Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 6, 2026

OPTIMIZING REAL-TIME BIG DATA SECURITY: A COMPLEX Q-RUNG ORTHOPAIR FUZZY BWM-MARCOS TECHNIQUE FOR ADVANCED CYBER DEFENSE SOLUTIONS

[1]Khurram Ali, [1]Tahir Mahmood, and [1]Hafiz Muhammad Waqas
[1]Department of Mathematics and Statistics, International Islamic University Islamabad, Pakistan.
khurram.ali8521@gmail.com; tahirbakhat@iiu.edu.pk; hafizmwaqas009@gmail.com
Correspondence: tahirbakhat@iiu.edu.pk

DOI:-https://doi.org/10.5281/zenodo.21234352

Keywords
Complex q-rung orthopair fuzzy sets; Best-worst method; MARCOS technique; Cyber defense solutions; Real-time big data security.

Article History
Received: 25 May, 2026
Accepted: 29 June, 2026
Published: 30 June, 2026

Corresponding Author: *
Tahir Mahmood,

Abstract
The rapid expansion of real-time big data systems has intensified cybersecurity challenges, making the selection of effective cyber defense solutions a crucial and complex decision-making task. Owing to the presence of uncertainty, vagueness, and hesitation in expert evaluations, conventional assessment approaches may fail to provide reliable decision support. To address this challenge, this study presents a complex q-rung orthopair fuzzy best-worst method and measurement alternatives and ranking according to the compromise solution (Cq-ROF BWM-MARCOS) framework for evaluating advanced cyber defense solutions in real-time big data security environments. The proposed framework utilizes Cq-ROFSs to represent uncertain expert judgments more comprehensively through membership and non-membership information. Subsequently, the best-worst method is employed to determine the relative importance of evaluation criteria, while the MARCOS method is used to assess the utility of alternatives and establish their final ranking with respect to ideal and anti-ideal reference solutions. To demonstrate the applicability of the proposed framework, a real-world case study involving advanced cyber defense solutions is conducted. The obtained results identify the most suitable security alternative and reveal the effectiveness of the proposed approach in handling complex and uncertain cybersecurity decision environments. The proposed framework provides a systematic and reliable decision-support tool for organizations and security practitioners seeking to strengthen real-time big data protection through informed selection of cyber defense technologies.

1 | Introduction

The unprecedented growth of real-time big data systems has transformed the way organizations collect, process, and utilize information across various domains, including finance, healthcare, transportation, smart cities, and critical infrastructures. While these systems provide significant operational and analytical advantages, they also expose organizations to increasingly sophisticated cyber threats, making security a critical concern. The massive volume, velocity, and variety of big data create complex attack

surfaces that challenge conventional cybersecurity mechanisms. Consequently, advanced cyber defense solutions capable of detecting, preventing, and mitigating cyberattacks in real time have become essential for maintaining the confidentiality, integrity, and availability of information assets. However, selecting the most appropriate cyber defense solution remains a challenging task due to the presence of multiple conflicting criteria, diverse security requirements, and uncertainty in expert evaluations. Therefore, the development of intelligent decision-support frameworks for evaluating cyber defense alternatives has become increasingly important in contemporary cybersecurity environments. In recent years, several studies have suggested sophisticated security solutions for big data ecosystems, based on advanced analytics and artificial intelligence techniques, to address new cybersecurity issues. Ofoegbu et al. [1] proposed a comprehensive solution that combines machine learning and big data analytics to develop a real-time cybersecurity threat detection system, showing the importance of utilizing data-driven methods for detecting malicious activities. Similarly, Hussen et al. [2] proposed a fully streaming big data cybersecurity framework, which uses an optimized deep learning algorithm, underscoring the need for real-time processing capability in cyber threat mitigation. Moreover, Ameedeen et al. [3] suggested an automatic big data analytics system for cybersecurity threat detection, highlighting the necessity of intelligent analytics for enhancing security monitoring and incident response. With the growing reliance on data-driven security architectures, researchers have been drawn to explore more sophisticated paradigms of cybersecurity that can tackle large-scale and dynamic cyber environments. Rawat et al. [4] gave a detailed discussion on cybersecurity in the big data era and showed how to move from the security of big data systems towards leveraging data-driven security mechanisms. Likewise, Xu et al. [5] presented a genetic algorithm-optimized fuzzy clustering method to enhance cybersecurity in a big data setting, which demonstrates the capability of intelligent computational methods in improving the cyber defence capability. In addition, Meng et al. [6] proposed a security-aware dynamic scheduling model for cloud-based industrial applications, highlighting the significance of incorporating security considerations into real-time operational decision-making processes. The ever-changing nature of cyber-attacks has only made it more important to have resilient and adaptable defensive measures. Alshamrani et al. [7] performed an extensive survey on advanced persistent threats and analyzed the different attack techniques, defense solutions, challenges, and future research directions. Similarly, Moustafa et al. [8] proposed an ensemble intrusion detection system to safeguard the Internet of Things network traffic, and showed that intelligent intrusion detection methods can detect complex attack patterns effectively. While these studies have made significant strides in the state-of-the-art of cybersecurity and threat detection, they are mostly centered on how to create security mechanisms and threat detection models and not on how to systematically evaluate and select the most appropriate cyber defense solutions in uncertain decision environments. In real-world cybersecurity applications, decision makers must assess multiple possible

cyber defense options, considering different technical, operational, economic, and security considerations. Those evaluations often are expressed in terms of fuzzy, ambiguous, and imprecise data that are difficult to manage using traditional decision-making processes. Thus, there is an increasing demand for powerful fuzzy multi-criteria decision-making (MCDM) methods that can effectively manage uncertainty and give reliable rankings of cyber defence solutions. With this motivation, the present study proposes a Cq-ROF BWM-MARCOS framework for the evaluation of advanced cyber defence solutions in real-time big data security environments. The suggested model integrates the influential uncertainty modeling ability of Cq-ROFSs with the objective weighting ability of BWM and the ranking ability of the MARCOS method, which makes it a comprehensive and reliable decision-supporting model for cybersecurity practitioners and organizations.

1.1 Study Framework

The rest of the paper is organized as follows. Section 1 presents the introduction and motivation for evaluating advanced cyber defense solutions in real-time big data security environments. In Section 2, we discuss the research problem and summarize the main contributions of the proposed framework. Section 3 provides a literature review of fuzzy MCDM approaches, BWM, and MARCOS methods. Section 4 presents the basic notions and definitions of Cq-ROFSs. In Section 5, we present the proposed aggregation operators and the Cq-ROF BWM-MARCOS methodology. In Section 6, a numerical example and a practical case study are presented to demonstrate the implementation of the proposed framework. The effectiveness of the proposed approach is validated by a comparative analysis in Section 7. Finally, we conclude our paper in Section 8. Moreover, the framework of the paper is shown in Figure 1.

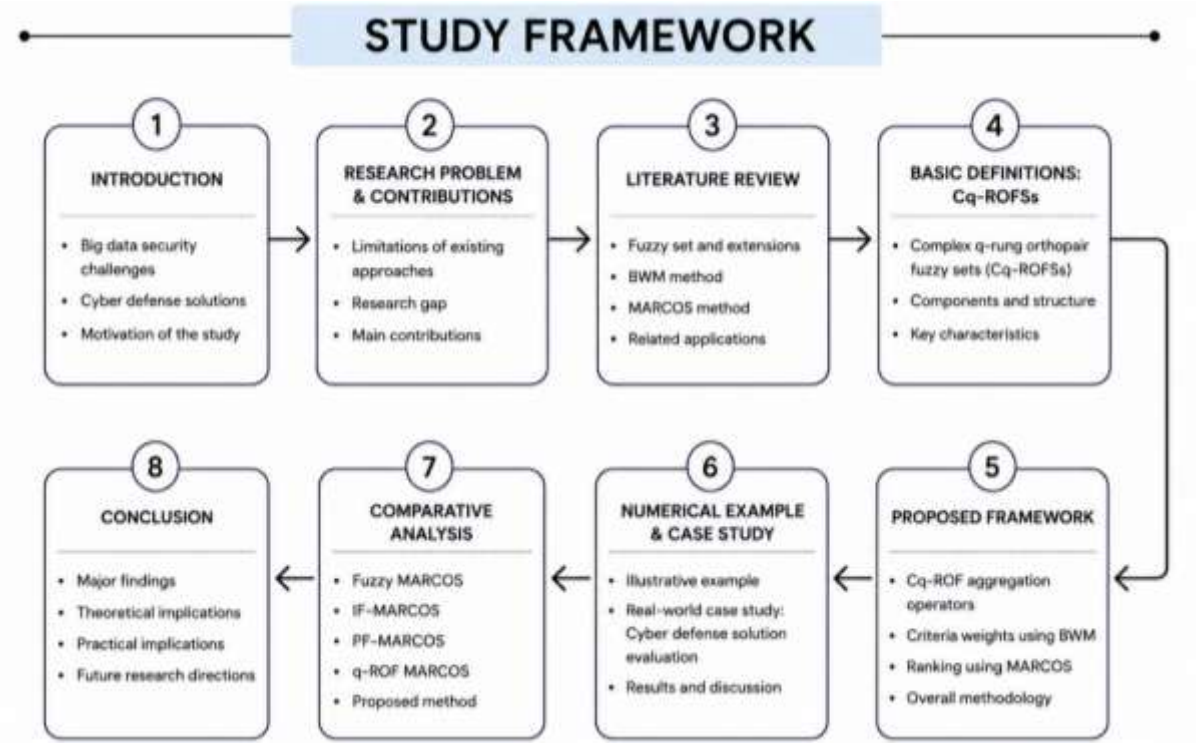

Figure 1: Study framework.

2 | Research Problem

The selection of advanced cyber defense solutions for real-time big data security is a complex MCDM problem involving numerous conflicting criteria, dynamic threat landscapes, and uncertain expert assessments. In today's big data world, the availability of cyber defense technologies demands a careful assessment across technical, operational, economic, and security criteria, as well as the need to deal with an ever-changing landscape of cyberattacks. Conventional strategies in decision-making processes are often inefficient at handling uncertainty and ambiguity in these types of assessments. While the new progress of fuzzy sets (FSs), Intuitionistic fuzzy sets (IFSs), Pythagorean fuzzy sets (PFSs), and q-rung orthopair fuzzy sets (q-ROFSs) in representing uncertainty in the decision-making processes has improved, they still have some restrictions when applied to highly complex cybersecurity information that has multiple degrees of uncertainty, hesitation, and complicated relationships between evaluation parameters. In the real-time big data security environment, expert judgments often include imprecise, vague, and uncertain information that is difficult to capture by conventional fuzzy structures. Thus, it is essential to have a more flexible and expressive knowledge representation system that can play a role in reliable security decision-making while representing complex, uncertain information. The capability is provided by Cq-ROFSs, which are an extension of q-ROFSs into the complex world with higher flexibility and better information representation in complex decision environments. Over the past few years, several researchers have used MCDM methods that have been applied to cybersecurity issues. Granat et al. [9] combined big data analytics with a multicriteria approach for event detection within the Internet of Things (IoT) environments and showed that the MCDM techniques are effective for processing large-scale data-driven systems. AbdelMouty and Abdel-Monem [10] suggested the neutrosophic MCDM method for evaluating cybersecurity risks in power management systems, emphasizing the role of uncertainty modeling in cyber risk assessment. Bhol [11] has extensively discussed the uses of MCDM techniques in cybersecurity and pointed out their importance for decision-making in various cyber-physical systems. Moreover, Khan et al. [12] used a fuzzy TOPSIS model to determine and rank the security issues of big data in cloud computing, showing the applicability of a fuzzy MCDM model for cybersecurity evaluation. Mohamed et al. [13] proposed an MCDM framework that is built upon the MITRE ATT and CK strategy to improve the effectiveness of cybersecurity defenses and aid in choosing mitigation strategies. Similarly, Al-Zaidawi and Cevik [14] leveraged advanced deep learning models and fused optimization and MCDM methods to enhance the monitoring of IoT networks, and Yang [15] introduced a fuzzy Off Logic-based MCDM framework to assess intrusion detection systems in cybersecurity environments. Though these studies have greatly advanced the cybersecurity assessment and decision support, there are still several important limitations.

The major research gaps identified from the existing literature are summarized as follows:

- The current studies that employ the MCDM technique in cybersecurity are mostly based on traditional fuzzy or neutrosophic or related uncertainty models, and these models may

not be sufficient to represent the complexity and uncertainty of the expert judgment in real-time big data security environments.

- Most of the studies are dedicated to cybersecurity risk assessment, threat detection, intrusion detection, or selection of the mitigation strategies instead of a thorough assessment and ranking of advanced cyber defense solutions.
- Limited attention has been devoted to utilizing Cq-ROFS for cybersecurity decision-making despite their superior capability to model uncertain and complex information.
- There is a lack of a good combination of a subjective weighing method and a utility-based ranking method in the existing cybersecurity assessment frameworks in the Cq-ROF environment.
- To our best knowledge, there have been no studies that have proposed a Cq-ROF BWM-MARCOS framework for real-time big data security environments to evaluate advanced cyber defense solutions.

To address these limitations, this study introduces a new Cq-ROF BWM-MARCOS approach for assessing advanced cyber defense solutions in real-time big data security environments. The proposed framework is based on Cq-ROFSs, which can well model the uncertain and imprecise expert evaluation, to effectively present the decision information with richer information content than existing fuzzy environments. Moreover, BWM is used to measure the relative importance of the evaluation criteria based on expert preferences, and MARCOS is used for assessing the utility of the cyber defense alternatives and ranking them with respect to ideal and anti-ideal reference solutions. The proposed framework features integrated uncertainty modelling, well-defined criteria weighting, and strong utility-based ranking, thereby offering a comprehensive decision support tool to determine the most appropriate solutions for cyber defence in real-time big data security applications.

2.1 Contributions

The increasing complexity of real-time big data security environments demands advanced decision-making frameworks capable of effectively handling uncertainty, conflicting criteria, and subjective expert judgments. Current cybersecurity evaluation techniques face challenges in using a model that captures the multidimensionality of uncertain information with today's cyber defense technologies. To solve those problems, the present work proposes a new framework, called the Cq-ROF BWM-MARCOS, which is proposed to evaluate advanced cyber defense solutions. The proposed framework brings together uncertainty modeling improvements, reliable criteria weighting, and robust alternative ranking in a single decision-support framework. The major findings of this research are stated below:

- In order to capture multidimensional uncertainty and complex expert evaluations better than the traditional fuzzy, IF, PF, and q-ROF environments, a Cq-ROF framework is introduced.
- A consistent and efficient weighting mechanism with a reduced number of pairwise comparisons is also introduced by the BWM to set the relative importance of cybersecurity evaluation criteria.
- The MARCOS method is embedded to rank advanced cyber defense solutions in terms of their utility, compared to ideal and anti-ideal alternatives, thus securing reliable and interpretable decision outcomes.

- A thorough decision-making system is built based on Cq-ROFS, BWM, and MARCOS to facilitate the evaluation of cybersecurity in an uncertain real-time big data environment.
- A practical case study involving advanced cyber defense solutions is performed to illustrate the applicability and effectiveness of the proposed framework, as well as the capability of supporting the decision-making process.

Moreover, the main contributions are shown in Figure 2.

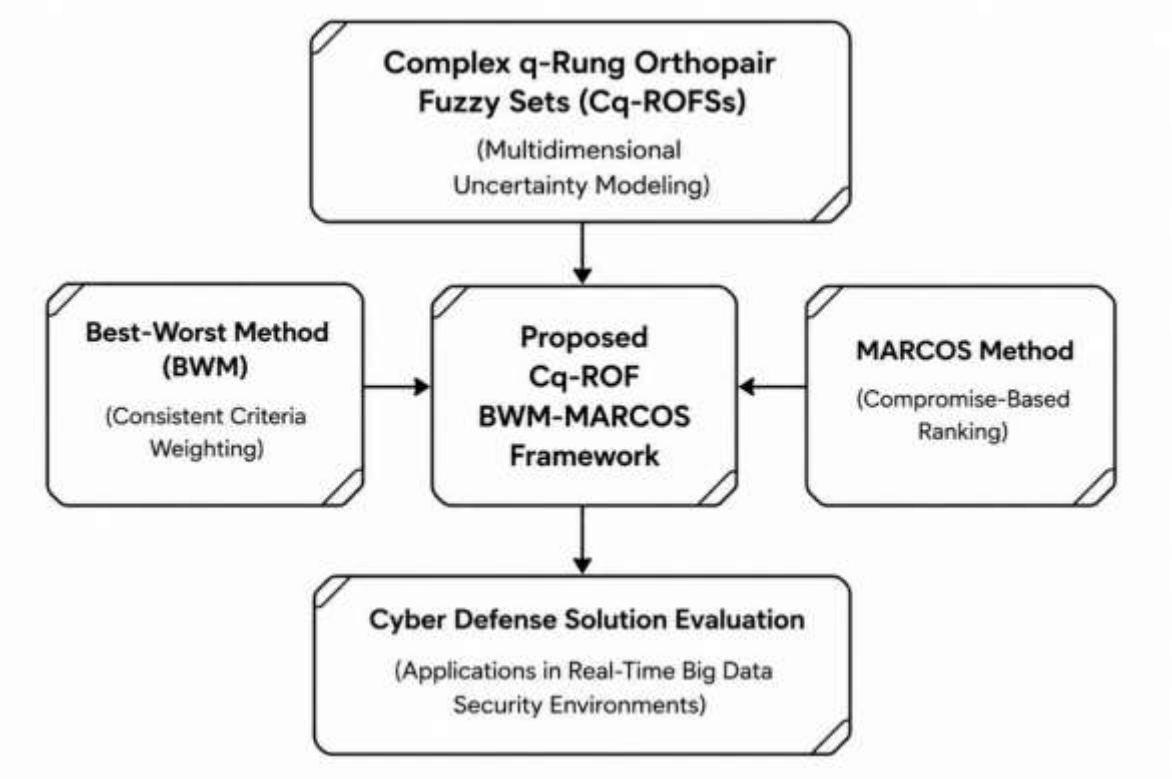

Figure 2: Main contributions.

3 | Literature Review

The increasing complexity of decision-making problems has stimulated the development of advanced MCDM methodologies capable of handling uncertainty, vagueness, and imprecise information. The reliability and effectiveness of decision-making processes in various application domains have been enhanced by proposing many fuzzy-based MCDM frameworks in the last few decades. These have paved the way for the modeling of uncertain information and expert judgments, and continue to improve their modeling ability starting from classical FSs and then to IFSs, PFSs, and q-ROFSs. At the same time, significant efforts have been made to develop effective criteria weighting and alternative ranking techniques, including the BWM and the MARCOS, which have proven to be simple, consistent, and decision-supportive. Hence, in order to build a theoretical base for the proposed framework, the evolution of fuzzy MCDM environments, recent developments in BWM-based decision models, and MARCOS-based approaches under different uncertainty frameworks are reviewed in this section.

3.1 Comparison of Cq-ROFSs with other fuzzy frameworks

The fuzzy set theory has greatly improved the ability of MCDM methods to deal with uncertainty and imprecision in complex decision-making contexts. The concept of FSs was introduced by Zadeh [16] to represent vague and uncertain information and has been used in various decision-making problems, such as the personnel selection problem used by Dursun and Karsak [17]. Although FSs are effective in considering the degree of membership, they don't explicitly take into account non-membership information, which makes them somewhat limited in capturing decision-makers' hesitation. To address this shortcoming, Atanassov [18] introduced IFSs that include membership and non-membership data and offer a more comprehensive description of uncertainty. Li [19] further showed the applicability of IFSs in MCDM. In the case of complex expert judgments, the ability of IFSs to model highly uncertain information is limited. Later, Yager [20] proposed PFSs to provide more flexibility in representing the uncertainty and has been applied in many decision-making applications, including the green supplier development model of Mohd et al. [21]. To make the representation of uncertain information more precise, Yager [22] introduced the q-ROFSs, which offer decision makers a larger and more flexible assessment space than IFSs and PFSs. In supply chain management selection problems, Erdebilli and Sıcakyuz [23] have shown that the effectiveness of q-ROFSs for real-world decision-making applications is very good. However, most of these frameworks are founded on information of real numbers, which may not capture the complexity of real-world evaluations of uncertainty in cybersecurity settings. Unlike the case of q-ROFSs, Cq-ROFSs have the ability to integrate complex values into the model, which makes them more useful to represent uncertainty and allows them to be more flexible in modeling expert judgments for advanced cyber defense evaluation problems.

3.2 Review of BWM

The BWM is one of the most efficient criteria-weighting methods in the MCDM field because it can overcome the drawbacks of the traditional pairwise comparison method by providing a set of reasonable weights and guaranteeing consistency while also requiring fewer pairwise comparisons. BWM is a new type of weighting method proposed by Rezaei [24], which requires the decision makers to select the most important (best) and least important (worst) criteria and then make pairwise comparisons based on these reference criteria. The BWM is an extensively used method in various decision-making applications, as it decreases the burden of comparing alternatives, and expert judgments are more consistent than in traditional weighting methods. Several researchers have extended BWM to the context of uncertainty in decision-making environments after its introduction. Mou et al. [25] proposed an IF multiplicative BWM model for MCDM, which can take both membership and non-membership information into account in the weighting process. Later, Guo and Zhao [26] presented a fuzzy BWM method that can be applied in fuzzy environments and imprecise and vague assessments, and applied it to practical cases. These developments made BWM much more useful in situations of uncertainty in the decision-making process and increased its use in other domains. BWM has also been successfully applied to many practical applications involving decision-

making problems in the real world. Rezaei et al. [27] used BWM for supplier selection, in which traditional and environmental criteria are taken into account throughout the supplier life cycle, demonstrating the ability of BWM to address complex evaluation problems using several conflicting criteria. Because of its simplicity, consistency, and flexibility, BWM is being added increasingly to applications of sustainability assessment, supply chain management, energy planning, healthcare, and risk assessment. With the increasing popularity of BWM, many researchers have been attracted to and have researched extending the methodologies and hybrid decision-making frameworks. Mi et al. [28] thoroughly reviewed the developments and applications of BWM and emphasized that it has been successfully combined with different fuzzy environments, optimization techniques, and MCDM methodologies. Their survey proved to be very effective in implementing BWM as a powerful weighting tool, and the important directions for future research were identified. Although these developments have been made, the use of BWM with advanced uncertainty frameworks for real-time cyber defense solution evaluation in big data security environments is not widely used. Hence, the use of BWM in the proposed Cq-ROF framework can offer a more reliable and accurate approach to determine the weights of the criteria in the presence of high uncertainty in decision-making.

3.3 Review of MARCOS technique

The MARCOS method has emerged as one of the most effective ranking techniques in the field of MCDM due to its ability to evaluate alternatives relative to both ideal and anti-ideal reference solutions. MARCOS has gained considerable popularity among researchers and practitioners due to its strong evaluation mechanism based on the utility of the algorithm and its simplicity of computation, as well as its precise ranking capacity. Since its introduction, many variants of MARCOS have been created with various fuzzy environments in order to enhance its capability to deal with uncertainty, vagueness, and imprecise information in real-world decision-making problems. A few of such developments are fuzzy MARCOS models, which are one of the earliest attempts to include uncertainty into the MARCOS model. Stankovic et al. [29] presented a fuzzy MARCOS algorithm for road traffic risk analysis and tested and evaluated its application in the assessment of uncertain information related to the problems of road traffic risks. Later, Puska et al. [30] used the fuzzy MARCOS method for sustainable supplier selection and demonstrated its applicability in resolving complex supplier selection problems. Moreover, Tus and Adalı [31] combined fuzzy SWARA with fuzzy MARCOS for green supplier selection, which allows both alternative ranking under uncertainty and criteria weighting. In a similar way, Wang et al. [32] recommended a hybrid OPA–fuzzy MARCOS model for the selection of suppliers that ensures sustainability in the context of Industry 4.0. All these studies have shown that the fuzzy MARCOS model is effective in assisting decision-making processes in which the evaluation is subjective and the situation is ambiguous. To achieve the representation of uncertainty in a richer manner, the researchers extended the MARCOS to IF environments. Chaurasiya and Jain [33] came up with a general IF-MARCOS framework that incorporates both positive and negative evaluations by the

experts due to IF entropy. Ecer and Pamucar [34] used the IF MARCOS approach to evaluate the performance of insurance companies in the healthcare sector in the COVID-19 pandemic and illustrated its application in real-world decision-making situations. Furthermore, Kizielewicz et al. [35] studied IF score functions in MARCOS models and helped to enhance the discrimination and reliability of the ranking results. These studies emphasized that the IF-MARCOS approaches can represent uncertainty more comprehensively than conventional fuzzy MARCOS approaches. However, the IF environments are not suitable for representing highly uncertain information, so researchers extended the MARCOS framework with PFSs. Mondal et al. [36] created a PF MEREC-MARCOS model for sustainable forest resource management to offer a systematic method of assessing the alternatives for environmental management. To tackle the complex problem of supplier evaluation, Wang et al. [37] presented a sustainable food supplier selection framework based on PF CRITIC-MARCOS and showed the validity of the proposed method through some numerical examples. Similarly, Chaurasiya and Jain [38] have developed a new PF decision-making algorithm and proved its usefulness in real-life decision-making environments. Recently, Younis et al. [39] used the Pythagorean hesitant fuzzy MARCOS framework for optimizing renewable energy investments, and Mishra et al. [40] proposed an integrated PF operator-based MARCOS method for sustainable circular supplier selection. The results of these studies also verified the flexibility and the uncertainty-handling ability of PF MARCOS models over their predecessors. As fuzzy decision-making theories are continuously developed, the q-ROF extension of MARCOS has gained much interest because of its better representation capability of uncertain information. As per Krishankumar et al. [41], the 'CRITIC-MARCOS' framework was proposed to evaluate the measures of zero-carbon transportation in smart cities using q-rung fuzzy preferences. Ali [42] proposed a q-ROF MARCOS model with a new score function for solid waste management problems, and illustrated the proposed model with a practical application, which was a complex environmental decision-making model. In order to solve the solid waste management problem, Ali [42] proposed a new score function for the q-ROF MARCOS model and illustrated the proposed model with a practical example that is a complex environmental decision-making model. Moreover, Mahmood and Ali [43] upgraded the MARCOS technique in a fuzzy environment of q-rung to assess insurance companies with respect to healthcare service. These contributions confirm that the q-ROF MARCOS model is more flexible and has more powerful uncertainty representation than the fuzzy, IF, and PF MARCOS models. Although a lot of work has already been done in the development of fuzzy, IF, PF, and q-ROF MARCOS models, most of the existing research has been based on real-valued information structures to represent the evaluation of experts. These may thus be unsuitable for modelling very complex, high-dimensional, and complex uncertainty as found in current decision environments. Real-time big data security assessment is particularly challenging because it requires complex expert judgments, the dynamic

nature of threats, and the complex relationships among the evaluation criteria, which call for more expressive uncertainty modeling frameworks. Thus, by combining the MARCOS method with the proposed Cq-ROF, it is possible to have a more comprehensive representation of uncertain information and a more effective ranking method for the assessment of advanced cyber defense solutions in real-time big data security environments.

4 | Fundamentals:

In this section, the basic definition of Cq-ROFs is discussed.

Definition 1: [44] A Cq-ROFS $\mathbb{K}$ corresponding to the universe of discourse $\mathcal{U}$ is described by;

$$\mathbb{K} = \left\{\left(\hbar, \mu^{\tilde{m}}(\hbar), \nu^{\tilde{n}}(\hbar)\right) | \hbar \in \mathcal{U}\right\} = \left\{\left(\hbar, \mu^{\widetilde{m-re}} + \iota\mu^{\widetilde{m-im}}, \nu^{\widetilde{n-re}} + \iota\nu^{\widetilde{n-im}}\right) | \hbar \in \mathcal{U}\right\} \quad (1)$$

Here, $\mu^{\tilde{m}}$ and $\nu^{\tilde{n}}$ denote the membership and non-membership functions, respectively. Their corresponding real and imaginary parts satisfy $0 \leq \left(\mu^{\widetilde{m-re}}\right)^{q} + \left(\nu^{\widetilde{n-re}}\right)^{q} \leq 1$ and $0 \leq \left(\mu^{\widetilde{m-im}}\right)^{q} + \left(\nu^{\widetilde{n-im}}\right)^{q} \leq 1$, where $q \geq 1$. These conditions guarantee the admissibility of the Cq-ROFS information.

5 | Aggregation Operators based on Cq-ROFSs

In this section, we have introduced weighted average and geometric aggregation operators based on Cq-ROFSs.

Definition 2: Suppose $\mathbb{K}_{ą} = \left(\mu_{ą}^{\tilde{m}}, \nu_{ą}^{\tilde{n}}\right) = \left(\mu_{ą}^{\widetilde{m-re}} + \iota\mu_{ą}^{\widetilde{m-im}}, \nu_{ą}^{\widetilde{n-re}} + \iota\nu_{ą}^{\widetilde{n-im}}\right)$ $(ą = 1,2, \dots, ņ)$ represents a set of Cq-ROFNs. Then the corresponding Cq-ROFWA operator is expressed as;

$$\text{Cq} - \text{ROFWA}\left(\mathbb{K}_1, \mathbb{K}_2, \dots, \mathbb{K}_{ņ}\right) = \mathbb{W}_1\mathbb{K}_1 \oplus \mathbb{W}_2\mathbb{K}_2 \oplus \dots \oplus \mathbb{W}_{ņ}\mathbb{K}_{ņ} = \sum_{ą=1}^{ņ} \mathbb{W}_{ą}\mathbb{K}_{ą} \quad (2)$$

Where the weight vector is given by $0 \leq \mathbb{W}_{ņ} \leq 1$ with $\sum_{ą=1}^{ņ} \mathbb{W}_{ą} = 1$.

Theorem 1: Employing the aggregation operator defined in Eq. (2) ensures that the aggregated result is still a Cq-ROFN. Moreover,

$$\text{Cq} - \text{ROFWA}\left(\mathbb{K}_1, \mathbb{K}_2, \dots, \mathbb{K}_{ņ}\right) =$$

$$\left(\left(1 - \prod_{ą=1}^{ņ}\left(1 - \left(\mu_{ą}^{\widetilde{m-re}}\right)^{q}\right)^{\mathbb{W}_{ą}}\right)^{\frac{1}{q}} + \iota\left(1 - \prod_{ą=1}^{ņ}\left(1 - \left(\mu_{ą}^{\widetilde{m-im}}\right)^{q}\right)^{\mathbb{W}_{ą}}\right)^{\frac{1}{q}}, \prod_{ą=1}^{ņ}\left(\nu_{ą}^{\widetilde{n-re}}\right)^{\mathbb{W}_{ą}} + \iota\prod_{ą=1}^{ņ}\left(\nu_{ą}^{\widetilde{n-im}}\right)^{\mathbb{W}_{ą}}\right)$$

Definition 3: Suppose $\mathbb{K}_{ą} = \left(\mu_{ą}^{\tilde{m}}, \nu_{ą}^{\tilde{n}}\right) = \left(\mu_{ą}^{\widetilde{m-re}} + \iota\mu_{ą}^{\widetilde{m-im}}, \nu_{ą}^{\widetilde{n-re}} + \iota\nu_{ą}^{\widetilde{n-im}}\right)$ $(ą = 1,2, \dots, ņ)$ represent a set of Cq-ROFNs. Then the corresponding Cq-ROFWG operator is expressed as;

$$\text{Cq} - \text{ROFWG}\left(\mathbb{K}_1, \mathbb{K}_2, \dots, \mathbb{K}_{ņ}\right) = \mathbb{W}_1\mathbb{K}_1 \otimes \mathbb{W}_2\mathbb{K}_2 \otimes \dots \otimes \mathbb{W}_{ņ}\mathbb{K}_{ņ} = \sum_{ą=1}^{ņ}\left(\mathbb{K}_{ą}\right)^{\mathbb{W}_{ą}} \quad (3)$$

Where the weight vector is given by $0 \leq \mathbb{W}_{ņ} \leq 1$ with $\sum_{ą=1}^{ņ} \mathbb{W}_{ą} = 1$.

Theorem 2: Employing the aggregation operator defined in Eq. (3) ensures that the aggregated result is still a Cq-ROFN. Moreover,

$$\mathrm{Cq-ROFWG}(\mathbb{K}_1, \mathbb{K}_2, \dots, \mathbb{K}_n) = \left(\prod_{q=1}^{n} \left(\mu_q^{\widehat{m-re}}\right)^{\mathbb{W}_q} + \iota \prod_{q=1}^{n} \left(\mu_q^{\widehat{m-im}}\right)^{\mathbb{W}_q}, \left(1 - \prod_{q=1}^{n} \left(1 - \left(\nu_q^{\widehat{n-re}}\right)^{q}\right)^{\mathbb{W}_q}\right)^{\frac{1}{q}} + \iota \left(1 - \prod_{q=1}^{n} \left(1 - \left(\nu_q^{\widehat{n-im}}\right)^{q}\right)^{\mathbb{W}_q}\right)^{\frac{1}{q}} \right)$$

6|BWM-MARCOS Technique

BWM-MARCOS has the following steps.

Step 1: In the first step, the decision matrix is established by collecting the performance evaluations of all alternatives with respect to the selected criteria. Let $\hat{\mathrm{A}}_i\ (i = 1,2,\dots,m)$ denote the alternatives and $\check{\mathrm{C}}_j\ (j = 1,2,\dots,n)$ represent the evaluation criteria. The obtained assessments are arranged in the form of a decision matrix $\underset{\wedge}{\mathrm{D}} = [\underset{\wedge}{\mathrm{d}}_{ij}]_{m\times n}$, where $\underset{\wedge}{\mathrm{d}}_{ij}$ indicates the performance value of the alternative $\hat{\mathrm{A}}_i$ under criterion $\check{\mathrm{C}}_j$. For group decision-making problems, the experts' evaluations are aggregated through the proposed Cq-ROFWA or Cq-ROFG operator to construct a collective decision matrix as given below.

$$\underset{\wedge}{\mathrm{D}} = \begin{bmatrix} \underset{\wedge}{\mathrm{d}}_{11} & \underset{\wedge}{\mathrm{d}}_{12} & \cdots & \underset{\wedge}{\mathrm{d}}_{1n} \\ \underset{\wedge}{\mathrm{d}}_{21} & \underset{\wedge}{\mathrm{d}}_{22} & \cdots & \underset{\wedge}{\mathrm{d}}_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \underset{\wedge}{\mathrm{d}}_{m1} & \underset{\wedge}{\mathrm{d}}_{m2} & \cdots & \underset{\wedge}{\mathrm{d}}_{mn} \end{bmatrix}$$

Step 2: Now, we will find the score values of $\underset{\wedge}{\mathrm{D}}_{ij}$ with the help of $\breve{\mathrm{S}}(\mathbb{K}) = \frac{1}{4}\left\{2 + (\mu^{\widehat{m-re}})^{q} + (\mu^{\widehat{m-im}})^{q} - \left(\nu^{\widehat{n-re}}\right)^{q} - \left(\nu^{\widehat{n-im}}\right)^{q}\right\}$.

$$\breve{\mathrm{S}} = \begin{bmatrix} \breve{\mathrm{s}}_{11} & \breve{\mathrm{s}}_{12} & \cdots & \breve{\mathrm{s}}_{1n} \\ \breve{\mathrm{s}}_{21} & \breve{\mathrm{s}}_{22} & \cdots & \breve{\mathrm{s}}_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \breve{\mathrm{s}}_{m1} & \breve{\mathrm{s}}_{m2} & \cdots & \breve{\mathrm{s}}_{mn} \end{bmatrix}$$

Step 3: Formation of an extended initial matrix. In this step, the ideal solution (AI) A_j^{+} and an anti-ideal solution (AAI) A_j^{-} are determined and appended to the decision matrix. The AI represents the best attainable performance of each criterion, and the AAI represents the worst attainable performance. The AI and AAI are obtained as;

$$A_j^{+} = \max_i \breve{\mathrm{s}}_{ij}, A_j^{-} = \min_i \breve{\mathrm{s}}_{ij} \text{ if } j \text{ is a benefit-type criterion;}$$

$$A_j^{+} = \min_i \breve{\mathrm{s}}_{ij}, A_j^{-} = \max_i \breve{\mathrm{s}}_{ij} \text{ if } j \text{ is a cost-type criterion.}$$

Step 4: The decision matrix is normalized to ensure comparability among criteria. The normalized matrix can be obtained as follows.

$$n_{ij} = \frac{\breve{\mathrm{s}}_{ij}}{A_j^{+}} \text{ if } j \text{ is a benefit type ; } n_{ij} = \frac{A_j^{-}}{\breve{\mathrm{s}}_{ij}} \text{ if } j \text{ is a cost type}$$

Step 5: Calculation of criteria weights by using the BWM technique.

Step 5.1: Identification of evaluation criteria by the experts.

Step 5.2: Selection of best and worst criteria. The DMs identify the most important criteria (best criteria) and the least important criteria (worst criteria) from the set of criteria.

Step 5.3: Construction of the best criteria for others' preference vector. The best criteria are compared with all other criteria using a preference scale from 1 to 9, where 1 indicates equal importance and 9 indicates extreme importance.

$$\hat{A}_B = (\alpha_{B1}, \alpha_{B2}, \dots, \alpha_{Bn})$$

Where α_{Bj} indicates the preference of criterion over the best criterion j.

Step 5.4: Construction of others-to-worst preference vector. By using the same scale, all criteria are compared with the worst criterion.

$$\hat{A}_w = (\alpha_{1w}, \alpha_{2w}, \dots, \alpha_{nw})^T$$

Where α_{jw} indicates the preference of criterion j over the worst criterion.

Step 5.5: Determination of optimal criteria weights. The optimal weights of the criteria we should find a solution where the maximum absolute differences for all j are minimized (min ξ) as follows.

$$\left| \frac{₩_B}{₩_j} - \alpha_{Bj} \right| \leq \xi \; for \; all \; j$$

$$\left| \frac{₩_j}{₩_w} - \alpha_{jw} \right| \leq \xi \; for \; all \; j$$

Where $\sum_j ₩ = 1$ and $₩_j > 0$ for all j.

Step 6: Next, we will determine the weighted normalized matrix. The weighted normalized matrix can be found by using the weights of the criteria.

$$v_{ij} = n_{ij} \times ₩_{ij}$$

Step 7: Calculation of the utility degree of alternatives K_i. The degree of the alternatives in relation to the anti-ideal and ideal solution is found as

$$K_i^+ = \sum_{i=1}^{n} \left(\frac{v_{ij}}{A_j^+} \right); K_i^- = \sum_{i=1}^{n} \left(\frac{v_{ij}}{A_j^-} \right)$$

Step 8: Determination of the utility function of alternatives $f(K_i)$. The utility function is the compromise of the observed alternative in relation to the ideal and anti-ideal solution. The utility function of alternatives can be found as

$$f(K_i) = \frac{K_i^+ + K_i^-}{1 + \frac{1 - f(K_i^+)}{f(K_i^+)} + \frac{1 - f(K_i^-)}{f(K_i^-)}}$$

where $f(K_i^-)$ represents the utility function in relation to the anti-ideal solution, while $f(K_i^+)$ represents the utility function in relation to the ideal solution and can be determined as

$$f(K_i^+) = \frac{K_i^-}{K_i^+ + K_i^-}; f(K_i^-) = \frac{K_i^+}{K_i^+ + K_i^-}$$

Step 9: Ranking the alternatives. Ranking of the alternatives is based on the final values of utility functions. The alternative with the highest value of the utility function is the best.

Where the BWM-MAROS methodology is shown in Figure 3.

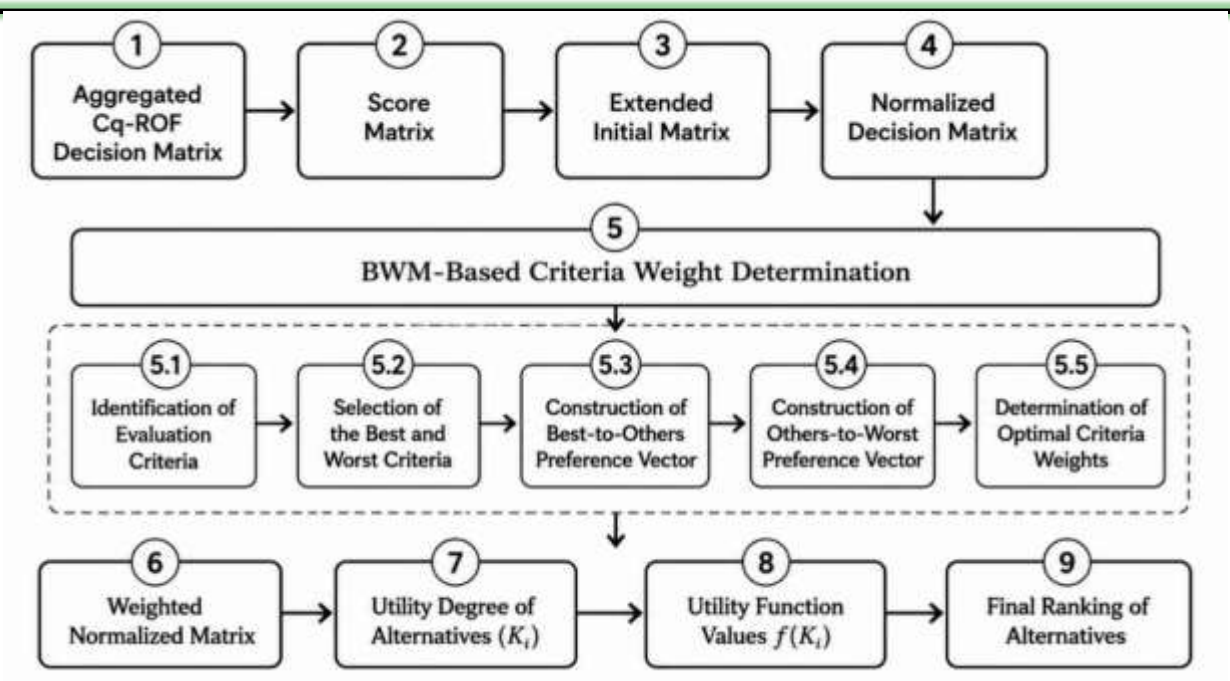

Figure 3: BWM-MARCOS methodology.

6.1 Case Study

Modern organizations increasingly rely on big data technologies to support real-time analytics, intelligent decision-making, cloud computing, IoT applications, and digital transformation initiatives. However, the continuous generation and transmission of massive data streams have significantly expanded the cyber threat landscape, exposing organizations to sophisticated attacks such as advanced persistent threats, ransomware, insider threats, data breaches, and zero-day exploits. Traditional security mechanisms often struggle to provide adequate protection in highly dynamic big data environments due to limitations in scalability, adaptability, and real-time threat response. Consequently, advanced cyber defense solutions have emerged as critical components for ensuring the confidentiality, integrity, and availability of large-scale data infrastructures.

Evaluation of Advanced Cyber Defense Solutions: There are several conflicting criteria governing the evaluation of advanced cyber defense solutions: processing performance, threat detection capability, scalability, adaptive response, and implementation requirements. The criteria are frequently vague, ambiguous, and subject to expert opinion, which can come from the dynamic and complex cybersecurity landscapes. In addition, the performance of a security solution can be different under different operating conditions, attack patterns, and organizational needs. As such, it is an MCDM problem that demands an effective evaluation framework under uncertainty where a cyber-defense solution is considered. Hence, choosing the most appropriate cyber defense solution is a challenging MCDM problem that needs a strong uncertainty-aware evaluation framework.

The effectiveness of the Proposed Framework: The proposed Cq-ROF BWMMARCOS framework is an effective tool for assessing complex cyber defense solutions in uncertain decision-making scenarios. The framework employs the Cq-ROF information to model multidimensional uncertainty from experts'

evaluations. Moreover, the BWM is used to assess the relative importance of the evaluation criteria, and MARCOS is used to rank the competing alternatives according to the utility of alternatives, relative to ideal and anti-ideal solutions. The proposed framework is a complete framework that combines advanced uncertainty modeling, reliable criteria weighting, and compromise-based ranking to provide a comprehensive decision-support tool for determining the most suitable cyber defense solution for improving real-time big data security. The alternatives chosen for evaluation are discussed in Table 1.

Table 1: Alternatives description.

Symbol	Alternative	Description
$\hat{A}_1$	**Automated Security Orchestration, Automation, and Response**	It unifies security tools and automates incident response workflows using pre-defined playbooks. It shortens response time, decreases human interaction, and improves security operations efficiency.
$\hat{A}_2$	**Digital Twin-Based Cyber Defense Platform**	A real-time digital replica of the cyber infrastructure that continuously simulates attack scenarios, predicts vulnerabilities, and evaluates the impact of cyber threats before they affect the operational environment. The platform combines AI-driven analytics, threat intelligence, and predictive security monitoring to enhance proactive cyber defense.
$\hat{A}_3$	**AI-Powered Network Detection and Response**	The solution uses AI technology and behavioral analytics to track network traffic and detect any suspicious activity. It supports proactive threat identification and quick response to incidents in expansive data centers.
$\hat{A}_4$	**Autonomous Security Operations Center**	An AI-based security operations platform that continuously monitors, detects, investigates, and responds to cyber threats. It brings automation, analytics, and intelligent decision-making together to enhance the organizational security posture.
$\hat{A}_5$	**AI-Driven Extended Detection and Response**	In the era of AI-driven extended detection and response, security data from various sources is unified and processed, and machine learning algorithms are used to detect, analyze, and respond to cyber threats in real-time. Delivers full visibility of endpoints, networks, cloud, and applications.
$\hat{A}_6$	**Cloud-Native SIEM with Real-Time User and Entity Behavior Analytics**	A cloud-based Security Information and Event Management platform that continuously monitors user and system activities. By employing behavioral analytics, it identifies anomalies and potential security breaches in real time.

$\hat{A}_7$	**Zero-Trust Network Access with Continuous Micro-Segmentation**	This is the "never trust, always verify" approach, and it will constantly verify users, devices, and applications. It increases security by increasing the separation of important big data assets and restricting unauthorized lateral data transfer in the network.
$\hat{A}_8$	**Decentralized Blockchain-Based Threat Intelligence Sharing**	The solution relies on blockchain technology to provide a secure, transparent, and tamper-proof exchange of threat intelligence between organizations. It enhances collective cybersecurity awareness and helps to speed up threat mitigation.

The selected criteria for evaluation are discussed in Table 2.

Table 2: Criteria description.

Symbol	Criteria	Description
$\check{C}_1$	**Processing Latency and Throughput**	This criterion assesses whether a cyber-defense solution can help to handle a huge amount of high-speed data without slowing down the system. A higher throughput and lower latency mean better performance in real-time big data environments.
$\check{C}_2$	**Detection Accuracy and False Positive Rate**	This criterion indicates the effectiveness of a solution's ability to accurately detect cyber threats with fewer false alarms. The more accurate the detection and with fewer false positives, the higher the reliability and efficiency of the solution.
$\check{C}_3$	**Scalability and Resource Efficiency**	This criterion evaluates the ability of a solution to sustain performance with the growth of data volumes and network complexity. It also takes into account efficient use of computational and storage resources.
$\check{C}_4$	**Real-Time Adaptive Agility**	This criterion assesses the ability of a solution to adapt to new cyber threats and attack patterns quickly and effectively. A highly adaptive solution can provide higher protection against sophisticated and emerging threats.
$\check{C}_5$	**Implementation Complexity**	This criterion is a measure of the technical difficulty, deployment effort, and operational challenges of implementing and maintaining the solution. The lower the implementation complexity, the easier the adoption and the less there is to do.

6.2 Numerical Example

A numerical example consisting of three decision experts with weights $(0.33, 0.37, 0.30)$, eight alternatives $(\hat{A}_1, \hat{A}_2, \hat{A}_3, \hat{A}_4, \hat{A}_5, \hat{A}_6, \hat{A}_7, \hat{A}_8)$, and five criteria $(\check{C}_1, \check{C}_2, \check{C}_3, \check{C}_4, \check{C}_5)$ is considered to

demonstrate the applicability of the proposed Cq-ROF BWM-MARCOS framework. The alternatives represent advanced cyber defense solutions, whereas the criteria correspond to key technical, security, operational, and economic aspects of real-time big data security environments.

Step 1: The decision matrices by three different experts are given in Tables 3, 4, and 5. The aggregated matrix using the Cq-ROFWA operator is given in Table 6.

Table 3: Decision matrix by expert 1.

	$\check{C}_1$	$\check{C}_2$	$\check{C}_3$	$\check{C}_4$	$\check{C}_5$
$\hat{A}_1$	$(0.550+\iota 0.291,\ 0.480+\iota 0.370)$	$(0.410+\iota 0.580,\ 0.710+\iota 0.411)$	$(0.481+\iota 0.590,\ 0.611+\iota 0.490)$	$(0.391+\iota 0.440,\ 0.490+\iota 0.580)$	$(0.590+\iota 0.191,\ 0.410+\iota 0.610)$
$\hat{A}_2$	$(0.652+\iota 0.441,\ 0.441+\iota 0.330)$	$(0.531+\iota 0.410,\ 0.490+\iota 0.581)$	$(0.491+\iota 0.380,\ 0.550+\iota 0.420)$	$(0.281+\iota 0.570,\ 0.670+\iota 0.430)$	$(0.370+\iota 0.430,\ 0.620+\iota 0.480)$
$\hat{A}_3$	$(0.760+\iota 0.381,\ 0.372+\iota 0.680)$	$(0.490+\iota 0.390,\ 0.381+\iota 0.410)$	$(0.750+\iota 0.660,\ 0.310+\iota 0.491)$	$(0.490+\iota 0.631,\ 0.560+\iota 0.380)$	$(0.440+\iota 0.290,\ 0.590+\iota 0.751)$
$\hat{A}_4$	$(0.480+\iota 0.590,\ 0.581+\iota 0.410)$	$(0.391+\iota 0.620,\ 0.510+\iota 0.620)$	$(0.410+\iota 0.720,\ 0.651+\iota 0.370)$	$(0.580+\iota 0.471,\ 0.460+\iota 0.521)$	$(0.610+\iota 0.491,\ 0.480+\iota 0.581)$
$\hat{A}_5$	$(0.810+\iota 0.671,\ 0.290+\iota 0.390)$	$(0.771+\iota 0.590,\ 0.280+\iota 0.411)$	$(0.671+\iota 0.390,\ 0.380+\iota 0.611)$	$(0.481+\iota 0.390,\ 0.571+\iota 0.690)$	$(0.550+\iota 0.550,\ 0.381+\iota 0.490)$
$\hat{A}_6$	$(0.491+\iota 0.580,\ 0.480+\iota 0.511)$	$(0.370+\iota 0.281,\ 0.630+\iota 0.480)$	$(0.281+\iota 0.570,\ 0.680+\iota 0.370)$	$(0.670+\iota 0.580,\ 0.380+\iota 0.481)$	$(0.710+\iota 0.390,\ 0.330+\iota 0.681)$
$\hat{A}_7$	$(0.581+\iota 0.390,\ 0.260+\iota 0.610)$	$(0.440+\iota 0.530,\ 0.581+\iota 0.511)$	$(0.150+\iota 0.451,\ 0.440+\iota 0.540)$	$(0.240+\iota 0.590,\ 0.660+\iota 0.511)$	$(0.471+\iota 0.550,\ 0.591+\iota 0.480)$
$\hat{A}_8$	$(0.390+\iota 0.221,\ 0.550+\iota 0.640)$	$(0.291+\iota 0.410,\ 0.620+\iota 0.630)$	$(0.741+\iota 0.280,\ 0.310+\iota 0.460)$	$(0.191+\iota 0.610,\ 0.710+\iota 0.470)$	$(0.520+\iota 0.480,\ 0.610+\iota 0.550)$

Table 4: Decision matrix by expert 2.

	$\check{C}_1$	$\check{C}_2$	$\check{C}_3$	$\check{C}_4$	$\check{C}_5$
$\hat{A}_1$	$(0.470+\iota 0.471,\ 0.390+\iota 0.570)$	$(0.390+\iota 0.491,\ 0.510+\iota 0.540)$	$(0.370+\iota 0.631,\ 0.710+\iota 0.331)$	$(0.511+\iota 0.590,\ 0.440+\iota 0.410)$	$(0.410+\iota 0.621,\ 0.630+\iota 0.370)$
$\hat{A}_2$	$(0.360+\iota 0.390,\ 0.671+\iota 0.630)$	$(0.581+\iota 0.290,\ 0.430+\iota 0.730)$	$(0.490+\iota 0.651,\ 0.530+\iota 0.410)$	$(0.370+\iota 0.490,\ 0.670+\iota 0.531)$	$(0.590+\iota 0.370,\ 0.340+\iota 0.570)$
$\hat{A}_3$	$(0.590+\iota 0.411,\ 0.520+\iota 0.710)$	$(0.630+\iota 0.370,\ 0.370+\iota 0.640)$	$(0.460+\iota 0.431,\ 0.590+\iota 0.470)$	$(0.671+\iota 0.290,\ 0.380+\iota 0.710)$	$(0.380+\iota 0.521,\ 0.670+\iota 0.470)$
$\hat{A}_4$	$(0.610+\iota 0.510,\ 0.480+\iota 0.530)$	$(0.490+\iota 0.581,\ 0.410+\iota 0.290)$	$(0.521+\iota 0.480,\ 0.470+\iota 0.530)$	$(0.480+\iota 0.370,\ 0.530+\iota 0.531)$	$(0.610+\iota 0.411,\ 0.370+\iota 0.510)$
$\hat{A}_5$	$(0.711+\iota 0.530,\ 0.390+\iota 0.601)$	$(0.610+\iota 0.490,\ 0.341+\iota 0.530)$	$(0.750+\iota 0.590,\ 0.371+\iota 0.420)$	$(0.691+\iota 0.420,\ 0.380+\iota 0.631)$	$(0.711+\iota 0.610,\ 0.281+\iota 0.370)$
$\hat{A}_6$	$(0.491+\iota 0.380,\ 0.610+\iota 0.680)$	$(0.530+\iota 0.510,\ 0.340+\iota 0.471)$	$(0.371+\iota 0.390,\ 0.710+\iota 0.630)$	$(0.410+\iota 0.620,\ 0.640+\iota 0.471)$	$(0.580+\iota 0.530,\ 0.411+\iota 0.430)$
$\hat{A}_7$	$(0.520+\iota 0.491,\ 0.570+\iota 0.570)$	$(0.291+\iota 0.440,\ 0.680+\iota 0.571)$	$(0.291+\iota 0.470,\ 0.630+\iota 0.550)$	$(0.390+\iota 0.580,\ 0.710+\iota 0.411)$	$(0.390+\iota 0.471,\ 0.610+\iota 0.510)$
$\hat{A}_8$	$(0.291+\iota 0.710,\ 0.620+\iota 0.410)$	$(0.441+\iota 0.380,\ 0.581+\iota 0.610)$	$(0.611+\iota 0.350,\ 0.490+\iota 0.741)$	$(0.281+\iota 0.490,\ 0.630+\iota 0.341)$	$(0.471+\iota 0.510,\ 0.510+\iota 0.480)$

Table 5: Decision matrix by expert 3.

	$\check{C}_1$	$\check{C}_2$	$\check{C}_3$	$\check{C}_4$	$\check{C}_5$

$\hat{A}_1$	$\begin{pmatrix}0.380+\iota 0.631,\\0.610+\iota 0.480\end{pmatrix}$	$\begin{pmatrix}0.531+\iota 0.490,\\0.480+\iota 0.530\end{pmatrix}$	$\begin{pmatrix}0.291+\iota 0.680,\\0.550+\iota 0.390\end{pmatrix}$	$\begin{pmatrix}0.410+\iota 0.610,\\0.680+\iota 0.381\end{pmatrix}$	$\begin{pmatrix}0.221+\iota 0.380,\\0.680+\iota 0.620\end{pmatrix}$
$\hat{A}_2$	$\begin{pmatrix}0.470+\iota 0.511,\\0.520+\iota 0.490\end{pmatrix}$	$\begin{pmatrix}0.481+\iota 0.530,\\0.530+\iota 0.490\end{pmatrix}$	$\begin{pmatrix}0.511+\iota 0.560,\\0.410+\iota 0.510\end{pmatrix}$	$\begin{pmatrix}0.390+\iota 0.580,\\0.731+\iota 0.430\end{pmatrix}$	$\begin{pmatrix}0.390+\iota 0.441,\\0.710+\iota 0.582\end{pmatrix}$
$\hat{A}_3$	$\begin{pmatrix}0.521+\iota 0.430,\\0.470+\iota 0.580\end{pmatrix}$	$\begin{pmatrix}0.391+\iota 0.620,\\0.630+\iota 0.410\end{pmatrix}$	$\begin{pmatrix}0.470+\iota 0.420,\\0.560+\iota 0.621\end{pmatrix}$	$\begin{pmatrix}0.521+\iota 0.490,\\0.550+\iota 0.570\end{pmatrix}$	$\begin{pmatrix}0.461+\iota 0.610,\\0.550+\iota 0.460\end{pmatrix}$
$\hat{A}_4$	$\begin{pmatrix}0.290+\iota 0.461,\\0.730+\iota 0.560\end{pmatrix}$	$\begin{pmatrix}0.410+\iota 0.631,\\0.650+\iota 0.380\end{pmatrix}$	$\begin{pmatrix}0.610+\iota 0.581,\\0.420+\iota 0.521\end{pmatrix}$	$\begin{pmatrix}0.631+\iota 0.372,\\0.390+\iota 0.611\end{pmatrix}$	$\begin{pmatrix}0.581+\iota 0.570,\\0.480+\iota 0.391\end{pmatrix}$
$\hat{A}_5$	$\begin{pmatrix}0.680+\iota 0.590,\\0.350+\iota 0.431\end{pmatrix}$	$\begin{pmatrix}0.710+\iota 0.571,\\0.350+\iota 0.470\end{pmatrix}$	$\begin{pmatrix}0.731+\iota 0.620,\\0.380+\iota 0.411\end{pmatrix}$	$\begin{pmatrix}0.681+\iota 0.510,\\0.410+\iota 0.580\end{pmatrix}$	$\begin{pmatrix}0.670+\iota 0.710,\\0.390+\iota 0.380\end{pmatrix}$
$\hat{A}_6$	$\begin{pmatrix}0.381+\iota 0.640,\\0.650+\iota 0.370\end{pmatrix}$	$\begin{pmatrix}0.390+\iota 0.611,\\0.610+\iota 0.390\end{pmatrix}$	$\begin{pmatrix}0.520+\iota 0.430,\\0.571+\iota 0.590\end{pmatrix}$	$\begin{pmatrix}0.520+\iota 0.670,\\0.581+\iota 0.380\end{pmatrix}$	$\begin{pmatrix}0.491+\iota 0.440,\\0.520+\iota 0.590\end{pmatrix}$
$\hat{A}_7$	$\begin{pmatrix}0.491+\iota 0.530,\\0.530+\iota 0.411\end{pmatrix}$	$\begin{pmatrix}0.450+\iota 0.571,\\0.580+\iota 0.471\end{pmatrix}$	$\begin{pmatrix}0.390+\iota 0.611,\\0.610+\iota 0.440\end{pmatrix}$	$\begin{pmatrix}0.470+\iota 0.561,\\0.610+\iota 0.481\end{pmatrix}$	$\begin{pmatrix}0.291+\iota 0.591,\\0.460+\iota 0.631\end{pmatrix}$
$\hat{A}_8$	$\begin{pmatrix}0.531+\iota 0.411,\\0.470+\iota 0.630\end{pmatrix}$	$\begin{pmatrix}0.520+\iota 0.490,\\0.491+\iota 0.530\end{pmatrix}$	$\begin{pmatrix}0.431+\iota 0.551,\\0.630+\iota 0.470\end{pmatrix}$	$\begin{pmatrix}0.330+\iota 0.510,\\0.530+\iota 0.570\end{pmatrix}$	$\begin{pmatrix}0.611+\iota 0.480,\\0.390+\iota 0.580\end{pmatrix}$

Table 6: Aggregated matrix.

	$\check{C}_1$	$\check{C}_2$	$\check{C}_3$	$\check{C}_4$	$\check{C}_5$
$\hat{A}_1$	$\begin{pmatrix}0.4804+\\\iota 0.5017,\\0.4776+\\\iota 0.4694\end{pmatrix}$	$\begin{pmatrix}0.4485+\\\iota 0.5241,\\0.5585+\\\iota 0.4903\end{pmatrix}$	$\begin{pmatrix}0.3984+\\\iota 0.6349,\\0.6255+\\\iota 0.3953\end{pmatrix}$	$\begin{pmatrix}0.4481+\\\iota 0.5587,\\0.5195+\\\iota 0.4494\end{pmatrix}$	$\begin{pmatrix}0.4644+\\\iota 0.4834,\\0.5594+\\\iota 0.5095\end{pmatrix}$
$\hat{A}_2$	$\begin{pmatrix}0.5252+\\\iota 0.4487,\\0.5404+\\\iota 0.4720\end{pmatrix}$	$\begin{pmatrix}0.5374+\\\iota 0.4270,\\0.4780+\\\iota 0.6004\end{pmatrix}$	$\begin{pmatrix}0.4962+\\\iota 0.5620,\\0.4968+\\\iota 0.4412\end{pmatrix}$	$\begin{pmatrix}0.3528+\\\iota 0.5473,\\0.6875+\\\iota 0.4646\end{pmatrix}$	$\begin{pmatrix}0.4843+\\\iota 0.4134,\\0.5170+\\\iota 0.5414\end{pmatrix}$
$\hat{A}_3$	$\begin{pmatrix}0.6501+\\\iota 0.4072,\\0.4509+\\\iota 0.6588\end{pmatrix}$	$\begin{pmatrix}0.5349+\\\iota 0.4849,\\0.4379+\\\iota 0.4834\end{pmatrix}$	$\begin{pmatrix}0.6059+\\\iota 0.5344,\\0.4697+\\\iota 0.5178\end{pmatrix}$	$\begin{pmatrix}0.5817+\\\iota 0.5093,\\0.4825+\\\iota 0.5408\end{pmatrix}$	$\begin{pmatrix}0.4269+\\\iota 0.5090,\\0.6055+\\\iota 0.5449\end{pmatrix}$
$\hat{A}_4$	$\begin{pmatrix}0.5089+\\\iota 0.5280,\\0.5794+\\\iota 0.4951\end{pmatrix}$	$\begin{pmatrix}0.4382+\\\iota 0.6093,\\0.5059+\\\iota 0.4041\end{pmatrix}$	$\begin{pmatrix}0.5256+\\\iota 0.6136,\\0.5057+\\\iota 0.4681\end{pmatrix}$	$\begin{pmatrix}0.5671+\\\iota 0.4092,\\0.4613+\\\iota 0.5494\end{pmatrix}$	$\begin{pmatrix}0.6014+\\\iota 0.4949,\\0.4359+\\\iota 0.4909\end{pmatrix}$
$\hat{A}_5$	$\begin{pmatrix}0.7428+\\\iota 0.6024,\\0.3424+\\\iota 0.4710\end{pmatrix}$	$\begin{pmatrix}0.7041+\\\iota 0.5515,\\0.3217+\\\iota 0.4697\end{pmatrix}$	$\begin{pmatrix}0.7206+\\\iota 0.5545,\\0.3763+\\\iota 0.4716\end{pmatrix}$	$\begin{pmatrix}0.6371+\\\iota 0.4436,\\0.4444+\\\iota 0.6333\end{pmatrix}$	$\begin{pmatrix}0.6558+\\\iota 0.6303,\\0.3421+\\\iota 0.4092\end{pmatrix}$
$\hat{A}_6$	$\begin{pmatrix}0.4630+\\\iota 0.5516,\\0.5745+\\\iota 0.5152\end{pmatrix}$	$\begin{pmatrix}0.4494+\\\iota 0.5043,\\0.4966+\\\iota 0.4475\end{pmatrix}$	$\begin{pmatrix}0.4111+\\\iota 0.4772,\\0.6553+\\\iota 0.5182\end{pmatrix}$	$\begin{pmatrix}0.5572+\\\iota 0.6249,\\0.5232+\\\iota 0.4440\end{pmatrix}$	$\begin{pmatrix}0.6145+\\\iota 0.4658,\\0.4099+\\\iota 0.5500\end{pmatrix}$
$\hat{A}_7$	$\begin{pmatrix}0.5341+\\\iota 0.4770,\\0.4304+\\\iota 0.5280\end{pmatrix}$	$\begin{pmatrix}0.4020+\\\iota 0.5158,\\0.6152+\\\iota 0.5186\end{pmatrix}$	$\begin{pmatrix}0.3044+\\\iota 0.5177,\\0.5542+\\\iota 0.5113\end{pmatrix}$	$\begin{pmatrix}0.3878+\\\iota 0.5776,\\0.6622+\\\iota 0.4620\end{pmatrix}$	$\begin{pmatrix}0.4001+\\\iota 0.5383,\\0.5544+\\\iota 0.5326\end{pmatrix}$

$\hat{A}_8$	$\begin{pmatrix}0.4212+\\ \iota 0.5563,\\ 0.5485+\\ \iota 0.5402\end{pmatrix}$	$\begin{pmatrix}0.4361+\\ \iota 0.4286,\\ 0.5637+\\ \iota 0.5911\end{pmatrix}$	$\begin{pmatrix}0.6324+\\ \iota 0.4220,\\ 0.4543+\\ \iota 0.5520\end{pmatrix}$	$\begin{pmatrix}0.2769+\\ \iota 0.5425,\\ 0.6222+\\ \iota 0.4418\end{pmatrix}$	$\begin{pmatrix}0.5366+\\ \iota 0.4916,\\ 0.4992+\\ \iota 0.5314\end{pmatrix}$

Step 2: The score matrix of the aggregated matrix is given as;

$$\breve{\breve{S}} = \begin{bmatrix} 0.5062 & 0.4855 & 0.5032 & 0.5084 & 0.4765 \\ 0.4931 & 0.4769 & 0.5228 & 0.4457 & 0.4718 \\ 0.4912 & 0.5175 & 0.5332 & 0.5146 & 0.4565 \\ 0.4908 & 0.5287 & 0.5361 & 0.4967 & 0.5344 \\ 0.6210 & 0.5950 & 0.5966 & 0.5011 & 0.6060 \\ 0.4851 & 0.5017 & 0.4394 & 0.5466 & 0.5245 \\ 0.5085 & 0.4575 & 0.4658 & 0.4655 & 0.4747 \\ 0.4811 & 0.4440 & 0.5165 & 0.4634 & 0.4997 \end{bmatrix}$$

Step 3: Formation of an extended initial matrix. In this step, the ideal solution (AI) A_j^+ and anti-ideal solution (AAI) A_j^- are determined and appended to the decision matrix. Where all criteria taken into account are of benefit type. The extended initial matrix is given in Table 7.

Table 7: Extended initial matrix.

AAI	0.4810	0.4440	0.4394	0.4457	0.4565
$\hat{A}_1$	0.5062	0.4855	0.5032	0.5084	0.4765
$\hat{A}_2$	0.4931	0.4769	0.5228	0.4457	0.4718
$\hat{A}_3$	0.4912	0.5175	0.5332	0.5146	0.4565
$\hat{A}_4$	0.4908	0.5287	0.5361	0.4967	0.5344
$\hat{A}_5$	0.6210	0.5950	0.5966	0.5011	0.6060
$\hat{A}_6$	0.4851	0.5017	0.4394	0.5466	0.5245
$\hat{A}_7$	0.5085	0.4575	0.4658	0.4655	0.4747
$\hat{A}_8$	0.4811	0.4440	0.5165	0.4634	0.4997
AI	0.6210	0.5950	0.5966	0.5466	0.6060

Step 4: The decision matrix is normalized to ensure comparability among criteria. The normalized matrix is given in Table 8.

Table 8: Normalized matrix.

AAI	0.7747	0.7463	0.7365	0.8154	0.7533
$\hat{A}_1$	0.8152	0.8160	0.8434	0.9301	0.7862
$\hat{A}_2$	0.7940	0.8015	0.8763	0.8154	0.7786
$\hat{A}_3$	0.7910	0.8698	0.8936	0.9415	0.7533
$\hat{A}_4$	0.7904	0.8886	0.8985	0.9088	0.8818
$\hat{A}_5$	1	1	1	0.9167	1
$\hat{A}_6$	0.7814	0.8433	0.7365	1	0.8655
$\hat{A}_7$	0.8188	0.7689	0.7806	0.8517	0.7833
$\hat{A}_8$	0.7747	0.7463	0.8658	0.8479	0.8247
AI	1	1	1	1	1

Step 5: Next, we will calculate the criteria weights by using the BWM technique.

Step 5.1: Identification of evaluation criteria by the experts.

Step 5.2: Selection of best and worst criteria. The DMs identify the most important criteria (best criteria) as $\check{C}_2$ and the least important criteria (worst criteria) $\check{C}_5$ from the set of criteria.

Step 5.3: Construction of the best criteria for others' preference vector. The preference vector from best to worst criteria is given as

$$\hat{A}_B = (4,1,3,2,7)$$

Step 5.4: Construction of others to the worst preference vector. The preference vector from worst to best criteria is given as

$$\hat{A}_w = (5,7,4,6,1)^T$$

Step 5.5: Determination of optimal criteria weights. The optimal weights of the criteria after employing BWM are given as

$$₩_1 = 0.1594, ₩_2 = 0.3927,$$
$$₩_3 = 0.1209, ₩_4 = 0.2810, ₩_5 = 0.0460$$

Step 6: Now we will calculate the weighted normalized matrix. The weighted normalized matrix is given in Table 9.

Table 9: Weighted normalized matrix.

AAI	0.12349	0.29306	0.08904	0.22913	0.03465
$\hat{A}_1$	0.12994	0.32045	0.10196	0.26136	0.03617
$\hat{A}_2$	0.12657	0.31474	0.10594	0.22913	0.03582
$\hat{A}_3$	0.12609	0.34158	0.10804	0.26456	0.03465
$\hat{A}_4$	0.12599	0.34897	0.10863	0.25538	0.04057
$\hat{A}_5$	0.15940	0.39270	0.12090	0.25760	0.04610
$\hat{A}_6$	0.12455	0.33114	0.08904	0.28100	0.03981
$\hat{A}_7$	0.13052	0.30195	0.09438	0.23933	0.03603
$\hat{A}_8$	0.12349	0.29306	0.10467	0.23827	0.03793
AI	0.15940	0.39270	0.12090	0.28100	0.0460

Step 7: Next, we will calculate the utility degree of alternatives K_i. The degree of the alternatives in relation to the anti-ideal and ideal solutions is given in Table 10.

Step 8: Determination of the utility function of alternatives $f(K_i)$. The utility function is the compromise of the observed alternative in relation to the ideal and anti-ideal solution. The utility function of alternatives is given in Table 10.

Table 10: Utility degree and utility function for alternatives.

	K_i^+	K_i^-	$f(K_i^+)$	$f(K_i^-)$	$f(K_i)$
$\hat{A}_1$	0.84988	1.10465	0.56517	0.43483	0.63684
$\hat{A}_2$	0.81219	1.05566	0.56517	0.43483	0.60859
$\hat{A}_3$	0.87493	1.13720	0.56517	0.43483	0.65560
$\hat{A}_4$	0.87953	1.14319	0.56517	0.43483	0.65905
$\hat{A}_5$	0.97660	1.26936	0.56517	0.43483	0.73179
$\hat{A}_6$	0.86555	1.12501	0.56517	0.43483	0.64857
$\hat{A}_7$	0.80222	1.04270	0.56517	0.43483	0.60112

$\hat{A}_8$	0.79742	1.03647	0.56517	0.43483	0.59752

Step 9: Ranking the alternatives. Since

$$f(K_5) > f(K_4) > f(K_3) > f(K_6) > f(K_1) > f(K_2) > f(K_7) > f(K_8)$$

So $\hat{A}_5$ is the best alternative.

Moreover, the graphical comparison of utility function values of alternatives is given in Figure 4.

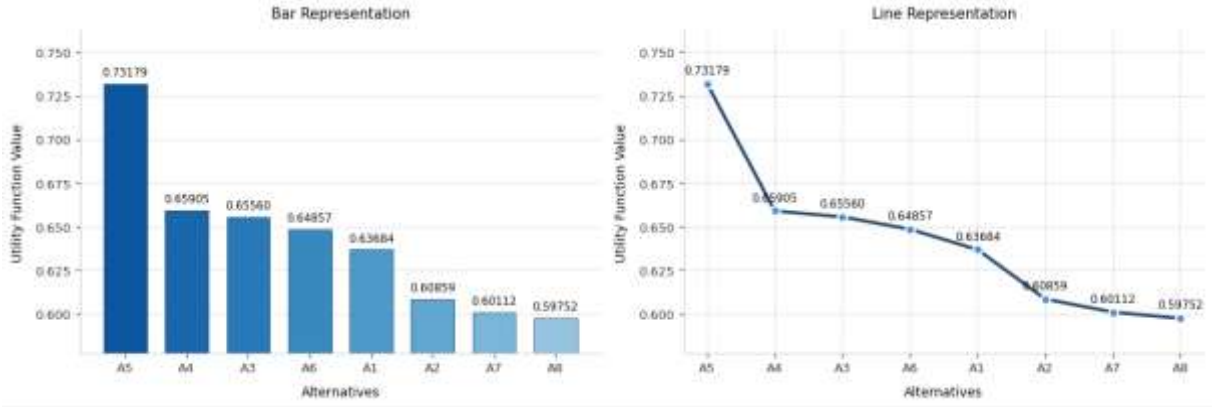

Figure 4: Utility function ranking of cyber defence alternatives.

7 | Comparative Analysis

To demonstrate the superiority and real effectiveness of the proposed Cq-ROF BWM-MARCOS framework, the proposed approach was compared to some representative approaches that have been developed under different fuzzy environments, like the fuzzy MARCOS method of Stankovic et al. [29], IF MARCOS model of Ecer and Pamucar [34], PF CRITIC-MARCOS framework of Wang et al. [37], and the q-ROF MARCOS approach of Ali [42]. These approaches are significant steps in the development of uncertainty-aware decision-making and can form an appropriate basis for assessing the benefits of the proposed framework. From the comparative results, it is seen that the existing approaches have been able to improve uncertainty representation in FSs to IFSs, PFSs, and q-ROFSs, but they are basically still based on real-valued information structures. As a result, they are not very useful in more complex cybersecurity decision contexts with multidimensional and complex uncertainty. The proposed Cq-ROF framework, on the other hand, offers a more expressive information structure that can capture the complex expert judgment and various uncertainty types of big data security assessment in a real-time environment. Moreover, such comparisons mainly involve the ranking of alternatives and are usually based on criterion weights that have been previously defined or imported from other studies. This is overcome by the proposed framework, which utilizes the BWM, which uses a consistent and efficient pairwise comparison mechanism to calculate criteria importance. This integration improves the trustworthiness of the weighting procedure and decreases the cognitive load on the decision-maker. Furthermore, the MARCOS method compares the alternatives with respect to both ideal and anti-ideal solutions, resulting in stable and interpretable rankings. The proposed Cq-ROF BWM-MARCOS approach has developed a comprehensive decision support mechanism by incorporating

advanced uncertainty modeling, reliable criteria weighting, and the compromise-based ranking into one framework. The proposed Cq-ROF BWM-MARCOS approach has overcome the limitations of the existing MARCOS-based approaches by providing a comprehensive decision support mechanism with the incorporation of advanced uncertainty modeling, reliable criteria weighting, and compromise-based ranking in one framework. Furthermore, the proposed framework was designed specifically for the evaluation of advanced cyber defense solutions in real-time big data security environments, whereas the related approaches were developed for different applications such as transportation, healthcare, supplier selection, and waste management. By converting the framework into an application-specific design, this application is able to tackle the specific issues of cybersecurity assessment, such as shifting attack patterns, competing evaluation criteria, unpredictable expert opinions, and changing threat landscapes. The proposed Cq-ROF BWM-MARCOS framework not only extends the theoretical development of MARCOS-based decision-making but also offers a reliable, intelligent, and practical tool for selecting cybersecurity strategies for highly uncertain operational situations. Moreover, the comparison is given in Table 11.

Table 11: Comparison of proposed work against existing theories.

	Stankovic et al. [29]	Ecer and Pamucar [34]	Wang et al. [37]	Ali [42]	Proposed
Fuzzy Environment	FS	IFS	PFS	$q-ROFS$	$Cq-ROFS$
Uncertainty Handling	$Moderate$	$Good$	$Very\ Good$	$High$	$Excellent$
Multidimensional Information	✗	✗	✗	✗	✓
Criteria Weighting	$External$	$External$	$CRITIC$	$External$	BWM
MARCOS Ranking	✓	✓	✓	✓	✓
Real Time Big Data Security	✗	✗	✗	✗	✓

8|Conclusion

This study proposed a novel framework for evaluating advanced cyber defense solutions in a real-time big data security environment: Cq-ROF BWM-MARCOS. The proposed framework can overcome the uncertainty, vagueness, and subjectivity in cybersecurity assessment, which is based on the Cq-ROFSs with its improved information representation capability. BWM and MARCOS integration allows for reliable criteria weighting and robust alternative ranking, respectively, which are used as sources of a comprehensive decision support mechanism for cybersecurity evaluation. The application of seven advanced cyber defense solutions to five important

evaluation criteria was shown to be practical and effective through a case study. Results achieved verified the capability of the framework to assist decision makers in making appropriate cyber defense decisions aimed at enhancing the security performance and fortifying the organizational resilience to emerging cyber threats. Furthermore, the main conclusions are

- An innovative Cq-ROF BWM-MARCOS model was designed to assess advanced cyber defense solutions in an uncertain big data security environment.
- The proposed Cq-ROF environment was more flexible and comprehensive for the representation of uncertain expert judgement than the existing fuzzy environment.
- The BWM was able to measure the relative importance of the cybersecurity evaluation criteria, and the MARCOS was able to rank competing alternatives based on utility measures.
- The case study proved the usability, validity, and efficacy of the proposed framework in the field of cybersecurity decision-making.
- The developed model can be practically applied as a decision-support tool for organizations interested in improving their real-time big data security and cyber resilience. In future our aim is extend the current study in WASPAS [45] and for the framework of Spherical fuzzy sets [46, 47].

References:

1. Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. Computer Science & IT Research Journal, 4(3), 478-501.
2. Hussen, N., Elghamrawy, S. M., Salem, M., & El-Desouky, A. I. (2023). A fully streaming big data framework for cyber security based on optimized deep learning algorithm. IEEE Access, 11, 65675-65688.
3. Ameedeen, M. A., Hamid, R. A., Aldhyani, T. H., Al-Nassr, L. A. K. M., Olatunji, S. O., & Subramanian, P. (2024). A framework for automated big data analytics in cybersecurity threat detection. Mesopotamian Journal of Big Data, 2024, 175-184.
4. Rawat, D. B., Doku, R., & Garuba, M. (2019). Cybersecurity in big data era: From securing big data to data-driven security. IEEE Transactions on Services Computing, 14(6), 2055-2072.
5. Xu, T., Ma, C., Su, Z., Su, J., Ma, Z., Wang, J., & Yang, Z. (2025). Enhancing Cybersecurity in the Big Data Era: A GA-Optimized Fuzzy Clustering Approach. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 33(03), 353-377.
6. Meng, S., Huang, W., Yin, X., Khosravi, M. R., Li, Q., Wan, S., & Qi, L. (2020). Security-aware dynamic scheduling for real-time optimization in cloud-based industrial applications. IEEE Transactions on Industrial Informatics, 17(6), 4219-4228.
7. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE

Communications Surveys & Tutorials, 21(2), 1851-1877.
8. Moustafa, N., Turnbull, B., & Choo, K. K. R. (2018). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 6(3), 4815-4830.
9. Granat, J., Batalla, J. M., Mavromoustakis, C. X., & Mastorakis, G. (2019). Big data analytics for event detection in the IoT-multicriteria approach. IEEE Internet of Things Journal, 7(5), 4418-4430.
10. AbdelMouty, A. M., & Abdel-Monem, A. (2023). Neutrosophic MCDM methodology for assessment risks of cyber security in power management. Neutrosophic systems with applications, 3, 53-61.
11. Bhol, S. G. (2025). Applications of multi criteria decision making methods in cyber security. Cyber-Physical Systems Security, 233-258.
12. Khan, A. W., Khan, M. U., Khan, J. A., Khan, J., & Gul, W. (2021). Identification and prioritization of security challenges of big data on cloud computing based on SLR: A fuzzy-TOPSIS analysis approach. Journal of Software: Evolution and Process, 33(12), e2387.
13. Mohamed, I., Hefny, H. A., & Darwish, N. R. (2024). Enhancing cybersecurity defenses: a multicriteria decision-making approach to MITRE ATT&CK mitigation strategy. arXiv preprint arXiv:2407.19222.
14. Qasim Jebur Al-Zaidawi, M., & Çevik, M. (2025). Advanced deep learning models for improved IoT network monitoring using hybrid optimization and MCDM techniques. Symmetry, 17(3), 388.
15. Yang, Z. (2025). Evaluation of intrusion detection systems in cyber security using fuzzy OffLogic and MCDM approach. Neutrosophic Sets and Systems, 85(1), 20.
16. Zadeh, L. A. (1965). Fuzzy sets. Information and control, 8(3), 338-353.
17. Dursun, M., & Karsak, E. E. (2010). A fuzzy MCDM approach for personnel selection. Expert Systems with applications, 37(6), 4324-4330.
18. Atanassov, K. T. (1999). Intuitionistic fuzzy sets. In Intuitionistic fuzzy sets: theory and applications (pp. 1-137). Heidelberg: Physica-Verlag HD.
19. Li, D. F. (2005). Multiattribute decision making models and methods using intuitionistic fuzzy sets. Journal of computer and System Sciences, 70(1), 73-85.
20. Yager, R. R. (2013, June). Pythagorean fuzzy subsets. In 2013 joint IFSA world congress and NAFIPS annual meeting (IFSA/NAFIPS) (pp. 57-61). IEEE.
21. Mohd, W. W., Abdullah, L., Yusoff, B., Taib, C. M. I. C., & Merigo, J. M. (2019). An integrated MCDM model based on Pythagorean fuzzy sets for green supplier development program. Malaysian Journal of Mathematical Sciences, 13, 23-37.

22. Yager, R. R. (2016). Generalized orthopair fuzzy sets. IEEE transactions on fuzzy systems, 25(5), 1222-1230.
23. Erdebilli, B., & Sıcakyüz, Ç. (2024). An integrated Q-rung orthopair fuzzy (Q-ROF) for the selection of supply-chain management. Sustainability, 16(12), 4901.s
24. Rezaei, J. (2015). Best-worst multi-criteria decision-making method. Omega, 53, 49-57.
25. Mou, Q., Xu, Z., & Liao, H. (2016). An intuitionistic fuzzy multiplicative best-worst method for multi-criteria group decision making. Information Sciences, 374, 224-239.
26. Guo, S., & Zhao, H. (2017). Fuzzy best-worst multi-criteria decision-making method and its applications. Knowledge-based systems, 121, 23-31.
27. Rezaei, J., Nispeling, T., Sarkis, J., & Tavasszy, L. (2016). A supplier selection life cycle approach integrating traditional and environmental criteria using the best worst method. Journal of cleaner production, 135, 577-588.
28. Mi, X., Tang, M., Liao, H., Shen, W., & Lev, B. (2019). The state-of-the-art survey on integrations and applications of the best worst method in decision making: Why, what, what for and what's next?. Omega, 87, 205-225.
29. Stanković, M., Stević, Ž., Das, D. K., Subotić, M., & Pamučar, D. (2020). A new fuzzy MARCOS method for road traffic risk analysis. Mathematics, 8(3), 457.
30. Puška, A., Stević, Ž., & Stojanović, I. (2021). Selection of sustainable suppliers using the fuzzy MARCOS method. Current Chinese Science, 1(2), 218-229.
31. Tuş, A., & Adalı, E. A. (2022). Green supplier selection based on the combination of fuzzy SWARA (SWARA-F) and fuzzy MARCOS (MARCOS-F) methods. Gazi University Journal of Science, 35(4), 1535-1554.
32. Wang, C. N., Nguyen, T. T. T., Dang, T. T., & Nguyen, N. A. T. (2022). A hybrid OPA and fuzzy MARCOS methodology for sustainable supplier selection with technology 4.0 evaluation. Processes, 10(11), 2351.
33. Chaurasiya, R., & Jain, D. (2021, April). Generalized intuitionistic fuzzy entropy on IF-MARCOS technique in multi-criteria decision making. In International conference on advances in computing and data sciences (pp. 592-603). Cham: Springer International Publishing.
34. Ecer, F., & Pamucar, D. (2021). MARCOS technique under intuitionistic fuzzy environment for determining the COVID-19 pandemic performance of insurance companies in terms of healthcare services. Applied Soft Computing, 104, 107199.
35. Kizielewicz, B., Paradowski, B., Więckowski, J., & Sałabun, W. (2022, September). Towards the identification of MARCOS models based on intuitionistic fuzzy score functions. In 2022 17th Conference on Computer Science and

Intelligence Systems (FedCSIS) (pp. 789-798). IEEE.

36. Mondal, M. K., Mahapatra, B. S., Bera, M. B., & Mahapatra, G. S. (2024). Sustainable forest resources management model through Pythagorean fuzzy MEREC–MARCOS approach: MK Mondal et al. Environment, Development and Sustainability, 1-32.
37. Wang, Y., Wang, W., Wang, Z., Deveci, M., Roy, S. K., & Kadry, S. (2024). Selection of sustainable food suppliers using the Pythagorean fuzzy CRITIC-MARCOS method. Information sciences, 664, 120326.
38. Chaurasiya, R., & Jain, D. (2023). A new algorithm on Pythagorean fuzzy-based multi-criteria decision-making and its application. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 47(3), 871-886.
39. Younis, M., Ashraf, S., Abdullah, S., Shahid, T., & KC, G. (2025). Strategic MARCOS model for optimizing renewable energy investments under pythagorean hesitant fuzzy assessments. Advances in Fuzzy Systems, 2025(1), 6193403.
40. Mishra, A. R., Rani, P., Pamucar, D., & Saha, A. (2024). An integrated Pythagorean fuzzy fairly operator-based MARCOS method for solving the sustainable circular supplier selection problem. Annals of Operations Research, 342(1), 523-564.
41. Krishankumar, R., Mishra, A. R., Rani, P., Ecer, F., & Ravichandran, K. S. (2023). Assessment of zero-carbon measures for sustainable transportation in smart cities: a CRITIC-MARCOS framework based on Q-rung fuzzy preferences. IEEE internet of things journal, 10(21), 18651-18662.
42. Ali, J. (2022). A q-rung orthopair fuzzy MARCOS method using novel score function and its application to solid waste management. Applied Intelligence, 52(8), 8770-8792.
43. Mahmood, T., & Ali, Z. (2022). MARCOS technique by using q-Rung orthopair fuzzy sets for evaluating the performance of insurance companies in terms of healthcare services. In q-Rung Orthopair Fuzzy Sets: Theory and Applications (pp. 357-375). Singapore: Springer Nature Singapore.
44. Ahmmad, J., Mahmood, T., Pamucar, D., & Waqas, H. M. (2025). A novel Complex q-rung orthopair fuzzy Yager aggregation operators and their applications in environmental engineering. Heliyon, 11(1).
45. Jaleel, A., (2022). WASPAS Technique Utilized for Agricultural Robotics System based on Dombi Aggregation Operators under Bipolar Complex Fuzzy Soft Information, *Journal of Innovative Research in Mathematical and Computational Sciences*, 1(2), 67-95.
46. Ali, A., Božanić, D., Akram, M., & Ijaz, S. (2022). Heronian Mean Operators Based Multi-Attribute Decision Making Algorithm Using T-

Spherical Fuzzy Information. *Journal of Innovative Research in Mathematical and Computational Sciences*, *1*(1), 55-82.

47. Ali, A., Božanić, D., Akram, M., & Ijaz, S. (2022). Heronian Mean Operators Based Multi-Attribute Decision Making Algorithm Using T-Spherical Fuzzy Information, *Journal of Innovative Research in Mathematical and Computational Sciences*, 1(1), 55-82.