10.24425/acs.2026.158421

Archives of Control Sciences
Volume 36(LXXII), 2026
No. 1, *pages 55–84*

AI-driven big data visualization for cybersecurity using bipolar fuzzy Einstein prioritized operators

Ubaid ur REHMAN, Tahir MAHMOOD,
Hafiz Muhammad WAQAS and Abaid ur REHMAN VIRK

As cyberattacks become more advanced, advanced AI-based big data visualization is now needed for effective threat detection. Yet, choosing the best visualization tools is some multi-criteria decision-making (MCDM) task that involves considering many criteria containing both positive and negative aspects. While MCDM methods that address the selection and classification of AI-driven big data visualization tools focus on the positive aspects of the evaluation criteria and ignore the negative aspects of the criteria, resulting in incomplete evaluations. Further, although Einstein operators have shown strong results in uncertain and imprecise situations and MCDM approaches, they have not yet been used in bipolar fuzzy frameworks, which leaves a major gap in decision-making methods. To overcome these problems, this article interprets a bipolar fuzzy MCDM methodology based on Einstein prioritized operators to systematically evaluate and classify AI-driven big data visualization tools for cybersecurity threat detection. For this method, Einstein prioritized operators within a bipolar fuzzy framework devised in this article, which can aggregate both positive and negative aspects of the criteria. A comprehensive case study is shown to assess and classify the prominent AI-driven big data visualization tools for cybersecurity threat detection, considering critical criteria with dual aspects. The proposed methodology is meticulously compared with the prevailing MCDM methods to validate its dominance in handling uncertainty and the bipolarity of the criteria. This article helps security professionals choose the right AI-powered visualization tools which, in turn improve the cybersecurity of their organizations and make it easier to detect threats.

Key words: optimization models, control problem, efficient solution

Copyright © 2026. The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (CC BY-NC-ND 4.0 https://creativecommons.org/licenses/by-nc-nd/4.0/), which permits use, distribution, and reproduction in any medium, provided that the article is properly cited, the use is non-commercial, and no modifications or adaptations are made

U. ur Rehman (e-mail: ubaid5@outlook.com) and A. ur Rehman Virk (e-mail: abaidrehman@umt.edu.pk) are with Department of Mathematics, University of Management and Technology, C-II, Johar Town, Lahore, 54700, Punjab, Pakistan.

T. Mahmood (corresponding author, e-mail: tahirbakhat@iiu.edu.pk) and H.M. Waqas (e-mail: hafizmwaqas009@gmail.com) are with Department of Mathematics and Statistics, International Islamic University Islamabad, Islamabad 44000, Pakistan.

Received 7.10.2025. Revised 14.01.2026.

1. Introduction

In a world where cyber-attacks are becoming increasingly sophisticated, traditional security solutions cannot detect and counter sophisticated attacks. AI-driven big data visualization applications have emerged as an excellent solution, enabling companies to process large volumes of cybersecurity data in real-time and identify threats more effectively. These tools apply machine learning algorithms, pattern detection, and anomaly-based detection techniques to identify concealed cyber threats that would otherwise not be identified using traditional methodologies. AI-driven visualization tools enhance the efficiency of how analysts can discover, interpret, and act on potential threats by offering an interactive visual understanding of raw security data. The rapid growth of cybersecurity threats and their cohort of ransomware and phishing attacks with insider threats have placed organizations in urgent need of AI-integrated security solutions. Various industrial sectors such as finance and healthcare and the government use AI-based visualization technologies to monitor network operations, identify malicious behavior, and enhance their online protection. These tools combined with incident response improve security monitoring as they can detect threats based on risk and severity grades. Furthermore, cybersecurity big data analytics can be used to support predictive threat intelligence, which can help organizations predict and prevent cyberattacks before they occur. As cybercriminals are constantly changing their attack methods, AI-based big data visualization has become a critical tool in today's cybersecurity environment. Below Fig. 1 and Fig. 2 show

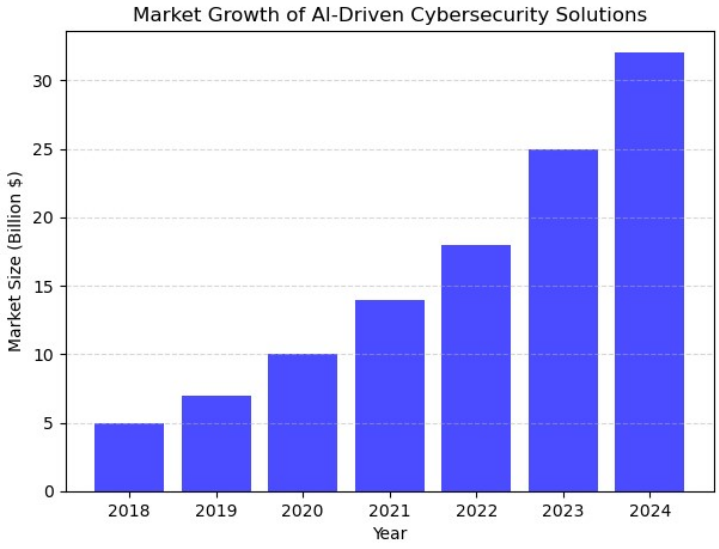


Figure 1: Market growth of AI-driven cybersecurity solutions

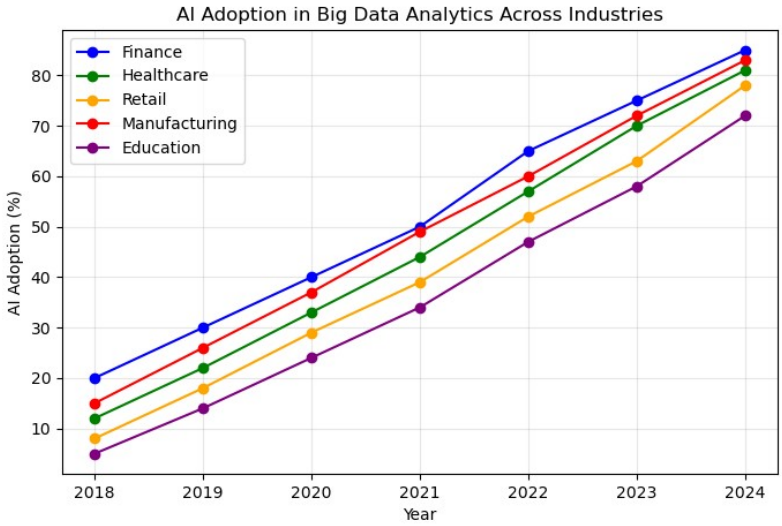


Figure 2: Adoption of AI in big data analytics across industries

the market growth of AI-driven cybersecurity solutions and AI adoption in big data analytics across industries respectively.

Despite these developments, choosing the most efficient AI-powered big data visualization tool for cybersecurity is still a multifaceted decision-making process. In this paper, these tools will be analyzed and classified based on BF-prioritized Einstein operators and MCDM. Our study provides a methodological framework to help decision makers identify the best visualization tool to use in cybersecurity threat detection, thus enhancing digital security resilience through an evaluation of some of the key features such as precision, real-time processing, scalability, and interpretability.

1.1. Contribution of the bipolar fuzzy approach to the MCDM methodology

MCDM systems are used by decision-makers in uncertain and imprecise conditions when they have to choose the most suitable alternative. Such complex decision-making situations can be addressed using bipolar fuzzy sets (BFSs) [1], as they provide dynamic solutions to composite problems. BFSs are more representationally powerful than regular fuzzy sets because they possess extra positive and negative membership functions that can be used to process information in two directions. BFSs show their greatest utility advantage in the context of MCDM since decision-makers must evaluate both desirable and undesirable qualities of alternatives at the same time. BFSs can be added to MCDM models to allow decision makers to formulate superior trade-offs and improve the accuracy of

alternative ranking and generate stronger rankings. The Einstein operators on BFS improve decision analysis by their ability to reflect criteria relationships that lead to improved alternative rankings. BFSs can be used effectively to solve complex decision-making problems that confront reality, such as threat analysis in cybersecurity, medical assessment and industrial process improvement.

1.2. Research problem

Assessing and classification of AI-based big data visualization tools for cybersecurity threat detection is a difficult MCDM challenge that needs advanced analysis methods. Current research often overlooks the negative sides of the criteria being studied, concentrating only on the positives. To choose the right cybersecurity tools, you need to consider that every evaluation factor can have both positive and negative, depending on the situation. For example, the ability of a visualization tool to handle a lot of data (positive) could also result in the use of more resources (negative). I suggest using a bipolar fuzzy framework to address this methodological problem by including both positive and negative aspects of each criterion. This method allows security analysts to create more detailed evaluation methods that match real-world issues, capture the mixed results of some features in different situations, produce fairer assessments that recognize the compromises involved in choosing tools, and increase the reliability of their decisions by considering all aspects of performance. When organizations use this bipolar approach in their classification, they can choose the right visualization tools for cybersecurity threat detection that help them improve their overall security.

When dealing with uncertain or vague information, multi-attribute, or group decisions, Einstein prioritization operators are most useful, as they provide strong benefits. One important benefit is that they naturally manage fuzzy data, making aggregation of values more accurate, even when some data are very extreme or an outlier [2]. When prioritization is used, the weight given to each criterion or decision maker can be easily adjusted, so that key elements have a greater impact on the outcome [3]. Einstein prioritized operators are more flexible and accurate in many fuzzy environments, making them helpful for both researchers and practitioners who handle detailed data aggregation and analysis [4]. In general, choosing Einstein's operator approach was a major advance in the way aggregation is done in fuzzy set theory and decision sciences. When these systems process inaccurate information properly, better decision outcomes are achieved, and fuzzy logic models can be applied to various real-life situations which are not easily defined. As studies progress, these operators are predicted to become more important in improving decision-support systems in many domains. Although there have been many improvements in MCDM, Einstein prioritization opera-

tors, which are strong at handling uncertain data, have not yet been used in the bipolar fuzzy framework. This area of research is very important and should be addressed right away. If we use Einstein operators in bipolar fuzzy environments, we can combine their strong uncertainty management with the unique skill of the bipolar fuzzy framework for handling both the positives and negatives in decision criteria. With this integration, security professionals would have a better system to evaluate cybersecurity tools and could handle complicated, sometimes conflicting information more accurately. The new approach would allow us to accurately compare and rank AI-driven visualization tools, which would guide us to make better and more effective cybersecurity infrastructure decisions.

1.3. Contribution

This paper introduces a set of new bipolar fuzzy prioritized Einstein aggregation operators that solve important issues in existing MCDM approaches. We introduce four new aggregation operators (AOs) – the bipolar fuzzy Einstein prioritized averaging (BFEPRA), bipolar fuzzy Einstein prioritized weighted averaging (BFEPRWA), bipolar fuzzy Einstein prioritized geometric (BFEPRG), and bipolar fuzzy Einstein prioritized weighted geometric (BFEPRWG) – that use Einstein operations in the bipolar fuzzy domain to handle positive and negative aspects of criteria at the same time. Based on these new theories, we design a complete bipolar fuzzy MCDM methodology and an algorithm, showing its usefulness through a case study on choosing and ranking AI-based big data visualization tools for cybersecurity threat detection. We validate our approach by using detailed mathematical illustrations that handle dualaspect bipolar fuzzy data, allowing us to discover insights that were not possible before. Through comparison, we reveal that our work is better than other frameworks when handling uncertainty and related criteria, while still being efficient and flexible for security professionals evaluating critical technology. The graphical interpretation of the contribution is devised in Fig. 3.

1.4. Study layout

The detailed study framework includes the following sections:

- Section 1 presents an introduction to the entire manuscript.
- Section 2 covers a review of the literature or background study.
- Section 3 discusses the key fundamental ideas related to the proposed theory.
- Section 4 introduces the Einstine aggregation operators that have been newly developed.

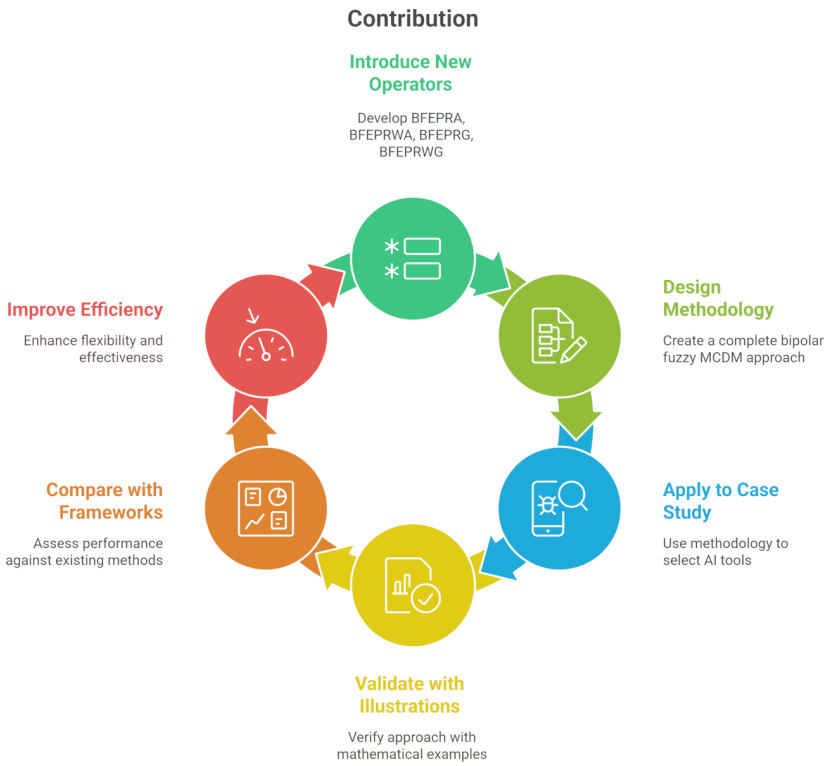


Figure 3: The contribution

- Section 5 covers the MCDM approach based on the bipolar fuzzy framework.
- Section 6 describes the comparative analysis of the proposed study.
- Section 7 summarizes the entire manuscript.

2. Literature review

The rapid rate of cybersecurity threats has necessitated the use of AI-based big data analytics to enhance the ability to detect and respond to threats. Scholars have found various approaches and models to ensure that cybersecurity is more efficient. Galla et al. [5] highlighted the need to bring big data to AI-based threat detection to ensure cybersecurity becomes more compliant. They studied how machine learning algorithms can process large volumes of data to detect anomalies and potential cyber-attacks in real time and provide proactive responses. Ameedeen et al. [6] introduced a model of automated big data analytics in cybersecurity threat detection. During their discussion, they found out that

AI could be applied to automate data processing, reduce human interaction, and speed up the process of identifying threats in large networks. Wickramasinghe [7] conducted a survey of AI algorithms in cybersecurity risk assessment and mitigation. The article has demonstrated that AI models based on big data can be helpful in detecting vulnerabilities and proposing real-time remedial actions. In the same vein, Chinta et al. [8] investigated the notion of combining big data and AI-based enterprise resource planning (ERP) systems to increase cybersecurity resilience. Maharjan [9] investigated the possibility of using AI-based big data analytics to enhance cybersecurity infrastructure of critical infrastructure. Moore [10] proposed an AI solution that integrates big data analytics and ERP systems to automatically detect cybersecurity vulnerabilities. Research has shown that AI-based ERP systems have the potential to improve security surveillance and reduce risks through intelligent automation. Ofoegbu et al. [11] proposed an end-to-end solution to real-time cybersecurity threat detection through machine learning and big data analytics. Ashfin [12] examined AI-based threat detection and response models in cybersecurity through the lens of AI algorithm flexibility to new attack vectors and security concerns. Fernando [13] proposed a multidimensional approach that leverages big data analytics and AI for digital forensic and cybersecurity investigations. The research highlighted the use of AI in forensic examination to ensure a more effective method of detecting and solving cybercrime. Alsulami [14] outlined an AI-based model to improve sustainability in detecting cyber threats in IoT environments. In their work, they demonstrated the way AI can be used to make IoT networks safer and less prone to cyberattacks without compromising the performance of their operations. The literature above shows the relevance of AI-based big data analytics for the identification of cybersecurity threats. However, most works only address either AI or big data on their own, without providing a comprehensive classification and evaluation of AI-driven big data visualization solutions that are specifically aimed at cybersecurity. Our research aims to bridge this gap by conducting an elaborate analysis and categorization of such tools by using bipolar fuzzy Einstein prioritized operators and MCDM methods. This classification will assist organizations to make decisions on the most suitable visualization tools to be used in the detection of cybersecurity threats to ensure the overall security infrastructure and cybersecurity threat resilience is effective.

2.1. MCDM Methodology

Big data security has been researched intensively alongside decision-making strategies in areas that demand decision guidance in uncertain situations and high complexity. Several research papers examine the combination of fuzzy logic

and MCDM approaches to increase cybersecurity and the precision of big data decision. Multiple points about this field get attention through this research review. Boutkhoum et al. [15] implemented the fuzzy Analytic Hierarchy Process (AHP) together with the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) to establish a decision model that selects cloud solutions suitable for big data project management. Hybrid MCDM approaches showed successful results in studying large-scale data variations and uncertain situations according to their research. Strong decision-making methods represent an essential need when managing big data through cloud platforms. To address the security issues of big data, Alassery et al. [16] presented a decision-making approach that uses fuzzy methods for threat evaluation and protection. While addressing big data security frameworks, the integration of fuzzy logic helps improve threat detection accuracy alongside decision reliability. Bhol [17] researched how MCDM approaches help cybersecurity by enabling the selection of the best security approaches. Through the incorporation of TOPSIS alongside AHP and VIKOR MCDM methodologies, the study explained how organizations can establish more organized and reasonable approaches for cyber risk management decisions. Attaallah et al. [18] developed big data security analysis through a merged decision system that incorporates various fuzzy logic methods. Due to the significance of security assessment in large data systems, scientists discussed the positive effects of using an integrated decisionmaking framework for safety measurement evaluations while addressing privacy security breaches and threat identification. Mardani et al. [19] presented the Big Data-driven Large-Scale Group DecisionMaking (BiGDM-U) model to help handle uncertainties in decision-making processes. Hussain et al. [20] presented a new MCDM framework designed to facilitate precise decision processes that are run in fuzzy environments. It was also revealed in the study that MCDM models that are developed on the foundation of fuzzy logic have the potential to increase the accuracy and speed of making a decision particularly when it comes to risk assessment and risk mitigation requirements like cybersecurity. Kumar et al. [21] based their study on the selection of cloud services using integrated MCDM techniques that ran on a fuzzy platform. In their work, the researchers showed that MCDM methods enhance the reliability of the decision-making process when your organization decides on cloud-based security solutions, in particular when you need to evaluate cost security performance and computational processing speed. The researchers of Falak et al. [22] established a hybrid MCDM model to assess continuous improvement techniques within fuzzy evaluation schemes. Security protocols, together with decision-making processes in real-time data analytics, experienced optimization through their research of the MCDM methodology. The research by Chen et al. [23] created a fuzzy MCDM

model to pick green suppliers by integrating economic criteria with environmental factors. The methodology presented in the investigation shows its applicability for cybersecurity decision-making through supplier selection monitoring despite its original target application.

3. Fundamentals

In this section, we discuss some of the basic concepts related to the newly developed work.

Definition 1. [1] *The set of BFS is originated as* $\varphi = \left\{\left(e, \left(J_\varphi^P(e), J_\varphi^N(e)\right)\right) \vee e \in E\right\}$, *where* $J_\varphi^P(e) \in [0,1]$ *is a positive degree of membership and* $J_\varphi^N(e) \in [-1,0]$ *is a negative degree of membership of* $e \in E$. *The pair* $\varphi = \left(J_\varphi^P, J_\varphi^N\right)$ *will be devised as a bipolar fuzzy number (BFN).*

The score value and the accuracy value of a BFN $\varphi = \left(J_\varphi^P, J_\varphi^N\right)$ is discussed as

$$S(\varphi) = \frac{1}{2}\left(1 + J_\varphi^P + J_\varphi^N\right), \qquad S(\varphi) \in [0,1],$$
$$H(\varphi) = \frac{J_\varphi^P - J_\varphi^N}{4}, \qquad H(\varphi) \in [0,1],$$

respectively.

Definition 2. [27] *Let us consider two BFNs* $\varphi_1 = \left(J_{\varphi_1}^P, J_{\varphi_1}^N\right)$ *and* $\varphi_2 = \left(J_{\varphi_2}^P, J_{\varphi_2}^N\right)$ *and* $\eth \geqslant 0$. *Then,*

1. $\varphi_1 \oplus \varphi_2 = \left(J_{\varphi_1}^P + J_{\varphi_2}^P - J_{\varphi_1}^P J_{\varphi_2}^P, -\left(J_{\varphi_1}^N J_{\varphi_2}^N\right)\right)$
2. $\varphi_1 \otimes \varphi_2 = \left(J_{\varphi_1}^P J_{\varphi_2}^P, J_{\varphi_1}^N + J_{\varphi_2}^N + J_{\varphi_1}^N J_{\varphi_2}^N\right)$
3. $\eth\varphi_1 = \left(1 - \left(1 - J_{\varphi_1}^P\right)^\eth, -\left|J_{\varphi_1}^N\right|^\eth\right)$
4. $\varphi_1^\eth = \left(\left(J_{\varphi_1}^P\right)^\eth, -1 + \left(1 + J_{\varphi_1}^N\right)^\eth\right)$

Definition 3. [28] *For real numbers* φ_{R-1} *and* φ_{R-2}, *the Einstein t-norm is diagnosed as*

$$J_N\left(\varphi_{R-1}, \varphi_{R-2}\right) = \frac{\varphi_{R-1}\varphi_{R-2}}{1 + \left(1 - \varphi_{R-1}\right)\left(1 - \varphi_{R-2}\right)}$$

and the t-conorm is interpreted as

$$J_{CN}\left(\varphi_{R-1}, \varphi_{R-2}\right) = \frac{\varphi_{R-1} + \varphi_{R-2}}{1 + \varphi_{R-1}\varphi_{R-2}}.$$

Definition 4. *Let us consider two BFNs* $\varphi_1 = \left(J^P_{\varphi_1}, J^N_{\varphi_1}\right)$ *and* $\varphi_2 = \left(J^P_{\varphi_2}, J^N_{\varphi_2}\right)$ *and* $\eth \geqslant 0$*. Then the algebraic operations based on Einstein's t-norm and t-conorm are devised as:*

1. $\varphi_1 \oplus_\varepsilon \varphi_2 = \left(\dfrac{J^P_{\varphi_1} + J^P_{\varphi_2}}{1 + J^P_{\varphi_1} J^P_{\varphi_2}}, -\dfrac{J^N_{\varphi_1} J^N_{\varphi_2}}{1 + \left(1 + J^N_{\varphi_1}\right)\left(1 + J^N_{\varphi_2}\right)} \right)$
2. $\varphi_1 \otimes_\varepsilon \varphi_2 = \left(\dfrac{J^P_{\varphi_1} J^P_{\varphi_2}}{1 + \left(1 - J^P_{\varphi_1}\right)\left(1 - J^P_{\varphi_2}\right)}, \dfrac{J^N_{\varphi_1} + J^N_{\varphi_2}}{1 + J^N_{\varphi_1} J^N_{\varphi_2}} \right)$
3. $(\varphi_1)^{\eth} = \left(\dfrac{2\left(J^P_{\varphi_1}\right)^{\eth}}{\left(2 - J^P_{\varphi_1}\right)^{\eth} + \left(J^P_{\varphi_1}\right)^{\eth}}, \dfrac{\left(1 + J^N_{\varphi_1}\right)^{\eth} - \left(1 - J^N_{\varphi_1}\right)^{\eth}}{\left(1 + J^N_{\varphi_1}\right)^{\eth} + \left(1 - J^N_{\varphi_1}\right)^{\eth}} \right)$
4. $\eth\varphi_1 = \left(\dfrac{\left(1 + J^P_{\varphi_1}\right)^{\eth} - \left(1 - J^P_{\varphi_1}\right)^{\eth}}{\left(1 + J^P_{\varphi_1}\right)^{\eth} + \left(1 - J^P_{\varphi_1}\right)^{\eth}}, -\dfrac{2\left|J^N_{\varphi_1}\right|^{\eth}}{\left(2 + J^N_{\varphi_1}\right)^{\eth} + \left|J^N_{\varphi_1}\right|^{\eth}} \right)$

4. Bipolar fuzzy Einstein prioritized AOs

In this part of the manuscript, we devise BFEPRA, BFEPRWA, BFEPRG, and BFEPRWG AOs.

Definition 5. *Let* $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right), \lambda = 1, 2, \ldots, \Omega$ *as an assembly of BFNs. The BFEPRA operator over* φ_λ *is designated as*

$$\text{BFEPRA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \bigoplus_{\lambda=1}^{\Omega}{}_\varepsilon \frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} \dot{T}_\lambda} \varphi_\lambda$$

observe that $\dot{T}_1 = 1$, $\dot{T}_\lambda = \prod_{\lambda=1}^{\Omega-1} \acute{S}\left(\varphi_\lambda\right)$, $\lambda = 1, 2, \ldots, \Omega$ *and* $\acute{S}\left(\varphi_\lambda\right)$ *is the score value of BFN* φ_λ*.*

Theorem 1. *Let* $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right)$, $\lambda = 1, 2, \ldots, \Omega$ *is an assembly of BFNs. Then by employing BFEPRA operator over* φ_λ*, the aggregated outcome is a BFN i.e.*

$$\text{BFEPRA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \left(\begin{array}{c} \dfrac{\prod\limits_{\lambda=1}^{\Omega}\left(1+J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \prod\limits_{\lambda=1}^{\Omega}\left(1-J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\prod\limits_{\lambda=1}^{\Omega}\left(1+J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \prod\limits_{\lambda=1}^{\Omega}\left(1-J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, \\ \dfrac{-2\prod\limits_{\lambda=1}^{\Omega}\left|J^N_{\varphi_\lambda}\right|^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\prod\limits_{\lambda=1}^{\Omega}\left(2+J^N_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \prod\limits_{\lambda=1}^{\Omega}\left|J^N_{\varphi_\lambda}\right|^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \end{array} \right). \quad (1)$$

Proof. Let $\Omega = 2$. Then to prove that

$$\text{BFEPRA}\left(\varphi_1, \varphi_2\right) = \frac{\dot{T}_1}{\sum\limits_{\lambda=1}^{\Omega}\dot{T}_\lambda}\varphi_1 \oplus_\varepsilon \frac{\dot{T}_2}{\sum\limits_{\lambda=1}^{\Omega}\dot{T}_\lambda}\varphi_2$$

$$= \left(\begin{array}{c} \dfrac{\prod\limits_{\lambda=1}^{2}\left(1+J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{2}\dot{T}_\lambda}} - \prod\limits_{\lambda=1}^{2}\left(1-J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{2}\dot{T}_\lambda}}}{\prod\limits_{\lambda=1}^{2}\left(1+J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{2}\dot{T}_\lambda}} + \prod\limits_{\lambda=1}^{2}\left(1-J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{2}\dot{T}_\lambda}}}, \\ \dfrac{-2\prod\limits_{\lambda=1}^{2}\left|J^N_{\varphi_\lambda}\right|^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{2}\dot{T}_\lambda}}}{\prod\limits_{\lambda=1}^{2}\left(2+J^N_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{2}\dot{T}_\lambda}} + \prod\limits_{\lambda=1}^{2}\left|J^N_{\varphi_\lambda}\right|^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{2}\dot{T}_\lambda}}} \end{array} \right).$$

Now we have

$$\frac{\dot{T}_1}{\sum\limits_{\lambda=1}^{\Omega}\dot{T}_\lambda}\varphi_1 = \left(\frac{\left(1+J^P_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \left(1-J^P_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(1+J^P_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(1-J^P_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, -\frac{2\left|J^N_{\varphi_1}\right|^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(2+J^N_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left|J^N_{\varphi_1}\right|^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \right),$$

$$\frac{\dot{T}_2}{\sum\limits_{\lambda=1}^{\Omega}\dot{T}_\lambda}\varphi_2 = \left(\frac{\left(1+J^P_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \left(1-J^P_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(1+J^P_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(1-J^P_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, -\frac{2\left|J^N_{\varphi_2}\right|^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(2+J^N_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left|J^N_{\varphi_2}\right|^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \right)$$

then,

$$\begin{aligned}
\text{BFEPRA}\left(\varphi_1,\varphi_2\right) &= \frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}\varphi_1 \oplus_\varepsilon \frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}\varphi_2 \\
&= \left(\frac{\left(1+J_{\varphi_1}^P\right)^{\frac{\dot{T}_1}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \left(1-J_{\varphi_1}^P\right)^{\frac{\dot{T}_1}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(1+J_{\varphi_1}^P\right)^{\frac{\dot{T}_1}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(1-J_{\varphi_1}^P\right)^{\frac{\dot{T}_1}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, -\frac{2\left|J_{\varphi_1}^N\right|^{\frac{\dot{T}_1}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(2+J_{\varphi_1}^N\right)^{\frac{\dot{T}_1}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left|J_{\varphi_1}^N\right|^{\frac{\dot{T}_1}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}\right) \\
&\quad \oplus_\varepsilon \left(\frac{\left(1+J_{\varphi_2}^P\right)^{\frac{\dot{T}_2}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \left(1-J_{\varphi_2}^P\right)^{\frac{\dot{T}_2}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(1+J_{\varphi_2}^P\right)^{\frac{\dot{T}_2}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(1-J_{\varphi_2}^P\right)^{\frac{\dot{T}_2}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, -\frac{2\left|J_{\varphi_2}^N\right|^{\frac{\dot{T}_2}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(2+J_{\varphi_2}^N\right)^{\frac{\dot{T}_2}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left|J_{\varphi_2}^N\right|^{\frac{\dot{T}_2}{\Sigma_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}\right) \\
&= \left(\begin{array}{c}
\dfrac{\prod_{\lambda=1}^{2}\left(1+J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{2}\dot{T}_\lambda}} - \prod_{\lambda=1}^{2}\left(1-J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{2}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{2}\left(1+J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{2}\dot{T}_\lambda}} + \prod_{\lambda=1}^{2}\left(1-J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{2}\dot{T}_\lambda}}}, \\
\dfrac{-2\prod_{\lambda=1}^{2}\left|J_{\varphi_\lambda}^N\right|^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{2}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{2}\left(2+J_{\varphi_\lambda}^N\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{2}\dot{T}_\lambda}} + \prod_{\lambda=1}^{2}\left|J_{\varphi_\lambda}^N\right|^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{2}\dot{T}_\lambda}}}
\end{array}\right).
\end{aligned}$$

Thus, Eq. (1) holds for $\Omega = 2$. Now let Eq. (1) holds for $\Omega = \chi$, i.e.

$$\text{BFEPRA}\left(\varphi_1,\varphi_2,\ldots,\varphi_\chi\right) = \left(\begin{array}{c}
\dfrac{\prod_{\lambda=1}^{\chi}\left(1+J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{T}_\lambda}} - \prod_{\lambda=1}^{\chi}\left(1-J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\chi}\left(1+J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\chi}\left(1-J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{T}_\lambda}}}, \\
\dfrac{-2\prod_{\lambda=1}^{\chi}\left|J_{\varphi_\lambda}^N\right|^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\chi}\left(2+J_{\varphi_\lambda}^N\right)^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\chi}\left|J_{\varphi_\lambda}^N\right|^{\frac{\dot{T}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{T}_\lambda}}}
\end{array}\right).$$

Next to show that Eq. (1) holds for $\Omega = \chi + 1$

$$\begin{aligned}\text{BFEPRA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\chi, \varphi_{\chi+1}\right) &= \text{BFEPRA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\chi\right) \oplus_\varepsilon \varphi_{\chi+1} \\ &= \bigoplus_{\lambda=1}^{\chi}{}_\varepsilon \frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi} \dot{T}_\lambda} \varphi_\lambda \oplus_\varepsilon \frac{\dot{T}_{\chi+1}}{\sum_{\lambda=1}^{\chi+1} \dot{T}_\lambda} \varphi_{\chi+1}\end{aligned}$$

$$= \left(\begin{array}{c} \dfrac{\prod_{\lambda=1}^{\chi}\left(1+J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} - \prod_{\lambda=1}^{\chi}\left(1-J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\chi}\left(1+J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\chi}\left(1-J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}, \\ \dfrac{-2\prod_{\lambda=1}^{\chi}\left|J_{\varphi_\lambda}^{N}\right|^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\chi}\left(2+J_{\varphi_\lambda}^{N}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\chi}\left|J_{\varphi_\lambda}^{N}\right|^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}} \end{array} \right)$$

$$\oplus_\varepsilon \left(\begin{array}{c} \dfrac{\left(1+J_{\varphi_{\chi+1}}^{P}\right)^{\frac{\dot{T}_{\chi+1}}{\sum_{\lambda=1}^{\chi+1}\dot{T}_\lambda}} - \left(1-J_{\varphi_{\chi+1}}^{P}\right)^{\frac{\dot{T}_{\chi+1}}{\sum_{\lambda=1}^{\chi+1}\dot{T}_\lambda}}}{\left(1+J_{\varphi_{\chi+1}}^{P}\right)^{\frac{\dot{T}_{\chi+1}}{\sum_{\lambda=1}^{\chi+1}\dot{T}_\lambda}} + \left(1-J_{\varphi_{\chi+1}}^{P}\right)^{\frac{\dot{T}_{\chi+1}}{\sum_{\lambda=1}^{\chi+1}\dot{T}_\lambda}}} \\ \dfrac{-2\left|J_{\varphi_{\chi+1}}^{N}\right|^{\frac{\dot{T}_{\chi+1}}{\sum_{\lambda=1}^{\chi+1}\dot{T}_\lambda}}}{\left(2+J_{\varphi_{\chi+1}}^{N}\right)^{\frac{\dot{T}_{\chi+1}}{\sum_{\lambda=1}^{\chi+1}\dot{T}_\lambda}} + \left|J_{\varphi_{\chi+1}}^{N}\right|^{\frac{\dot{T}_{\chi+1}}{\sum_{\lambda=1}^{\chi+1}\dot{T}_\lambda}}} \end{array} \right)$$

$$= \left(\begin{array}{c} \dfrac{\prod_{\lambda=1}^{\chi+1}\left(1+J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} - \prod_{\lambda=1}^{\chi+1}\left(1-J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\chi+1}\left(1+J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\chi+1}\left(1-J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}, \\ \dfrac{-2\prod_{\lambda=1}^{\chi+1}\left|J_{\varphi_\lambda}^{N}\right|^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\chi+1}\left(2+J_{\varphi_\lambda}^{N}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\chi+1}\left|J_{\varphi_\lambda}^{N}\right|^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}} \end{array} \right).$$

This implies that Eq. (1) holds $\forall\lambda$.

Properties of the BFEPRA operator

Let two assemblies of BFNs that are $\varphi_\lambda = \left(J_{\varphi_\lambda}^{P}, J_{\varphi_\lambda}^{N}\right)$, $\varphi_\lambda = \left(J_{\varphi_\lambda}^{P}, J_{\varphi_\lambda}^{N}\right)$, $\lambda = 1, 2, \ldots, \Omega$, then

1. Idempotency:
   If $\varphi_\lambda = \varphi \ \ \forall \lambda$ then,

$$\text{BFEPRA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \varphi$$

2. Monotonicity:
   If $J^P_{\varphi_\lambda} \leqslant J_{\varphi_\lambda}$, $J^N_{\varphi_\lambda} \leqslant J_{\varphi_\lambda}$ then

$$\text{BFEPRA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) \leqslant \text{BFEPRA}$$

3. Boundedness:
   If $\varphi^- = \left(\min\limits_\lambda \left\{J^P_{\varphi_\lambda}\right\}, \max\limits_\lambda \left\{J^N_{\varphi_\lambda}\right\}\right)$, and $\varphi^+ = \left(\max\limits_\lambda \left\{J^P_{\varphi_\lambda}\right\}, \min\limits_\lambda \left\{J^N_{\varphi_\lambda}\right\}\right)$, then

$$\varphi^- \leqslant \text{BFEPRA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) \leqslant \varphi^+.$$

Definition 6. *Let* $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right)$, $\lambda = 1, 2, \ldots, \Omega$ *as an assembly of BFNs. The BFEPRWA operator over* φ_λ *is designated as*

$$\text{BFEPRWA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \bigoplus_{\lambda=1}^{\Omega}{}_\varepsilon \frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda} \varphi_\lambda.$$

observe that $\dot{T}_1 = 1$, $\dot{T}_\lambda = \prod_{\lambda=1}^{\Omega-1} \acute{S}\left(\varphi_\lambda\right), \lambda = 1, 2, \ldots, \Omega$ *and* $\acute{S}\left(\varphi_\lambda\right)$ *is the score value of BFN* φ_λ *and* $w = \left(w_1, w_2, w_3, \ldots, w_\Omega\right)$ *is a weight vector, with the condition that* $w_\lambda \in [0, 1]\ \forall \lambda$ *and* $\sum_{\lambda=1}^{\Omega} w_\lambda = 1$.

Theorem 2. *Let* $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right)$, $\lambda = 1, 2, \ldots, \Omega$ *is an assembly of BFNs. Then by employing a BFEPRWA operator over* φ_λ*, the aggregated outcome is a BFN i.e.*

$$\text{BFEPRWA}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \left(\begin{array}{c} \dfrac{\prod\limits_{\lambda=1}^{\Omega}\left(1 + J^P_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}} - \prod\limits_{\lambda=1}^{\Omega}\left(1 - J^P_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}}{\prod\limits_{\lambda=1}^{\Omega}\left(1 + J^P_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}} + \prod\limits_{\lambda=1}^{\Omega}\left(1 - J^P_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}}, \\ \dfrac{-2\prod\limits_{\lambda=1}^{\Omega}\left|J^N_{\varphi_\lambda}\right|^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}}{\prod\limits_{\lambda=1}^{\Omega}\left(2 + J^N_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}} + \prod\limits_{\lambda=1}^{\Omega}\left|J^N_{\varphi_\lambda}\right|^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}} \end{array} \right).$$

The BFPREWA operator holds the properties of idempotency, monotonicity, and boundedness.

Definition 7. *Let* $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right)$, $\lambda = 1, 2, \ldots, \Omega$ *as an assembly of BFNs. The BFPREG operator over* φ_λ *is designated as*

$$\text{BFEPRG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \bigoplus_{\lambda=1}^{\Omega}{}_{\varepsilon} \left(\varphi_\lambda\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}$$

observe that $\dot{T}_1 = 1$, $\dot{T}_\lambda = \prod_{\lambda=1}^{\Omega-1} \acute{S}\left(\varphi_\lambda\right)$, $\lambda = 1, 2, \ldots, \Omega$ *and* $\acute{S}\left(\varphi_\lambda\right)$ *is the score value of BFN* φ_λ.

Theorem 3. *Let* $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right)$, $\lambda = 1, 2, \ldots, \Omega$ *is an assembly of BFNs. Then by employing BFEPRG operator over* φ_λ*, the aggregated outcome is a BFN i.e.*

$$\text{BFEPRG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \left(\begin{array}{c} \dfrac{2\prod_{\lambda=1}^{\Omega}\left(J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\Omega}\left(2-J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\Omega}\left(J^P_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, \\ \dfrac{\prod_{\lambda=1}^{\Omega}\left(1+J^{IP}_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \prod_{\lambda=1}^{\Omega}\left(1-J^{IP}_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\Omega}\left(1+J^{IP}_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\Omega}\left(1-J^{IP}_{\varphi_\lambda}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \end{array} \right). \quad (2)$$

Proof. Let $\Omega = 2$. Then to prove that

$$\text{BFEPRG}\left(\varphi_1, \varphi_2\right) = \left(\varphi_1\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} \otimes_\varepsilon \left(\varphi_2\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}$$

where

$$\left(\varphi_1\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} = \left(\frac{2\left(J^P_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(2-J^P_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(J^P_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, \frac{\left(1+J^N_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \left(1-J^N_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(1+J^N_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(1-J^N_{\varphi_1}\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \right),$$

$$\left(\varphi_2\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} = \left(\frac{2\left(J^P_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(2-J^P_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(J^P_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, \frac{\left(1+J^N_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \left(1-J^N_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(1+J^N_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(1-J^N_{\varphi_2}\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \right).$$

Now we have

$$(\varphi_1)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} \otimes_\varepsilon (\varphi_2)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} = \left(\begin{array}{c} \dfrac{2\left(J_{\varphi_1}^P\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(2-J_{\varphi_1}^P\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(J_{\varphi_1}^P\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, \\ \dfrac{\left(1+J_{\varphi_1}^N\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \left(1-J_{\varphi_1}^N\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(1+J_{\varphi_1}^N\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(1-J_{\varphi_1}^N\right)^{\frac{\dot{T}_1}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \end{array} \right)$$

$$\otimes_\varepsilon \left(\begin{array}{c} \dfrac{2\left(J_{\varphi_2}^P\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(2-J_{\varphi_2}^P\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(J_{\varphi_2}^P\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, \dfrac{\left(1+J_{\varphi_2}^N\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \left(1-J_{\varphi_2}^N\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\left(1+J_{\varphi_2}^N\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \left(1-J_{\varphi_2}^N\right)^{\frac{\dot{T}_2}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \end{array} \right)$$

$$= \left(\begin{array}{c} \dfrac{2\prod_{\lambda=1}^{2}\left(J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{2}\left(2-J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \prod_{\lambda=1}^{2}\left(J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}, \\ \dfrac{\prod_{\lambda=1}^{2}\left(1+J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} - \prod_{\lambda=1}^{2}\left(1-J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{2}\left(1+J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}} + \prod_{\lambda=1}^{2}\left(1-J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega}\dot{T}_\lambda}}} \end{array} \right)$$

$$= \mathrm{BFEPRG}\left(\varphi_1, \varphi_2\right).$$

Thus, Eq. (2) holds for $\Omega = 2$. Now let Eq. (2) holds for $\Omega = \chi$, i.e.

$$\mathrm{BFEPRG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\chi\right) = \left(\begin{array}{c} \dfrac{2\prod_{\lambda=1}^{\chi}\left(J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\chi}\left(2-J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\chi}\left(J_{\varphi_\lambda}^P\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}, \\ \dfrac{\prod_{\lambda=1}^{\chi}\left(1+J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} - \prod_{\lambda=1}^{\chi}\left(1-J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}}{\prod_{\lambda=1}^{\chi}\left(1+J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}} + \prod_{\lambda=1}^{\chi}\left(1-J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{T}_\lambda}{\sum_{\lambda=1}^{\chi}\dot{T}_\lambda}}} \end{array} \right)$$

Next to show that Eq. (2) holds for $\Omega = \chi + 1$

$$
\begin{aligned}
&\mathrm{BFEPRG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\chi, \varphi_{\chi+1}\right) = \mathrm{BFEPRG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\chi\right) \otimes_\varepsilon \varphi_{\chi+1} \\
&= \bigoplus_{\lambda=1}^{\chi}{}_\varepsilon \left(\varphi_\lambda\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\Omega}\dot{\tau}_\lambda}} \otimes_\varepsilon \left(\varphi_{\chi+1}\right)^{\frac{\dot{\tau}_{\chi+1}}{\Sigma_{\lambda=1}^{\Omega}\dot{\tau}_{\chi+1}}} \\
&= \left(\begin{array}{c} \dfrac{2\prod_{\lambda=1}^{\chi}\left(J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{\tau}_\lambda}}}{\prod_{\lambda=1}^{\chi}\left(2 - J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{\tau}_\lambda}} + \prod_{\lambda=1}^{\chi}\left(J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{\tau}_\lambda}}}, \\ \dfrac{\prod_{\lambda=1}^{\chi}\left(1 + J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{\tau}_\lambda}} - \prod_{\lambda=1}^{\chi}\left(1 - J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{\tau}_\lambda}}}{\prod_{\lambda=1}^{\chi}\left(1 + J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{\tau}_\lambda}} + \prod_{\lambda=1}^{\chi}\left(1 - J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi}\dot{\tau}_\lambda}}} \end{array} \right) \\
&\otimes_\varepsilon \left(\begin{array}{c} \dfrac{2\left(J_{\varphi_{\chi+1}}^{P}\right)^{\frac{\dot{\tau}_{\chi+1}}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}}}{\left(2 - J_{\varphi_{\chi+1}}^{P}\right)^{\frac{\dot{\tau}_{\chi+1}}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}} + \left(J_{\varphi_{\chi+1}}^{P}\right)^{\frac{\dot{\tau}_{\chi+1}}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}}}, \\ \dfrac{\left(1 + J_{\varphi_{\chi+1}}^{N}\right)^{\frac{\dot{\tau}_{\chi+1}}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}} - \left(1 - J_{\varphi_{\chi+1}}^{N}\right)^{\frac{\dot{\tau}_{\chi+1}}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}}}{\left(1 + J_{\varphi_{\chi+1}}^{N}\right)^{\frac{\dot{\tau}_{\chi+1}}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}} + \left(1 - J_{\varphi_{\chi+1}}^{N}\right)^{\frac{\dot{\tau}_{\chi+1}}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}}} \end{array} \right) \\
&= \left(\begin{array}{c} \dfrac{2\prod_{\lambda=1}^{\chi+1}\left(J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}}}{\prod_{\lambda=1}^{\chi+1}\left(2 - J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}} + \prod_{\lambda=1}^{\chi+1}\left(J_{\varphi_\lambda}^{P}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}}}, \\ \dfrac{\prod_{\lambda=1}^{\chi+1}\left(1 + J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}} - \prod_{\lambda=1}^{\chi+1}\left(1 - J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}}}{\prod_{\lambda=1}^{\chi+1}\left(1 + J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}} + \prod_{\lambda=1}^{\chi+1}\left(1 - J_{\varphi_\lambda}^{IP}\right)^{\frac{\dot{\tau}_\lambda}{\Sigma_{\lambda=1}^{\chi+1}\dot{\tau}_\lambda}}} \end{array} \right).
\end{aligned}
$$

This implies that Eq. (2) holds $\forall\lambda$.

Properties of the BFEPRG operator

Let two assemblies of BFNs are $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right), \varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right), \lambda = 1, 2, \ldots, \Omega$, then

1. Idempotency: If $\varphi_\lambda = \varphi\ \forall\lambda$ then,

$$\text{BFEPRG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \varphi$$

2. Monotonicity: If $J^P_{\varphi_\lambda} \leqslant J_{\varphi_\lambda}$, $J^N_{\varphi_\lambda} \leqslant J_{\varphi_\lambda}$ then

$$\text{BFEPRG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) \leqslant \text{BFEPRG}$$

3. Boundedness: If $\varphi^- = \left(\min\limits_\lambda \left\{J^P_{\varphi_\lambda}\right\}, \max\limits_\lambda \left\{J^N_{\varphi_\lambda}\right\}\right)$, and $\varphi^+ = \left(\max\limits_\lambda \left\{J^P_{\varphi_\lambda}\right\}, \min\limits_\lambda \left\{J^N_{\varphi_\lambda}\right\}\right)$, then $\varphi^- \leqslant \text{BFEPRG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) \leqslant \varphi^+$.

Definition 8. *Let $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right)$, $\lambda = 1, 2, \ldots, \Omega$ is an assembly of BFNs. The BFEPRWG operator over φ_λ is designated as*

$$\text{BFEPRWG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \bigoplus_{\lambda=1}^{\Omega}{}_\varepsilon \left(\varphi_\lambda\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}$$

observe that $\dot{T}_1 = 1$, $\dot{T}_\lambda = \prod_{\lambda=1}^{\Omega-1} \acute{S}\left(\varphi_\lambda\right)$, $\lambda = 1, 2, \ldots, \Omega$ and $\acute{S}\left(\varphi_\lambda\right)$ is the score value of BFN φ_λ and $w = \left(w_1, w_2, w_3, \ldots, w_\Omega\right)$ is a weight vector, with the condition that $w_\lambda \in [0, 1]\ \forall\lambda$ and $\sum_{\lambda=1}^{\Omega} w_\lambda = 1$.

Theorem 4. *Let $\varphi_\lambda = \left(J^P_{\varphi_\lambda}, J^N_{\varphi_\lambda}\right)$, $\lambda = 1, 2, \ldots, \Omega$ is an assembly of BFNs. Then by employing a BFEPRWG operator over φ_λ, the aggregated outcome is a BFN i.e.*

$$\text{BFEPRWG}\left(\varphi_1, \varphi_2, \ldots, \varphi_\Omega\right) = \left(\frac{2\prod\limits_{\lambda=1}^{\Omega}\left(J^P_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}}{\prod\limits_{\lambda=1}^{\Omega}\left(2 - J^P_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}} + \prod\limits_{\lambda=1}^{\Omega}\left(J^P_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}}, \frac{\prod\limits_{\lambda=1}^{\Omega}\left(1 + J^{IP}_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}} - \prod\limits_{\lambda=1}^{\Omega}\left(1 - J^{IP}_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}}{\prod\limits_{\lambda=1}^{\Omega}\left(1 + J^{IP}_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}} + \prod\limits_{\lambda=1}^{\Omega}\left(1 - J^{IP}_{\varphi_\lambda}\right)^{\frac{w_\lambda \dot{T}_\lambda}{\sum_{\lambda=1}^{\Omega} w_\lambda \dot{T}_\lambda}}} \right)$$

The BFEPRWG operator holds the properties of idempotency, monotonicity, and boundedness.

5. MCDM approach based on Einstein prioritized operators

Let $\{X_1, X_2, \ldots, X_\Omega\}$ be an assemble of Ω alternatives which have to be assessed by ϑ decision-makers $\{P_1, P_2, \ldots, P_\vartheta\}$ by considering ρ criteria $\{\tau_1, \tau_2, \ldots, \tau_\rho\}$. The decision-makers evaluate the considered alternatives and interpret their evaluation values in terms of linguistics to create a linguistic decision matrix (LDM) $E^{\varrho} = \left[\sigma_{\lambda\xi}^{(\varrho)}\right]_{\Omega\times\rho}$, where $\sigma_{\lambda\xi}^{(\varrho)}$ is the representation of the assessment outcome of λ^{th} alternative relying on ξ^{th} criterion interpreted by ϱ^{th} decision maker. As each decision maker has their importance and significance so according to their importance, they must have weight that is $(w_1, w_1, \ldots, w_\vartheta)$ with the condition that $0 \leqslant w_\varrho \leqslant 1$ and $\sum_{\varrho=1}^{\vartheta} w_\varrho = 1$.

The above problem is an MCDM (MCGDM) problem, the following are the stages to solve this problem.

Stage 1: Alter LDMs to bipolar fuzzy decision matrices (BFDMs)

As there are bipolarity and uncertainty involved in the criteria, so in the assessment of the alternatives, it is critical to consider both bipolarity and uncertainty. Thus, the evaluation values in the linguistic terms should alter to the BFNs to create BFDMs.

$$E_B^{\varrho} = \left[F_{\lambda\xi}^{(\varrho)}\right]_{\Omega\times\rho} = \begin{array}{c} \\ X_1 \\ X_2 \\ \vdots \\ X_\Omega \end{array} \begin{array}{c} \begin{array}{cccc} \tau_1 & \tau_2 & \ldots & \tau_\rho \end{array} \\ \begin{pmatrix} \left(\partial_{F_{11}}^{P,\varrho}, \partial_{F_{11}}^{N,\varrho}\right) & \left(\partial_{F_{12}}^{P,\varrho}, \partial_{F_{12}}^{N,\varrho}\right) & \ldots & \left(\partial_{F_{1\rho}}^{P,\varrho}, \partial_{F_{1\rho}}^{N,\varrho}\right) \\ \left(\partial_{F_{21}}^{P,\varrho}, \partial_{F_{21}}^{N,\varrho}\right) & \left(\partial_{F_{22}}^{P,\varrho}, \partial_{F_{22}}^{N,\varrho}\right) & \ldots & \left(\partial_{F_{2\rho}}^{P,\varrho}, \partial_{F_{2\rho}}^{N,\varrho}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \left(\partial_{F_{\Omega 1}}^{P,\varrho}, \partial_{F_{\Omega I}}^{N,\varrho}\right) & \left(\partial_{F_{\Omega 2}}^{P,\varrho}, \partial_{F_{\Omega 2}}^{N,\varrho}\right) & \ldots & \left(\partial_{F_{\Omega\rho}}^{P,\varrho}, \partial_{F_{\Omega\rho}}^{N,\varrho}\right) \end{pmatrix} \end{array}.$$

Stage 2: Convert all BFDMs to a single BFDM

Using any BFWA or BFWG operators to convert the BFDMS to a single BFDM (SBFDM).

$$E_B = \left[F_{\lambda\xi}\right]_{\Omega\times\rho} = \begin{array}{c} \\ X_1 \\ X_2 \\ \vdots \\ X_\Omega \end{array} \begin{array}{c} \begin{array}{cccc} \tau_1 & \tau_2 & \ldots & \tau_\rho \end{array} \\ \begin{pmatrix} \left(\partial_{F_{11}}^{P,}, \partial_{F_{11}}^{N,} \middle| \ \middle|\right) & \left(\partial_{F_{12}}^{P,}, \partial_{F_{12}}^{N,} \middle| \ \middle|\right) & \ldots & \left(\partial_{F_{1\rho}}^{P,}, \partial_{F_{1\rho}}^{N,} \middle| \ \middle|\right) \\ \left(\partial_{F_{21}}^{P,}, \partial_{F_{21}}^{N,} \middle| \ \middle|\right) & \left(\partial_{F_{22}}^{P,}, \partial_{F_{22}}^{N,} \middle| \ \middle|\right) & \ldots & \left(\partial_{F_{2\rho}}^{P,}, \partial_{F_{2\rho}}^{N,} \middle| \ \middle|\right) \\ \vdots & \vdots & \ddots & \vdots \\ \left(\partial_{F_{\Omega 1}}^{P,}, \partial_{F_{\Omega 1}}^{N,} \middle| \ \middle|\right) & \left(\partial_{F_{\Omega 2}}^{P,}, \partial_{F_{\Omega 2}}^{N,} \middle| \ \middle|\right) & \ldots & \left(\partial_{F_{\Omega\rho}}^{P,}, \partial_{F_{\Omega\rho}}^{N,} \middle| \ \middle|\right) \end{pmatrix} \end{array}.$$

Stage 3: Normalization of SBFDM

As some of the criteria can be cost type, it is important to normalize the SBFDM. For normalization, we have the following equation.

$$\left(\partial^{P,s}_{F_{\lambda\xi}}, \partial^{N,s}_{F_{\lambda\xi}}\right) = \begin{cases} \left(\partial^{P,}_{F_{\lambda\xi}}, \partial^{N,}_{F_{\lambda\xi}} \middle| \ \middle|\right) & \text{if } \xi \in B_\rho \\ \left(1 - \partial^{P,}_{F_{\lambda\xi}} \middle| \ \middle|, -1 - \partial^{N,}_{F_{\lambda\xi}} \middle|\right) & \text{if } \xi \in C_\rho \,. \end{cases}$$

Noted that B_ρ is an assembly of benefit sort and C_ρ is an assembly of cost sort of criteria.

$$\mathrm{SE}_B = \left[F^s_{\lambda\xi}\right]_{\Omega\times\rho} = \begin{array}{c} \\ X_1 \\ X_2 \\ \vdots \\ X_\Omega \end{array} \begin{array}{c} \begin{array}{cccc} \tau_1 & \tau_2 & \dots & \tau_\rho \end{array} \\ \begin{pmatrix} \left(\partial^{P,s}_{F_{11}}, \partial^{N,s}_{F_{11}}\right) & \left(\partial^{P,s}_{F_{12}}, \partial^{N,s}_{F_{12}}\right) & \dots & \left(\partial^{P,s}_{F_{1\rho}}, \partial^{N,s}_{F_{1\rho}}\right) \\ \left(\partial^{P,s}_{F_{21}}, \partial^{N,s}_{F_{21}}\right) & \left(\partial^{P,s}_{F_{22}}, \partial^{N,s}_{F_{22}}\right) & \dots & \left(\partial^{P,s}_{F_{2\rho}}, \partial^{N,s}_{F_{2\rho}}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \left(\partial^{P,s}_{F_{\Omega 1}}, \partial^{N,s}_{F_{\Omega 1}}\right) & \left(\partial^{P,s}_{F_{\Omega 2}}, \partial^{N,s}_{F_{\Omega 2}}\right) & \dots & \left(\partial^{P,s}_{F_{\Omega\rho}}, \partial^{N,s}_{F_{\Omega\rho}}\right) \end{pmatrix} \end{array}.$$

Stage 4: Find the prioritization $\dot{T}_{\lambda\xi}$

The following is the equation to find $\dot{T}_{\lambda\xi}$

$$\dot{T}_{\lambda\xi} = \prod_{\alpha=1}^{\xi-1} S\left(X_{\lambda\alpha}\right)$$

where, $\lambda = 1, 2, \dots, \Omega$, $\xi = 1, 2, \dots, \rho$ and $\dot{T}_{\lambda 1} = 1$ for $\lambda = 1, 2, \dots, \Omega$.

Stage 5: Aggregate the normalized SBFDM

In this stage, the normalized SBFDM will be aggregated to get the aggregated values of each alternative.

For this aggregation, any of the above-defined operators (BFEPRA, BFEPRWA, BFEPRG, BFEPRWG) can be utilized.

Stage 6: Get the score values.

Find the score values of alternatives, by using their aggregated outcomes.

Stage 7: Ordering and ranking the alternatives

With the assistance of score values of alternatives, order and rank the alternatives.

The graphical representation of the developed MCDM (MCGDM) approach is devised in Fig. 4.

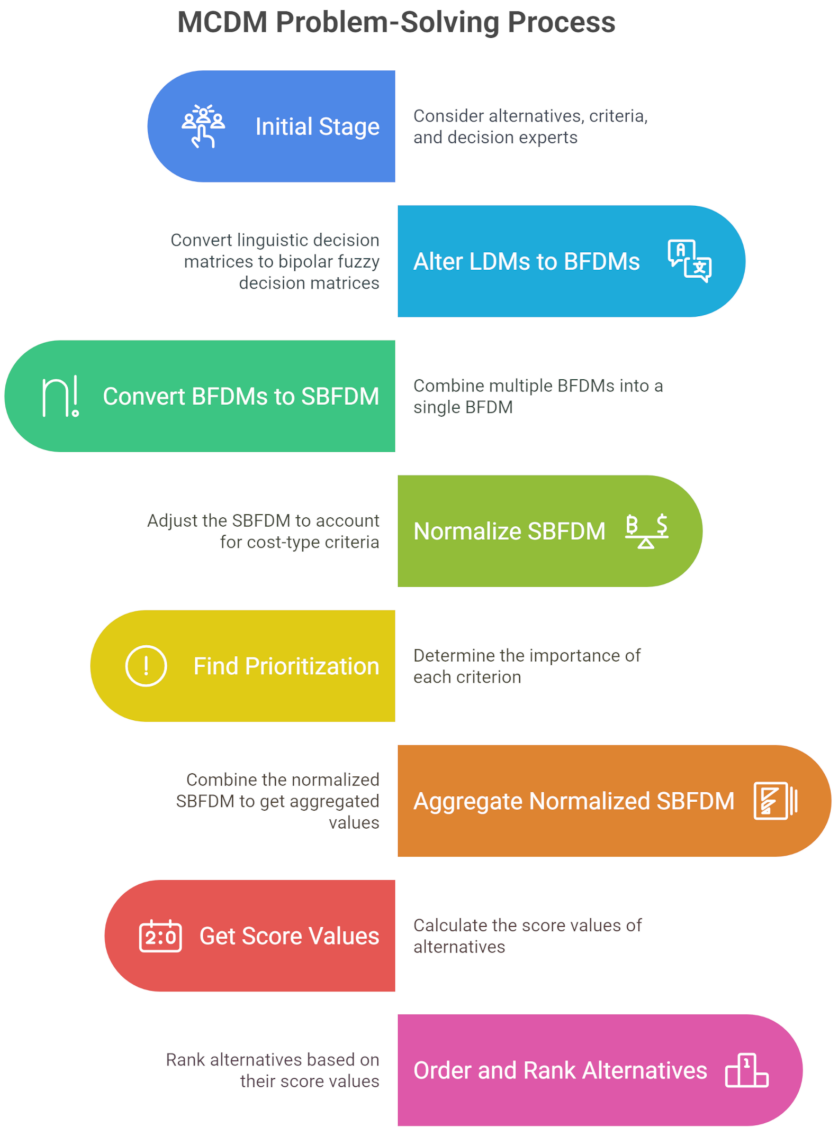


Figure 4: Developed MCDM (MCGDM) approach

Case study

A financial institution is experiencing an increasing number of cybersecurity threats, including phishing attacks, alongside ransomware incidents and data breaches. The organization requires an AI-driven big data visualization platform that processes enormous security data efficiently and detects active threats while providing useful findings for security risk reduction measures. Multiple

evaluation criteria generate an MCDM issue when organizations try to select their perfect visualization tool because each tool performs differently in detection accuracy and interpretation alongside scalability and processing speed capabilities.

BF prioritized Einstein operators to serve the organization by allowing it to evaluate and categorize suitable visualization tools based on extensive assessment of multiple criteria from multiple alternatives. The financial institution has the following AI-driven big data visualization tools as an alternative, which is given in Table 1.

Table 1: The AI-driven big data visualization tools

Notation	AI-driven big data visualization tools	Explanation
X_1	Splunk Security Analytics	Splunk security analytics functions as an advanced SIEM system that implements AI capabilities to detect threats in real time alongside incident response services. The system consolidates information from different sources to optimize security logging functions. Splunk delivers automated capacities that connect security events for visual presentation.
X_2	IBM QRadar	IBM QRadar operates as a cybersecurity analytics platform that implements machine learning to identify behavioral signatures and detect anomalies in organizational security. Security intelligence becomes automated through the tool's capability to unite network traffic with system logs. Users can extract a sophisticated understanding of attack methods from the platform updates offered by QRadar.
X_3	ELK Stack	The ELK stack is an open source big data visualization tool for realtime log analysis and security monitoring. The system shows a high ability to process security event logs and create their indexed version. ELK offers customizable dashboards for detailed threat analysis.
X_4	Microsoft Sentinel	Microsoft Sentinel serves as a cloud-native security platform that uses AI-powered threat detection alongside automation for its operations. The system detects cloud security risks in advance by automatically identifying advanced threat patterns. Machine learning functionality built into Sentinel helps Security Operation Centers operate more effectively.

For the evaluation of the above alternatives, the criteria are given in Table 2.

Based on these criteria, the decision expert provides his assessment values in the linguistic terms devised in Table 3.

To solve this case study, we use the developed MCDM approach.

Table 2: The criteria

Notation	Criteria	Explanation
τ_1	Threat Detection Accuracy	The performance in identifying threats must be evaluated through the ability to detect threats accurately while avoiding incorrect warnings and procedural misdiagnoses. Security monitoring achieves reliable performance when accuracy remains high.
τ_2	Scalability	The tool's capacity to deal effectively with growing security data sizes forms the basis of the scalability evaluation. The tool successfully operates at a high level in environments showing changing demand.
τ_3	Computational Efficiency	Assesses the processing speed and resource consumption of the tool. Security analytics functions in real time due to rapid and optimized tools.
τ_4	Visualization Quality	The assessment evaluates the readability along with a graphical view of the security analytics information. Analyzed data that is welldesigned enables analysts to better detect threats and respond effectively.

Table 3: The assessment values of AI-driven big data visualization tools

Criteria	τ_1	τ_2	τ_3	τ_4
X_1	E	I	I	M
X_2	S	E	S	I
X_3	S	M	M	S
X_4	I	M	E	E

where E is for exceptional, S is for satisfactory, M is for moderate and I is for inferior.

Stage 1: As there is one LDM, so alter it into BFDM, the scale given in Table 4 is used, and the BFDM is given in Table 5.

Table 4: The scale to convert linguistic terms into BFNs

Linguistic terms	BFNs
Exceptional (E)	(0.92, –0.27)
Satisfactory (S)	(0.68, –0.38)
Moderate (M)	(0.46, –0.53)
Inferior (I)	(0.19, –0.85)

Table 5: The BFDM

Criteria	τ_1	τ_2	τ_3	τ_4
X_1	(0.92, –0.27)	(0.19, –0.85)	(0.19, –0.85)	(0.46, –0.53)
X_2	(0.68, –0.38)	(0.92, –0.27)	(0.68, –0.38)	(0.19, –0.85)
X_3	(0.68, –0.38)	(0.46, –0.53)	(0.46, –0.53)	(0.68, –0.38)
X_4	(0.19, –0.85)	(0.46, –0.53)	(0.92, –0.27)	(0.92, –0.27)

Stage 2: In this case study, there is only one BFDM so there is no need for this stage.

Stage 3: All criteria are benefiting type, so after normalization, the same BFDM as given in Table 5 will be obtained.

Stage 4: The evaluated results

$$\dot{T}_{\lambda\xi} = \begin{bmatrix} 1 & 0.825 & 0.14 & 0.024 \\ 1 & 0.65 & 0.536 & 0.349 \\ 1 & 0.65 & 0.302 & 0.141 \\ 1 & 0.17 & 0.079 & 0.065 \end{bmatrix}.$$

Stage 5: After aggregating the evaluation values of the alternatives by using BFEPRA, BFEPRWA, BFEPRG, and BFEPRWG operators, the outcomes are devised in Table 6.

Table 6: The aggregated results of the AI-driven tools

Operators	X_1	X_1	X_1	X_1
BFEPRA	(0.716, –0.502)	(0.772, –0.349)	(0.59, –0.444)	(0.367, –0.724)
BFEPRWA	(0.747, –0.473)	(0.68, –0.435)	(0.599, –0.438)	(0.397, –0.712)
BFEPRG	(0.466, –0.639)	(0.739, –0.353)	(0.573, –0.451)	(0.263, –0.787)
BFEPRWG	(0.507, –0.606)	(0.774, –0.301)	(0.582, –0.445)	(0.27, –0.783)

Stage 6: The score values obtained by aggregating outcomes are displayed in Table 7.

The graphical interpretation of the score values is devised in Fig. 5.

Stage 7: The ordering and ranking are displayed in Table 8.

By employing the BFEPRWA operator in the MCDM technique, we have that X_1 i.e. Splunk Security Analytics is the finest one, while using other operators, we have that X_2 i.e. IBM QRadar is the finest one.

Table 7: The score values of AI-driven big data visualization tools

Operators	$S(X_1)$	$S(X_2)$	$S(X_3)$	$S(X_4)$
BFEPRA	0.607	0.712	0.573	0.321
BFEPRWA	0.637	0.623	0.58	0.342
BFEPRG	0.414	0.693	0.561	0.238
BFEPRWG	0.45	0.737	0.569	0.244

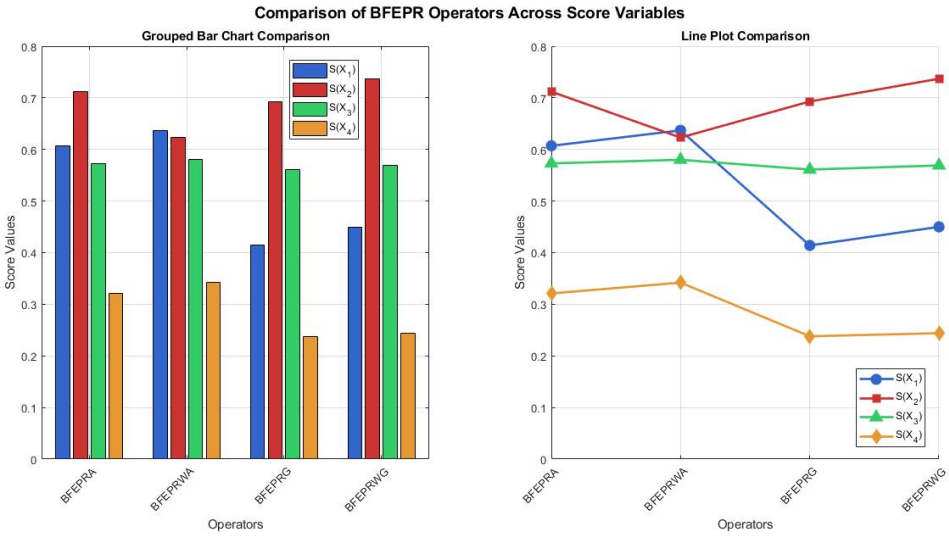


Figure 5: The graphical discussion of the score values

Table 8: Ranking of AI-driven big data visualization tools

Operators	Ranking
BFEPRA	$X_2 \geqslant X_1 \geqslant X_3 \geqslant X_4$
BFEPRWA	$X_1 \geqslant X_2 \geqslant X_3 \geqslant X_4$
BFEPRG	$X_2 \geqslant X_3 \geqslant X_1 \geqslant X_4$
BFEPRWG	$X_2 \geqslant X_3 \geqslant X_1 \geqslant X_4$

6. Comparative study

To establish the necessity and demonstrate the advantages of our developed theoretical framework, we conduct a comprehensive comparative analysis against several established methodologies in the literature. Our comparative study encompasses four prominent approaches: Verma and Sharma's [3] Einstein prioritized

averaging operators within intuitionistic fuzzy sets (IFS) coupled with their MultiCriteria Group Decision Making (MCGDM) methodology, Ali et al.'s [24] interpretation of Einstein prioritized operators within Pythagorean fuzzy sets (PFS) and their corresponding Multi-Attribute Group Decision Making (MAGDM) approach, Riaz et al.'s [25] construction of Einstein prioritized operators in q-rung orthopair fuzzy sets (q-ROFS) with associated MCGDM framework, and Jin et al.'s development of these operators within interval-valued hesitant fuzzy sets (IVHFS) for Multi-Attribute Decision Making (MADM) applications. To ensure methodological rigor, we apply both the existing theoretical frameworks and our newly proposed bipolar fuzzy Einstein prioritized operators to the identical cybersecurity tool evaluation dataset from our case study, with comprehensive results presented in Table 9 and Fig. 6.

Table 9: The result after employing existing and proposed theories

References	$S(X_1)$	$S(X_2)$	$S(X_3)$	$S(X_4)$	Ranking
Verma and Sharma [3]	x.x.x	x.x.x	x.x.x	x.x.x	x.x.x
Ali et al. [24]	x.x.x	x.x.x	x.x.x	x.x.x	x.x.x
Riaz et al. [25]	x.x.x	x.x.x	x.x.x	x.x.x	x.x.x
Jin et al. [26]	x.x.x	x.x.x	x.x.x	x.x.x	x.x.x
BFEPRA	0.607	0.712	0.573	0.321	$X_2 \geqslant X_1 \geqslant X_3 \geqslant X_4$
BFEPRWA	0.637	0.623	0.58	0.342	$X_1 \geqslant X_2 \geqslant X_3 \geqslant X_4$
BFEPRG	0.414	0.693	0.561	0.238	$X_2 \geqslant X_3 \geqslant X_1 \geqslant X_4$
BFEPRWG	0.45	0.737	0.569	0.244	$X_2 \geqslant X_3 \geqslant X_1 \geqslant X_4$

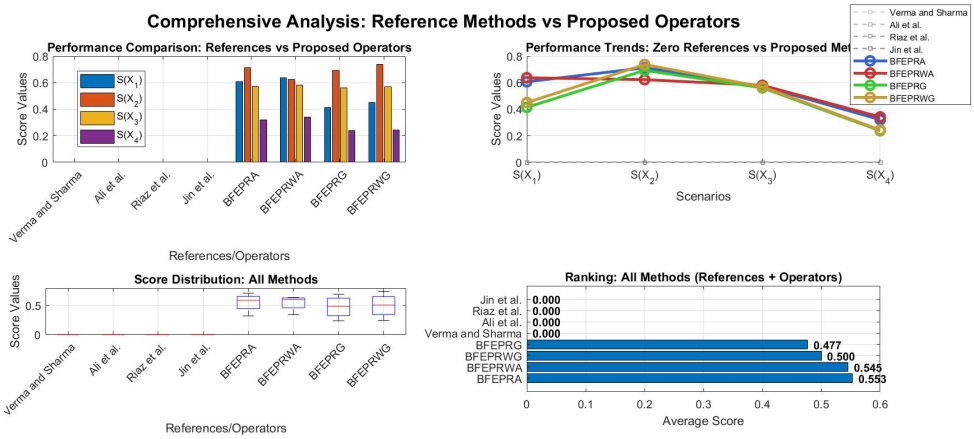


Figure 6: The graphical interpretation of the result after employing existing and proposed theories

The comparative analysis reveals a fundamental limitation in existing approaches: while these established Einstein prioritized operators excel within their respective fuzzy generalizations, they are inherently unable to process bipolar fuzzy information effectively due to their structural inability to simultaneously model and integrate both positive and negative aspects of decision criteria. This critical deficiency undermines decision accuracy, as any evaluation framework that fails to account for the dual nature of criteria attributes cannot claim to provide complete or reliable solutions. Our proposed bipolar fuzzy framework addresses this significant gap by explicitly incorporating both beneficial and detrimental aspects of each criterion, thereby delivering more comprehensive and realistic decision outcomes that better reflect the complex trade-offs inherent in real-world cybersecurity tool selection scenarios.

7. Conclusions

The significant role AI-driven big data visualization tools play in contemporary cybersecurity practices includes their ability to detect and respond to threats in real time. The tools use machine learning and innovative analytics to speed up security data processing operations. The decision process for identifying optimal tools faces difficulties because different methods show different capabilities in threat recognition accuracy in addition to their scalability features and computational speed along with data presentation quality. The proposed study uses bipolar fuzzy Einstein prioritized operators together with MCDM to create an automated classification system for these tools. The assessment of cybersecurity threats requires methods beyond traditional fuzzy approaches because intuitionistic and Pythagorean fuzzy sets cannot handle uncertainty along with hesitation in related security evaluations. The proposed methodology strengthens decision processes by using BF logic to process security parameters with effectiveness in dealing with positive and negative aspects. The research findings present an organized method for organizations to choose appropriate AI-driven cybersecurity visualization tools. The improved decision accuracy supported by our method helps protect organizations against cyber-attacks and optimize their large data security analytics operations.

In the future, we aim to expand this work to various other mathematical structures such as bipolar complex fuzzy soft set [29], multi-objective optimization model [30] and complex fuzzy rough set [31].

References

[1] W.R. Zhang: Bipolar fuzzy sets and relations: a computational framework for cognitive

modeling and multiagent decision analysis. *Proceedings of the First International Joint Conference of the North American Fuzzy Information Processing Society*, (1994), 305–309. DOI: 10.1109/IJCF.1994.375115

[2] A.B. Azim, A. Ali, A.S. Khan, F.A. Awwad, S. Ali and E.A. Ismail: Aggregation operators based on Einstein averaging under q-spherical fuzzy rough sets and their applications in navigation systems for automatic cars. *Heliyon*, **10**(15), (2024). DOI: 10.1016/j.heliyon.2024.e34698

[3] R. Verma and B. Sharma: Intuitionistic fuzzy Einstein prioritized weighted average operators and their application to multiple attribute group decision making. *Applied Mathematics and Information Sciences*, **9**(6), (2015), 3095. DOI: 10.12785/amis/090639

[4] C. Ying, W. Slamu and C. Ying: Multi-attribute decision making with Einstein aggregation operators in complex Q-rung orthopair fuzzy hypersoft environments. *Entropy*, **24**(10), (2022), 1494. DOI: 10.3390/e24101494

[5] E.P. Galla, S.K. Rajaram, G.K. Patra, C. Madhavram and J. Rao: AI-driven threat detection: leveraging big data for advanced cybersecurity compliance. *SSRN Electronic Journal*, (2022). DOI: 10.2139/ssrn.4980649

[6] M.A. Ameedeen, R.A. Hamid, T.H. Aldhyani, L.A.K.M. Al-Nassr, S.O. Olatunji and P. Subramanian: A framework for automated big data analytics in cybersecurity threat detection. *Mesopotamian Journal of Big Data*, **2024**, (2024), 175–184. DOI: 10.58496/MJBD/2024/012

[7] A. Wickramasinghe: An evaluation of big data-driven artificial intelligence algorithms for automated cybersecurity risk assessment and mitigation. *International Journal of Cybersecurity Risk Management, Forensics, and Compliance*, **7**(12), (2023), 1–15.

[8] P.C.R. Chinta, K.M. Jha, V.Velaga, C. Moore, K. Routhu and G. Sadaram: Harnessing big data and AI-driven ERP systems to enhance cybersecurity resilience in real-time threat environments. *SSRN Electronic Journal*, (2024). DOI: 10.2139/ssrn.5151788

[9] P. Maharjan: The role of artificial intelligence-driven big data analytics in strengthening cybersecurity frameworks for critical infrastructure. *Global Research Perspectives on Cybersecurity Governance, Policy, and Management*, **7**(11), (2023), 12–25.

[10] C. Moore: AI-powered big data and ERP systems for autonomous detection of cybersecurity vulnerabilities. *Nanotechnology Perceptions*, **19**, (2023), 46–64.

[11] K.D.O. Ofoegbu, O.S. Osundare, C.S. Ike, O.G. Fakeyede and A.B. Ige: Real-time cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. *Computer Science and IT Research Journal*, **4**(3), (2024). DOI: 10.51594/csitrj.v4i3.1500

[12] P. Ashfin: AI-driven threat detection and response in cybersecurity. *Bulletin of Engineering Science and Technology*, **1**(2), (2024), 125–143.

[13] K. Fernando: A multidimensional framework for utilizing big data analytics and AI in strengthening digital forensics and cybersecurity investigations. *International Journal of Cybersecurity Risk Management, Forensics, and Compliance*, **7**(12), (2023), 16–30.

[14] M.H. Alsulami: An AI-driven model to enhance sustainability for the detection of cyber threats in IoT environments. *Sensors*, **24**(22), (2024), 7179. DOI: 10.3390/s24227179

[15] O. Boutkhoum, M. Hanine, T. Agouti and A. Tikniouine: A decision-making approach based on fuzzy AHP–TOPSIS methodology for selecting the appropriate cloud solution to manage big data projects. *International Journal of System Assurance Engineering and Management*, **8**, (2017), 1237–1253. DOI: 10.1007/s13198-017-0592-x

[16] F. Alassery, A. Alzahrani, A.I. Khan, K. Sharma, M. Ahmad and R.A. Khan: Evaluating security of big data through fuzzy-based decision-making technique. *Computer Systems Science and Engineering*, **44**(1), (2023), 859–872. DOI: 10.32604/csse.2023.025796

[17] S.G. Bhol: Applications of multi-criteria decision-making methods in cyber security. *Cyber-Physical Systems Security*, (2025), 233–258. DOI: 10.1007/978-981-97-5734-3_11

[18] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B.K. Gupta and R.A. Khan: Analyzing the big data security through a unified decision-making approach. *Intelligent Automation and Soft Computing*, **32**(12), (2022). DOI: 10.32604/iasc.2022.022569

[19] A. Mardani, E.K. Zavadskas, H. Fujita and M. Köppen: Big data-driven large-scale group decision-making under uncertainty (BiGDM-U). *Applied Intelligence*, **52**(12), (2022), 13341–13344. DOI: 10.1007/s10489-022-04113-y

[20] A. Hussain, J. Chun and M. Khan: A novel multicriteria decision-making approach for precise decision making under a fuzzy environment. *Soft Computing*, **25**(7), (2021), 5645–5661. DOI: 10.1007/s00500-020-05561-9

[21] R.R. Kumar, S. Mishra and C. Kumar: Prioritizing the solution of cloud service selection using integrated MCDM methods under fuzzy environment. *The Journal of Supercomputing*, **73**, (2017), 4652–4682. DOI: 10.1007/s11227-017-2039-1

[22] J. Falak, M. Kunjan, D. Nagaraju and S. Narayanan: Evaluation of continuous improvement techniques using hybrid MCDM technique under fuzzy environment. *Materials Today: Proceedings*, **22**, (2020), 1295–1305. DOI: 10.1016/j.matpr.2020.01.422

[23] H.M. Wang Chen, S.Y. Chou, Q.D. Luu and T.H.K. Yu: A fuzzy MCDM approach for green supplier selection from the economic and environmental aspects. *Mathematical Problems in Engineering*, **2016**(1), (2016), 8097386. DOI: 10.1155/2016/8097386

[24] M.S. Ali Khan, S. Abdullah and A. Ali: Multiattribute group decision-making based on Pythagorean fuzzy Einstein prioritized aggregation operators. *International Journal of Intelligent Systems*, **34**(5), (2019), 1001–1033. DOI: 10.1002/int.22084

[25] M. Riaz, H.M. Athar Farid, H. Kalsoom, D. Pamučar and Y.M. Chu: A robust q-rung orthopair fuzzy Einstein prioritized aggregation operators with application towards MCGDM. *Symmetry*, **12**(6), (2020), 1058. DOI: 10.3390/sym12061058

[26] F. Jin, Z. Ni and H. Chen: Interval-valued hesitant fuzzy Einstein prioritized aggregation operators and their applications to multi-attribute group decision making. *Soft Computing*, **20**, (2016), 1863–1878. DOI: 10.1007/s00500-015-1887-y

[27] H. Garg, T. Mahmood, U. ur Rehman and G.N. Nguyen: Multi-attribute decision-making approach based on Aczel–Alsina power aggregation operators under bipolar fuzzy information and its application to quantum computing. *Alexandria Engineering Journal*, **82** (2023), 248–259. DOI: 10.1016/j.aej.2023.09.073

[28] K. Menger: Statistical metrics. *Proceedings of the National Academy of Sciences of the United States of America*, **28**(12), (1942), 535.

[29] A. Jaleel: 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), (2022), 67–95.

[30] S. Dhruv, R. Arora, S. Arora and S.A. Edalatpanah: A fully intuitionistic fuzzy multi-objective linear fractional fixed charge optimization model for sustainable transportation planning in the sugar-mill industry. *Archives of Control Sciences*, **35**, (2025), 455–483. DOI: 10.24425/acs.2025.156307

[31] M. Albaity, U. ur Rehman and T. Mahmood: Data source selection for integration in data sciences via complex hesitant fuzzy rough multi-attribute decision-making method. *IEEE Access*, **12**, (2024), 110146–110159. DOI: 10.1109/ACCESS.2024.3439359