ORIGINAL ARTICLE

OPEN ACCESS

Enhancing Cloud Security Through Ranking of Multi-Layer Authentication Based on a Complex q-Rung Orthopair Fuzzy Frank CRITIC-MABAC Model

Khurram Ali [1], Hafiz Muhammad Waqas [2], Özen Özer [3]

Authors' Affiliation:

[1,2]Department of Mathematics & Statistics, International Islamic University (IIU), Islamabad, Pakistan
Email: khurram.ali8521@gmail.com
Email: hafizmwaqas009@gmail.com

[3]Department of Mathematics, Faculty of Science & Arts, Kirklareli University, Kirklareli, Türkiye
Email: ozenozer@klu.edu.tr

Article History:

Submitted: January 28, 2026
Revised: May 23, 2026
Accepted: June 14, 2026
Published online: June 30, 2026

Corresponding author(s):

Khurram Ali
Email: khurram.ali8521@gmail.com

ABSTRACT

Multi-layer authentication (MLA) plays a critical role in enhancing cloud security by preventing unauthorized access and mitigating evolving cyber threats. Despite the availability of numerous MLA strategies, their evaluation and selection remain challenging due to conflicting criteria, uncertain information, and subjective expert judgments. Existing decision-making approaches often have limited capability to model complex uncertainty and effectively capture the interrelationships among evaluation criteria, which may affect the reliability of the final ranking results. Motivated by these limitations, this study proposes a novel Complex q-Rung Orthopair Fuzzy Frank CRITIC-MABAC (Cq-ROFF-CRITIC-MABAC) framework for the evaluation and ranking of MLA strategies in cloud computing environments. The proposed framework integrates Cq-ROFSs to represent uncertain information, Frank aggregation operators to combine expert assessments, the CRITIC method to determine objective criteria weights, and the MABAC method to rank competing alternatives. A real-world case study is conducted to demonstrate the applicability and effectiveness of the proposed framework. The results indicate that the proposed method generates stable, consistent, and discriminative rankings, while comparative and sensitivity analyses confirm its robustness and superiority over existing MCDM approaches. The proposed framework contributes a comprehensive decision-support model for cloud security assessment and provides practical guidance for cloud service providers and security practitioners in selecting the most appropriate MLA strategy.

Keywords: Cloud security; Multi-factor authentication; Complex q-rung orthopair fuzzy sets; Frank operators; CRITIC-MABAC; Multi-criteria decision-making.

(MSC2020) Codes: 03E72, 03B52,68M25

1. | INTRODUCTION

The rapid expansion of cloud computing has fundamentally transformed modern digital ecosystems by enabling scalable, flexible, and on-demand access to computing resources and services. With the growing deployment of critical data, applications, and large-scale user interactions in the cloud, data security, privacy, and access control in the cloud are of growing importance. Cloud computing systems face a myriad of security risks, including unauthorized access, identity theft, data breaches, and sophisticated cyber-attacks, that can impact their security, privacy, and availability. So, cloud access and authentication remain a backbone of secure and reliable cloud computing environments. MLA is a successful method to solve the above-mentioned problems, as it combines a number of authentication technologies including passwords, biometrics, cryptographic tokens, behavioral patterns, and context information. But the design and selection of an optimal MLA scheme is a non-trivial task, as cloud authentication strategies need to be evaluated based on several, sometimes conflicting criteria, such as security, usability, scalability, computational efficiency, adaptability to security threats, and user acceptance. In addition, these parameters are interlinked and may have different weights in different application scenarios and cloud service paradigms. The uncertainty, subjectivity, and vagueness inherent in the opinions of experts also complicate the assessment and prioritization of MLA strategies. The conventional security evaluation methods and classical MCDM methods are not adequate for coping with the multi-dimensional uncertainty and fuzziness. Classical methods of MCDM have been developed to rank alternatives based on multiple criteria, but they require and assume certain and deterministic information, which does not apply to actual problems in cloud security. To overcome this problem, the idea of fuzzy set (FS) theory has been widely applied to integrate MCDM techniques into the modelling of uncertainty or linguistic judgments. Generalizations such as intuitionistic fuzzy sets (IFSs) and Pythagorean fuzzy sets (PFSs) offer a higher degree of expressiveness as they take into account non-membership information; however, they are still not able to handle higher-order uncertainty and complex-valued expert judgements. With the challenges reported in the previous research, this research presents a Cq-ROFF-CRITIC-MABAC framework for structured evaluation and ranking of MLAs in cloud computing environments. The scheme incorporates a complex-valued uncertainty model, flexible Frank aggregation, objective criteria weighting, and an efficient ranking mechanism into one integrated decision support system. By bridging the gap between advanced fuzzy decision-making theories and the practical cloud security requirements, the proposed approach enables a robust, reliable, and scalable solution that will improve the security of authentication and facilitate informed decision-making in next-generation cloud systems. Further, many authors have applied this concept in various areas and presented their views, such as an MLA system, which has been recommended by [1], confirming the theory of having multiple verifications, which offers a better security mechanism against unauthorized access to the cloud. This model is in line with the theoretical notion of defense-in-depth, which is the use of multiple security mechanisms at multiple layers to ensure cumulative security against various threats. Kumar et al. [2] developed an MLA model that involves the use of quality-of-service performance analysis with a strong emphasis on the theory of security-performance trade-off. The paper highlights that the authentication mechanisms should not only be secure but also efficient, which means they should achieve the performance expectations of a system, and illustrates the idea of having well-balanced security mechanisms without impacting functionality or throughput. The multi-level security of the cloud issues described by [3] proposed an abstract model of vulnerability in the data, network, and application layers, which is theoretically illustrative. This classification re-emphasizes the concept of threat management at multiple levels, which implies that if there is control over the threat at different levels, its security will be comprehensive, and the vulnerability of security loopholes will be minimal. To support these models, [4] proposed an approach called a user-friendly and secure architecture, which uses a combination of strong authentication and user experience. To provide further standing for the theoretical and practical importance of MLA, [5] highlighted increased applications of multi-factor authentication techniques to various cloud computing systems and pointed out that it has been successful in minimizing unauthorized access and improving security. Otta et al. [6] have reviewed the MLA schemes, in which systematic evaluation frameworks are highlighted as a crucial element to compare authentication approaches in different aspects of quality, such as reliability, scalability, and usability. The studies mentioned above demonstrate that the best cloud security is based on a multi-layered, multi-user, and structured approach that is supported by theory and practice. The basic features of cloud security decisions are multiple criteria, including technical reliability, user experience, cost, efficiency, and flexibility against new threats. Secondly, fuzziness, imprecision, and subjective use of experts also complicate the decision-making process, which renders traditional approaches of evaluation ineffective. There is a pressing need for rigorous, systematic, and reliable frameworks that will be able to address these problems and provide practical recommendations on the most effective authentication schemes. To address this issue, the present study proposes a Cq-ROFF-CRITIC-MABAC approach to evaluate and prioritize MLA schemes to enhance cloud security. The Cq-ROFS is used to handle higher-order uncertainty in decision-making problems. It represents membership and non-membership degrees in complex form, allowing more flexible modeling of uncertain and imprecise information. The parameter q controls the range of these degrees, giving more freedom in expressing expert opinions and reducing information loss. This makes the Cq-ROF framework suitable for dealing with uncertainty in cloud security problems. Although the research in cloud security and MLA has made significant advances, there are still several shortcomings identified in the current evaluation models. Most traditional MCDM methods are deterministic and cannot well deal with uncertainty and vagueness arising from expert judgments. While fuzzy extensions like IFSs and PFSs have enhanced uncertainty modeling, they may not be sufficient for capturing the complexity of higher-order and complex-valued uncertain information that is typically found in cloud security assessment scenarios. Moreover, current research has not yet linked flexible aggregation mechanisms, objective criteria weighting, and powerful ranking methods together in the context of assessing MLA strategies. Thus, there is a need for a complete decision-support model that is suitable to deal with complex uncertainty and provides reliable and objective rankings. In order to fill this gap, this paper proposes a new framework called Cq-ROFF-CRITIC-MABAC which integrates the expressive power of Cq-ROFSs, the flexibility of Frank aggregation operators, the objectivity of CRITIC weighting, and the stability of MABAC ranking.

1.1. | Study Framework

This paper is organized into eight sections. Section 1 presents the introduction, which highlights why MLA should be used to secure the cloud environment, its history, and significance. Section 2 discusses the research problem and the contributions of the research. Section 3 provides a review of the literature in the areas of cloud security, fuzzy decision-making, and hybrid MCDM techniques. In Section 4, the fundamentals of Cq-ROFSs are given. Section 5 introduces the proposed Cq-ROFF aggregation operators, which have been developed to deal with uncertainty and the interdependency of multi-criteria assessments. Section 6 discusses the detailed usage of these operators in the CRITIC-MABAC decision-making method for secure cloud authentication mechanisms. Section 7 contrasts the proposed model with the existing fuzzy and MCDM models to demonstrate the stability and superiority of the proposed model. Finally, Section 8 concludes the study with a discussion of the results, implications, and future research lines. A graphical representation of the manuscript is shown in Figure 1.

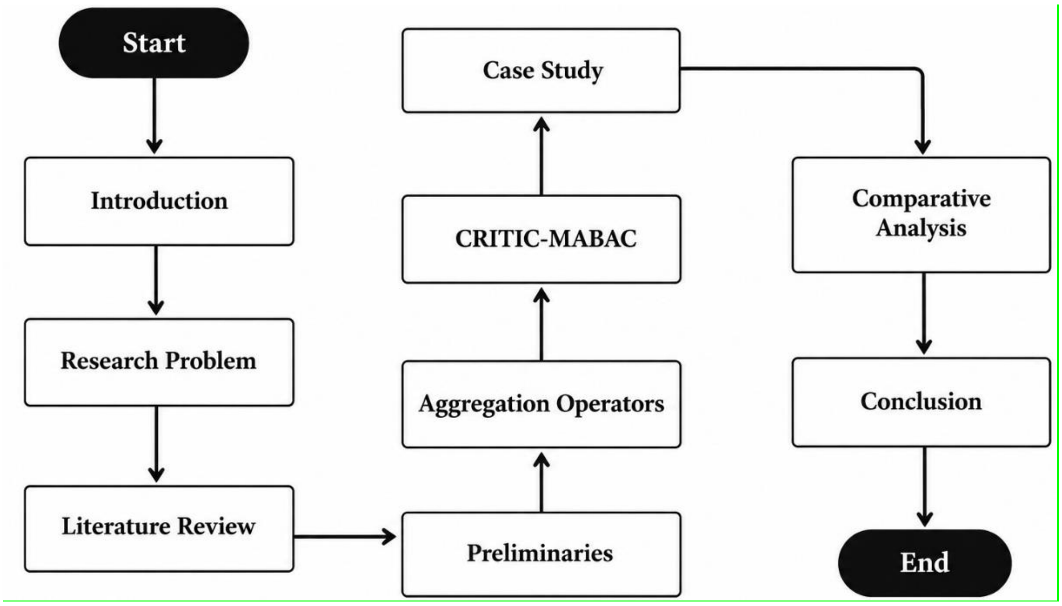

Figure 1. Manuscript Road Map.

1.2. | Research Problem

MLA has become a key security solution in cloud computing to protect systems from unauthorized access, data leakage, identity theft, and advanced cyberattacks. With the increasing adoption of cloud services, businesses are increasingly turning to MLA solutions to protect critical data, comply with regulatory standards, and maintain business continuity. But choosing the right MLA strategy is not straightforward. It involves multiple criteria that often conflict with each other, such as authentication strength, user convenience, computational cost, scalability, and resilience against future threats. This is a decision-making role that is further confused by expert assessments, which are usually vague, incomplete, and subjective. The problem of multidimensionality of uncertainty in cloud security assessment cannot be addressed by the traditional decision-making methods, including the classical and basic FS-based ones. Advanced fuzzy approaches like the IF approach, PF approach, and q-ROFSs can model uncertainty in terms of membership and non-membership grades, but cannot deal with higher-order uncertainty, interdependencies among the criteria, and the complex structure and the nature of the expert assessments. In order to overcome these challenges, the present work suggests a Cq-ROFF-CRITIC-MABAC framework for ranking the MLA strategies in cloud security. To model uncertainty and get a more realistic representation of expert opinions, the proposed model represents uncertainty by complex values on the membership and non-membership sets of the complex plane. Furthermore, the weights are assigned in an objective manner in the CRITIC method, and the MABAC method gives a systematic and strong ranking. The use of Frank aggregation operators retains expert preferences and the interdependencies between criteria, leading to stable, transparent, and highly discriminative decisions. Moreover, in the literature, different MCDM frameworks discuss MLA, such as Youssef et al. [7], who introduced an integrated framework of MCDM grounded on TOPSIS and BWM of cloud service selection to offer a structured approach to cloud alternative evaluation based on various criteria. Nevertheless, the framework is based on traditional real-valued information and is thus inappropriate to represent the multidimensional uncertainty that exists in the secure cloud and MLA environment, where uncertainty simultaneously depends upon authentication levels, threat interactions, and operating environments. Mostafa [8] suggested a cloud service selection model developed as a model of the MCDM best-only method, which is more effective in weighting but deterministic in assessments, and neglects all multidimensional uncertainty related to the changing authentication reliability and security risk. Tomar et al.[9] proposed a hybrid MCDM model that is more accurate in decision-making by combining several methods; however, the model uses the conventional uncertainty representations and is not expressive enough to represent the q-rung orthopair information of higher degrees of freedom, resulting in the loss of information in the complex cloud security assessment. Similarly, Tiwari and Kumar [10] introduced a strong MCDM model with modified TOPSIS to enhance the stability of the ranking, but the model fails to model the interrelations between the different evaluation criteria under multidimensional uncertainty, nor does it accommodate the flexibility of representing the uncertainty degree across different authentication levels.

A critical synthesis of these studies reveals several unresolved research gaps:

- Existing MCDM-based cloud evaluation frameworks are unable to model multidimensional q-rung orthopair uncertainty that naturally arises in MLA decision problems.
- The adjustable q-rung structure, where membership and non-membership information modeling are handled independently and flexibly, has not been explored much in cloud authentication assessment.
- Interdependence between security, usability, and cost quality under uncertainty of multidimensionality is not captured and, hence, results in poor prioritization results.
- Current ranking mechanisms exhibit limited discrimination and robustness when alternatives perform similarly under uncertain and dynamic conditions.

To bridge these gaps, this study proposes a Cq-ROFF-CRITIC-MABAC framework for the evaluation and ranking of MLA strategies in secure cloud environments. Moreover, characteristics of the proposed work and existing theories are given in Table 1.

Table 1. Characteristic coverage table (0=No, 1=Yes).

Characteristics Covered	Youssef et al. [7]	Mostafa [8]	Tomar et al. [9]	Tiwari and Kumar [10]	Proposed Work
Identification of cloud security threats	Yes	Yes	Yes	Yes	Yes
Discussion of authentication mechanisms	No	No	No	No	Yes
MLA security approach	No	No	No	No	Yes
Uncertainty handling	No	No	No	No	Yes
Systematic ranking frameworks	No	No	No	No	Yes
MCDM decision-making	Yes	Yes	Yes	Yes	Yes

Characteristic comparison of cloud security studies with the proposed work is shown in Figure 2.

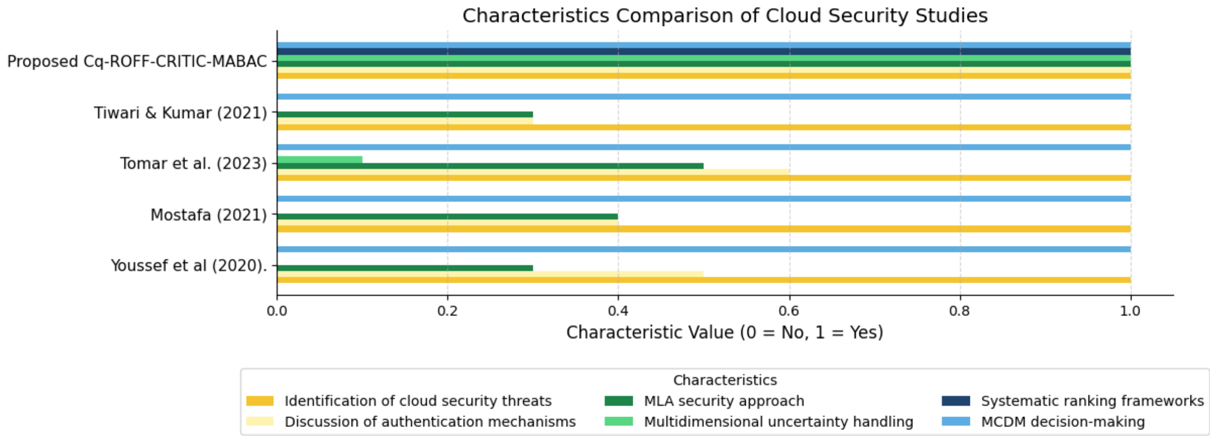

Figure 2. Characteristic comparison b/w other theories and the proposed work.

1.3. | Contributions

The evaluation of MLA strategies in cloud security is critically challenged by multidimensional, interdependent, and conflicting uncertainties inherent in expert judgments. Typical existing frameworks are not sufficient to model these uncertainties, leading to less reliable, robust, and interpretable security assessments. To overcome these limitations, this paper proposes a new Cq-ROFF-CRITIC-MABAC model that provides a systematic, uncertainty-conscious, and data-driven model to rank MLA strategies. The key contributions of this research are:

a) Development of four advanced Cq-ROF Frank aggregation operators:

- Cq-ROF Frank weighted average (Cq-ROFFWA) operators.
- Cq-ROF Frank ordered weighted average (Cq-ROFFOWA) operators.
- Cq-ROF Frank weighted geometric (Cq-ROFFWG) operators.
- Cq-ROF Frank ordered weighted geometric (Cq-ROFFOWG) operators.

These operators enable a good combination of multidimensional expert judgments, sustain interdependences between criteria, sustain critical reviews, and properly address hesitation and contradictory views. They greatly improve consistency, openness, and clarity of group decision-making.

b) The proposed model combines the operators of Cq-ROFF with the CRITIC weighting method and MABAC ranking method, and enables a systematic, objective, and uncertainty-aware prioritization of MLA strategies when there is incomparable and interdependent performance measurement.

c) The framework is applied to real-life cloud security contexts, and it proves to provide the capacity to support organizations in choosing the best authentication strategies.

d) The comparative analysis of the proposed Cq-ROFF-CRITIC-MABAC model and current methods of fuzzy, MCDM, and complex fuzzy models proves that the proposed approach is more accurate, more stable, and reliable in the process of making the decision, and could be called a powerful tool to optimize the management of cloud security.

The proposed study is organized into four main components, including mathematical foundations, research problem formulation, CRITIC-MABAC methodology, and comparative analysis. Each part explains a specific stage of the research, starting from basic concepts to final evaluation and results. This flow provides a clear understanding of how the proposed framework is developed and applied, as shown in Figure 3.

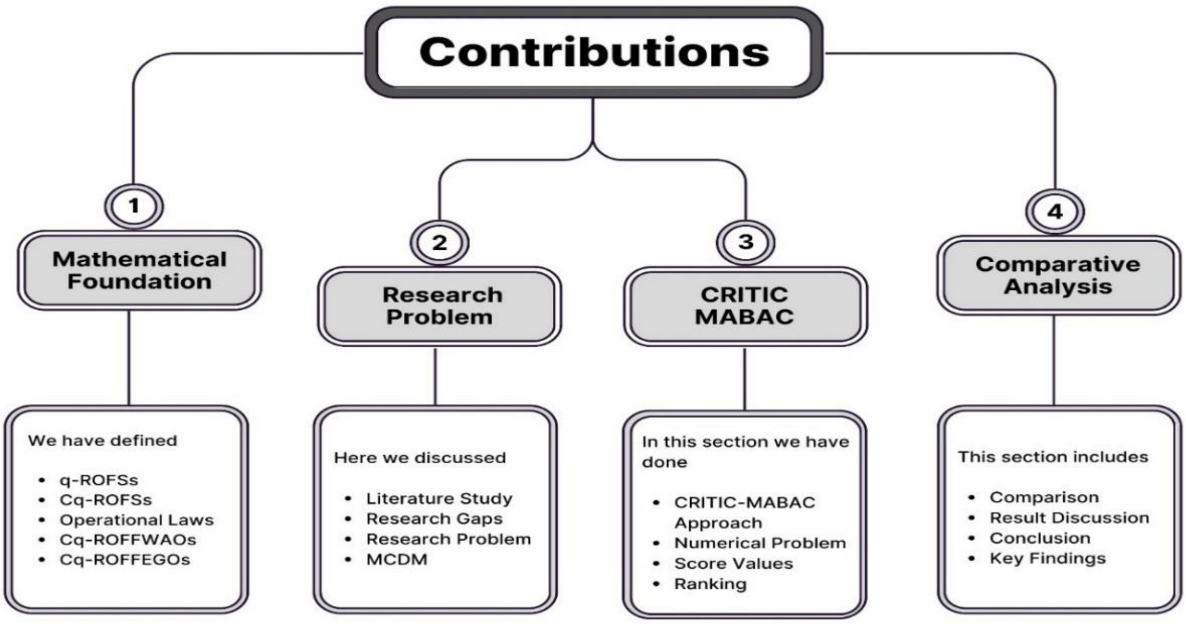

Figure 3. Main contributions of proposed work.

2. | LITERATURE REVIEW

Cloud security has emerged as one of the keystones of the contemporary digital infrastructure after the increasing use of cloud resources to store and process sensitive data in organizations. Cloud environments are truly the most flexible, scalable, and economical, but they also present some serious risks that may interfere with data confidentiality, integrity, and availability. Not only will cloud security help to avoid unauthorized access, data breaches, and cyber-attacks, but also guarantee regulatory compliance, business continuity, and organizational trust. When organizations do not have effective protection, they experience significant operational, financial, and reputational impacts, which makes it highly significant to prepare holistic and proactive security measures. Omer et al. [11] introduced a background survey of the concept of cloud security, types of services, limitations, and challenges, yet their research was not systematic in nature, as it was more of a description rather than a systematic assessment of security measures. [12] have examined the current cloud security models and pinpointed the loopholes in identity and access management, and suggested qualitative measures, but their method failed to offer objective ranking and prioritization of authentication measures. Kumar and Goyal [13] assessed cloud security requirements, threats, and vulnerabilities and countermeasures, but based on deterministic models and did not consider the uncertainty and interdependency of the security decisions in the real world. As the complexity of operations increases, feasible remediation methods have been sought. The cybersecurity vulnerabilities and mitigation identified by [14], based on cloud security tools, and the operational relevance of the focus on intrusion detection and automated access control, were not considered in this study. The vagueness and uncertainty of the expert judgment on the authentication strategies were not considered in this study. The review of security concerns of clouds, threats, and attack vectors offered by [15] emphasized the role of multi-factor and layered authentication as the means of fighting the hi-tech cyber threats, yet failed to offer a formal model upon which alternative strategies may be compared or ranked. Deshpande et al. [16] conducted a thorough cryptographic evaluation aimed at improving data confidentiality and integrity and found that encryption was effective in securing the cloud services, but the authentication was one-sided without advocating the multi-criteria trade-offs in terms of usability, scalability, and costs. Kumar and Sah [2] presented an MLA model for cloud environments that incorporates security and QoS aspects. They found that implementing multiple authentication layers could improve cloud security without compromising system performance and resource utilization. Saradha et al. [17] proposed an efficient auditing scheme to enhance the security of cloud data and access control. Their way of doing things strengthened data security and liability, highlighting the significance of robust audit trails in preventing unauthorized access and security dangers. Despite notable progress, significant research gaps persist. Most of the previous work focuses on cloud security from one technical or conceptual perspective, without offering integrated and uncertainty-aware frameworks for evaluating MLA. Moreover, the uncertainty of expert judgments in making decisions about cloud security is subjective and imprecise in many aspects, and there are many conflicting expert judgments. Traditional evaluation methods do not capture more complex uncertainty, reluctance, and inter-criteria relations in the real-world cloud environment. However, the procedures to determine the weighting and ranking of the MLA alternatives using objective criteria have not been standardized in MCDM. The limitations thus imposed pose an urgent need for better fuzzy decision-making models that can deliver strong-order uncertainty and deliver strong and defensible rankings. This paper, in turn, presents a Cq-ROFF-CRITIC-MABAC model to evaluate and rank MLA strategies in a systematic way, which satisfies critical gaps in the study of the topic of secure cloud authentication.

2.1. | Literature Review on MCDM with different fuzzy frameworks

MCDM is proven to be one of the most efficient analytical paradigms to deal with complex decision problems involving conflicting criteria, uncertain information, and subjective evaluations by experts. The application of fuzzy theory and MCDM has improved the capacity of decision-support systems to deal with imprecise and vague information much better. Abdullah [18] did an extensive review of fuzzy MCDM methodologies and showed their applicability in various decision domains. Similarly, [19] proposed a fuzzy MCDM model for supplier selection, and they demonstrated the effectiveness of fuzzy approaches in decision-making problems in the industry. [20] evaluated the energy performance of buildings with fuzzy MCDM techniques, and [21] proposed an integrated fuzzy decision-making model for prioritizing the renewable energy options. The [22] suggested a fuzzy MCDM model based on graph theory for the selection of the location of disaster containers, where uncertainty is present. They showed that fuzzy decision-making techniques can be useful in the real world for complex criteria and emphasized the necessity for using complex fuzzy MCDM techniques in real-world decision problems. These trailblazing research works laid the groundwork for fuzzy MCDM and showed its usefulness for practical applications in the solution of complex, real-world problems. But classical FSs are only capable of carrying membership information and therefore are limited in modelling the uncertainty and hesitation involved in an expert assessment. The drawbacks of the traditional FSs were overcome by the more expressive representation of membership and non-membership degrees, which is achievable through IFSs. Sharma et al. [23] presented a review on the development of fuzzy and IF-based MCDM methods and highlighted the significance of these methods in the field of decision making under uncertainty. The [24] defined knowledge measures in IFSs and showed their use in MCDM problems. To address the issue of the inconsistency of the decision, [25] proposed a modified IF MCDM methodology, and Tao et al. [26]

presented a dynamic group decision-making framework that can address evolving preference structures. Faizi et al. [27] also applied the IFSs approach to the problem of group decision-making. Furthermore, [28] used IF MCDM techniques in cloud service provider selection, which illustrates the actual importance of uncertainty-aware decision-making support in cloud computing environments. On one hand, IFSs provided a relatively better representation of uncertainty than classical FSs, but on the other hand, the limited feasible domain of IFSs limits their capability of modelling highly uncertain and complex decision information. To further improve the uncertainty representation, researchers adopted complex-valued fuzzy environments and developed advanced aggregation mechanisms. In order to solve complex decision-making problems, [29] proposed interval-valued complex single-valued neutrosophic aggregation operators and proved that they are effective in complex decision-making. Similarly, [30] presented complex IF power interaction aggregation operators and their applications to MCDM problems. These studies showed that complex-valued IFSs have more descriptive power than the traditional real-valued framework and offer a richer representation of experts' assessments of uncertainty. A big step forward in fuzzy decision-making was made by introducing PFSs, which extended the allowable range of membership and non-membership grades. Peng et al. [31] combined the PF information and CRITIC and CoCoSo methodologies to analyze the alternatives in the 5G industry to get better decision discrimination performance. The [32] introduced a hybrid PF MCDM model, while [33] used a PF CRITIC-VIKOR model for agricultural decision-making. Similarly, [34] made another effort to make aggregation more flexible by combining Schweizer-Sklar operational laws with PF rough sets. In spite of the fact that PF environments can represent more information than IFSs, they still have limitations in the decision structures to be real-valued and cannot represent more complicated uncertainty information. Recently, q-ROFSs have attracted considerable attention owing to their superior flexibility and stronger uncertainty modeling capability. The main difference between the IFS and q-ROFSs is that the latter allows a significantly larger information space for expressing expert judgments by relaxing the constraints imposed by IFSs and PFSs. Biswas et al. [35] applied the concept of q-ROF numbers to analyse EVs from a comparative perspective, and [36] presented a q-ROF PROMETHEE method for MCDM. The [37] proposed an orthopair fuzzy group decision-making model with supplier selection by using a new distance function, and [38] extended the use of orthopair fuzzy soft sets in group decision making. Some methodological improvements were introduced by [39], who combined the extended MABAC approach with Aczel–Alsina generalized weighted Bonferroni mean operators to better consider inter-criteria relationships. Then [40] suggested a holistic decision analytics framework, which explicitly accounts for the correlation among the criteria, and [41] went on to propose a Dice-Jaccard similarity-based decision model for the selection of a green hydrogen electrolyzer to enhance the discriminatory power of the alternatives. Moreover, [42] proposed a q-ROF MADM model with the use of Frank operational laws and power aggregation operators, which showed the effectiveness of the Frank operations in providing flexibility in aggregation and robustness in decision making. Moreover, [43] presented entropy-based measures under q-ROF soft sets, which further enhanced the theoretical aspect and practical application of the q-ROF decision-making models. Ali et al. [44] proposed circular p, q-quasirung FSs and new aggregation operators for improving the uncertainty modelling of decision-making problems. The proposed framework was applied to the problem of green supplier selection, showing its ability to deal with the information of evaluation in a complex and uncertain situation. While there have been important advances in fuzzy MCDM, several research challenges have been left open. The classical fuzzy model, IF model, PF model, and q-ROF model have been evolving in the direction of representing uncertain information, but most models of decision-making are still created under real-valued environments. They may, therefore, not be representative of the complex nature of expert assessments that one might encounter in modern decision problems with a security concern. Moreover, although the latest advances have studied higher-order aggregation rules like Aczel-Alsina, Schweizer-Sklar, and Frank operational laws, these rules have been investigated mostly within the traditional fuzzy structures. One of the challenges is the integration of the operational laws of Frank fuzzy logic in the Cq-ROF environment, which has not yet been explored. The provided gap justifies the addition of the Cq-ROFF-CRITIC-MABAC model, which adds much more detailed information to the existing paradigms and provides multidimensional decision details and, in the end, the opportunity to rank the MLA approaches used to ensure the security of clouds more correctly and reliably.

3. | PRELIMINARIES

This section presents the basic definition of Cq-ROFSs and explains their operational laws and main mathematical properties.

Definition 1: [49] Let $\hat{\mathrm{H}}$ be the universal set. Then Cq-ROFS Ŧ can be expressed as;

$$\text{Ŧ} = \left\{\left(\hat{\mathrm{h}}, \text{ß}^{\breve{\mathrm{m}}}(\hat{\mathrm{h}}), \text{ß}^{\breve{\mathrm{n}}}(\hat{\mathrm{h}})\right) | \hat{\mathrm{h}} \in \hat{\mathrm{H}}\right\} = \left\{\left(\hat{\mathrm{h}}, \text{ß}^{\overline{\breve{\mathrm{m}}\mathrm{r}}} + \iota\text{ß}^{\overline{\breve{\mathrm{m}}\iota}}, \text{ß}^{\overline{\breve{\mathrm{n}}\mathrm{r}}} + \iota\text{ß}^{\overline{\breve{\mathrm{n}}\iota}}\right) | \hat{\mathrm{h}} \in \hat{\mathrm{H}}\right\} \tag{1}$$

Where, $\text{ß}^{\breve{\mathrm{m}}} : \hat{\mathrm{H}} \to [0,1]$ is the grade of membership and $\text{ß}^{\breve{\mathrm{n}}} : \hat{\mathrm{H}} \to [0,1]$ is the grade of non-membership satisfying the condition

$$0 \leq \left(\text{ß}^{\overline{\breve{\mathrm{m}}\mathrm{r}}}\right)^{\hat{\mathrm{q}}} + \left(\text{ß}^{\overline{\breve{\mathrm{n}}\mathrm{r}}}\right)^{\hat{\mathrm{q}}} \leq 1 \text{ and } 0 \leq \left(\text{ß}^{\overline{\breve{\mathrm{m}}\iota}}\right)^{\hat{\mathrm{q}}} + \left(\text{ß}^{\overline{\breve{\mathrm{n}}\iota}}\right)^{\hat{\mathrm{q}}} \leq 1$$

Where, $\hat{\mathrm{q}} \geq 1$.

For simplicity, Cq-ROFN is denoted by: $\text{Ŧ} = \left\{\text{ß}^{\overline{\breve{\mathrm{m}}\mathrm{r}}} + \iota\text{ß}^{\overline{\breve{\mathrm{m}}\iota}}, \text{ß}^{\overline{\breve{\mathrm{n}}\mathrm{r}}} + \iota\text{ß}^{\overline{\breve{\mathrm{n}}\iota}}\right\}$.

Definition 2: [49] Let $\text{Ŧ} = \left\{\text{ß}^{\overline{\breve{\mathrm{m}}\mathrm{r}}} + \iota\text{ß}^{\overline{\breve{\mathrm{m}}\iota}}, \text{ß}^{\overline{\breve{\mathrm{n}}\mathrm{r}}} + \iota\text{ß}^{\overline{\breve{\mathrm{n}}\iota}}\right\}$ be a Cq-ROFN, then the score and accuracy are defined as;

$$\mathcal{S}(\text{Ŧ}) = \frac{1}{4}\left\{2 + \left(\text{ß}^{\overline{\text{mr}}}\right)^{\hat{q}} + \left(\text{ß}^{\overline{\text{mi}}}\right)^{\hat{q}} - (\text{ß}^{\overline{\text{nr}}})^{\hat{q}} - (\text{ß}^{\overline{\text{ni}}})^{\hat{q}}\right\}$$

$$\mathcal{A}(\text{Ŧ}) = \frac{1}{4}\left\{2 + (\text{ß}^{\overline{\text{mr}}})^{\hat{q}} + \left(\text{ß}^{\overline{\text{nr}}}\right)^{\hat{q}} + (\text{ß}^{\overline{\text{mi}}})^{\hat{q}} + (\text{ß}^{\overline{\text{ni}}})^{\hat{q}}\right\}$$

Definition 3: [49] Let $\text{Ŧ}_1 = \left\{\text{ß}_1^{\overline{\text{mr}}} + \iota\text{ß}_1^{\overline{\text{mi}}}, \text{ß}_1^{\overline{\text{nr}}} + \iota\text{ß}_1^{\overline{\text{ni}}}\right\}$ and $\text{Ŧ}_2 = \left\{\text{ß}_2^{\overline{\text{mr}}} + \iota\text{ß}_2^{\overline{\text{mi}}}, \text{ß}_2^{\overline{\text{nr}}} + \iota\text{ß}_2^{\overline{\text{ni}}}\right\}$ be two Cq-ROFNs; the following operational laws are satisfied

$$1.\, \text{Ŧ}_1 \oplus \text{Ŧ}_2 = \left(\begin{array}{c} \sqrt[\hat{q}]{\left(\text{ß}_1^{\overline{\text{mr}}}\right)^{\hat{q}} + \left(\text{ß}_2^{\overline{\text{mr}}}\right)^{\hat{q}} - \left(\text{ß}_1^{\overline{\text{mr}}}\right)^{\hat{q}}\left(\text{ß}_2^{\overline{\text{mr}}}\right)^{\hat{q}}} + \\ \iota\sqrt[\hat{q}]{(\text{ß}_1^{\overline{\text{mi}}})^{\hat{q}} + (\text{ß}_2^{\overline{\text{mi}}})^{\hat{q}} - (\text{ß}_1^{\overline{\text{mi}}})^{\hat{q}}(\text{ß}_2^{\overline{\text{mi}}})^{\hat{q}}}, \\ \left(\text{ß}_1^{\overline{\text{nr}}}\right)\left(\text{ß}_2^{\overline{\text{nr}}}\right) + \iota\left(\text{ß}_1^{\overline{\text{ni}}}\right)\left(\text{ß}_2^{\overline{\text{ni}}}\right) \end{array}\right)$$

$$2.\text{Ŧ}_1 \otimes \text{Ŧ}_2 = \left(\begin{array}{c} (\text{ß}_1^{\overline{\text{mr}}})(\text{ß}_2^{\overline{\text{mr}}}) + \iota(\text{ß}_1^{\overline{\text{mi}}})(\text{ß}_2^{\overline{\text{mi}}}), \\ \sqrt[\hat{q}]{\left(\text{ß}_1^{\overline{\text{nr}}}\right)^{\hat{q}} + \left(\text{ß}_2^{\overline{\text{nr}}}\right)^{\hat{q}} - \left(\text{ß}_1^{\overline{\text{nr}}}\right)^{\hat{q}}\left(\text{ß}_2^{\overline{\text{nr}}}\right)^{\hat{q}}} + \\ \iota\sqrt[\hat{q}]{\left(\text{ß}_1^{\overline{\text{ni}}}\right)^{\hat{q}} + \left(\text{ß}_2^{\overline{\text{ni}}}\right)^{\hat{q}} - \left(\text{ß}_1^{\overline{\text{ni}}}\right)^{\hat{q}}\left(\text{ß}_2^{\overline{\text{NI}}}\right)^{\hat{q}}} \end{array}\right)$$

$$3.\, \lambda(\text{Ŧ}) = \left(\sqrt[\hat{q}]{1 - (1 - (\text{ß}^{\overline{\text{mr}}})^{\hat{q}})^{\lambda}} + \iota\sqrt[\hat{q}]{1 - (1 - (\text{ß}^{\overline{\text{mi}}})^{\hat{q}})^{\lambda}}, \text{ß}^{\overline{\text{nr}}} + \iota\text{ß}^{\overline{\text{ni}}}\right)$$

$$4.\, \text{Ŧ}^{\lambda} = \left(\text{ß}^{\overline{\text{mr}}} + \iota\text{ß}^{\overline{\text{mi}}}, \sqrt[\hat{q}]{1 - (1 - (\text{ß}^{\overline{\text{nr}}})^{\hat{q}})^{\lambda}} + \iota\sqrt[\hat{q}]{1 - (1 - (\text{ß}^{\overline{\text{ni}}})^{\hat{q}})^{\lambda}}\right)$$

Definition 4: [50] Consider μ and ν to be two real numbers. Then the Frank t norm and t conorm are defined as

$$\text{Fra}^{t}(\mu, \nu) = \log_{\xi}\left(1 + \frac{(\xi^{\mu} - 1)(\xi^{\nu} - 1)}{\xi - 1}\right)$$

$$\text{Fra}^{c}(\mu, \nu) = 1 - \log_{\xi}\left(1 + \frac{(\xi^{1-\mu} - 1)(\xi^{1-\nu} - 1)}{\xi - 1}\right)$$

Where $(\mu, \nu) \in [0,1] \times [0,1]$ and $\xi \neq 1$.

4. | FRANK AGGREGATION OPERATORS BASED ON CQ-ROFNS

Frank operational laws provide a flexible aggregation framework through a tunable parameter that adapts to different levels of criteria interaction. They generalize multiple t-norms and t-conorms, offering a unified and consistent structure. Their smoothness and stability improve the reliability of results. Overall, they effectively capture complex relationships in uncertain decision-making environments.

In this section, Frank operational laws for Cq-ROFNs are formulated, followed by the development of several Frank aggregation operators, namely Cq-ROFFWA and Cq-ROFFWG.

Definition 5: Let λ and ξ be two real numbers. Then Frank t-norm and Frank t-conorm for three Cq-ROFNs Ŧ, Ŧ_1, and Ŧ_2 are defined as;

$$1.\ \text{Ŧ}_1 \oplus \text{Ŧ}_2 = \begin{pmatrix} \sqrt[\hat{q}]{1 - log_\xi\left(1 + \frac{\left(\xi^{1-\left(\text{ß}_1^{\widetilde{mr}}\right)^{\hat{q}}} - 1\right)\left(\xi^{1-\left(\text{ß}_2^{\widetilde{mr}}\right)^{\hat{q}}} - 1\right)}{\xi - 1}\right)} + \\ \iota\sqrt[\hat{q}]{1 - log_\xi\left(1 + \frac{\left(\xi^{1-\left(\text{ß}_1^{\widetilde{m\iota}}\right)^{\hat{q}}} - 1\right)\left(\xi^{1-\left(\text{ß}_2^{\widetilde{m\iota}}\right)^{\hat{q}}} - 1\right)}{\xi - 1}\right)} \\ \sqrt[\hat{q}]{log_\xi\left(1 + \frac{\left(\xi^{\left(\text{ß}_1^{\widetilde{nr}}\right)^{\hat{q}}} - 1\right)\left(\xi^{\left(\text{ß}_2^{\widetilde{nr}}\right)^{\hat{q}}} - 1\right)}{\xi - 1}\right)} + \iota\sqrt[\hat{q}]{log_\xi\left(1 + \frac{\left(\xi^{\left(\text{ß}_1^{\widetilde{n\iota}}\right)^{\hat{q}}} - 1\right)\left(\xi^{\left(\text{ß}_2^{\widetilde{n\iota}}\right)^{\hat{q}}} - 1\right)}{\xi - 1}\right)} \end{pmatrix}$$

$$2.\ \text{Ŧ}_1 \otimes \text{Ŧ}_2 = \begin{pmatrix} \sqrt[\hat{q}]{log_\xi\left(1 + \frac{\left(\xi^{\left(\text{ß}_1^{\widetilde{mr}}\right)^{\hat{q}}} - 1\right)\left(\xi^{\left(\text{ß}_2^{\widetilde{mr}}\right)^{\hat{q}}} - 1\right)}{\xi - 1}\right)} + \iota\sqrt[\hat{q}]{log_\xi\left(1 + \frac{\left(\xi^{\left(\text{ß}_1^{\widetilde{m\iota}}\right)^{\hat{q}}} - 1\right)\left(\xi^{\left(\text{ß}_2^{\widetilde{m\iota}}\right)^{\hat{q}}} - 1\right)}{\xi - 1}\right)}, \\ \sqrt[\hat{q}]{1 - log_\xi\left(1 + \frac{\left(\xi^{1-\left(\text{ß}_1^{\widetilde{nr}}\right)^{\hat{q}}} - 1\right)\left(\xi^{1-\left(\text{ß}_2^{\widetilde{nr}}\right)^{\hat{q}}} - 1\right)}{\xi - 1}\right)} + \\ \iota\sqrt[\hat{q}]{1 - log_\xi\left(1 + \frac{\left(\xi^{1-\left(\text{ß}_1^{\widetilde{n\iota}}\right)^{\hat{q}}} - 1\right)\left(\xi^{1-\left(\text{ß}_2^{\widetilde{n\iota}}\right)^{\hat{q}}} - 1\right)}{\xi - 1}\right)} \end{pmatrix}$$

$$3.\ \lambda\text{Ŧ} = \begin{pmatrix} \sqrt[\hat{q}]{1 - log_\xi\left(1 + \frac{\left(\xi^{1-\left(\text{ß}^{\widetilde{mr}}\right)^{\hat{q}}} - 1\right)^{\lambda}}{(\xi - 1)^{\lambda-1}}\right)} + \iota\sqrt[\hat{q}]{1 - log_\xi\left(1 + \frac{\left(\xi^{1-\left(\text{ß}^{\widetilde{m\iota}}\right)^{\hat{q}}} - 1\right)^{\lambda}}{(\xi - 1)^{\lambda-1}}\right)}, \\ \sqrt[\hat{q}]{log_\xi\left(1 + \frac{\left(\xi^{\left(\text{ß}^{\widetilde{nr}}\right)^{\hat{q}}} - 1\right)^{\lambda}}{(\xi - 1)^{\lambda-1}}\right)} + \iota\sqrt[\hat{q}]{log_\xi\left(1 + \frac{\left(\xi^{\left(\text{ß}^{\widetilde{n\iota}}\right)^{\hat{q}}} - 1\right)^{\lambda}}{(\xi - 1)^{\lambda-1}}\right)} \end{pmatrix}$$

$$4.\ \text{Ŧ}^{\lambda} = \begin{pmatrix} \sqrt[\hat{q}]{log_\xi\left(1 + \frac{\left(\xi^{\left(\text{ß}^{\widetilde{mr}}\right)^{\hat{q}}} - 1\right)^{\lambda}}{(\xi - 1)^{\lambda-1}}\right)} + \iota\sqrt[\hat{q}]{log_\xi\left(1 + \frac{\left(\xi^{\left(\text{ß}^{\widetilde{m\iota}}\right)^{\hat{q}}} - 1\right)^{\lambda}}{(\xi - 1)^{\lambda-1}}\right)}, \\ \sqrt[\hat{q}]{1 - log_\xi\left(1 + \frac{\left(\xi^{1-\left(\text{ß}^{\widetilde{nr}}\right)^{\hat{q}}} - 1\right)^{\lambda}}{(\xi - 1)^{\lambda-1}}\right)} + \iota\sqrt[\hat{q}]{1 - log_\xi\left(1 + \frac{\left(\xi^{1-\left(\text{ß}^{\widetilde{n\iota}}\right)^{\hat{q}}} - 1\right)^{\lambda}}{(\xi - 1)^{\lambda-1}}\right)} \end{pmatrix}$$

Definition 6: Let $Ŧ_{ķ} = (ß_{ķ}^{\check{m}}, ß_{ķ}^{\check{n}}) = \{ß_{ķ}^{\check{m}r} + \iota ß_{ķ}^{\check{m}\iota}, ß_{ķ}^{\check{n}r} + \iota ß_{ķ}^{\check{n}\iota}\} (ķ = 1,2,3, \dots, ź)$ be a collection of Cq-ROFNs with the weight $w_{ķ}$ $(ķ = 1,2,3, \dots, ź)$ satisfying $w_{ķ} \in [0,1]$ and $\sum_{ķ=1}^{ź} w_{ķ} = 1$. Then the Cq-ROFFWA operator is defined as;

$$\mathrm{Cq} - \mathrm{ROFFWA}(Ŧ_1, Ŧ_2, \dots, Ŧ_{ķ}) = \sum_{ķ=1}^{ź} w_{ķ} Ŧ_{ķ} \tag{2}$$

Theorem 1: By using eq. (2), the Cq-ROFN aggregation operator consistently generates a result that is itself a Cq-ROFN and;

$$\mathrm{Cq} - \mathrm{ROFFWA}(Ŧ_1, Ŧ_2, \dots, Ŧ_{ķ})$$

$$= \left(\begin{array}{c} \sqrt[\hat{q}]{1 - log_{\xi}\left(1 + \prod_{ķ=1}^{ź}\left(\xi^{1-\left(ß_{ķ}^{\check{m}r}\right)^{\hat{q}}} - 1\right)^{w_{ķ}}\right)} + \iota \sqrt[\hat{q}]{1 - log_{\xi}\left(1 + \prod_{ķ=1}^{ź}\left(\xi^{1-\left(ß_{ķ}^{\check{m}\iota}\right)^{\hat{q}}} - 1\right)^{w_{ķ}}\right)}, \\ \sqrt[\hat{q}]{log_{\xi}\left(1 + \prod_{ķ=1}^{ź}\left(\xi^{\left(ß_{ķ}^{\check{n}r}\right)^{\hat{q}}} - 1\right)^{w_{ķ}}\right)} + \iota \sqrt[\hat{q}]{log_{\xi}\left(1 + \prod_{ķ=1}^{ź}\left(\xi^{\left(ß_{ķ}^{\check{n}\iota}\right)^{\hat{q}}} - 1\right)^{w_{ķ}}\right)} \end{array} \right) \tag{3}$$

Definition 7: Let $Ŧ_{ķ} = (ß_{ķ}^{\check{m}}, ß_{ķ}^{\check{n}}) = \{ß_{ķ}^{\check{m}r} + \iota ß_{ķ}^{\check{m}\iota}, ß_{ķ}^{\check{n}r} + \iota ß_{ķ}^{\check{n}\iota}\} (ķ = 1,2,3, \dots, ź)$ be a collection of Cq-ROFNs with the weight $w_{ķ}$ $(ķ = 1,2,3, \dots, ź)$ satisfying $w_{ķ} \in [0,1]$ and $\sum_{ķ=1}^{ź} w_{ķ} = 1$. Then the Cq-ROFFWG operator is defined as;

$$\mathrm{Cq} - \mathrm{ROFFWG}(Ŧ_1, Ŧ_2, \dots, Ŧ_{ķ}) = \prod_{ķ=1}^{ź} (Ŧ_{ķ})^{w_{ķ}} \tag{4}$$

Theorem 2: By using eq. (4), the Cq-ROFN aggregation operator consistently generates a result that is itself a Cq-ROFN and

$$\mathrm{Cq} - \mathrm{ROFFWG}(Ŧ_1, Ŧ_2, \dots, Ŧ_{ķ})$$

$$= \left(\begin{array}{c} \sqrt[\hat{q}]{log_{\xi}\left(1 + \prod_{ķ=1}^{ź}\left(\xi^{\left(ß_{ķ}^{\check{m}r}\right)^{\hat{q}}} - 1\right)^{w_{ķ}}\right)} + \iota \sqrt[\hat{q}]{log_{\xi}\left(1 + \prod_{ķ=1}^{ź}\left(\xi^{\left(ß_{ķ}^{\check{m}\iota}\right)^{\hat{q}}} - 1\right)^{w_{ķ}}\right)}, \\ \sqrt[\hat{q}]{1 - log_{\xi}\left(1 + \prod_{ķ=1}^{ź}\left(\xi^{1-\left(ß_{ķ}^{\check{n}r}\right)^{\hat{q}}} - 1\right)^{w_{ķ}}\right)} + \iota \sqrt[\hat{q}]{1 - log_{\xi}\left(1 + \prod_{ķ=1}^{ź}\left(\xi^{1-\left(ß_{ķ}^{\check{n}\iota}\right)^{\hat{q}}} - 1\right)^{w_{ķ}}\right)} \end{array} \right) \tag{5}$$

5. | CRITIC-MABAC APPROACH

In this section, we introduce the CRITIC-MABAC method using Cq-ROFNs in consideration of the introduced aggregation operators. The CRITIC method can be used to calculate the objective weight of the criteria, taking into account the conflict between them and the variability of the criteria. This helps to minimize subjectivity and increase the reliability of the evaluation process. The MABAC method was chosen because it is based on measuring the distance of the alternatives from the border approximation area and has the ability to give stable and reliable rankings. In contrast to some traditional ranking approaches, MABAC is a simple, robust, and effective alternative ranking approach that can effectively distinguish between the competing alternatives. These features make it especially appropriate for testing MLA approaches of different authentication criteria and uncertain expert judgements.

The algorithm of CRITIC-MABAC is shown in Figure 4.

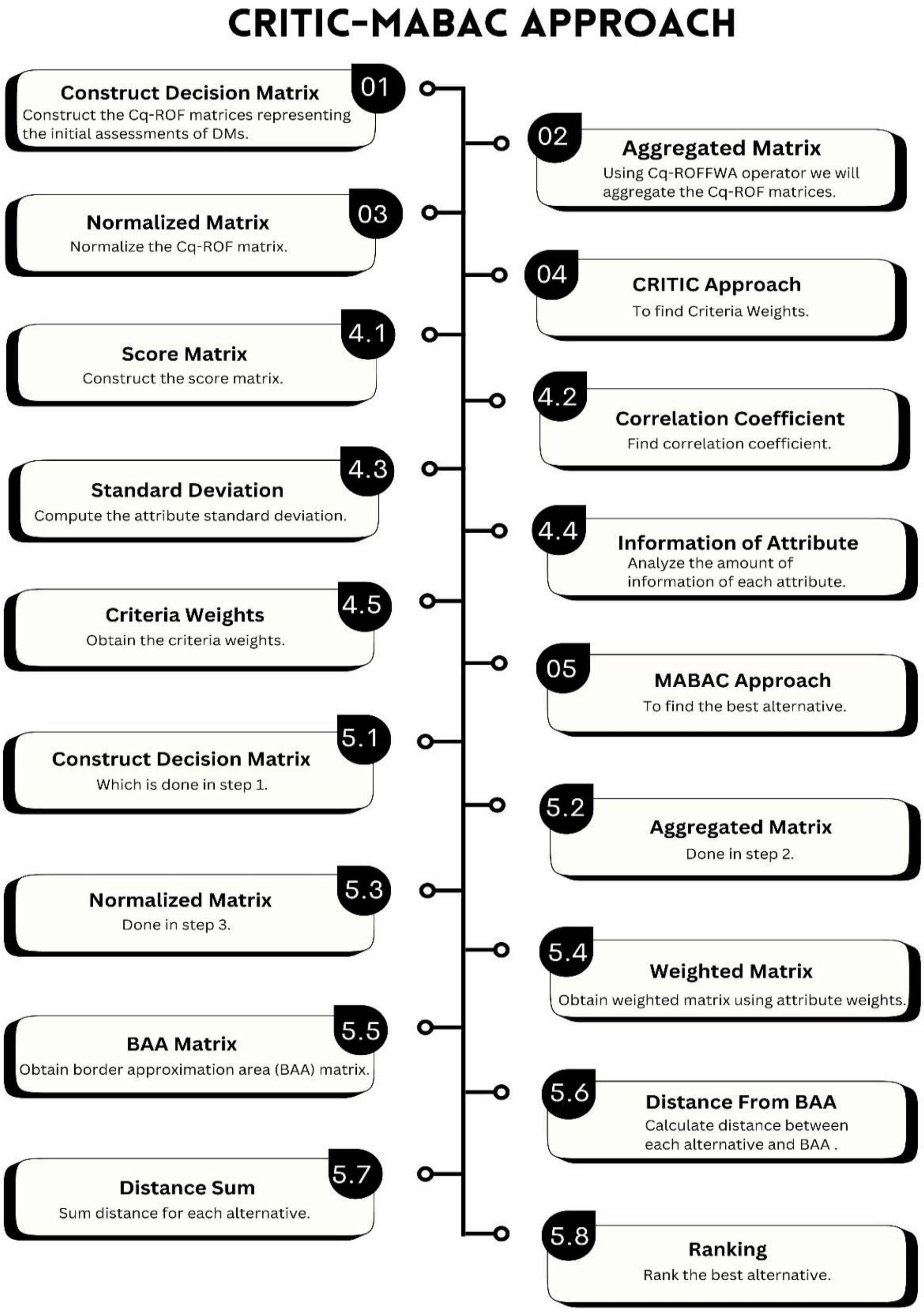

Figure 4. CRITIC-MABAC approach roadmap.

To address an MCDM problem involving $ź$ alternatives $(₦_1, ₦_2, \dots, ₦_{ź})$, where these alternatives are evaluated by experts $(\tilde{E}_1, \tilde{E}_2, \dots, \tilde{E}_{ź})$ in a Cq-ROF environment across a set of $ķ$ distinct attributes $(Å_1, Å_2, \dots, Å_{ķ})$. Additionally, expert weight is given as $w = (w_1, w_1, \dots, w_{ķ})$ where $w_t \in [0,1]$ and $\sum_{t=1}^{ķ} w_t = 1$. Where the weight of attributes calculated by the CRITIC method is $\omega = (\omega_1, \omega_1, \dots, \omega_{ķ})$ where $\omega_t \in [0,1]$ and $\sum_{t=1}^{ķ} \omega_t = 1$.

Algorithm;

The algorithm of CRITIC-MABAC has the following steps.

Step 1: Construct the Cq-ROF matrices representing the initial assessments of DMs.

$$D_{ij}^{t} = \begin{pmatrix} \begin{pmatrix} \left(ß_{11}^{\overline{m}r}\right)^t + \iota\left(ß_{11}^{\overline{m}\iota}\right)^t, \\ (ß_{11}^{\overline{n}r})^t + \iota(ß_{11}^{\overline{n}\iota})^t \end{pmatrix} & \begin{pmatrix} \left(ß_{12}^{\overline{m}r}\right)^t + \iota\left(ß_{12}^{\overline{m}\iota}\right)^t, \\ (ß_{12}^{\overline{n}r})^t + \iota(ß_{12}^{\overline{n}\iota})^t \end{pmatrix} & \cdots & \begin{pmatrix} \left(ß_{1y}^{\overline{m}r}\right)^t + \iota\left(ß_{1y}^{\overline{m}\iota}\right)^t, \\ (ß_{1y}^{\overline{n}r})^t + \iota(ß_{1y}^{\overline{n}\iota})^t \end{pmatrix} \\ \begin{pmatrix} \left(ß_{21}^{\overline{m}r}\right)^t + \iota\left(ß_{21}^{\overline{m}\iota}\right)^t, \\ (ß_{21}^{\overline{n}r})^t + \iota(ß_{21}^{\overline{n}\iota})^t \end{pmatrix} & \begin{pmatrix} \left(ß_{22}^{\overline{m}r}\right)^t + \iota\left(ß_{22}^{\overline{m}\iota}\right)^t, \\ (ß_{22}^{\overline{n}r})^t + \iota(ß_{22}^{\overline{n}\iota})^t \end{pmatrix} & \cdots & \begin{pmatrix} \left(ß_{2y}^{\overline{m}r}\right)^t + \iota\left(ß_{2y}^{\overline{m}\iota}\right)^t, \\ (ß_{2y}^{\overline{n}r})^t + \iota(ß_{2y}^{\overline{n}\iota})^t \end{pmatrix} \\ \vdots & \vdots & \vdots & \vdots \\ \begin{pmatrix} \left(ß_{x1}^{\overline{m}r}\right)^t + \iota\left(ß_{x1}^{\overline{m}\iota}\right)^t, \\ (ß_{x1}^{\overline{n}r})^t + \iota(ß_{x1}^{\overline{n}\iota})^t \end{pmatrix} & \begin{pmatrix} \left(ß_{x2}^{\overline{m}r}\right)^t + \iota\left(ß_{x2}^{\overline{m}\iota}\right)^t, \\ (ß_{x2}^{\overline{n}r})^t + \iota(ß_{x2}^{\overline{n}\iota})^t \end{pmatrix} & \cdots & \begin{pmatrix} \left(ß_{xy}^{\overline{m}r}\right)^t + \iota\left(ß_{xy}^{\overline{m}\iota}\right)^t, \\ (ß_{xy}^{\overline{n}r})^t + \iota(ß_{xy}^{\overline{n}\iota})^t \end{pmatrix} \end{pmatrix}$$

Step 2: Using the Cq-ROFFWA operator, we will aggregate the Cq-ROF matrices.

Step 3: Normalize the Cq-ROF matrix.

For benefit type data.

$$D'_{ij} = \left\{ß^{\overline{m}r} + \iota ß^{\overline{m}\iota}, ß^{\overline{n}r} + \iota ß^{\overline{n}\iota}\right\}$$

For benefit type data.

$$D'_{ij} = \left\{(1 - ß^{\overline{m}r}) + \iota\left(1 - ß^{\overline{m}\iota}\right), (1 - ß^{\overline{n}r}) + \iota(1 - ß^{\overline{n}\iota})\right\}$$

Step 4: Calculation of criteria weights through the CRITIC approach

Step 4.1: Construct the score matrix;

$$\mathbb{S}_{ij} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1y} \\ c_{21} & c_{22} & \cdots & c_{2y} \\ \vdots & \vdots & \ddots & \vdots \\ c_{x1} & c_{x2} & \cdots & c_{xy} \end{bmatrix}$$

Step 4.2: Find the correlation coefficient.

$$\tau_{jk} = \frac{\sum_{i=1}^{x}\left(c_{ij} - \overline{c_j}\right)\left(c_{ik} - \overline{c_k}\right)}{\sqrt{\sum_{i=1}^{x}\left(c_{ij} - \overline{c_j}\right)^2 \sum_{i=1}^{x}\left(c_{ik} - \overline{c_k}\right)^2}}$$

Step 4.3: Compute the attribute standard deviation;

$$ꞩ_j = \sqrt{\frac{\sum_{i=1}^{x}\left(c_{ij} - \overline{c_j}\right)^2}{x}}$$

Step 4.4: Now we will analyze the amount of information of each attribute, which represents the degree of useful discriminatory information carried by a criterion. It is determined based on the variability of the criterion values and their interrelationships with other criteria. A higher value indicates greater importance and contribution of that attribute in the decision-making process.

$$\phi_j = \text{ş}_j \sum_{k=1}^{y} (1 - \tau_{jk}), \qquad j = 1,2, \dots y$$

Step 4.5: Obtain the criteria weights.

$$\omega_j = {\phi_j}\Big/{\sum_{j=1}^{y} \phi_j}$$

Step 5: Now we will use the MABAC method, which has the following steps.

Step 5.1: Construct an initial decision matrix representing the assessments of decision-makers, as obtained in Step 1.

Step 5.2: Using the Cq-ROFFWA operator, we will aggregate the matrices as done in Step 2.

Step 5.3: Next, we will normalize the data as done in Step 3.

Step 5.4: Now we will obtain the normalized matrix using weights of attributes (obtained in Step 4.5) by the following formula.

$$\mathcal{N}_{ij} = \omega_j D_{ij} = \left(\begin{array}{c} \sqrt[\hat{q}]{1 - log_{\xi}\left(1 + \frac{\left(\xi^{1-(\text{ß}^{\overline{mr}})^{\hat{q}}} - 1\right)^{\omega_j}}{(\xi - 1)^{\omega_j - 1}}\right)} + \iota \sqrt[\hat{q}]{1 - log_{\xi}\left(1 + \frac{\left(\xi^{1-(\text{ß}^{\overline{m\iota}})^{\hat{q}}} - 1\right)^{\omega_j}}{(\xi - 1)^{\omega_j - 1}}\right)}, \\ \sqrt[\hat{q}]{log_{\xi}\left(1 + \frac{\left(\xi^{(\text{ß}^{\overline{nr}})^{\hat{q}}} - 1\right)^{\omega_j}}{(\xi - 1)^{\omega_j - 1}}\right)} + \iota \sqrt[\hat{q}]{log_{\xi}\left(1 + \frac{\left(\xi^{(\text{ß}^{\overline{n\iota}})^{\hat{q}}} - 1\right)^{\omega_j}}{(\xi - 1)^{\omega_j - 1}}\right)} \end{array} \right)$$

Step 5.5: Obtain the BAA matrix.

$$\mathcal{B}_{ij} = (\mathcal{N}_{ij})^{\frac{1}{g}} = \left(\begin{array}{c} \sqrt[\hat{q}]{log_{\xi}\left(1 + \prod_{i=1}^{g}\left(\xi^{\left(\text{ß}_{ij}^{\overline{mr}}\right)^{\hat{q}}} - 1\right)^{\frac{1}{g}}\right)} + \iota \sqrt[\hat{q}]{log_{\xi}\left(1 + \prod_{i=1}^{g}\left(\xi^{\left(\text{ß}_{ij}^{\overline{m\iota}}\right)^{\hat{q}}} - 1\right)^{\frac{1}{g}}\right)}, \\ \sqrt[\hat{q}]{1 - log_{\xi}\left(1 + \prod_{i=1}^{g}\left(\xi^{1-\left(\text{ß}_{ij}^{\overline{nr}}\right)^{\hat{q}}} - 1\right)^{\frac{1}{g}}\right)} + \iota \sqrt[\hat{q}]{1 - log_{\xi}\left(1 + \prod_{i=1}^{g}\left(\xi^{1-\left(\text{ß}_{ij}^{\overline{n\iota}}\right)^{\hat{q}}} - 1\right)^{\frac{1}{g}}\right)} \end{array} \right)$$

Step 5.6: Calculate the distance between each alternative and BAA by;

$$\mathfrak{D}(\mathcal{N}_{ij}, \mathcal{B}_{ij}) = \frac{1}{4}\left(\left|\mathcal{N}_{ij}^{\overline{mr}} - \mathcal{B}_{ij}^{\overline{mr}}\right| + \left|\mathcal{N}_{ij}^{\overline{m\iota}} - \mathcal{B}_{ij}^{\overline{m\iota}}\right| + \left|\mathcal{N}_{ij}^{\overline{nr}} - \mathcal{B}_{ij}^{\overline{nr}}\right| + \left|\mathcal{N}_{ij}^{\overline{n\iota}} - \mathcal{B}_{ij}^{\overline{n\iota}}\right|\right)$$

Step 5.7: Now, we will sum up the alternatives by using the following formula;

$$\dot{S}(\text{₦}_i) = \sum_{j=1}^{y} \mathfrak{D}_{ij}$$

6. | CASE STUDY

A cloud service provider aims to enhance the security of its infrastructure by implementing advanced MLA schemes. The primary goal of the provider is to choose the best option that guarantees a high level of security, ease of use, economical nature, and ability to resist unpredictable/partial threat data. The provider has difficulties in making a definite choice because of the unclear definition of the security threats, different user behavior, and incomplete assessment data. Therefore, an uncertainty-aware evaluation is essential to rank feasible MLA schemes under multiple conflicting criteria.

Need for Evaluation: The cloud provider must rigorously evaluate MLA alternatives before full-scale deployment to avoid potential security breaches, user inconvenience, and unnecessary financial burden. Each authentication method imposes different requirements in terms of technical complexity, usability, cost, and uncertainty management. Since expert judgments about these criteria are often vague, imprecise, or hesitant, conventional crisp evaluation techniques are inadequate. A robust MCDM framework capable of handling uncertainty, expert hesitation, and interdependent criteria is therefore crucial.

Proposed Framework Effectiveness: The proposed Cq-ROFF-CRITIC-MABAC model enables the provider to be more flexible and more precise in outlining the uncertain expert opinions. The CRITIC method objectively computes the weights of criteria by considering conflict and variability, in contrast to the Frank aggregation operator, which classifies the nonlinear connection between expert evaluations. MABAC also compares alternatives on the basis of their distance to the ideal solution, which provides fair and operationally viable comparisons. Together, this framework produces a realistic, defensible, and uncertainty-aware ranking of MLA schemes, guiding the provider toward the most secure and practical authentication strategy.

A cloud services provider is changing to a hybrid cloud, for which it has the alternatives shown in Table 2.

Table 2. Alternatives to secure clouds.

Symbols	Alternative	Description
$₦_1$	Passwordless Authentication via Hardware Tokens + Biometric Layer	This will remove traditional passwords, and instead, it will use hardware tokens that adhere to the FIDO2 standard and biometrics. It has a high cost of hardware and deployment and is much more limiting in scalability to millions of users, but it greatly mitigates the risk of phishing.
$₦_2$	Multi-Context Adaptive Authentication (MCAA)	Innovative and smart solution where the authentication system is dynamically set to adjust to the user context, location, device risk, and behavior. Although it has good resilience and flexibility, it is expensive to invest in machine

		learning systems and can be subject to regulatory challenges with the issue of data privacy.
$₦_3$	Password + Mobile App Push Notification + Behavioral Biometrics	An innovative authentication system that combines passwords and push notification applications, and ongoing behavioral biometrics. It enhances user-friendliness and privacy but requires high-level AI-based infrastructure and constant connectivity of the equipment.
$₦_4$	Password + SMS OTP + Biometric Authentication	One of the widely accepted MLA approaches is the use of a password with an SMS based one-time password and biometric authentication. It is very strong in terms of defense layering and susceptible to SIM swapping and phishing, and can be a source of user friction.

Criteria evaluation is discussed in Table 3.

Table 3. Criteria for evaluation.

Symbols	Attribute	Description
$Å_1$	Security Strength	Such a requirement is used to assess the general strength of the MLA approach to withstand brute-force and phishing, man-in-the-middle, and insider attacks. Financial organizations focus on those approaches that reduce the risk of breaches.
$Å_2$	Usability and User Experience	This must be user-friendly; no one will adopt a very complicated authentication system. Customers must be assured of access and security, which balances the need to keep a balance between being friction-free and offering security.
$Å_3$	Implementation Cost and Scalability	This attribute quantifies the preliminary deployment, hardware/software, and capability to expand to millions of customers. Financial institutions are required to make sure that the security investments are long-lasting over the infrastructure through which they operate.
$Å_4$	Adaptability and Regulatory Compliance	Authentication solutions should be able to keep up with the changing threat environment, as well as comply with financial laws such as PCI-DSS, GDPR, and PSD2. Adaptive solutions are preferred for long-term resilience and compliance.

6.1. | Numerical Illustration

For this assessment, three experts are engaged with weights $(0.35, 0.25, 0.4)$. Then the evaluation comprises four attributes of MLA, whose weights are objectively obtained through the CRITIC process. The Cq-ROFF-CRITIC-MABAC model is thereafter utilized to rank the alternatives of authentication.

Step 1: Cq-ROF matrices of every expert are given in Tables 4, 5, and 6.

Table 4. Values described by expert 1.

	Ả_1	Ả_2	Ả_3	Ả_4
₦_1	$\begin{pmatrix}0.84+\iota 0.74,\\0.47+\iota 0.39\end{pmatrix}$	$\begin{pmatrix}0.77+\iota 0.54,\\0.47+\iota 0.42\end{pmatrix}$	$\begin{pmatrix}0.29+\iota 0.74,\\0.81+\iota 0.55\end{pmatrix}$	$\begin{pmatrix}0.33+\iota 0.75,\\0.88+\iota 0.38\end{pmatrix}$
₦_2	$\begin{pmatrix}0.71+\iota 0.24,\\0.55+\iota 0.93\end{pmatrix}$	$\begin{pmatrix}0.65+\iota 0.69,\\0.35+\iota 0.71\end{pmatrix}$	$\begin{pmatrix}0.47+\iota 0.85,\\0.77+\iota 0.22\end{pmatrix}$	$\begin{pmatrix}0.46+\iota 0.66,\\0.71+\iota 0.29\end{pmatrix}$
₦_3	$\begin{pmatrix}0.67+\iota 0.38,\\0.74+\iota 0.74\end{pmatrix}$	$\begin{pmatrix}0.92+\iota 0.44,\\0.55+\iota 0.68\end{pmatrix}$	$\begin{pmatrix}0.88+\iota 0.67,\\0.39+\iota 0.37\end{pmatrix}$	$\begin{pmatrix}0.86+\iota 0.47,\\0.38+\iota 0.66\end{pmatrix}$
₦_4	$\begin{pmatrix}0.94+\iota 0.49,\\0.61+\iota 0.63\end{pmatrix}$	$\begin{pmatrix}0.33+\iota 0.71,\\0.78+\iota 0.37\end{pmatrix}$	$\begin{pmatrix}0.58+\iota 0.83,\\0.44+\iota 0.49\end{pmatrix}$	$\begin{pmatrix}0.77+\iota 0.61,\\0.55+\iota 0.39\end{pmatrix}$

Table 5. Values described by expert 2.

	Ả_1	Ả_2	Ả_3	Ả_4
₦_1	$\begin{pmatrix}0.74+\iota 0.59,\\0.35+\iota 0.73\end{pmatrix}$	$\begin{pmatrix}0.49+\iota 0.37,\\0.52+\iota 0.87\end{pmatrix}$	$\begin{pmatrix}0.65+\iota 0.71,\\0.48+\iota 0.44\end{pmatrix}$	$\begin{pmatrix}0.59+\iota 0.61,\\039+\iota 0.27\end{pmatrix}$
₦_2	$\begin{pmatrix}0.59+\iota 0.87,\\0.47+\iota 0.68\end{pmatrix}$	$\begin{pmatrix}0.67+\iota 0.69,\\0.46+\iota 0.37\end{pmatrix}$	$\begin{pmatrix}0.47+\iota 0.63,\\0.59+\iota 0.37\end{pmatrix}$	$\begin{pmatrix}0.66+\iota 0.49,\\0.47+\iota 0.52\end{pmatrix}$
₦_3	$\begin{pmatrix}0.67+\iota 0.68,\\0.39+\iota 0.82\end{pmatrix}$	$\begin{pmatrix}0.82+\iota 0.19,\\0.38+\iota 0.97\end{pmatrix}$	$\begin{pmatrix}0.71+\iota 0.33,\\0.36+\iota 0.74\end{pmatrix}$	$\begin{pmatrix}0.39+\iota 0.82,\\0.63+\iota 0.37\end{pmatrix}$
₦_4	$\begin{pmatrix}0.29+\iota 0.57,\\0.88+\iota 0.39\end{pmatrix}$	$\begin{pmatrix}0.63+\iota 0.28,\\0.37+\iota 0.83\end{pmatrix}$	$\begin{pmatrix}0.88+\iota 0.27,\\0.51+\iota 0.85\end{pmatrix}$	$\begin{pmatrix}0.76+\iota 0.36,\\0.45+\iota 0.77\end{pmatrix}$

Table 6. Values described by expert 3.

	Ả_1	Ả_2	Ả_3	Ả_4
₦_1	$\begin{pmatrix}0.73+\iota 0.29,\\0.29+\iota 0.93\end{pmatrix}$	$\begin{pmatrix}0.59+\iota 0.63,\\0.46+\iota 0.29\end{pmatrix}$	$\begin{pmatrix}0.68+\iota 0.71,\\0.33+\iota 0.42\end{pmatrix}$	$\begin{pmatrix}0.37+\iota 0.95,\\0.64+\iota 0.08\end{pmatrix}$
₦_2	$\begin{pmatrix}0.37+\iota 0.31,\\0.71+\iota 0.84\end{pmatrix}$	$\begin{pmatrix}0.38+\iota 0.71,\\0.66+\iota 0.33\end{pmatrix}$	$\begin{pmatrix}0.71+\iota 0.51,\\0.29+\iota 0.47\end{pmatrix}$	$\begin{pmatrix}0.48+\iota 0.19,\\0.31+\iota 0.88\end{pmatrix}$
₦_3	$\begin{pmatrix}0.66+\iota 0.71,\\0.37+\iota 0.27\end{pmatrix}$	$\begin{pmatrix}0.17+\iota 0.55,\\0.88+\iota 0.41\end{pmatrix}$	$\begin{pmatrix}0.39+\iota 0.63,\\0.57+\iota 0.37\end{pmatrix}$	$\begin{pmatrix}0.74+\iota 0.38,\\0.37+\iota 0.63\end{pmatrix}$
₦_4	$\begin{pmatrix}0.57+\iota 0.61,\\0.44+\iota 0.37\end{pmatrix}$	$\begin{pmatrix}0.91+\iota 0.53,\\0.09+\iota 0.41\end{pmatrix}$	$\begin{pmatrix}0.71+\iota 0.34,\\0.44+\iota 0.84\end{pmatrix}$	$\begin{pmatrix}0.59+\iota 0.55,\\0.45+\iota 0.61\end{pmatrix}$

Step 2: The aggregated matrix using the Cq-ROFFWA operator is shown in Table 7.

Table 7. Aggregated matrix.

	Ả_1	Ả_2	Ả_3	Ả_4
₦_1	$\begin{pmatrix}0.78+\iota 0.63,\\0.36+\iota 0.66\end{pmatrix}$	$\begin{pmatrix}0.67+\iota 0.57,\\0.48+\iota 0.44\end{pmatrix}$	$\begin{pmatrix}0.62+\iota 0.72,\\0.50+\iota 0.47\end{pmatrix}$	$\begin{pmatrix}0.47+\iota 0.87,\\0.64+\iota 0.19\end{pmatrix}$

$₦_2$	$\begin{pmatrix}0.61+\iota 0.68,\\0.59+\iota 0.83\end{pmatrix}$	$\begin{pmatrix}0.60+\iota 0.70,\\0.48+\iota 0.37\end{pmatrix}$	$\begin{pmatrix}0.61+\iota 0.73,\\0.49+\iota 0.34\end{pmatrix}$	$\begin{pmatrix}0.55+\iota 0.55,\\0.46+\iota 0.53\end{pmatrix}$
$₦_3$	$\begin{pmatrix}0.67+\iota 0.65,\\0.48+\iota 0.52\end{pmatrix}$	$\begin{pmatrix}0.82+\iota 0.48,\\0.62+\iota 0.62\end{pmatrix}$	$\begin{pmatrix}0.76+\iota 0.62,\\0.45+\iota 0.44\end{pmatrix}$	$\begin{pmatrix}0.77+\iota 0.65,\\0.43+\iota 0.56\end{pmatrix}$
$₦_4$	$\begin{pmatrix}0.81+\iota 0.57,\\0.59+\iota 0.57\end{pmatrix}$	$\begin{pmatrix}0.80+\iota 0.61,\\0.28+\iota 0.48\end{pmatrix}$	$\begin{pmatrix}0.75+\iota 0.69,\\0.46+\iota 0.71\end{pmatrix}$	$\begin{pmatrix}0.72+\iota 0.55,\\0.48+\iota 0.56\end{pmatrix}$

Step 3: As the given data is of a benefit type, the normalized matrix will be the same and displayed in Table 8.

Table 8. Normalized matrix.

	$\mathring{A}_1$	$\mathring{A}_2$	$\mathring{A}_3$	$\mathring{A}_4$
$₦_1$	$\begin{pmatrix}0.78+\iota 0.63,\\0.36+\iota 0.66\end{pmatrix}$	$\begin{pmatrix}0.67+\iota 0.57,\\0.48+\iota 0.44\end{pmatrix}$	$\begin{pmatrix}0.62+\iota 0.72,\\0.50+\iota 0.47\end{pmatrix}$	$\begin{pmatrix}0.47+\iota 0.87,\\0.64+\iota 0.19\end{pmatrix}$
$₦_2$	$\begin{pmatrix}0.61+\iota 0.68,\\0.59+\iota 0.83\end{pmatrix}$	$\begin{pmatrix}0.60+\iota 0.70,\\0.48+\iota 0.37\end{pmatrix}$	$\begin{pmatrix}0.61+\iota 0.73,\\0.49+\iota 0.34\end{pmatrix}$	$\begin{pmatrix}0.55+\iota 0.55,\\0.46+\iota 0.53\end{pmatrix}$
$₦_3$	$\begin{pmatrix}0.67+\iota 0.65,\\0.48+\iota 0.52\end{pmatrix}$	$\begin{pmatrix}0.82+\iota 0.48,\\0.62+\iota 0.62\end{pmatrix}$	$\begin{pmatrix}0.76+\iota 0.62,\\0.45+\iota 0.44\end{pmatrix}$	$\begin{pmatrix}0.77+\iota 0.65,\\0.43+\iota 0.56\end{pmatrix}$
$₦_4$	$\begin{pmatrix}0.81+\iota 0.57,\\0.59+\iota 0.57\end{pmatrix}$	$\begin{pmatrix}0.80+\iota 0.61,\\0.28+\iota 0.48\end{pmatrix}$	$\begin{pmatrix}0.75+\iota 0.69,\\0.46+\iota 0.71\end{pmatrix}$	$\begin{pmatrix}0.72+\iota 0.55,\\0.48+\iota 0.56\end{pmatrix}$

Step 4: Calculation of attribute weights by the CRITIC Method.

Step 4.1: Score of the normalized matrix;

$$\mathbb{S} = \begin{bmatrix} 0.56 & 0.54 & 0.56 & 0.60 \\ 0.44 & 0.55 & 0.57 & 0.51 \\ 0.55 & 0.55 & 0.58 & 0.58 \\ 0.57 & 0.59 & 0.55 & 0.54 \end{bmatrix}$$

Step 4.2: The Correlation coefficient matrix is given as;

$$\tau = \begin{bmatrix} 1 & 0.26 & -0.33 & 0.74 \\ 0.26 & 1 & -0.50 & -0.45 \\ -0.33 & -0.50 & 1 & 0.11 \\ 0.74 & -0.45 & 0.11 & 1 \end{bmatrix}$$

Step 4.3: Now, we calculate the attribute standard deviation using the formula.

$$\mathfrak{s}_j = \sqrt{\frac{\sum_{i=1}^{m}\left(c_{ij} - \bar{c}_j\right)^2}{m}}$$

$$\mathfrak{s}_1 = 0.052, \mathfrak{s}_2 = 0.02097, \mathfrak{s}_3 = 0.01033, \mathfrak{s}_4 = 0.03474$$

Step 4.4: Analyze the amount of information of each attribute using the following formula.

$$\phi_j = \mathfrak{s}_j \sum_{k=1}^{n} (1 - \tau_{jk})$$

$$\phi_1 = 0.12102, \phi_2 = 0.07716, \phi_3 = 0.03837, \phi_4 = 0.03474$$

Step 4.5: Now, calculate the criteria weights using;

$$\omega_j = \phi_j \Big/ \sum_{j=1}^{n} \phi_j$$

$$\omega_1 = 0.3704, \omega_2 = 0.2362, \omega_3 = 0.1174, \omega_4 = 0.276$$

Step 5: MABAC method.

Step 5.1: Construct an initial matrix representing the initial assessment of DMs, which is constructed in step 1.

Step 5.2: Using the Cq-ROFFWA operator, we will aggregate the matrices as done in step 2.

Step 5.3: Next, we will normalize the data as done in step 3.

Step 5.4: Now, the normalized matrix using the weights of attributes (obtained in step 4.5) is displayed in Table 9.

Table 9. Standardized weighted matrix.

	$\mathring{A}_1$	$\mathring{A}_2$	$\mathring{A}_3$	$\mathring{A}_4$
₦$_1$	$\begin{pmatrix}0.65+\iota 0.52,\\0.72+\iota 0.88\end{pmatrix}$	$\begin{pmatrix}0.50+\iota 0.42,\\0.87+\iota 0.86\end{pmatrix}$	$\begin{pmatrix}0.40+\iota 0.47,\\0.94+\iota 0.94\end{pmatrix}$	$\begin{pmatrix}0.36+\iota 0.69,\\0.90+\iota 0.68\end{pmatrix}$
₦$_2$	$\begin{pmatrix}0.50+\iota 0.56,\\0.85+\iota 0.94\end{pmatrix}$	$\begin{pmatrix}0.45+\iota 0.53,\\0.87+\iota 0.83\end{pmatrix}$	$\begin{pmatrix}0.40+\iota 0.48,\\0.94+\iota 0.91\end{pmatrix}$	$\begin{pmatrix}0.42+\iota 0.43,\\0.84+\iota 0.87\end{pmatrix}$
₦$_3$	$\begin{pmatrix}0.55+\iota 0.53,\\0.79+\iota 0.81\end{pmatrix}$	$\begin{pmatrix}0.63+\iota 0.36,\\0.91+\iota 0.91\end{pmatrix}$	$\begin{pmatrix}0.50+\iota 0.40,\\0.93+\iota 0.93\end{pmatrix}$	$\begin{pmatrix}0.60+\iota 0.50,\\0.83+\iota 0.88\end{pmatrix}$
₦$_4$	$\begin{pmatrix}0.68+\iota 0.47,\\0.85+\iota 0.84\end{pmatrix}$	$\begin{pmatrix}0.61+\iota 0.46,\\0.78+\iota 0.87\end{pmatrix}$	$\begin{pmatrix}0.50+\iota 0.45,\\0.93+\iota 0.97\end{pmatrix}$	$\begin{pmatrix}0.56+\iota 0.43,\\0.85+\iota 0.88\end{pmatrix}$

Step 5.5: Now we evaluate BAA values

$$\mathcal{B}_1 = (0.59 + \iota 0.52\,, 0.81 + \iota 0.88\,)\,, \mathcal{B}_2 = (0.54 + \iota 0.44\,, 0.87 + \iota 0.87\,)$$

$$\mathcal{B}_3 = (0.45 + \iota 0.45\,, 0.94 + \iota 0.94\,)\,, \mathcal{B}_4 = (0.48 + \iota 0.50\,, 0.86 + \iota 0.84\,)$$

Step 5.6: The Distance between each alternative and BAA is displayed in Table 10.

Table 10. Distance between alternative and BAA.

	$\mathring{A}_1$	$\mathring{A}_2$	$\mathring{A}_3$	$\mathring{A}_4$
₦$_1$	0.03683	0.01731	0.01955	0.12864
₦$_2$	0.05654	0.05706	0.02736	0.04214
₦$_3$	0.03487	0.06122	0.02934	0.04784
₦$_4$	0.05406	0.04187	0.01978	0.04932

Step 7: Now, we will sum up the values of alternatives.

$$\dot{S}(₦_1) = 0.03683 + 0.01731 + 0.01955 + 0.12864 = 0.20232$$

$$\dot{S}(₦_2) = 0.05654 + 0.05706 + 0.02736 + 0.04214 = 0.18311$$

$$\dot{S}(₦_3) = 0.03487 + 0.06122 + 0.02934 + 0.04784 = 0.17327$$

$$\dot{S}(₦_4) = 0.05406 + 0.04187 + 0.01978 + 0.04932 = 0.16504$$

Here we notice that

$$\text{₦}_1 > \text{₦}_2 > \text{₦}_3 > \text{₦}_4$$

So, the best alternative is ₦_1. In practical terms, the study underscores the suitability of Passwordless Authentication with Hardware Tokens + Biometric Layer as the most powerful MLA solution for bolstering cloud security. This discovery can help cloud service providers choose more secure and reliable authentication methods. The graphical representation of alternative scores is shown in Figure 5.

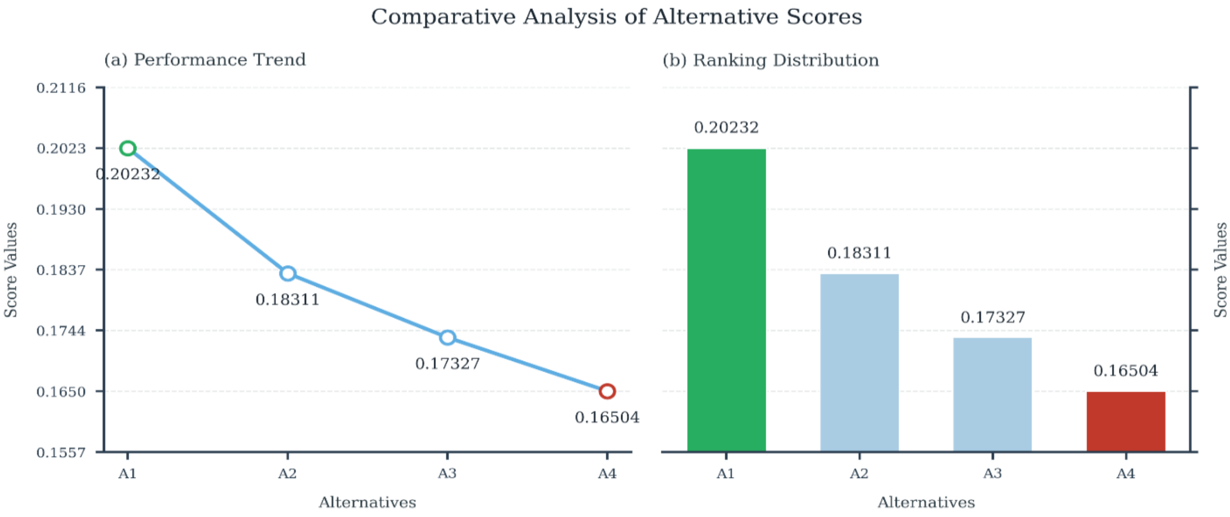

Figure 5. Comparative analysis of alternative scores.

6.2. | Sensitivity Analysis

A sensitivity analysis is performed to assess the robustness and consistency of the proposed decision-making model with different parameter settings. In this research, we focus on the impact of the Frank aggregation parameter and the q-rung parameter, which play a crucial role in determining the aggregation properties and the degree of flexibility in uncertainty representation. Through the variation of these parameters, the stability of the outcomes and consistency of alternative rankings are assessed. This procedure assists in showing the effectiveness and reliability of the proposed method under varying parameters.

Sensitivity analysis of the proposed method under different Frank parameter values is shown in Table 11.

Table 11. Alternative performance under Frank parameter.

Different Values of Parameter ξ	Sum of Values of Alternatives	Ranking
$\xi = 3$	$\dot{S}(₦_1) = 0.20232, \dot{S}(₦_2) = 0.18311$ $\dot{S}(₦_3) = 0.17327, \dot{S}(₦_4) = 0.16504$	$₦_1 > ₦_2 > ₦_3 > ₦_4$
$\xi = 10$	$\dot{S}(₦_1) = 0.17988, \dot{S}(₦_2) = 0.16853$ $\dot{S}(₦_3) = 0.15653, \dot{S}(₦_4) = 0.14739$	$₦_1 > ₦_2 > ₦_3 > ₦_4$
$\xi = 17$	$\dot{S}(₦_1) = 0.17106, \dot{S}(₦_2) = 0.16308$ $\dot{S}(₦_3) = 0.15040, \dot{S}(₦_4) = 0.14082$	$₦_1 > ₦_2 > ₦_3 > ₦_4$
$\xi = 24$	$\dot{S}(₦_1) = 0.16580, \dot{S}(₦_2) = 0.15989$ $\dot{S}(₦_3) = 0.14688, \dot{S}(₦_4) = 0.13697$	$₦_1 > ₦_2 > ₦_3 > ₦_4$
$\xi = 31$	$\dot{S}(₦_1) = 0.16218, \dot{S}(₦_2) = 0.15771$ $\dot{S}(₦_3) = 0.14448, \dot{S}(₦_4) = 0.13433$	$₦_1 > ₦_2 > ₦_3 > ₦_4$
$\xi = 38$	$\dot{S}(₦_1) = 0.15948, \dot{S}(₦_2) = 0.15608$ $\dot{S}(₦_3) = 0.14271, \dot{S}(₦_4) = 0.13236$	$₦_1 > ₦_2 > ₦_3 > ₦_4$
$\xi = 45$	$\dot{S}(₦_1) = 0.15736, \dot{S}(₦_2) = 0.15480$ $\dot{S}(₦_3) = 0.14133, \dot{S}(₦_4) = 0.13081$	$₦_1 > ₦_2 > ₦_3 > ₦_4$
$\xi = 52$	$\dot{S}(₦_1) = 0.15564, \dot{S}(₦_2) = 0.15376$ $\dot{S}(₦_3) = 0.14020, \dot{S}(₦_4) = 0.12955$	$₦_1 > ₦_2 > ₦_3 > ₦_4$
$\xi = 59$	$\dot{S}(₦_1) = 0.15419, \dot{S}(₦_2) = 0.15289$ $\dot{S}(₦_3) = 0.13926, \dot{S}(₦_4) = 0.12848$	$₦_1 > ₦_2 > ₦_3 > ₦_4$

The variation of alternatives for different Frank parameter values is shown in Figure 6.

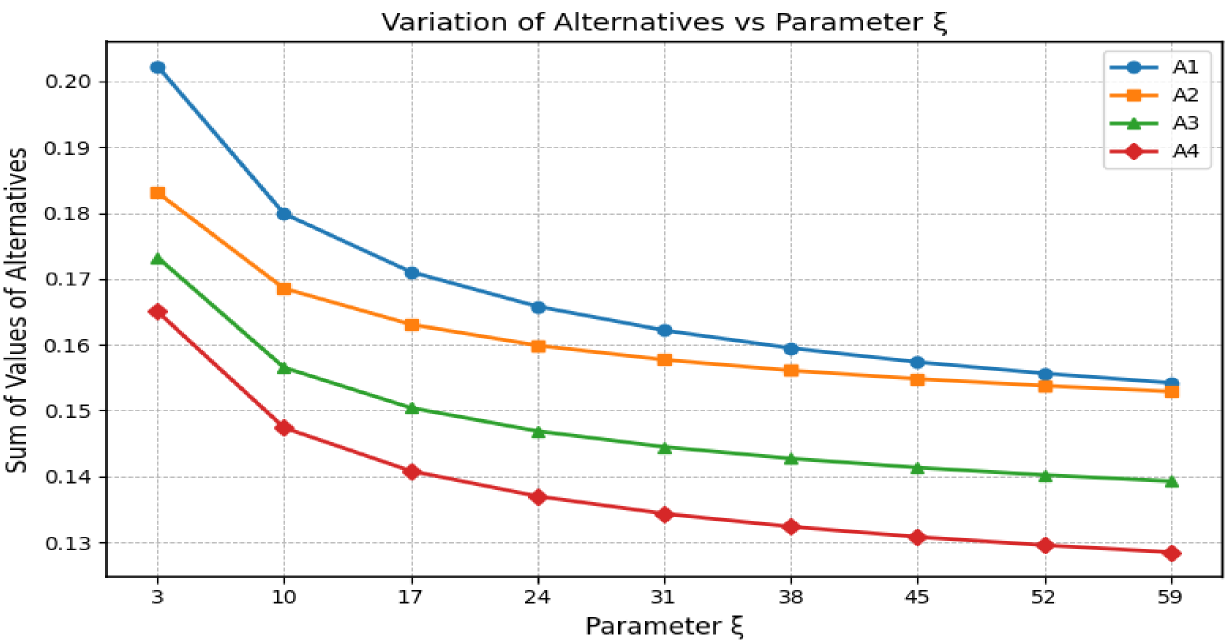

Figure 6. Variation of alternatives under the Frank parameter.

Sensitivity analysis of the proposed method under different q parameter values is shown in Table 12.

Table 12. Alternative performance under the q parameter.

Different Values of Parameter q	Sum of Values of Alternatives	Ranking
$q = 3$	$\dot{S}(\text{₦}_1) = 0.17657, \dot{S}(\text{₦}_2) = 0.16870$ $\dot{S}(\text{₦}_3) = 0.15960, \dot{S}(\text{₦}_4) = 0.14870$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_3 > \text{₦}_4$
$q = 4$	$\dot{S}(\text{₦}_1) = 0.18945, \dot{S}(\text{₦}_2) = 0.17784$ $\dot{S}(\text{₦}_3) = 0.16832, \dot{S}(\text{₦}_4) = 0.15837$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_3 > \text{₦}_4$
$q = 5$	$\dot{S}(\text{₦}_1) = 0.20232, \dot{S}(\text{₦}_2) = 0.18311$ $\dot{S}(\text{₦}_3) = 0.17327, \dot{S}(\text{₦}_4) = 0.16504$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_3 > \text{₦}_4$
$q = 6$	$\dot{S}(\text{₦}_1) = 0.21028, \dot{S}(\text{₦}_2) = 0.18833$ $\dot{S}(\text{₦}_3) = 0.17872, \dot{S}(\text{₦}_4) = 0.17379$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_3 > \text{₦}_4$
$q = 7$	$\dot{S}(\text{₦}_1) = 0.21566, \dot{S}(\text{₦}_2) = 0.19248$ $\dot{S}(\text{₦}_3) = 0.18337, \dot{S}(\text{₦}_4) = 0.18090$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_3 > \text{₦}_4$
$q = 8$	$\dot{S}(\text{₦}_1) = 0.21877, \dot{S}(\text{₦}_2) = 0.19606$ $\dot{S}(\text{₦}_3) = 0.18803, \dot{S}(\text{₦}_4) = 0.18737$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_3 > \text{₦}_4$
$q = 9$	$\dot{S}(\text{₦}_1) = 0.22062, \dot{S}(\text{₦}_2) = 0.19928$ $\dot{S}(\text{₦}_3) = 0.19255, \dot{S}(\text{₦}_4) = 0.19336$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_4 > \text{₦}_3$
$q = 10$	$\dot{S}(\text{₦}_1) = 0.22204, \dot{S}(\text{₦}_2) = 0.20208$ $\dot{S}(\text{₦}_3) = 0.19668, \dot{S}(\text{₦}_4) = 0.19875$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_4 > \text{₦}_3$
$q = 11$	$\dot{S}(\text{₦}_1) = 0.22332, \dot{S}(\text{₦}_2) = 0.20450$ $\dot{S}(\text{₦}_3) = 0.20040, \dot{S}(\text{₦}_4) = 0.20355$	$\text{₦}_1 > \text{₦}_2 > \text{₦}_4 > \text{₦}_3$

The variation of alternatives for different q parameter values is shown in Figure 7.

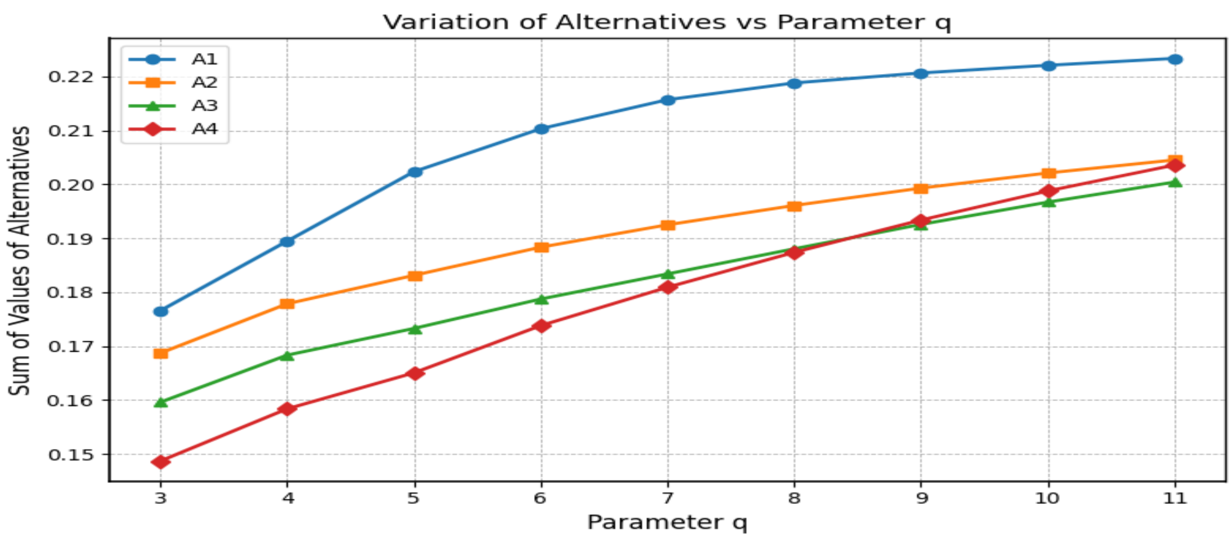

Figure 7. Variation of alternatives under parameter q.

Sensitivity analysis shows that the proposed method is very robust with regard to the Frank parameter, since the ranking of alternatives does not change for the nine examined values of the Frank parameter. This suggests that the proposed aggregation method is stable with respect to the Frank parameter. On the other hand, for the q-rung parameter, we observe a similar ranking pattern in most cases, with only a slight fluctuation in the last two alternatives for three of the nine different values tested. This minimal variation does not impact the top alternatives and, hence, does not affect the decision-making process. These results demonstrate that the proposed approach is highly stable and reliable across a range of parameter values.

7. | COMPARATIVE ANALYSIS

In constructing any new theoretical model, it is necessary to contrast it with current methods in order to ascertain its relative effectiveness and applied relevance. Without comparison, however, the proposed model's strengths and weaknesses and its novel contributions cannot be defined. Hence, to assess our framework's effectiveness, we have chosen a few established and well-known theories from current literature as benchmark measures for comparative evaluation.

- Theory of hesitant fuzzy MABAC (HF-MABAC) by [45].
- Theory of intuitionistic fuzzy Frank power aggregation operators (IFFPAOs) by [46].
- Theory of Pythagorean cubic fuzzy Frank aggregation operators (PCFFAOs) by [47].
- Theory of q-rung orthopair fuzzy Aczel Alsina generalized weighted Bonferroni mean operator (q-ROFAAGWBM) by [39].
- Theory of complex q-rung orthopair fuzzy Frank aggregation operators (Cq-ROFFAOs) by [48].

Moreover, a comparison is presented in Table 13.

Table 13. Comparative analysis and results.

Methods	Score Values	Ranking
HF-MABAC method by Qin et al. [45]	$\dot{S}(₦_1)$ = No result $\dot{S}(₦_2)$ = No result $\dot{S}(₦_3)$ = No result $\dot{S}(₦_4)$ = No result	No Ranking
IFFPAOs by Zhang et al. [46]	$\dot{S}(₦_1)$ = No result $\dot{S}(₦_2)$ = No result $\dot{S}(₦_3)$ = No result $\dot{S}(₦_4)$ = No result	No Ranking
PCFFAOs by Rahim, M. [47]	$\dot{S}(₦_1)$ = No result $\dot{S}(₦_2)$ = No result $\dot{S}(₦_3)$ = No result $\dot{S}(₦_4)$ = No result	No Ranking
q-ROFAAGWBM by Debnath et al. [39]	$\dot{S}(₦_1)$ = No result $\dot{S}(₦_2)$ = No result $\dot{S}(₦_3)$ = No result $\dot{S}(₦_4)$ = No result	No Ranking
Cq-ROFFAOs by Du et al. [48]	$\dot{S}(₦_1)$ = No result $\dot{S}(₦_2)$ = No result $\dot{S}(₦_3)$ = No result $\dot{S}(₦_4)$ = No result	No Ranking
Cq-ROFFWAOs (Proposed)	$\dot{S}(₦_1) = 0.2194$ $\dot{S}(₦_2) = 0.19983$ $\dot{S}(₦_3) = 0.21548$ $\dot{S}(₦_4) = 0.20455$	$₦_1 > ₦_3 > ₦_4 > ₦_2$

Discussion of Table 11 has the following steps.

- Qin et al. [45] suggested Frank aggregation operators of hesitant fuzzy sets (HFSs), which combine several membership values to deal with hesitancy among the decision-makers in a state of uncertainty. Their approach is, however, one-dimensional, based on membership values, and fails to establish multidimensional uncertainty such as non-membership, hesitation, and criteria contradictions. By contrast, our Cq-ROFF-CRITIC-MABAC model utilizes the membership and non-membership degrees and the multifaceted uncertainty characteristics, and allows us to evaluate the MLA schemes in cloud security, providing a robust and multi-dimensional evaluation.
- Zhang et al. [46] generalized IF power aggregation to group decision-making, which represents hesitation and uncertainty. But IFSs have certain limitations since membership and non-membership cannot add up to greater than one, thus limiting complex uncertainty modelling. Our Cq-ROFF-CRITIC-MABAC model approaches this problem by adopting a Cartesian structure. This allows flexible allocation of membership and non-membership values while representing multidimensional uncertainty.
- Rahim [47] used the Pythagorean cubic FSs in Frank aggregation to make group decisions under uncertainty, but his method cannot effectively represent the multidimensional and interdependent uncertainty in cloud security because it uses real-value space. As an alternative, our Cq-ROFF-CRITIC-MABAC model uses q-ROF constructions and Cartesian complex numbers, which offer flexibility in the membership allocation and a more detailed representation of uncertainty, allowing more reliable and precise ranking of MLA strategies in a cloud environment.
- Debnath et al. [39] introduced an integrated approach for MADM using an extended MABAC method combined with the Aczel-Alsina generalized weighted Bonferroni mean operator to model the inter-relationships between criteria under a q-ROF environment. But their model is limited to real-valued representations and Aczel–Alsina operations, which may result in less flexibility in capturing the dynamic and complex relationships between criteria. On the other hand, the proposed Cq-ROFF-CRITIC-MABAC model uses Cq-ROFSs and Frank operational laws to provide a more flexible and rich representation of uncertainty and to include objective criteria weighting using the CRITIC method to improve the decision process.
- Du et al. [48] proposed exponential aggregation operators of q-ROFNs to obtain uncertainty in amplitude and phase and gave a sophisticated theory modeling of MCDM. Their method is, however, limited to operator design; it does not have objective criteria weighting and

strong ranking, and is hard to interpret within real-life applications of clouds. Our Cq-ROFF-CRITIC-MABAC model addresses these gaps by using Cartesian-form complex numbers to represent both values and characteristics of uncertainty. It integrates CRITIC for objective weighting, Frank aggregation to capture interdependencies, and MABAC for consistent, interpretable ranking.

The hybrid model has the following merits over the current decision-making processes. The Cq-ROF environment has enabled a more comprehensive representation of uncertainty, and Frank aggregation operators have made it possible to integrate the opinions of experts in a flexible way. Moreover, CRITIC objectively assigns the criteria weights, and MABAC can generate trustworthy rankings, which leads to more comprehensive and informative decision results for the evaluation of cloud security. Comparative analysis is displayed graphically in Figure 8.

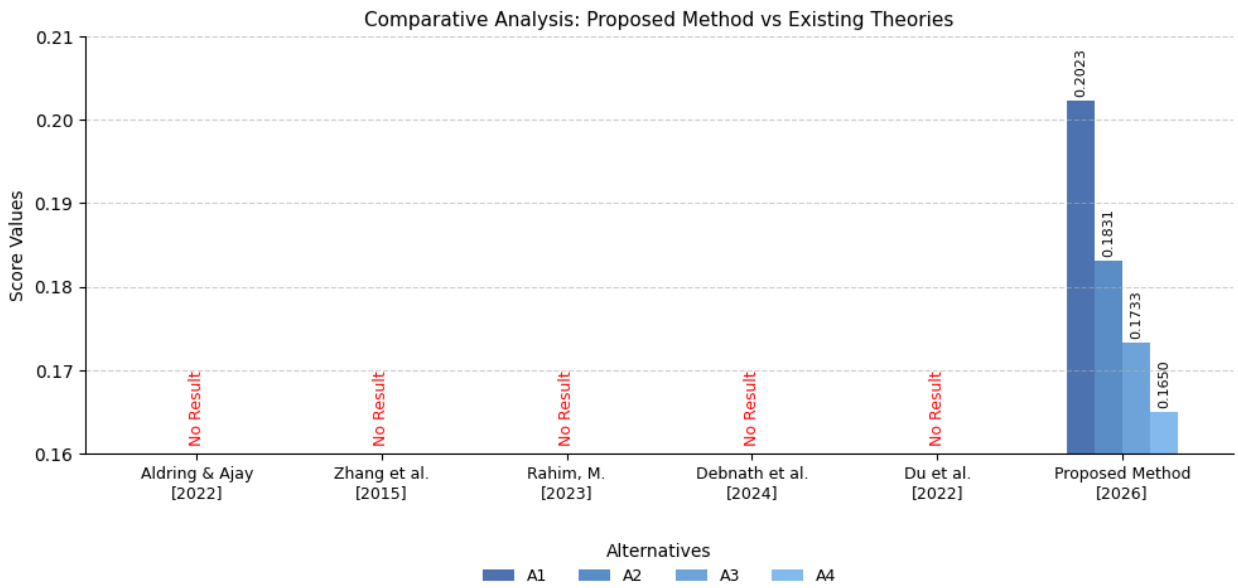

Figure 8. Comparative analysis of proposed work vs existing work.

8. | CONCLUSION

In the study, the Cq-ROFF-CRITIC-MABAC framework is proposed as a decision-making method to assess and prioritize MLA strategies in cloud computing environments. The presented framework is intended to overcome the disadvantages of the current fuzzy decision-making systems, which are based on only real-valued information and are not able to describe complex uncertainty in the system. The framework is flexible and informative enough to be used in a Cartesian form of Cq-ROFNs, which gives a more accurate depiction of uncertainty and hesitation in expert assessments. Further, the addition of Frank aggregation operators increases the versatility of the framework, as they are able to effectively capture different interactions between the expert opinions and the evaluation criteria. By taking both contrast intensity and inter-criteria conflict into account, the CRITIC method is used for the objective determination of the weights of the criteria to enhance the reliability of the evaluation process. Moreover, the MABAC method ensures a transparent ranking procedure and is a stable one that efficiently discriminates competing authentication alternatives. Therefore, the proposed framework is robust, reliable, and practical for making cloud security assessment decisions and choosing the best authentication strategies in an uncertain environment.

Moreover, key findings are;

- Introduced a novel family of Cq-ROF Frank aggregation operators to ensure robust and reliable processing of expert judgments.
- Developed a CRITIC-MABAC framework for systematic evaluation and ranking of MLA strategies under uncertainty.
- Demonstrated the superior performance and effectiveness of the proposed methodology compared to existing MCDM approaches.

6.1. | Limitations

The proposed Cq-ROFF-CRITIC-MABAC model offers a robust framework for ranking MLA mechanisms under uncertainty; however, several limitations should be acknowledged. The model relies on expert-driven evaluations, which may introduce subjectivity despite the use of objective weighting through the CRITIC method. Additionally, the framework assumes a static decision environment and does not explicitly account for the dynamic and evolving nature of cloud security threats and authentication technologies. The computational complexity associated with Cq-ROFSs and Frank aggregation operators may also limit scalability when dealing with large-scale decision problems. Furthermore, the applicability of the proposed approach is primarily validated within a specific case context, which may affect its generalizability across diverse cloud infrastructures and real-world scenarios.

6.1. | Future Research Direction

The framework proposed could be further developed in the future to include dynamic and adaptive decision-making to capture the dynamic nature of cloud security and authentication technologies. Incorporation of real-time data analytics and machine learning algorithms may benefit the model in terms of responsiveness and predictive power when it comes to the detection of emerging threats and more effective authentication strategies. Moreover, the framework can be extended to support more varied and larger decision environments, such as cross-cloud and hybrid architectures, to enhance its scalability and applicability in practice. The proposed technique can be validated further by comparing it with other advanced aggregation operators and extensions to fuzzy logic. In addition, researchers could consider integrating behavioral and contextual variables, and policy and regulatory implications to present a more detailed and realistic analysis of MLA systems.

Acknowledgment: The authors thank the anonymous reviewers for their valuable comments and constructive suggestions, which helped improve the quality of this manuscript.

Author Contributions: Conceptualization, K.A.; Methodology, K.A. and H.M.W.; Software, K.A. and H.M.W.; Validation, H.M.W. and O.O.; Investigation, H.M.W. and O.O.; Writing – Original Draft, K.A.; Writing – Review & Editing, H.M.W. and O.O. All authors have read and agreed to the published version of the manuscript.

Declaration of Conflicting Interest: The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding: The author(s) received no financial support for the research, authorship, and/or publication of this article.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Plagiarism Statement: This manuscript was screened for textual similarity using Turnitin. The similarity results were found to be within the plagiarism thresholds prescribed by the Higher Education Commission (HEC) of Pakistan and the journal's editorial policy.

Artificial Intelligence (AI) Statement: The authors declare that no generative artificial intelligence tools or AI-assisted technologies were used in the preparation of this manuscript.

REFERENCES

[1] A. M. Mostafa *et al.*, "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication," *Appl. Sci.*, vol. 13, no. 19, p. 10871, Sep. 2023, doi: 10.3390/app131910871.

[2] B. S. A. Kumar and B. Sah, "Enhancing Cloud Security Through a Multi-Level Authentication Model: A QoS-Based Approach to Performance Measurement for Source Management," *SN Comput. Sci.*, vol. 6, no. 4, p. 365, Apr. 2025, doi: 10.1007/s42979-025-03922-5.

[3] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, "Multilevel classification of security concerns in cloud computing," *Appl. Comput. Inform.*, vol. 13, no. 1, pp. 57–65, Jan. 2017, doi: 10.1016/j.aci.2016.03.001.

[4] R. Fathi, M. A. Salehi, and E. L. Leiss, "User-Friendly and Secure Architecture (UFSA) for Authentication of Cloud Services," in *2015 IEEE 8th International Conference on Cloud Computing*, New York City, NY, USA: IEEE, Jun. 2015, pp. 516–523. doi: 10.1109/CLOUD.2015.75.

[5] S. Gudimetla, "Multi-Factor Authentication for Cloud," *Int. Res. J. Mod. Eng. Technol. Sci.*, Mar. 2024, doi: 10.56726/IRJMETS51190.

[6] S. P. Otta, S. Panda, M. Gupta, and C. Hota, "A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure," *Future Internet*, vol. 15, no. 4, p. 146, Apr. 2023, doi: 10.3390/fi15040146.

[7] A. E. Youssef, "An Integrated MCDM Approach for Cloud Service Selection Based on TOPSIS and BWM," *IEEE Access*, vol. 8, pp. 71851–71865, 2020, doi: 10.1109/ACCESS.2020.2987111.

[8] A. M. Mostafa, "An MCDM Approach for Cloud Computing Service Selection Based on Best-Only Method," *IEEE Access*, vol. 9, pp. 155072–155086, 2021, doi: 10.1109/ACCESS.2021.3129716.

[9] A. Tomar, R. R. Kumar, and I. Gupta, "Decision making for cloud service selection: a novel and hybrid MCDM approach," *Clust. Comput.*, vol. 26, no. 6, pp. 3869–3887, Dec. 2023, doi: 10.1007/s10586-022-03793-y.

[10] R. K. Tiwari and R. Kumar, "A Robust and Efficient MCDM-Based Framework for Cloud Service Selection Using Modified TOPSIS:," *Int. J. Cloud Appl. Comput.*, vol. 11, no. 1, pp. 21–51, Jan. 2021, doi: 10.4018/IJCAC.2021010102.

[11] M. A. Omer, A. A. Yazdeen, H. S. Malallah, and L. M. Abdulrahman, "A Survey on Cloud Security: Concepts, Types, Limitations, and Challenges," *J. Appl. Sci. Technol. Trends*, vol. 3, no. 02, pp. 101–111, Dec. 2022, doi: 10.38094/jastt301137.

[12] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *Network*, vol. 3, no. 3, pp. 422–450, Sep. 2023, doi: 10.3390/network3030018.

[13] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, Aug. 2019, doi: 10.1016/j.cosrev.2019.05.002.

[14] F. Jimmy, "Cyber security Vulnerabilities and Remediation Through Cloud Security Tools," *J. Artif. Intell. Gen. Sci. JAIGS ISSN3006-4023*, vol. 2, no. 1, pp. 129–171, Apr. 2024, doi: 10.60087/jaigs.v2i1.102.

[15] A. Patel, N. Shah, D. Ramoliya, and A. Nayak, "A detailed review of Cloud Security: Issues, Threats & Attacks," in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India: IEEE, Nov. 2020, pp. 758–764. doi: 10.1109/ICECA49313.2020.9297572.

[16] A. G. Deshpande, C. Srinivasan, R. Raman, S. Rajarajan, and R. Adhvaryu, "Enhancing Cloud Security: A Deep Cryptographic Analysis," in *2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, Faridabad, India: IEEE, Nov. 2023, pp. 1118–1123. doi: 10.1109/ICAICCIT60255.2023.10465863.

[17] Mrs.M.SARADHA, D. G, and K. S, "Enhancing Cloud Data Security And Access Control: An Efficient Auditing Scheme," in *2025 5th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN)*, Coimbatore, India: IEEE, Nov. 2025, pp. 1626–1630. doi: 10.1109/ICECMSN68058.2025.11383346.

[18] L. Abdullah, "Fuzzy Multi Criteria Decision Making and its Applications: A Brief Review of Category," *Procedia - Soc. Behav. Sci.*, vol. 97, pp. 131–136, Nov. 2013, doi: 10.1016/j.sbspro.2013.10.213.

[19] D. Dalalah, M. Hayajneh, and F. Batieha, "A fuzzy multi-criteria decision making model for supplier selection," *Expert Syst. Appl.*, vol. 38, no. 7, pp. 8384–8391, Jul. 2011, doi: 10.1016/j.eswa.2011.01.031.

[20] M. Kabak, E. Köse, O. Kırılmaz, and S. Burmaoğlu, "A fuzzy multi-criteria decision making approach to assess building energy performance," *Energy Build.*, vol. 72, pp. 382–389, Apr. 2014, doi: 10.1016/j.enbuild.2013.12.059.

[21] M. Çolak and İ. Kaya, “Prioritization of renewable energy alternatives by using an integrated fuzzy MCDM model: A real case application for Turkey,” *Renew. Sustain. Energy Rev.*, vol. 80, pp. 840–853, Dec. 2017, doi: 10.1016/j.rser.2017.05.194.

[22] E. Yoruk, A. Baykasoglu, and H. Sozbilir, “Graph theory based fuzzy multi-criteria decision-making model for locating disaster containers incorporating fuzzy set covering along with a case study,” *J. Oper. Res. Soc.*, pp. 1–34, Feb. 2026, doi: 10.1080/01605682.2026.2623060.

[23] B. Sharma, Suman, N. Saini, and N. Gandotra, “Multi criteria decision making under the fuzzy and intuitionistic fuzzy environment: A review,” presented at the DIDACTIC TRANSFER OF PHYSICS KNOWLEDGE THROUGH DISTANCE EDUCATION: DIDFYZ 2021, Terchová, Slovakia, 2022, p. 110003. doi: 10.1063/5.0080577.

[24] S. Singh, S. Lalotra, and A. H. Ganie, “On Some Knowledge Measures of Intuitionistic Fuzzy Sets of Type Two with Application to MCDM,” *Cybern. Inf. Technol.*, vol. 20, no. 1, pp. 3–20, Mar. 2020, doi: 10.2478/cait-2020-0001.

[25] M. R. Shahriari, “Soft computing based on a modified MCDM approach under intuitionistic fuzzy sets,” *Iran. J. Fuzzy Syst.*, vol. 14, no. 1, p. 23, 2017.

[26] R. Tao, Z. Liu, R. Cai, and K. H. Cheong, “A dynamic group MCDM model with intuitionistic fuzzy set: Perspective of alternative queuing method,” *Inf. Sci.*, vol. 555, pp. 85–103, May 2021, doi: 10.1016/j.ins.2020.12.033.

[27] S. Faizi, W. Sałabun, T. Rashid, S. Zafar, and J. Wątróbski, “Intuitionistic Fuzzy Sets in Multi-Criteria Group Decision Making Problems Using the Characteristic Objects Method,” *Symmetry*, vol. 12, no. 9, p. 1382, Aug. 2020, doi: 10.3390/sym12091382.

[28] N. Ghorui *et al.*, “Selection of cloud service providers using MCDM methodology under intuitionistic fuzzy uncertainty,” *Soft Comput.*, vol. 27, no. 5, pp. 2403–2423, Mar. 2023, doi: 10.1007/s00500-022-07772-8.

[29] M. Liaqat, S. Yin, M. Akram, and S. Ijaz, “Aczel-alsina aggregation operators based on interval-valued complex single-valued neutrosophic information and their application in decision-making problems,” *J. Innov. Res. Math. Comput. Sci.*, vol. 1, no. 2, pp. 40–66, 2022, doi: https://doi.org/10.62270/jirmcs.v1i2.9.

[30] Z. Ali, “Decision-making techniques based on complex intuitionistic fuzzy power interaction aggregation operators and their applications,” *J. Innov. Res. Math. Comput. Sci.*, vol. 1, no. 1, pp. 107–125, 2022, doi: https://doi.org/10.62270/jirmcs.v1i1.6.

[31] X. Peng, X. Zhang, and Z. Luo, “Pythagorean fuzzy MCDM method based on CoCoSo and CRITIC with score function for 5G industry evaluation,” *Artif. Intell. Rev.*, vol. 53, no. 5, pp. 3813–3847, Jun. 2020, doi: 10.1007/s10462-019-09780-x.

[32] Department of Mathematics, Jaypee University of Engineering and Technology, India, R. Chaurasiya, D. Jain, and Department of Mathematics, Jaypee University of Engineering and Technology, India, “Hybrid MCDM method on pythagorean fuzzy set and its application,” *Decis. Mak. Appl. Manag. Eng.*, vol. 6, no. 1, pp. 379–398, Apr. 2023, doi: 10.31181/dmame0306102022c.

[33] A. R. Mishra, P. Rani, and S. Bharti, “Assessment of Agriculture Crop Selection Using Pythagorean Fuzzy CRITIC–VIKOR Decision-Making Framework,” in *Pythagorean Fuzzy Sets: Theory and Applications*, H. Garg, Ed., Singapore: Springer Singapore, 2021, pp. 167–191. doi: 10.1007/978-981-16-1989-2_7.

[34] A. Hussain and D. Pamucar, “Multi-attribute group decision-making based on pythagorean fuzzy rough set and novel schweizer-sklar T-norm and T-conorm,” *J. Innov. Res. Math. Comput. Sci.*, vol. 1, no. 2, pp. 1–17, 2022.

[35] S. Biswas, A. Sanyal, D. Božanić, S. Kar, A. Milić, and A. Puška, “A Multicriteria-Based Comparison of Electric Vehicles Using q-Rung Orthopair Fuzzy Numbers,” *Entropy*, vol. 25, no. 6, p. 905, Jun. 2023, doi: 10.3390/e25060905.

[36] M. Akram, “Multi-criteria decision making based on q-rung orthopair fuzzy promethee approach”.

[37] A. Pinar and F. E. Boran, “A q-rung orthopair fuzzy multi-criteria group decision making method for supplier selection based on a novel distance measure,” *Int. J. Mach. Learn. Cybern.*, vol. 11, no. 8, pp. 1749–1780, Aug. 2020, doi: 10.1007/s13042-020-01070-1.

[38] V. Salsabeela, T. M. Athira, S. J. John, and T. Baiju, “Multiple criteria group decision making based on q-rung orthopair fuzzy soft sets,” *Granul. Comput.*, vol. 8, no. 5, pp. 1067–1080, Sep. 2023, doi: 10.1007/s41066-023-00369-y.

[39] K. Debnath, S. K. Roy, M. Deveci, and H. Tomášková, “Integrated MADM approach based on extended MABAC method with Aczel–Alsina generalized weighted Bonferroni mean operator,” *Artif. Intell. Rev.*, vol. 58, no. 1, p. 27, Nov. 2024, doi: 10.1007/s10462-024-10980-3.

[40] K. Debnath and S. K. Roy, “Decision analytics for Indian culinary tourism: A holistic group approach considering correlation,” *Appl. Soft Comput.*, vol. 185, p. 113812, Dec. 2025, doi: 10.1016/j.asoc.2025.113812.

[41] K. Debnath, E. B. Tirkolaee, and S. K. Roy, "A decision-making model with new Dice–Jaccard similarity measure: Green hydrogen electrolyzer selection," *Eng. Appl. Artif. Intell.*, vol. 160, p. 111817, Nov. 2025, doi: 10.1016/j.engappai.2025.111817.

[42] S. Giri, S. K. Roy, and M. Deveci, "An MADM model using Frank operations based power aggregation operator under p,q-quasirung orthopair fuzzy sets for highway selection in war-plane landing," *Appl. Soft Comput.*, vol. 185, p. 113918, Dec. 2025, doi: 10.1016/j.asoc.2025.113918.

[43] J. Ahmmad, "Classification of Renewable Energy Trends by Utilizing the Novel Entropy Measures under the Environment of q-rung Orthopair Fuzzy Soft Sets," *J. Innov. Res. Math. Comput. Sci.*, vol. 2, no. 2, pp. 1–17, Dec. 2023, doi: 10.62270/jirmcs.v2i2.19.

[44] M. Ali, Y. Akhtar, M. Rahim, and M.-S. Yang, "On circular p,q-quasirung orthopair fuzzy sets with their aggregation operators and application to green supplier selection," *Complex Intell. Syst.*, vol. 12, no. 3, p. 115, Mar. 2026, doi: 10.1007/s40747-026-02236-0.

[45] J. Qin, X. Liu, and W. Pedrycz, "Frank aggregation operators and their application to hesitant fuzzy multiple attribute decision making," *Appl. Soft Comput.*, vol. 41, pp. 428–452, Apr. 2016, doi: 10.1016/j.asoc.2015.12.030.

[46] X. Zhang, P. Liu, and Y. Wang, "Multiple attribute group decision making methods based on intuitionisticfuzzy frank power aggregation operators," *J. Intell. Fuzzy Syst.*, vol. 29, no. 5, pp. 2235–2246, Jul. 2015, doi: 10.3233/IFS-151699.

[47] M. Rahim, "Multi-criteria group decision-making based on frank aggregation operators under Pythagorean cubic fuzzy sets," *Granul. Comput.*, vol. 8, no. 6, pp. 1429–1449, Nov. 2023, doi: 10.1007/s41066-023-00376-z.

[48] Y. Du, X. Du, Y. Li, J. Cui, and F. Hou, "Complex q-rung orthopair fuzzy Frank aggregation operators and their application to multi-attribute decision making," *Soft Comput.*, vol. 26, no. 22, pp. 11973–12008, Nov. 2022, doi: 10.1007/s00500-022-07465-2.

[49] J. Ahmmad, T. Mahmood, D. Pamucar, and H. M. Waqas, "A novel Complex q-rung orthopair fuzzy Yager aggregation operators and their applications in environmental engineering," *Heliyon*, vol. 11, no. 1, 2025.

[50] M. J. Frank, "On the simultaneous associativity of F (x, y) and x+ y− F (x, y)," *Aequationes Math.*, vol. 19, no. 1, pp. 194–226, 1979.