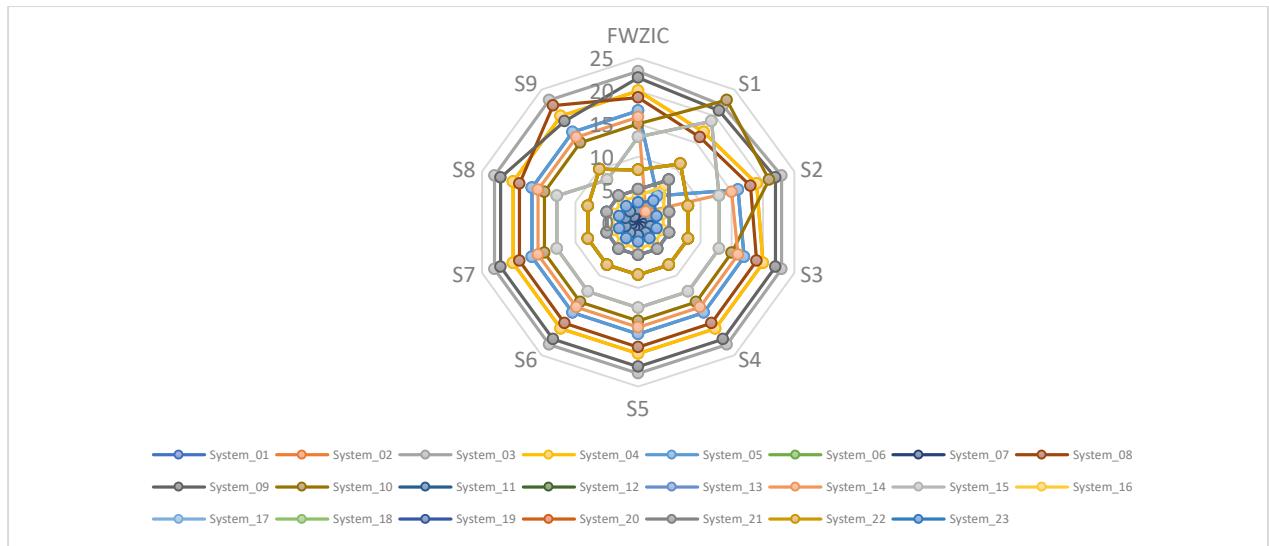


Figure 24 : Sensitivity Analysis of Encryption Delegation Method Alternatives Benchmarking in nine scenarios

As shown in Figure 25 In relation to the **Security modules of Dynamic Offloading delegation method alternatives**, the alteration in the ordering of security modules was only observed in the

first scenario, wherein SM_01 exhibited a decrement in rank from third to sixth. However, in the succeeding scenarios, the security modules adhered to the same sequential arrangement as prescribed in the PINHFZ-FWZIC protocol.

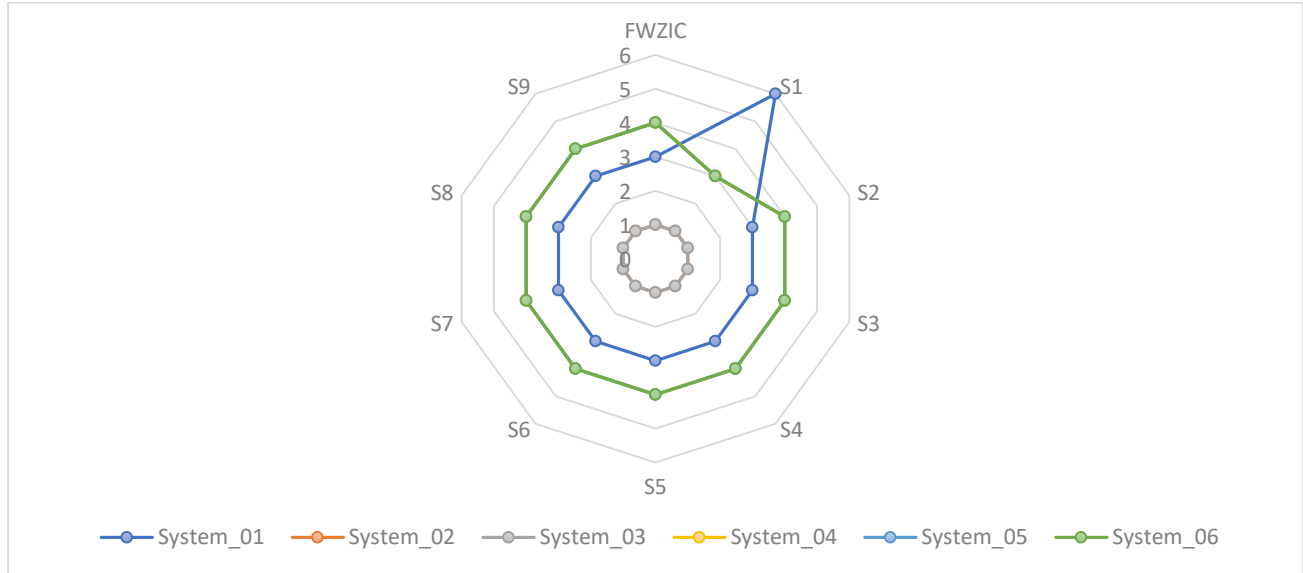


Figure 25 : Sensitivity Analysis of Dynamic Offloading Delegation Method Alternatives Benchmarking in nine scenarios

The presented figure (Figure 26) indicates that the weight change in the **Security Modules of Authentication delegation method** affected the ranking of the security modules, and the difference in the arrangement was observed in only three out of the nine scenarios. Specifically, in the first scenario (S1), four security modules demonstrated a notable progress in their ranking. SM_01, which was previously ranked 12, advanced to the 11th position, SM_04 moved from the 11th to the 6th position, SM_09 advanced from the 9th to the 3rd position, and SM_12 improved its ranking from the 10th to the 5th position. In contrast, six security modules experienced a decline in their ranking and moved to a lower order compared to their previous ranking. These security modules include SM_05, which was ranked 4th and moved down to the 7th position, SM_06, which was ranked 8th and dropped to the 12th position, SM_07, which was ranked 5th and dropped to the 12th position, SM_08, which was ranked 7th and dropped to the 10th position, SM_10, which

maintained its ranking of 4th, and SM_11, which was ranked 5th and moved down to the 8th position. Regarding the second scenario (**S2**), only four alternatives experienced changes, with three of them increasing in ranking and one decreasing. Specifically, SM_04, SM_09, and SM_12 increased from the 11th to the 10th rank, from the 9th to the 8th rank, and from the 10th to the 9th rank, respectively. These changes were observed to be relatively minor, only affecting a one-degree shift in ranking. However, SM_06 fell from the 8th rank to the 11th rank. The remaining alternatives maintained their original ranking. In the third scenario (**S3**), SM_05's ranking decreased from the 4th to the 6th rank, while SM_07 and SM_11 increased from the 5th to the 4th rank. The rankings of the other security modules remained unchanged.

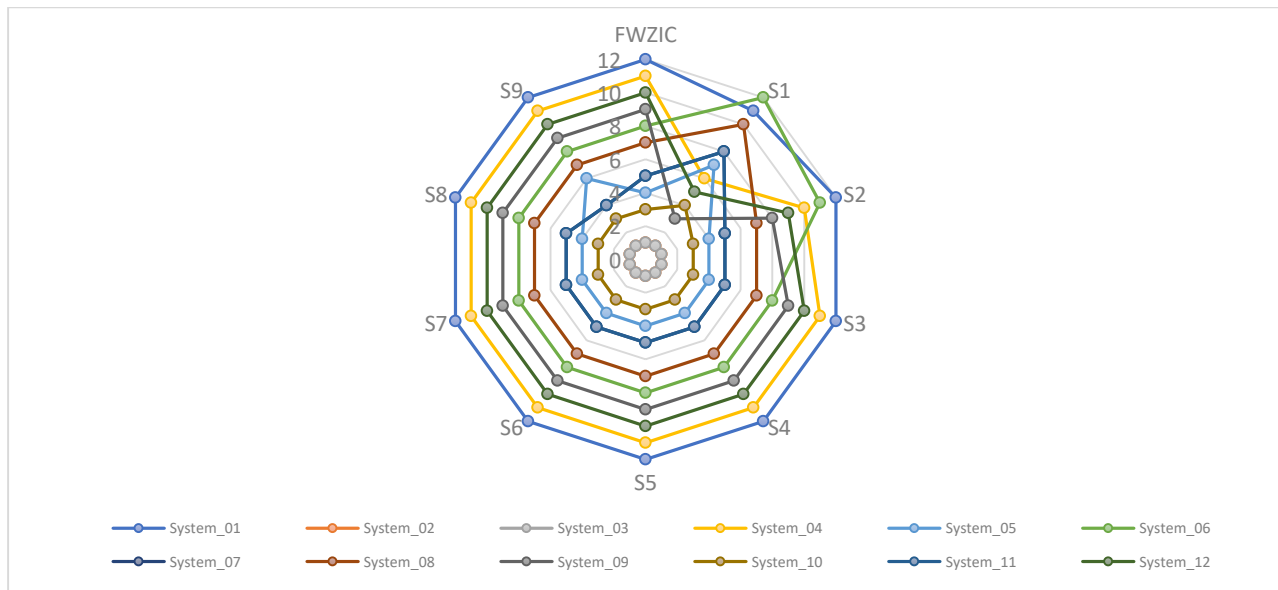


Figure 26 : Sensitivity Analysis of Authentication Delegation Method Alternatives Benchmarking in nine scenarios

According to all above analysis , the main observation is that the effect of the weight change was limited to only a few scenarios, and small impact on the ranking of the alternatives in all categories which prove the validity of the MCDM Methods used for ranking.

Finally , Pearson's correlation coefficient is a statistical tool used to evaluate the correlation between FWZIC and the nine scenarios. As for Security **Modules of layering delegation method**

as shown in the Figure 27 the coefficient between "FWZIC" and "S1" is 0.549, indicating a moderate positive correlation. This implies that there is a tendency for high scores on the FWZIC variable to be associated with high scores on the S1 variable, and vice versa. For the rest of scenarios form (S2 – S9) there is a strong positive correlation.

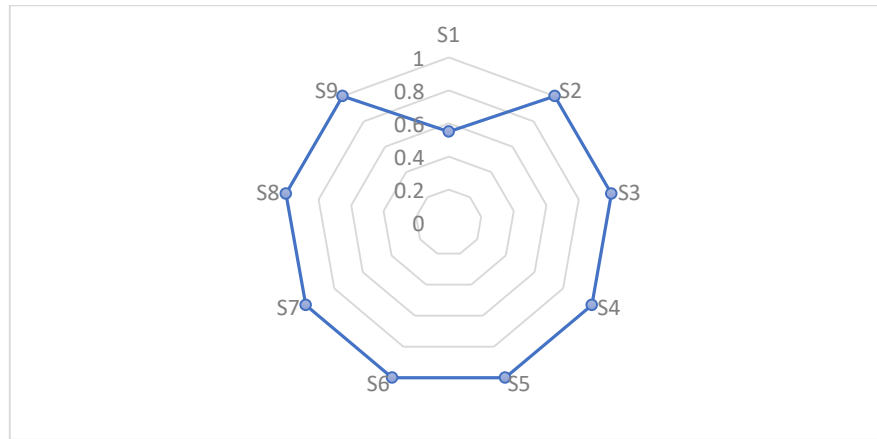


Figure 27: Layering Delegation method Correlation result

The **Security Modules of Encryption delegation method** has a generally strong positive correlation with most scenarios (S2, S3, S4, S5, S6, S7, S8, and S9), indicating a high degree of association between the variables. Specifically, S2 and S9 exhibit a correlation result of 0.980 and 0.957, respectively, indicating a strong positive correlation. On the other hand, S1 shows a moderate positive correlation with a result of 0.643, suggesting a somewhat weaker relationship between the variables compared to the other scenarios. It is worth noting that a correlation result of 1 for scenarios from S3 to S8 indicates a perfect positive correlation, implying that the variables move in perfect unison as shown in Figure 28.

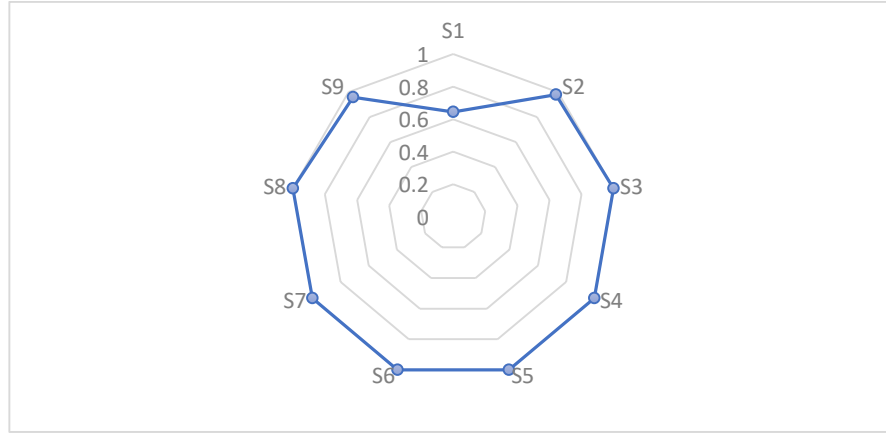


Figure 28: Encryption Delegation method Correlation result

With respect to Dynamic Offloading, a strong positive correlation was observed for scenarios ranging from S2 to S9, with a correlation coefficient of 1, except for scenario S1, which showed a moderately positive correlation with a coefficient of 0.580 as illustrated in Figure 29.

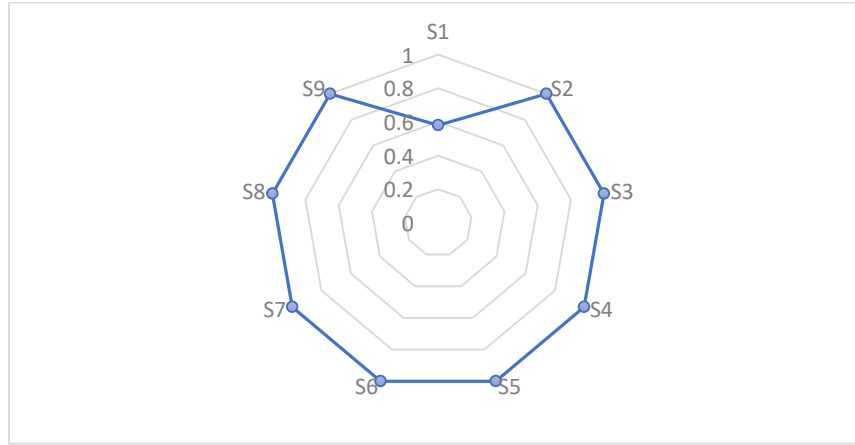


Figure 29: Dynamic Offloading Delegation method Correlation result

For **Security Modules of Authentication delegation method** with 12 security modules, as presented in Figure 30 FWZIC and scenario S1 exhibited a moderate positive correlation with a correlation coefficient of 0.538. Furthermore, FWZIC was found to have a strong positive correlation with scenario S2 (correlation coefficient of 0.961), as well as with scenario S9 (correlation coefficient of 0.980). Moreover, a very strong positive correlation was observed

between FWZIC and all other scenarios (correlation coefficient of 1). However, it should be noted that the correlation coefficients between FWZIC and S1, S2, and S9 were statistically significant, while the correlation coefficient of 1 indicates perfect correlation.

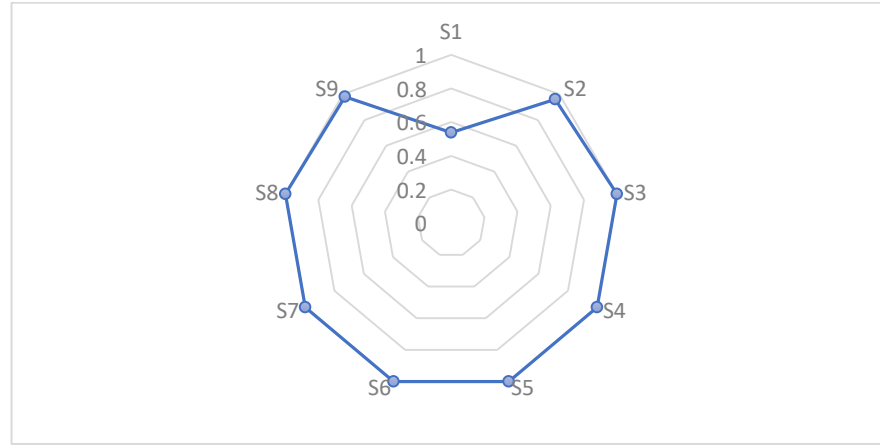


Figure 30: Authentication Delegation method Correlation result

To summarize, the weight variations had an impact solely on scenario 1 among all the analyzed security modules, whereas scenarios 2 and 3 were influenced exclusively by the Authentication and Encryption delegation approach. Based on these findings, it can be inferred that the ranking outcome obtained via EDAS is robust and not substantially impacted by changes in weights.

5.3.2. Systematic Ranking Result

This section details the validation procedures for evaluating the benchmarking outcomes of Security Modules of Delegation Methods in MCC based on the EDAS approach, with regards to the weight of security criteria. The validation processes employed in this study are objective in nature. As explained in Chapter 3-Section 3.4.2, the validation process for ranking Security Modules of Delegation Methods in MCC was carried out by segregating the ranking results for each delegation method as per Table 25 into three groups.

Table 25: Ranking Results Segregation for Each Delegation Method

Delegation Method	Group 1	Group 2	Group 3
Layering	3	3	3
Encryption	7	7	9
Dynamic offloading	3	3	-
Authenticaiton	4	4	4

The Layering method, consisting of 12 security modules, was divided into three groups with three security modules in each group. The Encryption method, comprising of 23 security modules, was divided into three groups as 7, 7, and 9 security modules in Group 1, Group 2, and Group 3, respectively. The Dynamic offloading delegation methods, which include six security modules, were divided into two groups with three security modules in each group. The final groups were associated with Authentication delegation methods, which comprised of 12 security modules, and were divided into three groups with four security modules in each group. The obtained results are considered valid, as the assigned linguistic terms for the ideal solution of each criterion by the experts yielded the lowest mean value.

Table 26: Group Distribution Validation Results

MCC Delegation Method	Group 1	Group 2	Group 3
Layering	SM_07	SM_09	SM_03
	SM_06	SM_04	SM_02
	SM_08	SM_01	SM_05
Mean	0.871795641	0.794871795	0.58974359
Encryption	SM_07	SM_12	SM_10
	SM_11	SM_17	SM_14
	SM_23	SM_18	SM_01
	SM_16	SM_20	SM_05
	SM_13	SM_22	SM_08
	SM_19	SM_06	SM_02
	SM_21	SM_15	SM_04

MCC Delegation Method	Group 1	Group 2	Group 3
			SM_09
			SM_03
Mean	0.868131868	0.846153846	0.700854701
Dynamic Offloading	SM_02	SM_04	
	SM_03	SM_05	
	SM_01	SM_06	
Mean	0.871794872	0.846153846	
Authentication	SM_02	SM_07	SM_09
	SM_03	SM_11	SM_12
	SM_10	SM_08	SM_04
	SM_05	SM_06	SM_01
Mean	0.846154231	0.826923077	0.788461538

The findings from Table 26 demonstrate that in the **Layering delegation method**, the third group of alternatives exhibited the lowest mean value (0.58974359) in comparison to the first and second groups. Additionally, the mean value of the second group (0.794871795) was found to be lower than that of the first group (0.871795641). With respect to the **Encryption delegation method** alternatives, Group 3 demonstrates the lowest mean value of 0.700854701, while Group 2 displays a marginally higher mean value of 0.846153846, and Group 1 exhibits the highest mean value of 0.868131868 which is same ranking for the previous delegation method. Meanwhile, In the given table it presents the mean values of two different groups of alternatives for the **Dynamic Offloading Delegation Method**, Group 2 exhibits the lowest mean value of 0.846153846. On the other hand, Group 1 has the highest mean value of 0.871794872. Similarly, the table presents the mean values of three different groups of **alternatives for the Authentication Delegation Method**. According to the table, Group 1 exhibits the lowest mean value of 0.788461538, Group 2 has a slightly higher mean value of 0.826923077, and Group 3 has the highest mean value of 0.846154231.

The study findings indicate that the MCC delegation method's alternatives evaluation and benchmarking results are reliable and consistent. This implies that the benchmarking results obtained using the EDAS method are reliable and have been systematically ranked across all categories. These results are of significant importance for decision-makers who need to make informed choices based on a reliable and valid evaluation of different alternatives.

5.3.3. Benchmarking Checklist Result

In this section, the outcomes of the benchmarking assessment are presented. As previously elaborated in Section 3.4.3 of Chapter 3. The proposed approach is evaluated against a benchmark study that concentrates on evaluating different approaches for the Agriculture-Food 4.0 supply chain. This is achieved by employing a decision-making model based on Fermatean probabilistic hesitant-fuzzy sets and this research is using probabilistic interval necroscopic hesitant-fuzzy sets. The comparison was carried out utilizing a set of ten main points, which some of them were further subdivided into fourteen subpoints and subsequently presented in Table 26. The assessment encompassed a comparison of theoretical aspects from both weighing and ranking perspectives, and an evaluation of application aspects that were focused on addressing the critical issues pertaining to MCDM.

Table 27: Comparing the Proposed Study to the Benchmark Study: Key Points of Comparison.

Aspects	Comparison Points		Proposed study	Benchmark study		
Theoretical Aspects	Weighting perspective		Use the weighting method to address inconsistencies.	Yes	Yes	
			Ensure that the criteria are not interdependent.	Yes	Yes	
			The weighting method is not overly time-consuming.	Yes	Yes	
			The weighting method does not involve complex mathematical operations.	Yes	Yes	
			Gathering input from experts is a simple process	Yes	Yes	
		Vagueness, hesitancy, and uncertainty		The weighting method is more dependable when it comes to solving imprecision and ambiguity in practical situations	Yes	Yes
				The weighting approach can handle cases where the decision-maker's rejection is crucial to the evaluation process.	Yes	Yes
				The weighting method preserves probability data.	Yes	Yes
				The weighting method provides a wider variety of choices to decision-makers compared to other fuzzy sets.	Yes	No
				The weighting method is more effective and efficient in handling vagueness, hesitancy, and uncertainty than other fuzzy sets.	Yes	Yes
	Ranking perspective		Assign weights to criteria.	No	No	
			Integrated with Fuzzy environment	Yes	Yes	
			Not computationally demanding.	Yes	Yes	
			Take into account the significance of the distances.	Yes	Yes	
			Incorporate positive and negative ideal solutions into decision matrices.	Yes	No	
			Calculates utility degrees based on proximity to ideal solutions.	Yes	No	
			Calculate utility functions.	Yes	No	
			Remains stable even with a large number of alternatives and criteria.	Yes	Yes	
			Can perform multiple tasks simultaneously.	Yes	Yes	
Application Aspects			The evaluation process involves considering several different criteria.	Yes	Yes	
			Prioritization of the criteria is determined based on their relative importance.	Yes	Yes	
			The proposed method takes into account variations in the data.	Yes	Yes	
Total score			95.5%	77.3%		
Accumulative difference			4.5%	22.7%		

Table 26 summarizes the comparison between the proposed study and the benchmark study in terms of theoretical and application aspects. For the theoretical aspects, there were 19 comparison points, with the proposed study having a "Yes" response for 18 comparison points and a "No"

response for one comparison point. On the other hand, the benchmark study had a "Yes" response for 14 comparison points and a "No" response for five comparison points. For the application aspects, there were three comparison points, with both the proposed and benchmark studies having a "Yes" response for all three comparison points.

In details and starting with **Theoretical Aspects**, the main five points in weighting perspective, the proposed study and the benchmark study show a "Yes" response for all comparison points, indicating that both approaches fulfill these requirements. In regard to handling vagueness, hesitancy, and uncertainty in multi-criteria decision-making using the weighting perspective, the results indicate that the proposed study and the benchmark study have a "Yes" response for all comparison points, except for the comparison point related to providing a wider variety of choices to decision-makers, where the benchmark study has a "No" response. Therefore, the proposed study and the benchmark study have similar capabilities in addressing vagueness, hesitancy, and uncertainty in MCDM, with minor differences related to the number of choices provided to decision-makers.

In terms of ranking perspective, the results indicate that the proposed study has a "Yes" response for all comparison points except for assigning weights to criteria, while the benchmark study has a "No" response for assigning weights to criteria and incorporating positive and negative ideal solutions into decision matrices and calculating utility degrees based on proximity to ideal solutions. Overall, the proposed study and the benchmark study have similar capabilities in most of the comparison points, except for the assigned weights to criteria and the incorporation of ideal solutions and calculation of utility degrees. However, when considering the ranking perspective, the proposed study has a more comprehensive approach in handling multi-criteria decision-making compared to the benchmark study.

On the other side, regarding the **Application Aspects**, Both the proposed study and benchmark study received a "Yes" response for all comparison points, indicating their similarity in addressing the MCDM critical issues.

In Conclusion, the proposed study achieved a total score of 95% compared to the benchmark study's 77% that use. However, the accumulative difference between the two studies is 4.5% and 22.7%, respectively. Therefore, the proposed Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing under probabilistic interval necroscopic hesitant-fuzzy sets demonstrates better performance in terms of the total score compared to the benchmark study which is under Fermatean probabilistic hesitant-fuzzy sets.

5.4.Conclusion and Future Review

The final section of this study is composed of four parts, including Objectives Achieving, Research Contributions, Limitations, and Future Work. Details for each of these sections are presented below.

5.4.1. Objectives Achieving

MCDM research contributes greatly to helping service providers, future academic researchers and developers of programs and applications in choosing the appropriate systems or more precisely the right choice for any field that has many options. In this research, Modeling decesion based approach for choosing the best Security Modules of Delegation Methods in MCC was designed based on the evaluation of security criteria, which is one of the criteria that can be compared. This was done by achieving several objectives, the most important of which are:

- **To demonstrates the existing evaluation techniques for Security modules of delegation methods of MCC and drawing attention to the evaluation drawbacks.** Through an extensive

analysis of 50 research papers focused on security modules for four delegation methods in Mobile Cloud Computing which are (Layering, Encryption, Dynamic Offloading, and Authentication) it has been revealed that no previous evaluation techniques have been applied to assess the security modules for these delegation methods. By accomplishing this objective, this research successfully demonstrates the existing evaluation gaps in the field of security modules of delegation methods in MCC. The study highlights the need for effective evaluation techniques and draws attention to the drawbacks associated with the lack of evaluation in this domain. This achievement contributes to the advancement of knowledge in MCC security and provides a foundation for future research and development in the evaluation of security modules for delegation methods in MCC

- **To articulate the decision matrices based on the intersection of Security Modules of delegation method for MCC with the security evaluation criteria.** In this study, four decision matrices were constructed to evaluate different security modules based on thirteen distinct security evaluation criteria. The security modules were compared within each matrix, with nine security modules compared to the Layering delegation method, twenty-three security modules compared to the Encryption delegation method, six security modules compared to the Offloading delegation method, and twelve security modules compared to the Authentication delegation method. The comparison was conducted based on the thirteen security evaluation criteria, which included privacy, authentication (cloud to client, client to cloud, and multi-factor), data security, encryption key, single failure point, security threats, communication channel issues, improper access control, authorization issues, and anonymity.

- **To formulate and develop an extension of FWZIC method under a Probabilistic Interval Neutrosophic Hesitant Fuzzy Set called (PINHFS).** With the aim of achieving the research objective and tackling the critical issue of criteria importance, the study proposes the

development of the PINHFS-FWZIC method to prioritize and weight the security evaluation criteria for the Security Modules of Delegation Methods in MCC based on their level of significance. The integration of the FWZIC method into the PINHFS framework enables effective handling of uncertainties and inaccuracies in the decision-making process.

- **To develop a Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing using the formulated decision matrices and the integration of EDAS and new extension of FWZIC under PINHFS..** This study develops a benchmarking framework by integrating two distinct methods, namely PINHFS-FWZIC and EDAS. The PINHFS-FWZIC method is utilized to supplement the EDAS method, by providing weights for the security evaluation criteria that are based on expert preferences. Meanwhile, the EDAS method is employed for benchmarking and ranking the various Security Modules of Delegation Methods in MCC.

- **To assess and verify the outcomes of the suggested modelling approach, by utilizing sensitivity analysis, systematic ranking, and benchmarking checklist (Evaluation and Validation process).** By accomplishing this objective, the research has successfully applied sensitivity analysis techniques to examine the robustness and reliability of the suggested modelling approach, exploring various input parameters and their impacts on the model outputs. Additionally, systematic ranking methodologies were employed to objectively assess and compare the performance of the proposed approach against existing methods or benchmarks, providing insights into its strengths, weaknesses, and comparative advantages. Furthermore, a benchmarking checklist was developed and utilized to validate the suggested modelling approach, using predetermined criteria and performance indicators to assess its efficacy, accuracy, and applicability. The achievement of this objective contributes to the research field by providing a

comprehensive evaluation and validation process for the suggested modelling approach, enhancing its credibility and reliability. Ultimately, this research offers practitioners a reliable and effective methodology for decision-making processes, backed by a thorough assessment and verification of the suggested approach.

5.4.2. Research Contributions

The fundamental contribution of this research work lies in the creation of a Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing by leveraging the PINHFS-FWZIC and EDAS methods. This approach successfully tackles the intricate challenges and issues related to benchmarking Security Modules of Delegation Methods in Mobile Cloud Computing, thereby providing valuable support to stakeholders in selecting the most secure and suitable security modules, while simultaneously resolving the multiple criteria decision making (MCDM) concerns highlighted in this study. The contributions of this research are achieved through three principal components:

- **The first point**, the proposed of four decision matrices, each of which intersect with the identified Security Modules of Delegation Methods in MCC and their associated security evaluation criteria. This matrix is based on an extensive literature review, where approximately 50 papers were analyzed to identify the Security Modules of Delegation Methods in MCC.
- **The subsequent point**, is the introduces a novel weighting method called PINHFS-FWZIC to address the problem of criteria importance. This method prioritizes and assigns weights to the security evaluation criteria of Security Modules of Delegation Methods in MCC, and the resulting weights are then employed in the EDAS ranking method.

- **In the last point**, the PINHFS-FWZIC method is integrated with the EDAS method to rank the Security Modules of Delegation Methods in MCC. A Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing is presented, which considers the decision matrices, the resulting criteria weights, and the integration with EDAS to rank each security module in each delegation method. It is noteworthy that this integration between PINHFS-FWZIC and EDAS has not been previously attempted.

This study employs a multidisciplinary approach to integrate insights from the field of decision-making (MCDM) with those of software engineering to devise a benchmarking framework for MCC delegation methods systems. The research contribution and innovation mapping are presented in Figure31.

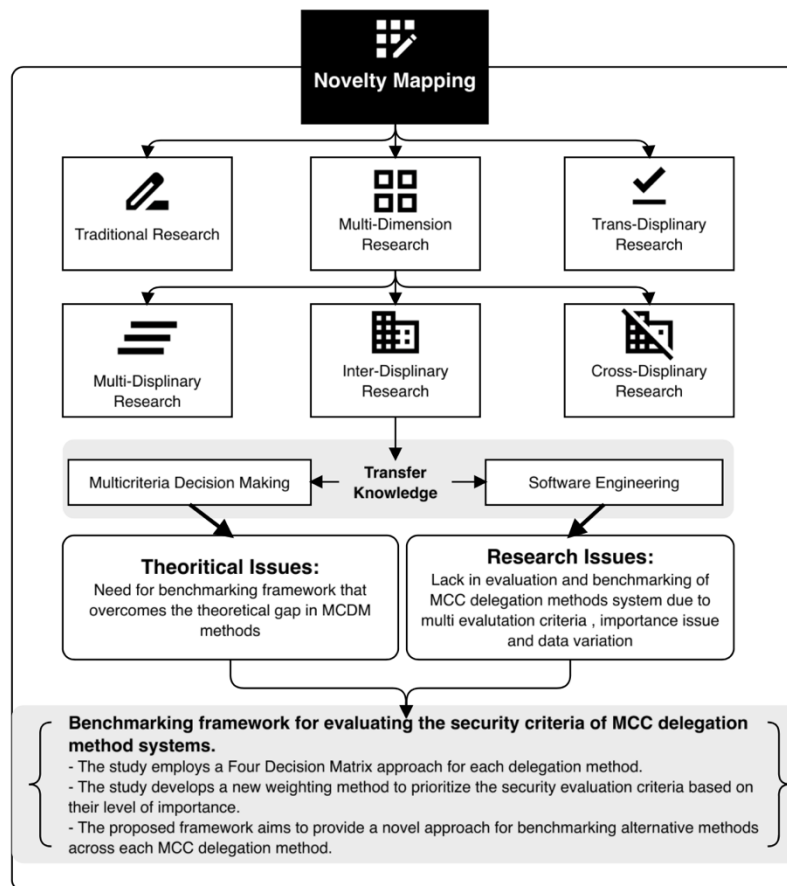


Figure 31: Research Contributions and Novelty Mapping

In summary, research can be categorized into traditional research, trans-disciplinary research, and multidimensional research. Multidimensional research includes multidisciplinary, interdisciplinary, and cross disciplinary research, each with its own unique approach and benefits. Multidisciplinary research involves collaboration among researchers from different disciplines without necessarily integrating their knowledge, interdisciplinary research involves integration of knowledge and methods from multiple disciplines to develop a shared conceptual framework, and cross-disciplinary research involves the application of knowledge from one discipline to another. Interdisciplinary research involves the integration of knowledge and methods from multiple disciplines, leading to a more comprehensive understanding of complex problems, innovative solutions, and broader impacts.

In the context of mobile cloud computing, interdisciplinary research plays a crucial role in ensuring the transfer of knowledge from the field of multicriteria decision making (MCDM) to software engineering. MCDM provides a framework for evaluating and ranking options based on multiple criteria, and interdisciplinary research that combines the knowledge and methods of MCDM and software engineering can help ensure that the best alternative is chosen when designing delegation methods for mobile cloud computing systems. This can ultimately lead to the development of more efficient and secure systems that meet the needs of users and organizations.

5.4.3. Practical Contributions

The practical contribution of creating a Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing lies in the below area:

- Providing a valuable tool for service providers in the field. By developing this approach, practitioners can effectively evaluate and select appropriate security modules for MCC delegation methods, enhancing the overall security of their systems.

- The Decision Modelling Approach offers a systematic framework for decision-making, considering various factors such as security requirements, performance, scalability, and cost-effectiveness. It enables practitioners to make informed decisions based on a comprehensive evaluation of available security modules, ensuring the selection of the most suitable and effective options for their specific MCC environment.
- Moreover, the approach assists developers in managing the complexities associated with security module selection by providing a structured and standardized methodology. It guides them through the process of defining evaluation criteria, weighting factors, and performing evaluations based on real-world considerations.
- By utilizing this Decision Modelling Approach, practitioners can make more informed decisions regarding the security modules to be integrated into their MCC systems. This contributes to enhancing the overall security posture of their infrastructure, protecting sensitive data, mitigating risks, and ensuring compliance with relevant security standards and regulations.
- Furthermore, the developing of this approach lies in its flexibility and adaptability to different MCC environments and organizational requirements. It can be customized and tailored to specific contexts, allowing service providers to align the decision-making process with their unique security objectives, resource constraints, and operational needs.

In summary, the practical contribution of creating a Decision Modelling Approach for the Security Modules of Delegation Methods in Mobile Cloud Computing is empowering software developer, security providers with a robust, structured, and customizable methodology for evaluating and selecting security modules. This aids in strengthening the security of MCC systems, improving risk management, and facilitating informed decision-making in the context of security module integration.

5.4.4. Limitation

- This study employed five linguistic measurements of importance to build the EDM. However, exploring additional linguistic measurements, such as seven or ten, may improve the construction of the EDAS method.
- The experts involved in the study were treated equally, regardless of their level of experience. However, prioritizing experts based on their expertise may yield more accurate and reliable results.
- The Probabilistic Interval Neutrosophic Hesitant Fuzzy Set (PINHFS) involves the incorporation of multiple degrees, such as membership, non-membership, and hesitancy degrees, which may increase the computational complexity and demand more computational resources compared to other fuzzy set theories.
- The PINHFS-FWIZC model employs a singular aggregation operator and a one defuzzification technique for the purpose of generating conclusive weighting and ranking outcomes.
- The EDAS method has certain limitations that should be considered. Firstly, it requires a weighting method to assign importance to the criteria. This means that an additional step is necessary to determine the relative weights of the criteria, which can be a challenge in itself. Furthermore, the use of linear functions for aggregating values in the weighted matrix is a significant limitation of the EDAS method. Linear functions may not adequately capture the complexity of the decision-making process and may oversimplify the aggregation process. To address this limitation, the implementation of nonlinear weighing functions, such as Dobmi, Bonferroni, Aczel-Alsina, among others, can be explored. Nonlinear functions have the potential to provide more nuanced and accurate results by considering the intricacies and interactions among criteria

Due to the exploratory approach adopted in this study, some of the limitations encountered have had a partial impact on the present results. These limitations have highlighted potential emerging challenges that require further exploration and provide new avenues for future research. Nevertheless, despite these limitations, the findings of this study remain trustworthy and robust

5.4.5. Future Work

- Future research studies should prioritize experts based on their level of experience and expertise to enhance the validity and reliability of results.
- Future research should explore additional linguistic expressions and numerical scales, such as seven or ten, to further refine the (EDM) method.
- The integration of other operators with the (PINHFS-FWZIC) method in future research can enhance the precision and accuracy of the results.
- The proposed framework in this study could serve as a useful benchmark for evaluating other security modules across various delegation methods in Mobile cloud computing (MCC) Security Modules in future research.
- Future research studies may consider integrating other MCDM ranking methods with the PINHFS-FWZIC method to investigate new benchmarking results and enhance the accuracy and reliability of the approach.

5.5. Chapter Summary

Chapter 5 presents the findings and discussion of the research study conducted. The chapter begins with an introduction to the section, followed by the results of the benchmarking framework. The results include the decision matrix results, the criteria weight result, and the ranking result of Security Modules of Delegation Methods in MCC using EDAS. The validation and evaluation results are also discussed, which consist of the sensitivity analysis result, systematic ranking result, and benchmarking checklist result. Finally, the chapter concludes with the achievement of objectives, research contributions, limitations, and future work. The study provides significant Research and Practical contributions to the field of benchmarking Security Modules of Delegation Methods in MCC. However, limitations and future research opportunities are also identified for further improvement and exploration. Overall, the chapter highlights the importance of benchmarking as an effective tool for evaluating and improving the performance of Security Modules of Delegation Methods in MCC.

REFERENCES

A. Almusaylim, Z. & Jhanjhi, N. (2020). Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. *Wireless Personal Communications*. Springer US, vol. 111(1), pp. 541–564.

Abd Ali, R., Chen, W., Jin, K., Bao, Y. & Hussein, A. W. (2019). Formability and failure analyses of Al/SUS bilayer sheet in single point incremental forming. *International Journal of Advanced Manufacturing Technology*, vol. 105(7–8), pp. 2785–2798.

Abdel-Basset, M., Gamal, A., Chakraborty, R. K. & Ryan, M. J. (2021). Evaluation of sustainable hydrogen production options using an advanced hybrid MCDM approach: A case study. *International Journal of Hydrogen Energy*. Elsevier Ltd, vol. 46(5), pp. 4567–4591.

Ahmad, A., Alzahrani, A. S., Ahmed, N. & Ahsan, T. (2020). A delegation model for SDN-driven federated cloud. *Alexandria Engineering Journal*. Faculty of Engineering, Alexandria University, vol. 59(5), pp. 3653–3663.

Al-Humairi, S., Hizami, A., Zaidan, A. A., Zaidan, B. B., Alsattar, H. A., Qahtan, S., Albahri, O. S., Talal, M., Alamoodi, A. H. & Mohammed, R. T. (2022). Towards Sustainable Transportation: A Pavement Strategy Selection Based on the Extension of Dual-Hesitant Fuzzy Multi-Criteria Decision-Making Methods. *IEEE Transactions on Fuzzy Systems*, pp. 1–1.

Al-Samarraay, M. S., Zaidan, A. A., Albahri, O. S., Pamucar, D., AlSattar, H. A., Alamoodi, A. H., Zaidan, B. B. & Albahri, A. S. (2022a). Extension of interval-valued Pythagorean FDOSM for evaluating and benchmarking real-time SLRSs based on multidimensional criteria of hand gesture recognition and sensor glove perspectives[Formula presented]. *Applied Soft Computing*. Elsevier B.V., vol. 116, p. 108284.

Al-Samarraay, M. S., Zaidan, A. A., Albahri, O. S., Pamucar, D., AlSattar, H. A., Alamoodi, A. H., Zaidan, B. B. & Albahri, A. S. (2022b). Extension of interval-valued Pythagorean FDOSM for evaluating and benchmarking real-time SLRSs based on multidimensional criteria of hand gesture recognition and sensor glove perspectives. *Applied Soft Computing*. Elsevier, vol. 116, p. 108284.

AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O. & Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review. *Journal of Network and Computer Applications*. Elsevier Ltd, vol. 190(March), p. 103152.

Alamoodi, A. H., Albahri, O. S., Zaidan, A. A., AlSattar, H. A., Ahmed, M. A., Pamucar, D., Zaidan, B. B., Albahri, A. S. & Mahmoud, M. S. (2022). New Extension of Fuzzy-Weighted Zero-Inconsistency and Fuzzy Decision by Opinion Score Method Based on Cubic Pythagorean Fuzzy Environment: A Benchmarking Case Study of Sign Language Recognition Systems. *International Journal of Fuzzy Systems*. Springer, pp. 1–18.

Alamoodi, A. H., Mohammed, R. T., Albahri, O. S., Qahtan, S., Zaidan, A. A., Alsattar, H. A., Albahri, A. S., Aickelin, U., Zaidan, B. B., Baqer, M. J. & Jasim, A. N. (2022a). Based on neutrosophic fuzzy environment: a new development of FWZIC and FDOSM for benchmarking smart e-tourism applications. *Complex and Intelligent Systems*. Springer International Publishing, vol. 8(4), pp. 3479–3503.

Alamoodi, A. H., Mohammed, R. T., Albahri, O. S., Qahtan, S., Zaidan, A. A., Alsattar, H. A., Albahri, A. S., Aickelin, U., Zaidan, B. B., Baqer, M. J. & Jasim, A. N. (2022b). Based on neutrosophic fuzzy environment: a new development of FWZIC and FDOSM for benchmarking smart e-tourism applications. *Complex & Intelligent Systems*. Springer International Publishing.

Albahri, A. S., Al-Obaidi, J. R., Zaidan, A. A., Albahri, O. S., Hamid, R. A., Zaidan, B. B., Alamoodi, A. H. & Hashim, M. (2020). Multi-Biological Laboratory Examination Framework for the Prioritization of Patients with COVID-19 Based on Integrated AHP and Group VIKOR Methods. *International Journal of Information Technology and Decision Making*. World Scientific Publishing Company , vol. 19(5), pp. 1247–1269.

Albahri, A. S., Albahri, O. S., Zaidan, A. A., Alnoor, A., Alsattar, H. A., Mohammed, R., Alamoodi, A. H., Zaidan, B. B., Aickelin, U., Alazab, M., Garfan, S., Ahmaro, I. Y. Y. & Ahmed, M. A. (2022a). Integration of fuzzy-weighted zero-inconsistency and fuzzy decision by opinion score methods under a q-rung orthopair environment: A distribution case study of COVID-19 vaccine doses. *Computer Standards and Interfaces*. Elsevier B.V., vol. 80(March 2021), p. 103572.

Albahri, A. S., Albahri, O. S., Zaidan, A. A., Alnoor, A., Alsattar, H. A., Mohammed, R., Alamoodi, A. H., Zaidan, B. B., Aickelin, U., Alazab, M., Garfan, S., Ahmaro, I. Y. Y. & Ahmed, M. A. (2022b). Integration of fuzzy-weighted zero-inconsistency and fuzzy decision by opinion score methods under a q-rung orthopair environment: A distribution case study of COVID-19 vaccine doses. *Computer Standards and Interfaces*. North-Holland, vol. 80, p. 103572.

Albahri, O. S., AlSattar, H. A., Garfan, S., Qahtan, S., Zaidan, A. A., Ahmaro, I. Y. Y., Alamoodi, A. H., Zaidan, B. B., Albahri, A. S., Al-Samarraay, M. S., Jasim, A. N. & Baqer, M. J. (2022). Combination of Fuzzy-Weighted Zero-Inconsistency and Fuzzy Decision by Opinion Score Methods in Pythagorean m-Polar Fuzzy Environment: A Case Study of Sing Language Recognition Systems. *International Journal of Information Technology & Decision Making*, pp. 1–29.

Albahri, O. S., Zaidan, A. A., Albahri, A. S., Alsattar, H. A., Mohammed, R., Aickelin, U., Kou, G., Jumaah, F. M., Salih, M. M., Alamoodi, A. H., Zaidan, B. B., Alazab, M., Alnoor, A. & Al-Obaidi, J. R. (2022a). Novel dynamic fuzzy Decision-Making framework for COVID-19 vaccine dose recipients. *Journal of Advanced Research*. Cairo University, vol. 37, pp. 147–168.

Albahri, O. S., Zaidan, A. A., Albahri, A. S., Alsattar, H. A., Mohammed, R., Aickelin, U., Kou, G., Jumaah, F. M., Salih, M. M., Alamoodi, A. H., Zaidan, B. B., Alazab, M., Alnoor, A. & Al-Obaidi, J. R. (2022b). Novel dynamic fuzzy Decision-Making framework for COVID-19 vaccine dose recipients. *Journal of Advanced Research*. Cairo University, vol. 37, pp. 147–168.

Aldmour, R., Yousef, S., Baker, T. & Benkhelifa, E. (2021). An approach for offloading in mobile cloud computing to optimize power consumption and processing time. *Sustainable Computing: Informatics and Systems*. Elsevier Inc., vol. 31(August 2020), p. 100562.

Alinezhad, A. & Khalili, J. (2019). *New methods and applications in multiple attribute decision making (MADM)*. *International Series in Operations Research and Management Science*.

Alnajrani, H. M., Norman, A. A. & Ahmed, B. H. (2020). Privacy and data protection in mobile cloud computing: A systematic mapping study. *PLoS ONE*, vol. 15(6), pp. 1–29.

Alsalem, M. A., Albahri, O. S., Zaidan, A. A., Al-Obaidi, J. R., Alnoor, A., Alamoodi, A. H., Albahri, A. S., Zaidan, B. B. & Jumaah, F. M. (2022). Rescuing emergency cases of COVID-19 patients: An intelligent real-time MSC transfusion framework based on multicriteria decision-making methods. *Applied Intelligence*. Springer, vol. 52(9), pp. 9676–9700.

Alsalem, M. A., Alsattar, H. A., Albahri, A. S., Mohammed, R. T., Albahri, O. S., Zaidan, A. A., Alnoor, A., Alamoodi, A. H., Qahtan, S., Zaidan, B. B., Aickelin, U., Alazab, M. & Jumaah, F. M. (2021a). Based on T-spherical fuzzy environment: A combination of FWZIC and FDOSM for prioritising COVID-19 vaccine dose recipients. *Journal of Infection and Public Health*. King Saud Bin Abdulaziz University for Health Sciences, vol. 14(10), pp. 1513–1559.

Alsalem, M. A., Alsattar, H. A., Albahri, A. S., Mohammed, R. T., Albahri, O. S., Zaidan, A. A., Alnoor, A., Alamoodi, A. H., Qahtan, S., Zaidan, B. B., Aickelin, U., Alazab, M. & Jumaah, F. M. (2021b). Based on T-spherical fuzzy environment: A combination of FWZIC and FDOSM for prioritising COVID-19 vaccine dose recipients. *Journal of Infection and Public Health*. King Saud Bin Abdulaziz University for Health Sciences, vol. 14(10), pp. 1513–1559.

Anor, A., Ajoubory, A. Z., Akashif, S. Q., Abayati, H., Tahri, R. & Khaw, K. (2022). Toward a Sustainable Transportation Industry: Oil Company Benchmarking based on the Extension of Linear Diophantine Fuzzy Rough Sets and Multicriteria Decision-Making Methods. *IEEE Transactions on Fuzzy Systems*.

Asadabadi, M. R., Chang, E. & Saberi, M. (2019). Are MCDM methods useful? A critical review of Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP). *Cogent Engineering*. Cogent, vol. 6(1).

Asante, D., He, Z., Adjei, N. O. & Asante, B. (2020). Exploring the barriers to renewable energy adoption utilising MULTIMOORA- EDAS method. *Energy Policy*. Elsevier Ltd, vol. 142(2006), p. 111479.

Bai, Y., Yao, L., Wei, T., Tian, F., Jin, D. Y., Chen, L. & Wang, M. (2020). Presumed Asymptomatic Carrier Transmission of COVID-19. *JAMA - Journal of the American Medical Association*. American Medical Association, vol. 323(14), pp. 1406–1407.

Behzad, M., Hashemkhani Zolfani, S., Pamucar, D. & Behzad, M. (2020). A comparative assessment of solid waste management performance in the Nordic countries based on BWM-EDAS. *Journal of Cleaner Production*. Elsevier Ltd, vol. 266, p. 122008.

Bhatia, T., Verma, A. K. & Sharma, G. (2020). Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing. *Concurrency and Computation: Practice and Experience*, vol. 32(5), pp. 1–16.

Carchiolo, V., Longheu, A., Malgeri, M., Ianniello, S., Marroccia, M. & Randazzo, A. (2019). Authentication and authorization issues in mobile cloud computing: A case study. *CLOSER 2019 - Proceedings of the 9th International Conference on Cloud Computing and Services Science*, (Closer), pp. 249–256.

Chen, T. C. T. & Lin, C. W. (2022). An FGM decomposition-based fuzzy MCDM method for selecting smart technology applications to support mobile health care during and after the COVID-19 pandemic. *Applied Soft Computing*. Elsevier B.V., vol. 121, p. 108758.

Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E. & Song, Z. (2010). Authentication in the clouds: A framework and its application to mobile users. *Proceedings of the ACM Conference on Computer and Communications Security*, (January), pp. 1–6.

Derhab, A., Belaoued, M., Guerroumi, M. & Khan, F. A. (2020). Two-Factor Mutual Authentication Offloading for Mobile Cloud Computing. *IEEE Access*, vol. 8, pp. 28956–28969.

Dr. A Sahaya Sudha. (2019). Application of EDAS Method on Water Requirement in Agriculture. *International Journal of Engineering Research and*, vol. V8(12).

Duarte Alonso, A., Kok, SK & O'Brien, S. (2018). LJMU Research Online m. *Tourism Recreation Research*, p. 19 [online]. Available at: <http://researchonline.ljmu.ac.uk/id/eprint/8705/>.

Fan, J. P., Li, Y. J. & Wu, M. Q. (2019). Technology Selection Based on EDAS Cross-Efficiency Evaluation Method. *IEEE Access*. IEEE, vol. 7, pp. 58974–58980.

Fan LEI, Guiwu WEI, Weijie SHEN, Y. G. (2022). Pdhl-Edas Method for Multiple Attribute To 3D Printer Selection, vol. 28(1), pp. 179–200.

Figueira, A. & Vaz, B. (2022). Survey on Synthetic Data Generation, Evaluation Methods and GANs. *Mathematics*, vol. 10(15), pp. 1–41.

Ghorabae, M. K., Zavadskas, E. K., Amiri, M. & Turskis, Z. (2016). Extended EDAS method for fuzzy multi-criteria decision-making: An application to supplier selection. *International Journal of Computers, Communications and Control*, vol. 11(3), pp. 358–371.

Ghorabae, M. K., Zavadskas, E. K., Olfat, L. & Turskis, Z. (2015). Multi-Criteria Inventory Classification Using a New Method of Evaluation Based on Distance from Average Solution (EDAS). *Informatica (Netherlands)*, vol. 26(3), pp. 435–451.

Gnana Jeevan, A. N. & Maluk Mohamed, M. A. (2020). DyTO: Dynamic Task Offloading Strategy for Mobile Cloud Computing Using Surrogate Object Model. *International Journal of Parallel Programming*. Springer US, vol. 48(3), pp. 399–415.

Hamid, R. A., Albahri, A. S., Albahri, O. S. & Zaidan, A. A. (2021). Dempster–Shafer theory for classification and hybridised models of multi-criteria decision analysis for prioritisation: a telemedicine framework for patients with heart diseases. *Journal of Ambient Intelligence and Humanized Computing*. Springer Science and Business Media Deutschland GmbH, pp. 1–35.

Hamid, R. A., Albahri, A. S., Alwan, J. K., Al-Qaysi, Z. T., Albahri, O. S., Zaidan, A. A., Alnoor, A., Alamoodi, A. H. & Zaidan, B. B. (2021). How smart is e-tourism? A systematic review of smart tourism recommendation system applying data management. *Computer Science Review*. Elsevier, vol. 39, p. 100337.

Himadri, B. & Seema, J. (2020). A Review on Authentication Techniques in Mobile Cloud Computing. *International Journal of Engineering Research and*, vol. V9(05), pp. 283–287.

Hou, W. hui, Wang, X. kang, Zhang, H. yu, Wang, J. qiang & Li, L. (2021). Safety risk assessment of metro construction under epistemic uncertainty: An integrated framework using credal networks and the EDAS method. *Applied Soft Computing*. Elsevier B.V., vol. 108, p.

107436.

Huang, D., Zhang, X., Kang, M. & Luo, J. (2010). MobiCloud: Building secure cloud framework for mobile computing and communication. *Proceedings - 5th IEEE International Symposium on Service-Oriented System Engineering, SOSE 2010*, pp. 27–34.

Huang, Y., Lin, R. & Chen, X. (2021). An enhancement edas method based on prospect theory. *Technological and Economic Development of Economy*, vol. 27(5), pp. 1019–1038.

Hussien, H. M., Yasin, S. M., Udzir, N. I., Ninggal, M. I. H. & Salman, S. (2021). Blockchain technology in the healthcare industry: Trends and opportunities. *Journal of Industrial Information Integration*, vol. 22.

Ibrahim, H. A., Zaidan, A. A., Qahtan, S. & Zaidan, B. B. (2023). Sustainability assessment of palm oil industry 4.0 technologies in a circular economy applications based on interval-valued Pythagorean fuzzy rough set-FWZIC and EDAS methods. *Applied Soft Computing*. Elsevier B.V., vol. 136, p. 110073.

Irshad, A., Chaudhry, S. A., Alomari, O. A., Yahya, K. & Kumar, N. (2020). A Novel Pairing-Free Lightweight Authentication Protocol for Mobile Cloud Computing Framework. *IEEE Systems Journal*, vol. 15(3), pp. 3664–3672.

Jannath, J. N. & S, M. S. B. (2021). Detection of malicious Android applications using Ontology-based intelligent model in mobile cloud environment. *Journal of Information Security and Applications*. Elsevier Ltd, vol. 58(February), p. 102751.

Joyner, C. C. & Lotrionte, C. (2017). ‘Information warfare as international coercion: elements of a legal framework’. , in *The Use of Force in International Law*. Routledge, pp. 433–473.

Khaira, A. & Dwivedi, R. K. (2018). A State of the Art Review of Analytical Hierarchy Process. *Materials Today: Proceedings*. Elsevier Ltd, vol. 5(2), pp. 4029–4035.

Khan, A. N., Mat Kiah, M. L., Madani, S. A., Khan, A. U. R. & Ali, M. (2013). Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. *Journal of Supercomputing*, vol. 66(3), pp. 1687–1706.

Khan, M. F., Haq, A., Ahmed, A. & Ali, I. (2021). Multiobjective multi-product production planning problem using intuitionistic and neutrosophic fuzzy programming. *IEEE Access*, vol. 9, pp. 37466–37486.

Kołodziej, J. & Jaatun, M. G. (2021a). Secure mobile cloud computing. *Concurrency and Computation: Practice and Experience*, vol. 33(18), pp. 44–48.

Kołodziej, J. & Jaatun, M. G. (2021b). Secure mobile cloud computing. *Concurrency and Computation: Practice and Experience*, vol. 33(18).

Krishnan, E., Mohammed, R., Alnoor, A., Albahri, O. S., Zaidan, A. A., Alsattar, H., Albahri, A. S., Zaidan, B. B., Kou, G., Hamid, R. A., Alamoodi, A. H. & Alazab, M. (2021). Interval type 2 trapezoidal-fuzzy weighted with zero inconsistency combined with VIKOR for evaluating smart e-tourism applications. *International Journal of Intelligent Systems*, vol. 36(9), pp. 4723–4774.

Krishnan, R. (2017). ScholarWorks at WMU Security and Privacy in Cloud Computing.

Kruthika & Valarmathi. (2018). A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. *IEEE Transactions on Cloud Computing*, vol. 6(2), pp. 344–357.

Kumar, R. R., Kumari, B. & Kumar, C. (2021). CCS-OSSR: A framework based on Hybrid MCDM for Optimal Service Selection and Ranking of Cloud Computing Services. *Cluster Computing*. Springer US, vol. 24(2), pp. 867–883.

Kumar Tiwari, R. & Kumar, R. (2022). A framework for prioritizing cloud services in neutrosophic environment. *Journal of King Saud University - Computer and Information Sciences*. The Authors, vol. 34(6), pp. 3151–3166.

Lawal, M., Nuraddeen, T., Muhammad, A., Rabi, A., Amin, M., Abdulrazaq, G. & Kasim, A. (2021). Security , Privacy Issues and Solutions of Mobile Cloud Computing. *United International Journal for Research & Technology*, vol. 02(07), pp. 112–117.

Lee, H. C. & Chang, C. Ter. (2018). Comparative analysis of MCDM methods for ranking renewable energy sources in Taiwan. *Renewable and Sustainable Energy Reviews*. Elsevier Ltd,

vol. 92(April 2017), pp. 883–896.

Lopez-Arboleda, E., Sarmiento, A. T. & Cardenas, L. M. (2019). Systematic review of integrated sustainable transportation models for electric passenger vehicle diffusion. *Sustainability (Switzerland)*, vol. 11(9).

Madhurya, C., Kumar, T. L. K., Bhargav, D., Sai, N. N. & Venkateswarlu, D. (2021). An Enhanced Scheme for protecting Data in Mobile Cloud Computing. *A Journal Of Composition Theory*, vol. 14(02), pp. 19–26.

Mardani, A., Zavadskas, E. K., Govindan, K., Senin, A. A. & Jusoh, A. (2016). VIKOR technique: A systematic review of the state of the art literature on methodologies and applications. *Sustainability (Switzerland)*, vol. 8(1).

Mavromoustakis, C. X., Mastorakis, G., Bourdena, A., Pallis, E., Stratakis, D., Perakakis, E., Kopanakis, I., Papadakis, S., Zaharis, Z. D., Skeberis, C. & Xenos, T. D. (2015). A social-oriented mobile cloud scheme for optimal energy conservation. *Resource Management of Mobile Cloud Computing Networks and Environments*, (March), pp. 97–121.

Mayssara A. Abo Hassanin Supervised, A., Munawarah, S. H., Misnaniarti, M., Isnurhadi, I., Komunitas, J. K., Rumbai, P., City, P., Komitmen, P., Kbpkp, P., Commitment, S., Kbpkp, F., Dewi, N. M. ., Hardy, I. P. D. ., Sugianto, M. ., 19, T., Ninla Elmawati Falabiba, Anton Kristijono, Sandra, C., Herawati, Y. T., Baroya, N., Trirahayu, P., Akbar, K. A., Ramani, A., Pencapaian, A., Kapitasi, I., Komitmen, B., Victor, J., Maramis, F., Mandagi, C. K. F., Wowor, R., Kesehatan, F., Universitas, M., Ratulangi, S., Febriawati, H., Yandrizal, Y., Afriza, Y., Pratiwi, B. A., Yanuarti, R., Suryani, D., Hiv, K., Aids, D. A. N., Rumah, D. I., Utara, U. S., Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, Mayssara A. Abo Hassanin Supervised, A., Vii, B. A. B., Husada, F. R. K., Info BPJS Kesehatan, Anugrah, S. 2015, BPJS-Kesehatan, Trisnantoro, L., LAILY, E. N., Utami, D. siwi, Murti, B., Suryani, N., Kurnia, R., Fadli, Kemkes RI, BPJS Kesehatan, Laksono, T., dkk, Indonesia, U., Maujudah, S. A., Masyarakat, F. K., Studi, P. & Kesehatan, I. (2019). APPLYING EDAS AS AN APPLICABLE MCDM METHOD FOR INDUSTRIAL ROBOT SELECTION Neşe. *Paper Knowledge . Toward a Media History of Documents*, vol. 7(1), pp. 1–33 [online]. Available at:

https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/MT_Globalization_Report_2018.pdf[http://eprints.lse.ac.uk/43447/1/India_globalisation%2C society and inequalities%28Isero%29.pdf](http://eprints.lse.ac.uk/43447/1/India_globalisation%2C_society_and_inequalities%28Isero%29.pdf)<https://www.quora.com/What-is-the>.

Mitra, A. (2020). Selection of Cotton Fabrics Using EDAS Method. *Journal of Natural Fibers*. Taylor & Francis, vol. 00(00), pp. 1–13.

Mohammed, T. J., Albahri, A. S., Zaidan, A. A., Albahri, O. S., Al-Obaidi, J. R., Zaidan, B. B., Larbani, M., Mohammed, R. T. & Hadi, S. M. (2021). Convalescent-plasma-transfusion intelligent framework for rescuing COVID-19 patients across centralised/decentralised telemedicine hospitals based on AHP-group TOPSIS and matching component. *Applied Intelligence*. Springer, vol. 51(5), pp. 2956–2987.

Moslem, S., Gul, M., Farooq, D., Celik, E., Ghorbanzadeh, O. & Blaschke, T. (2020). An integrated approach of best-worst method (bwm) and triangular fuzzy sets for evaluating driver behavior factors related to road safety. *Mathematics*, vol. 8(3).

Nădăban, S., Dzitac, S. & Dzitac, I. (2016). Fuzzy TOPSIS: A General View. *Procedia Computer Science*, vol. 91(Itqm), pp. 823–831.

Nawrocki, P., Pajor, J., Sniezynski, B. & Kolodziej, J. (2022). Modeling adaptive security-aware task allocation in mobile cloud computing. *Simulation Modelling Practice and Theory*. Elsevier B.V., vol. 116(September 2021), p. 102491.

No, R. K. G., Niroomand, S., Didehkhani, H. & Mahmoodirad, A. (2021). Modified interval EDAS approach for the multi-criteria ranking problem in banking sector of Iran. *Journal of Ambient Intelligence and Humanized Computing*. Springer Berlin Heidelberg, vol. 12(7), pp. 8129–8148.

Ogwara, N. O., Petrova, K., Yang, M. L. & MacDonell, S. (2021). Enhancing Data Security in the User Layer of Mobile Cloud Computing Environment: A Novel Approach, pp. 129–145.

Özkan, B., Erdem, M. & Özceylan, E. (2022). Evaluation of Asian Countries using Data Center

Security Index: A Spherical Fuzzy AHP-based EDAS Approach. *Computers and Security*, vol. 122.

Pamučar, D., Ecer, F., Cirovic, G. & Arlasheedi, M. A. (2020). Application of improved best worst method (BWM) in real-world problems. *Mathematics*, vol. 8(8).

Panos M. Pardalos. (2000). A Comparative Study Applied Optimization.

Paul, A. B., Biswas, S., Nandi, S. & Chakraborty, S. (2018). MATEM: A unified framework based on trust and MCDM for assuring security, reliability and QoS in DTN routing. *Journal of Network and Computer Applications*. Elsevier, vol. 104(November 2016), pp. 1–20.

Poongavanam, G., Sivalingam, V., Prabakaran, R., Salman, M. & Kim, S. C. (2021). Selection of the best refrigerant for replacing R134a in automobile air conditioning system using different MCDM methods: A comparative study. *Case Studies in Thermal Engineering*. Elsevier Ltd, vol. 27(August), p. 101344.

Qahtan, S., Alsattar, H. A., Zaidan, A. A., Deveci, M., Pamucar, D. & Ding, W. (2023). A novel fuel supply system modelling approach for electric vehicles under Pythagorean probabilistic hesitant fuzzy sets. *Information Sciences*. Elsevier Inc., vol. 622, pp. 1014–1032.

Qahtan, S., Alsattar, H. A., Zaidan, A. A., Deveci, M., Pamucar, D. & Martinez, L. (2023). A comparative study of evaluating and benchmarking sign language recognition system-based wearable sensory devices using a single fuzzy set. *Knowledge-Based Systems*. Elsevier B.V., vol. 269, p. 110519.

Qahtan, S., Alsattar, H. A., Zaidan, A. A., Pamucar, D. & Deveci, M. (2022). Integrated sustainable transportation modelling approaches for electronic passenger vehicle in the context of industry 5.0. *Journal of Innovation and Knowledge*. Elsevier Espana, S.L., vol. 7(4), p. 100277.

Qahtan, S., H.A.Alsattar, A.A.Zaidan, Pamucar, D. & Deveci, M. (2022a). Feed-forward and Backward Procedures to Benchmark the Integrated Sustainable Transportation Modelling Approaches for Electronic Passenger Vehicle based on the Extension of Probabilistic Hesitant

Fuzzy Set and Multi Criteria Decision Making. *ieee transactions on fuzzy systems*.

Qahtan, S., H.A.Alsattar, A.A.Zaidan, Pamucar, D. & Deveci, M. (2022b). Integrated Sustainable Transportation Modelling Approaches for Electronic Passenger Vehicle in the Context of Industry 5.0 Under Probabilistic Hesitant Fuzzy Set. *Journal of Innovation & Knowledge*.

Qahtan, S., Yatim, K., Zaidan, A. A., Alsattar, H. A., Albahri, O. S., Zaidan, B. B., Alamoodi, A. H., Zulzalil, H., Osman, M. H. & Mohammed, R. T. (2022). Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems. *IEEE Transactions on Industrial Informatics*, (February).

Qahtan, S., Yatim, K., Zulzalil, H., Osman, M. H., Zaidan, A. A. & Alsattar, H. A. (2023). Review of healthcare industry 4.0 application-based blockchain in terms of security and privacy development attributes: Comprehensive taxonomy, open issues and challenges and recommended solution. *Journal of Network and Computer Applications*. Elsevier Ltd, vol. 209(July 2022), p. 103529.

Salem, G., OS, A., AA, Z., HA, A., AH, A. & BB, Z. (2022). Formulation of FWZIC and FDOSM under Complex Neutrosophic Environment: A Benchmarking of Smart E-Tourism Applications. *Applied Intelligence*.

Salih, M. M., Albahri, O. S., Zaidan, A. A., Zaidan, B. B., Jumaah, F. M. & Albahri, A. S. (2021). Benchmarking of AQM methods of network congestion control based on extension of interval type-2 trapezoidal fuzzy decision by opinion score method. *Telecommunication Systems*. Springer, vol. 77(3), pp. 493–522.

Salih, M. M., Zaidan, B. B. & Zaidan, A. A. (2020). Fuzzy decision by opinion score method. *Applied Soft Computing Journal*. Elsevier B.V., vol. 96, p. 106595.

Sarah, Q., Alsattar, H. A., Zaidan, A. A. & Pamucar, D. (2022). Toward and Performance Measure of Sustainable Transportation in the Shipping Industry: An Energy System Benchmarking Based on the Extension of q-Rung Orthopair Fuzzy Rough Sets and Multicriteria Decision-Making Methods. *ieee transactions on fuzzy systems*.

Sarah Qahtan, Alsattara, H. A., Zaidan, A. A., Deveci, M., Pamucar, D., Abbasa, I. . & Ding, W. (2022). Multiple Fuel Supply System Modelling Approaches for Electric Vehicles Under Pythagorean Probabilistic Hesitant Fuzzy Sets. *Information science*. Elsevier Inc., vol. 622, pp. 1014–1032.

Seada Abdu Wakene, Sisay Muleta Hababa, Gutema Seboka Daba & K S Ananda Kumar. (2021). Data Storage Security in Mobile Cloud Computing (MCC) using Improved Blowfish Algorithm. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, (November 2021), pp. 100–111.

Shao, S., Zhang, X., Li, Y. & Bo, C. (2018). Probabilistic single-valued (Interval) neutrosophic hesitant fuzzy set and its application in multi-attribute decision making. *Symmetry*, vol. 10(9), pp. 1–21.

Sharma, S. & Sharma, B. (2020). EDAS based selection of machine learning algorithm for diabetes detection. *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020*, (February), pp. 240–244.

Sridhar, S. & Smys, S. (2020). Hybrid RSAECC Based Secure Communication in Mobile Cloud Environment. *Wireless Personal Communications*. Springer US, vol. 111(1), pp. 429–442.

Sukumaran, S. C. & Misbahuddin, M. (2021). PCR and Bio-signature for data confidentiality and integrity in mobile cloud computing. *Journal of King Saud University - Computer and Information Sciences*. King Saud University, vol. 33(4), pp. 426–435.

Talal, M., Ramli, K. N., Zaidan, A. A., Zaidan, B. B. & Jumaa, F. (2020). Review on car-following sensor based and data-generation mapping for safety and traffic management and road map toward ITS. *Vehicular Communications*. Elsevier, vol. 25, p. 100280.

Tanwar, S., Mehrotra, D. & Nagpal, R. (2020). Identifying the best network security using EDAS. *Proceedings of the Confluence 2020 - 10th International Conference on Cloud Computing, Data Science and Engineering*. IEEE, pp. 445–449.

Torbacki, W. (2021). A hybrid mcdm model combining danp and promethee ii methods for the

assessment of cybersecurity in industry 4.0. *Sustainability (Switzerland)*, vol. 13(16).

Trivyza, N. L., Rentizelas, A., Theotokatos, G. & Boulougouris, E. (2022). Decision support methods for sustainable ship energy systems: A state-of-the-art review. *Energy*. Pergamon, vol. 239, p. 122288.

Turskis, Z., Goranin, N., Nurusheva, A. & Boranbayev, S. (2019). Information security risk assessment in critical infrastructure: A hybrid MCDM approach. *Informatica (Netherlands)*, vol. 30(1), pp. 187–211.

U.S.Mahmoud, A.S.Albahri, H.A.AlSattar, A.A.Zaidan, M.Talal, R.A.Mohammed, O.S.Albahri, Zaidan, B. B., A.H.Alamoodi & Qahtan, S. (2022). DAS Benchmarking Methodology based on FWZIC II and FDOSM II to Support Industrial Community Characteristics in the Design and Implementation of Advanced Driver Assistance Systems in Vehicles. *Journal of Ambient Intelligence and Humanized Computing*.

Wilczynski, A., Kolodziej, J. & Grzonka, D. (2021). Security aspects in blockchain-based scheduling in mobile multi-cloud computing. *Proceedings - 21st IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, CCGrid 2021*, pp. 696–703.

Yang, X., Huang, X. & Liu, J. K. (2016). Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing. *Future Generation Computer Systems*. Elsevier B.V., vol. 62, pp. 190–195.

Youssef, A. E. (2020). An integrated MCDM approach for cloud service selection based on TOPSIS and BWM. *IEEE Access*. IEEE, vol. 8, pp. 71851–71865.

Zavadskas, E. K., Stević, Ž., Turskis, Z. & Tomašević, M. (2019). A novel extended EDAS in Minkowski space (EDAS-M) method for evaluating autonomous vehicles. *Studies in Informatics and Control*, vol. 28(3), pp. 255–264.

Zhang, N., Su, W., Zhang, C. & Zeng, S. (2022). Evaluation and selection model of community group purchase platform based on WEPLPA-CPT-EDAS method. *Computers & Industrial Engineering*. Elsevier Ltd, vol. 172(PA), p. 108573.

Zhang, S., Gao, H., Wei, G., Wei, Y. & Wei, C. (2019). Evaluation based on distance from average solution method for multiple criteria group decision making under picture 2-tuple linguistic environment. *Mathematics*, vol. 7(3).

Zheng, J., Cai, Y., Wu, Y. & Shen, X. (2019). Dynamic computation offloading for mobile cloud computing: A stochastic game-theoretic approach. *IEEE Transactions on Mobile Computing*. IEEE, vol. 18(4), pp. 771–786.

Zhou, Z. & Huang, D. (2012). Efficient and secure data storage operations for mobile cloud computing. *Proceedings of the 2012 8th International Conference on Network and Service Management, CNSM 2012*, pp. 37–45.

APPENDIXES

Appendix A : Security Evaluation Criteria



Weighting Security Evaluation Criteria for Mobile Cloud Computing Delegation Methods: A Survey

Greetings and salutations to the participant,

This is Sendeyah Salem Al Hantoobi, a Ph.D. graduate student at British University in Dubai from United Arab Emirates, conducting research on the evaluation criteria of Mobile Cloud computing (MCC) delegation methods systems. The aim of this study is to determine the significance of security criteria in the context of MCC delegation method. The research question is "Weighting the security evaluation criteria of MCC delegation methods".

We would like to invite you to participate in this research by assess the importance level of each criterion in terms of securing MCC delegation methods systems. You will be asked to place a tick in the respective column to indicate your answer, ranging from "Not Important" to "Very Important".

Your participation in this study is highly appreciated, and your input will contribute significantly to the success of this research.

Thank you for your valuable assistance.

Brief about the research topic

The purpose of this survey is to collect data on the weighting of security evaluation criteria regarding security issues of Mobile Cloud Computing (MCC) delegation methods. The concept of delegation involves transferring operations from mobile devices to the cloud to achieve optimal performance, given the mobile's limited resources and capabilities. For this research, only four delegation methods, namely Layering, Encryption, Dynamic Offloading, and Authentication, will be considered. The survey comprises two parts, with the first part being Personal Information and the second part focused on weighting the security evaluation criteria.

Part A: Personal Information

The confidentiality and privacy of the survey participants' personal information will be maintained throughout the research study. Any personal information collected will be solely utilized for research purposes and will not be disclosed to any external parties

1. Your current position:
2. Your organization:
3. Your working experience (Years) :

1 - 2	3 – 5	6 – 10	10 – 15	More than 15

Part B: Weighting the security evaluation criteria.

Kindly specify the degree of significance for each security assessment measure concerning the Mobile Cloud Computing (MCC) delegation methods

	Weighting Scale	Not important	Slight important	Moderately important	Important	Very important
	Security Criteria					
1	General Security					
2	Privacy					
3	Authentication					
4	Cloud to Client Authentication					
5	Multi-factor authentication					
6	Communication channel					
7	Data Security					
8	Security Threats set					
9	Encryption Key					
10	Single Failure point					
11	un proper Access Control					
12	Authorization					

13	Anonymity					
----	-----------	--	--	--	--	--

Appendix B : Decision Matrix Results

Table 28: Encryption Delegation Method Decision matrix

Delegation Method	MCC Modules	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity
Encryption	SM_01	1	1	1	0	1	1	0	1	1	1	0	1	1
	SM_02	1	1	1	0	1	1	0	1	0	1	1	1	1
	SM_03	1	1	0	0	1	1	0	1	0	1	1	0	1
	SM_04	1	1	1	0	1	1	0	1	0	1	1	1	1
	SM_05	1	1	1	0	1	1	0	1	1	1	0	1	1
	SM_06	1	1	1	0	1	1	1	1	0	1	1	1	1
	SM_07	1	1	0	1	1	1	1	1	1	1	1	1	1
	SM_08	1	0	1	0	1	1	0	0	1	1	1	1	1
	SM_09	1	1	0	0	1	1	0	1	1	1	1	1	1
	SM_10	0	0	0	0	0	0	1	0	0	0	1	1	1
	SM_11	1	1	1	0	1	1	1	1	1	1	1	1	1
	SM_12	1	1	1	0	1	1	1	0	1	1	1	1	1
	SM_13	1	1	1	0	1	0	1	1	1	1	1	1	1
	SM_14	1	1	1	0	1	1	0	1	1	1	1	1	1
	SM_15	1	1	1	0	1	1	1	1	0	1	1	1	1
	SM_16	1	1	1	0	1	1	1	1	1	1	1	0	1
	SM_17	1	1	1	0	1	1	1	0	1	1	1	1	1
	SM_18	1	1	1	0	1	1	1	0	1	1	1	1	1
	SM_19	1	1	1	0	1	0	1	1	1	1	1	1	1
	SM_20	1	1	1	0	1	1	1	0	1	1	1	1	1
	SM_21	1	1	1	0	1	0	1	1	1	1	1	1	1
	SM_22	1	1	1	0	1	1	1	0	1	1	1	1	1
	SM_23	1	1	1	0	0	1	1	1	1	1	1	1	1

Table 29: Dynamic Offloading Delegation Method Decision matrix

Delegation Method	MCC Modules	General Security	Privacy	Authentication		Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity
Dynamic Offloading	SM_01	1	0	1	0	1	1	1	1	0	1	1	1	1
	SM_02	1	1	1	1	1	1	1	0	1	1	1	1	1
	SM_03	1	1	1	1	1	1	1	0	1	1	1	1	1
	SM_04	1	1	1	0	1	1	0	1	1	1	1	1	1
	SM_05	1	1	1	0	1	1	0	1	1	1	1	1	1
	SM_06	1	1	1	0	1	1	0	1	1	1	1	1	1

Table 30: Authentication Delegation Method Decision matrix

Delegation Method	MCC Modules	General Security	Privacy	Authentication	Cloud to Client Authentication	Multi-factor authentication	Communication channel	Data Security	Security Threats set	Encryption Key	Single Failure point	un proper Access Control	Authorization	Anonymity
Authentication	SM_01	1	1	0	0	1	1	0	1	1	1	1	1	1
	SM_02	1	1	0	0	1	1	1	1	1	1	1	1	1
	SM_03	1	1	0	0	1	1	1	1	1	1	1	1	1
	SM_04	1	1	1	0	1	1	0	0	1	1	1	1	1
	SM_05	1	1	1	0	1	1	1	0	1	1	1	1	1
	SM_06	1	1	0	0	1	1	1	1	1	1	1	1	1
	SM_07	1	1	1	0	1	1	1	1	1	1	1	0	1
	SM_08	1	0	1	0	1	1	1	0	1	1	1	1	1
	SM_09	1	1	1	0	1	1	0	1	1	1	1	1	1
	SM_10	1	1	1	0	1	1	1	1	1	0	1	1	1
	SM_11	1	1	1	0	1	1	1	1	1	1	1	0	1
	SM_12	1	1	1	0	1	0	0	1	1	1	1	1	1