Neutrosophic Sets and Systems, Vol. 58, 2023
University of New Mexico

Neutrosophic Intelligence Approach Safeguarding Patient Data in Blockchain-based Smart Healthcare

Jamal A Alenizi[1] and Ibrahim Alrashdi[2*]
[1,2]Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka 2014, Saudi Arabia
*Correspondence: irrashdi@ju.edu.sa

Abstract: In the ever-evolving landscape of blockchain-based smart healthcare, ensuring the security and integrity of patient data stands as an utmost priority. This paper is dedicated to unveiling the pivotal role of Neutrosophic sets theory within our methodology as we tackle the multifaceted challenges of safeguarding patient data. Central to our approach is the innovative integration of Neutrosophic sets theory, a mathematical framework adept at handling the inherent uncertainties and imprecisions often encountered in healthcare decision-making. Leveraging Neutrosophic sets, we construct a comprehensive evaluation model that accommodates the complexities of the smart healthcare environment. Our methodology harnesses Multi-Criteria Decision Making (MCDM) techniques, notably the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), to systematically assess and rank service providers based on their proximity to ideal solutions. The Neutrosophic aspect comes to the forefront as we apply Neutrosophic sets in representing and managing decision-makers' judgments, which often exhibit varying degrees of truth, indeterminacy, and falsity. Furthermore, the Ordered Weighted Averaging (OWA) operator is strategically employed to aggregate these Neutrosophic judgments, accentuating the role of Neutrosophic sets in our decision fusion process. Our empirical study, firmly rooted in Neutrosophic sets theory, showcases the efficacy of this innovative model. It offers a structured and robust framework for healthcare organizations to fortify patient data security in the realm of blockchain-based smart healthcare systems. This paper advances the understanding of the indispensable role played by Neutrosophic sets in enhancing data security, thereby facilitating the adoption of blockchain technology within healthcare, while contributing to the burgeoning field of Neutrosophic Intelligence.
.

Keywords: Neutrosophic Intelligence; Blockchain Technology; Smart Healthcare; Data Privacy; Trustworthiness, Confidentiality, Neutrosophic Sets.

1. Introduction

Neutrosophic sets, a mathematical framework introduced by Smarandache in 1995, have gained significant attention in recent years due to their unique ability to model and manage uncertainty, vagueness, and imprecision. This innovative concept extends traditional set theory by accommodating indeterminate elements—those elements whose membership, non-membership, and neutral status are all concurrently possible within a set [1]. Such inherent flexibility makes Neutrosophic sets a powerful tool for capturing and quantifying complex, real-world phenomena, particularly in decision-making processes. The core premise of Neutrosophic sets is rooted in the notion of "neutrality," signifying the coexistence of opposites within a set. This neutrality allows for the representation of incomplete, vague, or conflicting information, mirroring the inherent ambiguity frequently encountered in various domains, including healthcare [2].

In the context of blockchain-based smart healthcare, where the security and privacy of patient data are paramount, Neutrosophic sets emerge as a promising solution to address the inherent uncertainties that permeate this dynamic environment. Blockchain technology, known for its transparency and immutability, has transformed the healthcare sector by offering secure and decentralized data storage and management. However, the adoption of blockchain in healthcare introduces multifaceted uncertainties, including fluctuating regulatory landscapes, evolving technological challenges, and variable patient data requirements [3-5]. Neutrosophic sets offer a means to navigate these complexities effectively. By enabling the representation of vague or imprecise data within the blockchain, healthcare stakeholders can make informed decisions, even when faced with incomplete or conflicting information. For instance, patient consent, a critical component of healthcare data management, often exhibits varying degrees of consent, uncertainty, or ambiguity. Neutrosophic sets can elegantly capture and quantify these nuanced consent dynamics, facilitating more accurate decision-making [6-7]. Moreover, within the realm of Multi-Criteria Decision Making (MCDM) for evaluating service providers, Neutrosophic sets provide a structured framework to handle the diverse judgments of experts. Decision-makers' assessments, often characterized by differing degrees of truth, falsity, and indeterminacy, can be systematically integrated, allowing for a more holistic evaluation [8-9].

This paper introduces a pioneering Neutrosophic Intelligence approach, placing Neutrosophic sets theory at the forefront of our methodology. Neutrosophic sets provide a mathematical foundation capable of handling the inherent uncertainties, vagueness, and imprecisions often encountered in healthcare decision-making. As the healthcare industry navigates the complexities of blockchain technology, the integration of Neutrosophic sets theory emerges as a powerful means to enhance patient data security and privacy. Our work revolves around the utilization of MCDM techniques, particularly the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), to systematically evaluate and rank service providers within blockchain-based smart healthcare systems. However, what sets our methodology apart is the pervasive role of Neutrosophic sets in the representation and management of decision-makers' judgments. These judgments inherently possess varying degrees of truth, indeterminacy, and falsity, a challenge that Neutrosophic sets adeptly address. Furthermore, we employ the Ordered Weighted Averaging (OWA) operator to aggregate these Neutrosophic judgments, emphasizing the integral role of Neutrosophic sets in our decision fusion process. Through this approach, we strive to provide a structured and robust framework for healthcare organizations to fortify patient data security while embracing the potential of blockchain technology in smart healthcare [10].

Our paper is organized as follows: In Section 2, we provide a comprehensive review of related work in the fields of healthcare data security, blockchain technology, and Neutrosophic Intelligence, highlighting the current state of research and identifying the gaps that motivate our study. Section 3 outlines our methodology, detailing the Neutrosophic Intelligence approach we have developed for safeguarding patient data within blockchain-based smart healthcare systems. In Section 4, we present the results of our empirical evaluation and provide a thorough analysis of the data collected during our study. Section 5 offers a discussion of our findings, emphasizing their implications for healthcare data security, privacy, and the broader adoption of blockchain in healthcare. In Section 6, we conclude our research, summarizing the key insights and contributions of our study.

2. Related Works

This section provides a comprehensive overview of the existing research and literature relevant to our study, setting the stage for the development of a neutrosophic approach for anomaly detection in smart agriculture systems using edge intelligence. Yaqoob et al. [11] conducted a comprehensive review of skin cancer detection and classification using federated learning, emphasizing the importance of privacy in healthcare applications. Their work highlights the relevance of advanced machine-learning techniques in medical contexts, which resonates with our exploration of anomaly detection in smart agriculture. Alaba et al. [12] explored the security applications and challenges of smart contracts, which is an area of interest when considering the secure execution of algorithms, especially in edge computing environments. Their insights into the security aspects of smart contracts provide valuable context for our work. Kumar et al. [13] presented an approach to region-of-interest detection in COVID-19 CT images using neutrosophic logic. While their focus is on medical imaging, their utilization of neutrosophic logic is relevant to our proposed methodology, as it demonstrates the applicability of this logic in image analysis and pattern recognition. Thillaigovindan et al. [14] developed an integrated model for heart disease prediction using cryptographic and machine learning methods. Their work showcases the potential benefits of integrating different technologies for enhanced accuracy and security, which aligns with our approach to integrating edge intelligence and neutrosophic logic. Saha et al. [15] discussed AI-enabled human and machine activity monitoring in industrial IoT systems. Their exploration of AI in the context of IoT is relevant to our study, as it highlights the broader implications of AI and edge computing in monitoring and managing complex systems. Fernandez-Vazquez et al. [16] investigated the use of blockchain in sustainable supply chain management, applying analytical hierarchical process (AHP) methodology. Their work demonstrates the versatility of blockchain technology, which can be considered in the context of data security and integrity in smart agriculture systems. Mohammed et al. [17] proposed a Bitcoin network-based anonymity and privacy model for metaverse implementation in Industry 5.0. Their research touches upon privacy and security concerns in decentralized systems, which can provide insights into securing data in agricultural edge environments. Singh et al. [18] discussed transfer fuzzy learning for security in industrial IoT, which can be relevant to our study's focus on secure anomaly detection. Their work showcases advanced cryptographic techniques that can be considered in securing edge devices. Morhaim [19] provided a comprehensive overview of blockchain and cryptocurrency technologies. While not focused on agriculture, this reference offers foundational knowledge about blockchain technology, which can be useful when discussing potential applications in the context of smart agriculture systems.

3. Methodology

In this section, we elucidate the rigorous methodology employed in our study, outlining the systematic steps undertaken to develop and implement our Neutrosophic Intelligence approach for safeguarding patient data in the context of blockchain-based smart healthcare systems. In this section, we elucidate the systematic methodology employed to comprehensively assess the performance of blockchain technology as a fundamental safeguard for patient data within blockchain-based smart healthcare systems. The integration of blockchain technology in healthcare settings is driven by a multitude of factors and challenges by various complexities. To shed light on this intricate landscape, our study integrates expert surveys to construct a holistic understanding of blockchain technology's impact on patient data security in smart healthcare environments. We specifically focus on the perspectives of industry experts, decision-makers, and stakeholders, who offer valuable insights into the drivers, barriers, and risks associated with

blockchain implementation. It is important to note that the opinions of decision-makers and experts are inherently diverse and may lack clear consensus, reflecting the multifaceted nature of this field. Therefore, our study places a particular emphasis on the decision-making processes that underpin the safeguarding of patient data within blockchain-based smart healthcare, categorizing them according to three critical dependent factors.

Stakeholder Proficiency and Attitudes

a. Decision-Maker Expertise: In the context of smart healthcare, decision-maker expertise is crucial for understanding the intricacies of integrating blockchain technology. Their familiarity with healthcare data security, blockchain protocols, and the nuances of smart healthcare systems can significantly impact the success of implementation. Expertise allows decision-makers to make informed choices, anticipate potential challenges, and devise strategies for maximizing the benefits of blockchain.
b. Risk Appetite: Smart healthcare introduces innovative approaches to patient care through technologies like IoT devices, AI-driven diagnostics, and telemedicine. Decision-makers' risk appetite plays a critical role in adopting blockchain, as it often involves a departure from conventional data security methods. Embracing blockchain may require a willingness to accept initial uncertainties and invest in new technologies that promise long-term security and efficiency gains.
c. Organizational Culture: The culture within healthcare institutions can either facilitate or hinder the integration of blockchain. An organizational culture that values innovation, collaboration, and a patient-centric approach is more likely to embrace the changes brought about by smart healthcare and the implementation of blockchain for enhanced patient data security. Conversely, a resistant or risk-averse culture may present challenges to adoption.

Environmental Conditions

a. Regulatory Landscape: Smart healthcare operates within a complex regulatory environment that varies by region. Decision-makers must navigate these regulations to ensure compliance when implementing blockchain solutions. A supportive regulatory landscape can encourage blockchain adoption by providing clear guidelines for data security and patient privacy in smart healthcare.
b. Technological Infrastructure: The readiness of the technological infrastructure in smart healthcare settings is essential. Decision-makers need to assess whether the existing IT infrastructure can seamlessly integrate with blockchain. Compatibility with electronic health record (EHR) systems, IoT devices, and other smart healthcare components is critical for successful implementation.
c. Industry Collaboration: Collaboration within the healthcare industry and with blockchain solution providers can foster innovation in smart healthcare. Decision-makers must evaluate the extent to which partnerships and collaborations can accelerate the adoption of blockchain for patient data security. Partnerships may involve healthcare providers, technology companies, research institutions, and regulatory bodies working together to develop standards and best practices.

Multiple Criteria and Alternatives (MCDM)

a. Evaluation Criteria: Decision-makers in smart healthcare need to define and prioritize evaluation criteria. These criteria may include data privacy, scalability, cost-effectiveness, interoperability with IoT devices, and the ability to ensure data integrity in real time. The selection of these criteria influences the decision-making process.

b. Alternative Solutions: Decision-makers should consider a spectrum of alternatives alongside blockchain. This might encompass traditional data security methods, cloud-based solutions, or hybrid approaches. Evaluating the strengths and weaknesses of each alternative helps decision-makers make well-informed choices aligned with smart healthcare goals.
c. Decision-Making Methodology: Formal decision-making methodologies, such as Multi-Criteria Decision Analysis (MCDA) or Analytic Hierarchy Process (AHP), can aid decision-makers in systematically evaluating criteria and alternatives. These methodologies provide a structured approach to assessing the suitability of blockchain and other options, ensuring that the final choice aligns with the unique requirements of smart healthcare.

Incorporating these considerations into the decision-making process for implementing blockchain in smart healthcare ensures a comprehensive approach that accounts for the complexities and nuances of this evolving field. By addressing personality conditions, environmental conditions, and multiple criteria and alternatives, decision-makers can navigate the dynamic landscape of smart healthcare to enhance patient data security effectively.

In our work, we adopted a comprehensive approach to collect and aggregate specialists' perspectives on the adoption of blockchain technology for safeguarding patient data in smart healthcare environments. The data collection process involved a series of discussions, meetings, and qualitative discrete choice experiments [19], which allowed us to capture a diverse range of decision-making experts' insights and opinions. To aggregate the experts' perspectives effectively, we employed the OWA [20], a method that enables the combination of individual expert viewpoints into a consensus representation. This approach helps mitigate potential biases and ensures a more comprehensive assessment of criteria and alternatives relevant to our research. Furthermore, we applied the MCDM method to analyze the decision-makers' perspectives on criteria and alternatives. MCDM provides a structured framework for evaluating and prioritizing multiple criteria and alternatives, aiding in the systematic assessment of the suitability of blockchain technology for patient data security in smart healthcare. To assess the robustness and reliability of our results, we conducted a Monte Carlo simulation. This simulation involved iteratively generating random variations in the input parameters and evaluating their impact on the decision outcomes.

The process of aggregating the specialists' perspectives was executed using the OWA operator, which serves as a valuable tool to harmonize the diverse judgments of decision-making experts and mitigate the impact of inconsistent assessments. To elaborate on its application, let's consider a scenario involving q specialists, denoted as $D_1, D_2, \dots, D_q$, participating in a decision-making problem. Each expert's viewpoint contributes to the overall decision process, with $1 \leq k \leq q$ representing the index of each expert. The OWA operator is employed to calculate a consensus outcome by considering the ordered weights assigned to individual experts' judgments. Specifically, it follows a defined formula that systematically combines these perspectives, considering their relative importance: Figure 1 shows the steps of the proposed method.

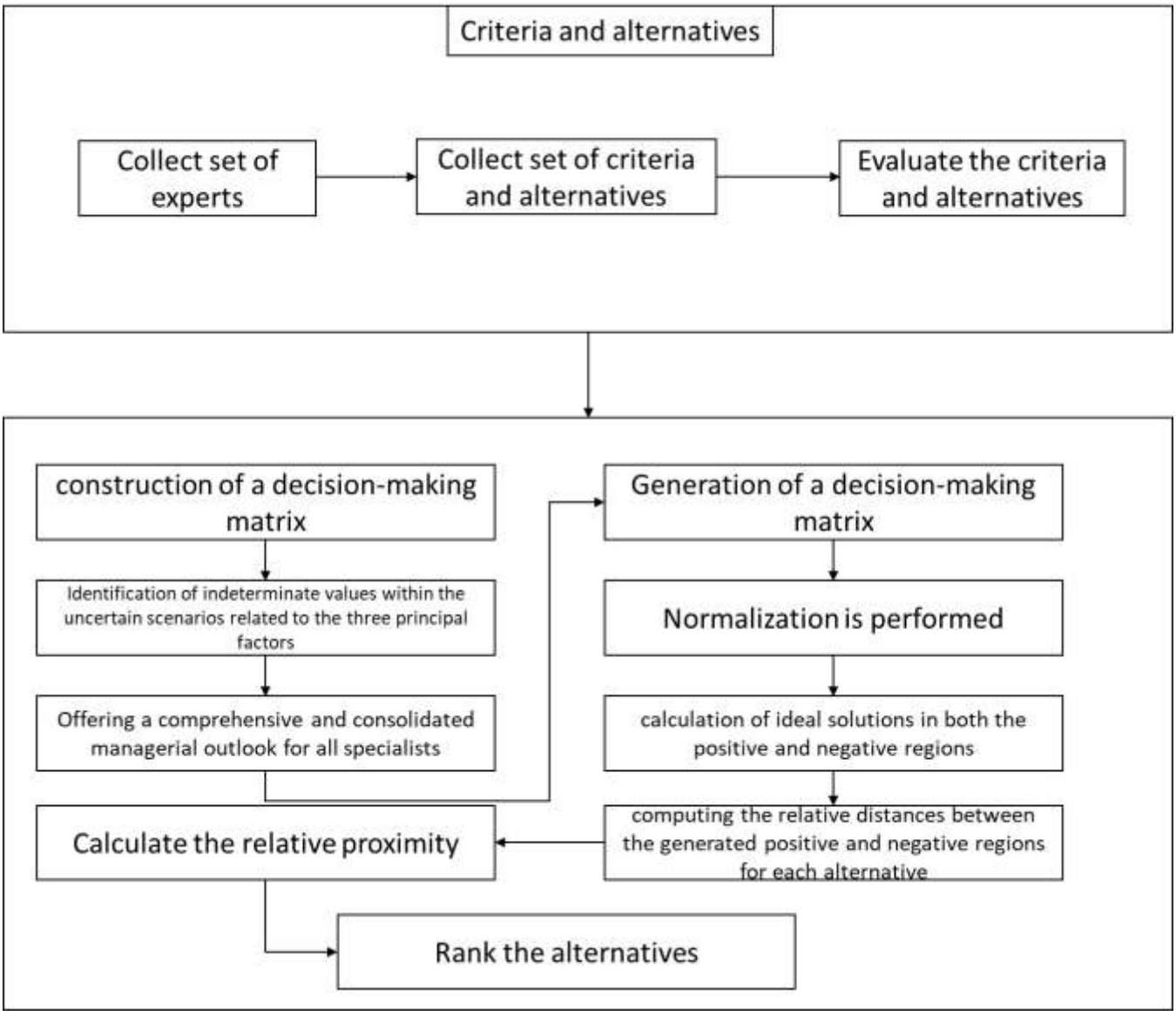

Figure 1. The steps of the proposed method.

Some definitions show the mathematical operations of triangular neutrosophic numbers.

***Definition* 1**

The truth, indeterminacy, and falsity membership functions can be computed as:

$$T_X(y) = \begin{cases} \alpha\left(\frac{y - x_1}{y_2 - y_1}\right) & (x_1 \le y \le x_2) \\ \alpha \quad (y = x\_2) \\ \alpha\left(\frac{x_3 - y}{y_3 - y_2}\right) & (x_2 \le y \le x_3) \\ 0 \quad otherwise \end{cases} \tag{1}$$

$$I_X(y) = \begin{cases} \left(\frac{x_{2-y+\theta-(y-x_1)}}{y_2 - y_1}\right) & (x_1 \le y \le x_2) \\ \theta \quad (y = x\_2) \\ \left(\frac{y_{-x_2+\theta-(x_3-y)}}{y_3 - y_2}\right) & (x_2 \le y \le x_3) \\ 0 \quad otherwise \end{cases} \tag{2}$$

$$F_X(y) = \begin{cases} \left(\frac{x_{2-y+\beta-(y-x_1)}}{y_2 - y_1}\right) & (x_1 \le y \le x_2) \\ \beta \quad (y = x\_2) \\ \left(\frac{y_{-x_2+\beta-(x_3-y)}}{y_3 - y_2}\right) & (x_2 \le y \le x_3) \\ 0 \quad otherwise \end{cases} \tag{3}$$

***Definition* 2**

The arithmetic operations can be computed as:

$let\ x =< (x_1, x_2, x_3); \alpha_x, \theta_x, \beta_x >, z =< (z_1, z_2, z_3); \alpha_z, \theta_z, \beta_z >$

$$x \oplus z =< (x_1 + z_1, x_2 + z_2, x_3 + z_3\ ); \alpha_x \wedge \alpha_z, \theta_x \vee \theta_z, \beta_x \vee \beta_z > \tag{4}$$

$$x \ominus z =< (x_1 - z_1, x_2 - z_2, x_3 - z_3\ ); \alpha_x \wedge \alpha_z, \theta_x \vee \theta_z, \beta_x \vee \beta_z > \tag{5}$$

$$x \otimes z = \begin{cases} < (x_1 z_1, x_2 z_2, x_3 z_3); \alpha_x \wedge \alpha_z, \theta_x \vee \theta_z, \beta_x \vee \beta_z, > if\ (x_3 > 0, z_3 > 0) \\ < (x_1 z_3, x_2 z_2, x_3 z_1); \alpha_x \wedge \alpha_z, \theta_x \vee \theta_z, \beta_x \vee \beta_z, > if\ (x_3 < 0, z_3 > 0) \\ < (x_3 z_3, x_2 z_2, x_3 z_3); \alpha_x \wedge \alpha_z, \theta_x \vee \theta_z, \beta_x \vee \beta_z, > if\ (x_3 > 0, z_3 < 0) \end{cases} \tag{6}$$

$$x \oslash z = \begin{cases} < \left(\frac{x_1}{z_3}, \frac{x_2}{z_2}, \frac{x_3}{z_1}\right); \alpha_x \wedge \alpha_z, \theta_x \vee \theta_z, \beta_x \vee \beta_z > if\ (x_3 > 0, z_3 > 0) \\ < \left(\frac{x_3}{z_3}, \frac{x_2}{z_2}, \frac{x_1}{z_1}\right); \alpha_x \wedge \alpha_z, \theta_x \vee \theta_z, \beta_x \vee \beta_z, > if\ (x_3 < 0, z_3 > 0) \\ < \left(\frac{x_3}{z_1}, \frac{x_2}{z_2}, \frac{x_1}{z_3}\right); \alpha_x \wedge \alpha_z, \theta_x \vee \theta_z, \beta_x \vee \beta_z, > if\ (x_3 > 0, z_3 < 0) \end{cases} \tag{7}$$

$$\curlyvee \oslash x = \begin{cases} < \left(\frac{x_1}{\curlyvee}, \frac{x_2}{\curlyvee}, \frac{x_3}{\curlyvee}\right); \alpha_x, \theta_x, \beta_x if\ \curlyvee > 0 > \\ < \left(\frac{x_3}{\curlyvee}, \frac{x_2}{\curlyvee}, \frac{x_1}{\curlyvee}\right); \alpha_x, \theta_x, \beta_x if\ \curlyvee < 0 > \end{cases} \tag{8}$$

$$x^{-1} =< \left(\frac{1}{x_3}, \frac{1}{x_2}, \frac{1}{x_1}\right); \alpha_x, \theta_x, \beta_x > \tag{9}$$

Step 1 involves the construction of a decision-making matrix, denoted as DM_{ij}^K, to represent the viewpoints of experts (indexed as D_k) and model their perspectives regarding blockchain technology as criteria. The DM_{ij}^K matrix adopts a neutrosophic triangular scale [2] for its structure, and its definition is as follows [6]:

$$DM_{ij}^{K} = \begin{matrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{matrix} \begin{bmatrix} x_{11}^{k} & x_{12}^{k} & \dots & x_{1m}^{k} \\ x_{21}^{k} & x_{22}^{k} & \dots & x_{2m}^{k} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1}^{k} & x_{n2}^{k} & \dots & x_{nm}^{k} \end{bmatrix} \quad (10)$$

In the above formula, the x_{ij}^{k} denote the performance ranking of the constituent of the $i-th$ criterion regarding $f_1, f_2, \dots, f_n$. it is worth noting that the category of x_{ij}^{k} symbolizes the viewpoint of experts based on the neutrosophic scale.

Step 2 involves the identification of indeterminate values within the uncertain scenarios related to the three principal factors. During this step, the neutrosophic scale can be transformed into tangible numerical values using the score function outlined in [18]. The resultant values for the de-neutrosophic specialists' viewpoint matrix, denoted as DM_{ij}^{K}, are presented in as follows:

$$DM_{ij}^{K} = \begin{matrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{matrix} \begin{bmatrix} x_{11}^{k} & x_{12}^{k} & \dots & x_{1m}^{k} \\ x_{21}^{k} & x_{22}^{k} & \dots & x_{2m}^{k} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1}^{k} & x_{n2}^{k} & \dots & x_{nm}^{k} \end{bmatrix} \quad (11)$$

Step 3 involves offering a comprehensive and consolidated managerial outlook for all specialists, indexed as k = 1, 2, …, q, using the DM_{ij} matrix in conjunction with OWA operators. The resulting outcome is then presented in Form (3) as follows:

$$DM_{ij} = \begin{matrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{matrix} \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{bmatrix} \quad (12)$$

Then, the TOPSIS method, which stands for Technique for Order Preference by Similarity to Ideal Solution, is applied to order potential alternatives based on the generation of principle solutions. In our case, let's consider a situation in which, we have p substitutions denoted as $O_1, O_2, \dots, O_p$, and these substitutes are evaluated across m criteria represented as $x_1, x_2, \dots, x_m$. Moreover, there are q experts participating in this decision-making endeavor, as previously mentioned. To facilitate this process, we utilize a weighting vector consisting of $w_1, w_2, \dots, w_m$ for the m criteria, following the condition $1 \leq j \leq m$. These weights, denoted as w_j, satisfy the conditions $w_j \geq 0$, and their sum $\sum_{j=1}^{m} w_j = 1$.

Step 4 involves the generation of a decision-making matrix denoted as Y_{rt}^{K}. This matrix is designed to capture the viewpoints of experts indexed as D_k regarding blockchain solutions as criteria and their impact on smart healthcare systems. The Y_{rt}^{K} matrix, presented in Form 6, is subsequently transformed into a numerical format through the application of the score function as expressed below:

$$Y_{rt}^{K} = \begin{matrix} O_1 \\ O_2 \\ \vdots \\ O_p \end{matrix} \begin{bmatrix} y_{11}^{k} & y_{12}^{k} & \dots & y_{1m}^{k} \\ y_{21}^{k} & y_{22}^{k} & \dots & y_{2m}^{k} \\ \vdots & \vdots & \vdots & \vdots \\ y_{p1}^{k} & y_{p2}^{k} & \dots & y_{pm}^{k} \end{bmatrix} \quad (13)$$

The consolidation of judgments from decision-makers is accomplished as follows:

$$y_{rt} = \frac{\sum_{t=1}^{m} (y_{rt}^{k})}{D_q} \quad (14)$$

Here, y_{rt} denotes the evaluations provided by decision-makers for the alternatives, and D_q signifies the count of decision-makers involved in the process. The resulting outcome is expressed as follows:

$$Y_{rt} = \begin{matrix} O_1 \\ O_2 \\ \vdots \\ O_p \end{matrix} \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1m} \\ y_{21} & y_{22} & \cdots & y_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ y_{p1} & y_{p2} & \cdots & y_{pm} \end{bmatrix} \tag{15}$$

TOPSIS is structured around three fundamental steps to aid in decision-making:

Normalization: In the first step, normalization is performed to standardize the data. This step ensures that all the criteria are on the same scale and avoids biases that could result from the use of different units or measurement scales. By normalizing the data, TOPSIS makes it possible to directly compare the importance of various criteria, regardless of their original units or magnitudes. This step transforms the raw data into a format that can be uniformly analyzed, which is essential for effective multi-criteria decision-making.

$$z_{rt} = w_j * \frac{y_{r\ t}}{\sqrt{\sum_{t=1}^{m} x_{rt}^2}}; r = 1,2,3 \dots p; t = 1,2,3 \dots m \tag{16}$$

Calculating the Ideal Solution in Positive and Negative Regions: The second step involves the calculation of ideal solutions in both the positive and negative regions. The ideal solutions represent the best possible outcomes based on the selected criteria. In the positive region, the ideal solution is characterized by having the highest values for beneficial criteria and the lowest values for non-beneficial criteria. Conversely, in the negative region, the ideal solution has the lowest values for beneficial criteria and the highest values for non-beneficial criteria. By identifying these ideal solutions, TOPSIS establishes a reference point for evaluating and ranking the alternatives.

$$z_t^+ = \begin{Bmatrix} \langle \max(z_{rt} | r = 1,2, \dots, p) \, | j \in j^+ \rangle, \\ \langle \min(z_{rt} | r = 1,2, \dots, p) \, | j \in \ j^- \rangle \end{Bmatrix} \tag{17}$$

$$z_t^- = \begin{Bmatrix} \langle \min(z_{rt} | r = 1,2, \dots, p) \, | j \in j^+ \rangle, \\ \langle \max(z_{rt} | r = 1,2, \dots, p) \, | j \in j^- \rangle \end{Bmatrix} \tag{18}$$

Computing the Relative Distances between the Generated Positive and Negative Regions: The third step focuses on computing the relative distances between the generated positive and negative regions for each alternative. This distance calculation is performed to determine how closely each alternative aligns with the ideal solutions. Alternatives that are closer to the positive ideal solution and farther from the negative ideal solution are considered more favorable and receive higher rankings. Conversely, alternatives that are closer to the negative ideal solution and farther from the positive ideal solution are considered less desirable and receive lower rankings.

$$d_r^+ = \sqrt{\sum_{t=1}^{m} (z_{rt} - z_t^+)^2}, r = 1,2, \dots, p \tag{19}$$

$$d_r^- = \sqrt{\sum_{t=1}^{m} (z_{rt} - z_t^-)^2}, r = 1,2, \dots, p \tag{20}$$

Finally, we calculate the relative proximity by combining the positive and negative regions of the solutions to attain the ideal solutions, as outlined below:

$$c_r = \frac{d_r^-}{d_r^+ + d_r^-}; r = 1,2, \dots, p \quad (21)$$

4. Results and Analysis

This section delves into the pivotal phase of our research, where we present the results of our Neutrosophic Intelligence approach in action and offer a comprehensive analysis of the data obtained during our study. Through meticulous experimentation and evaluation, we assess the performance, security, and adaptability of our approach within the complex landscape of blockchain-based smart healthcare systems. To substantiate the practical applicability of our proposed model for safeguarding healthcare patient data, we conducted an empirical study encompassing a comprehensive case study analysis. The chosen case study revolves around the evaluation of fifteen critical criteria for the security of healthcare patient data, as outlined in Table 1.

Table 1. Criteria for Patient Data Security in Healthcare Systems

Group	Criteria	ID	Description
Drivers	Regulatory Compliance	D1	The extent of compliance with data privacy regulations (e.g., HIPAA, GDPR)
	Technology Adoption	D2	The level of adoption of advanced security technologies (e.g., blockchain, encryption)
	Interoperability	D3	The ability of systems to communicate and share data securely
	Cybersecurity Training	D4	The level of training provided to staff and employees on cybersecurity best practices
	Patient Engagement	D5	The degree to which patients actively participate in maintaining the security of their health data
Barriers	Legacy Systems	B1	The presence of outdated legacy systems that lack modern security features
	Budget Constraints	B2	Financial limitations that hinder investments in robust cybersecurity measures
	Resistance to Change	B3	Organizational resistance to adopting new security protocols and technologies
	Third-party Vulnerabilities	B4	Risks associated with reliance on third-party vendors and service providers
	Data Volume and Complexity	B5	The challenges posed by growing volumes and complexity of patient data, requiring scalable solutions
Risks	Data Breach Risk	R1	Likelihood and potential impact of data breaches, including unauthorized exposure of patient data
	Malware and Ransomware Risk	R2	Risk associated with malware and ransomware attacks that can compromise or encrypt patient data
	Insider Threat Risk	R3	Risk of insider threats, including employees mishandling data intentionally or unintentionally
	IoT Vulnerabilities	R4	Vulnerabilities introduced by the use of IoT devices in healthcare, which can be exploited
	Regulatory Non-compliance Risk	R5	The risk of failing to comply with data privacy regulations, leading to penalties and legal consequences

To comprehensively assess the security of patient data within healthcare systems, we conducted an illuminating case study that drew upon the aforementioned fifteen criteria, categorized into three pivotal groups: Driver Criteria, Barrier Criteria, and Risk Criteria. The case study unfolded within the dynamic landscape of a modern healthcare institution, where the critical importance of patient data security is magnified. Leveraging a multidisciplinary team of experts, we embarked on a meticulous examination of the organization's data security ecosystem. This encompassed evaluating the impact of regulatory compliance, technology adoption, and patient engagement as drivers that underpin a robust data security framework. Simultaneously, we scrutinized the hurdles posed by legacy systems, budget constraints, and resistance to change as barriers that often necessitate strategic solutions. Moreover, we probed the intricacies of data breach risks, malware vulnerabilities, insider threats, IoT-related concerns, and the looming specter of regulatory non-compliance as formidable risks to be mitigated. By systematically evaluating these criteria, we aim to identify vulnerabilities, strengths, and opportunities for improving data security. The case study involves interviews with key stakeholders, a thorough examination of existing security measures, and the application of our proposed model to assess the overall data security posture.

In this section, we leveraged the OWA operator to systematically aggregate the perspectives and evaluations of experts. To maintain transparency and consistency in our analysis, we adopted predefined weights for the OWA operator, as detailed in Table 2. These weights were thoughtfully determined to reflect the relative importance of various criteria within the decision-making process.

Table 2. Predefined Weights for OWA Operator

Criteria	**Weights**
Regulatory Compliance	0.217744
Technology Adoption	0.304067
Interoperability	0.251275
Cybersecurity Training	0.288399
Patient Engagement	0.186048
Legacy Systems	0.146608
Budget Constraints	0.229047
Resistance to Change	0.224132
Third-party Vulnerabilities	0.237017
Data Volume and Complexity	0.084615
Data Breach Risk	0.171464
Malware and Ransomware Risk	0.144085
Insider Threat Risk	0.147436
IoT Vulnerabilities	0.112711
Regulatory Non-compliance Risk	0.222641

We present the outcomes of the decision-making process, which were meticulously generated using the OWA operator. To achieve this, we harnessed the collective expertise of our decision-makers, each of whom provided valuable insights and evaluations across a spectrum of criteria. The OWA operator, guided by predefined weights as detailed in Table 3, played a pivotal role in harmonizing these diverse perspectives and aggregating them into a coherent whole. This process facilitated the creation of OWA general and aggregated decision-makers decisions, offering a holistic view of the evaluation outcomes. These

judgments reflect the consensus reached by our expert panel, embodying their collective wisdom and expertise in assessing the critical aspects of patient data security within the healthcare system.

Table 3. The ultimate matrix produced employs OWA for the evaluation of decision-maker judgments regarding driver, barrier, and risk criteria

	D_1	**D2**	**D3**	**D4**	**D5**	**B1**	**B2**	**B3**	**B4**	**B5**	**R1**	**R2**	**R3**	**R4**	**R5**
D1	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877	0.32877
D2	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401	0.36401
D3	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230	0.26230
D4	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992	0.34992
D5	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303	0.40303
B1	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105	0.28105
B2	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335	0.22335
B3	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423	0.23423
B4	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997	0.13997
B5	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324	0.24324
R1	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704	0.21704
R2	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627	0.07627
R3	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483	0.13483
R4	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613	0.21613
R5	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277	0.04277

5. Discussion and implications

In this pivotal section, we embark on a thoughtful examination of the results presented in the preceding section and delve into their broader significance. Our discussion transcends the numerical findings, focusing on the qualitative insights, the implications of our Neutrosophic Intelligence approach, and the potentially transformative effects on the landscape of healthcare data security within blockchain-based smart healthcare systems.

To facilitate decision-making in uncertain conditions, our case study incorporates the use of the TOPSIS methodology. This method was applied to assess and rank five distinct service providers operating within the realm of blockchain-based smart healthcare systems. These service providers were meticulously evaluated based on the predefined weights assigned to the criteria established in our study. To maintain confidentiality and impartiality, we have anonymized these providers, referring to them as "Alternative A," "Alternative B," "Alternative C," Alternative D." and "Alternative E.". To ensure a comprehensive analysis, we employed a triangular neutrosophic scale to collect the judgments of our decision-makers. This scale effectively captures the nuances and uncertainties inherent in decision-making processes, allowing our experts to express their evaluations with precision. Subsequently, these neutrosophic judgments were transformed into numerical values, which served as the foundation for our TOPSIS-based assessments. This robust approach allowed us to methodically evaluate the service providers' performance across various criteria while accommodating the inherent complexities of real-world decision-making in the context of blockchain-based smart healthcare systems.

The ultimate ranking of the alternatives, derived from the TOPSIS analysis based on their relative closeness to the ideal solutions, has been methodically compiled and is presented in Table 4. This table serves as a comprehensive summary of our evaluation process, showcasing the performance of each alternative in comparison to the others. The relative closeness values in Table 4 provide valuable insights into how well each alternative aligns with the predefined ideal solutions, which were carefully determined following the specified criteria. Alternatives that exhibit higher relative closeness values are positioned at the top of the ranking, indicating their superior alignment with the ideal solutions across the considered criteria. Conversely, those with lower relative closeness values are situated lower in the ranking, reflecting comparatively weaker performance in meeting the specified criteria. This ranking, displayed in Table 4, offers a clear and concise visualization of the outcomes of our analysis, enabling stakeholders and decision-makers to make informed choices based on the relative strengths and weaknesses of each alternative within the context of blockchain-based smart healthcare systems. It serves as a valuable reference point for identifying the most suitable service providers for specific healthcare scenarios and requirements.

Table 4. Results of Alternatives Based on Relative Closeness to Ideal Solutions

	d_r^+	d_r^-	c_r
Alternative A	0.251449	0.298566	0.817441
Alternative B	0.137375	0.189318	0.719279
Alternative C	0.103608	0.086685	0.458436
Alternative D	0.169257	0.16279	0.558562
Alternative C	0.288908	0.282441	0.678213

The findings of this research carry profound implications for the healthcare industry and its ongoing transformation towards blockchain-based smart healthcare systems. By developing a Neutrosophic Intelligence approach and integrating it with established decision-making methodologies, this study contributes significantly to the enhancement of patient data security. As blockchain technology gains prominence in healthcare, our model empowers decision-makers with a robust framework to navigate the complexities of this dynamic landscape. The ability to rank service providers objectively based on a multitude of criteria, while accounting for uncertainty, offers healthcare organizations a vital tool to strengthen their data security strategies. This, in turn, can bolster patient trust, facilitate data sharing among healthcare providers, and pave the way for more efficient and secure healthcare services.

Beyond its immediate applications, our research underscores the potential for Neutrosophic Intelligence to stimulate innovation and adaptation within healthcare and other data-sensitive domains. The successful integration of Neutrosophic theory with established decision-making techniques opens doors to novel approaches for handling uncertainty and ambiguity. By embracing this paradigm, organizations can better address the ever-evolving challenges in safeguarding sensitive data. Moreover, our study encourages further exploration of Neutrosophic Intelligence's applicability in diverse contexts where decision-making involves intricate, multifaceted criteria. As healthcare and technology continue to evolve, the principles and methodologies advanced in this research may find broader utility in addressing complex problems, fostering resilience in decision-making, and shaping a more secure and efficient future for various industries.

6. Conclusions

This study presents a novel Neutrosophic Intelligence approach that leverages advanced methodologies like OWA and TOPSIS to address the intricate challenge of safeguarding patient data in blockchain-based smart healthcare systems. By integrating the insights and evaluations of decision-makers across a spectrum of driver, barrier, and risk criteria, we have formulated a comprehensive framework that enhances decision-making in uncertain conditions. The results demonstrate the effectiveness of our approach in systematically assessing and ranking service providers, ultimately aiding in the selection of the most suitable alternatives. Furthermore, the study underscores the significance of factors such as regulatory compliance, technology adoption, and data breach risk in shaping the security landscape of healthcare systems. As the smart healthcare ecosystem continues to evolve, our research offers valuable guidance for stakeholders, enabling them to make informed choices and fortify patient data security in an increasingly dynamic and technology-driven healthcare landscape.

In light of the ever-expanding role of blockchain technology in healthcare, our findings emphasize the pivotal importance of adopting advanced security measures and fostering a culture of data privacy. We conclude by highlighting the potential of Neutrosophic Intelligence as a robust decision-making tool in smart healthcare, not only for patient data security but also for addressing broader challenges in this transformative field. As the healthcare industry continues to embrace innovation, our research provides a significant step toward ensuring the confidentiality, integrity, and availability of patient data, ultimately enhancing the quality and safety of healthcare services for all.

Data Availability: All data generated or analyzed during this study are included in this article.

Acknowledgment: The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

Conflict of Interest: The authors declare no conflict of interest.

References

[1]. Khalaf, Osamah Ibrahim, Rajesh Natarajan, Natesh Mahadev, Prasanna Ranjith Christodoss, Thangarasu Nainan, Carlos Andrés Tavera Romero, and Ghaida Muttashar Abdulsahib. 2022. “Blinder Oaxaca and Wilk Neutrosophic Fuzzy Set-Based IoT Sensor Communication for Remote Healthcare Analysis.” IEEE Access.

[2]. Ranulfo Paiva Barbosa (Sobrinho), & Smarandache, F. (2023). Pura Vida Neutrosophic Algebra. Neutrosophic Systems with Applications, 9, 101–106. https://doi.org/10.61356/j.nswa.2023.68

[3]. Kumar, Ravinder, Ritu Rana, and Sunil Kumar Jha. 2023. "Scalable Blockchain Architecture of Internet of Medical Things (IoMT) for Indian Smart Healthcare System." In AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications, 231–59. Springer.

[4]. Mishra, Arunodaya Raj, Pratibha Rani, Adel Fahad Alrasheedi, and Rajeev Dwivedi. 2023. "Evaluating the Blockchain-Based Healthcare Supply Chain Using Interval-Valued Pythagorean Fuzzy Entropy-Based Decision Support System." Engineering Applications of Artificial Intelligence 126: 107112.

[5]. Binti Rosli , S. N. I., & Bin Zulkifly , M. I. E. (2023). A Neutrosophic Approach for B-Spline Curve by Using Interpolation Method. Neutrosophic Systems with Applications, 9, 29–40. https://doi.org/10.61356/j.nswa.2023.43

[6]. Aiden, Manpreet Kaur, Shweta Mayor Sabharwal, Sonia Chhabra, and Mustafa Al-Asadi. 2023. "AI and Blockchain for Cyber Security in Cyber-Physical System." In AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications, 203–30. Springer.

[7]. Abdel-Monem, Ahmed, and Mohamed Abouhawwash. 2022. "A Machine Learning Solution for Securing the Internet of Things Infrastructures". Sustainable Machine Intelligence Journal 1 (October). https://doi.org/10.61185/SMIJ.HPAO9103.

[8]. Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta. 2023. "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0." Infrastructures 8 (2): 22.

[9]. M.Ali , A., & Abdelhafeez , A. (2022). DeepHAR-Net: A Novel Machine Intelligence Approach for Human Activity Recognition from Inertial Sensors. Sustainable Machine Intelligence Journal, 1. https://doi.org/10.61185/SMIJ.2022.8463

[10]. Panja, Subir, Arup Kumar Chattopadhyay, Amitava Nag, and Jyoti Prakash Singh. 2023. "Fuzzy-Logic-Based IoMT Framework for COVID19 Patient Monitoring." Computers & Industrial Engineering 176: 108941.

[11]. Yaqoob, Muhammad Mateen, Musleh Alsulami, Muhammad Amir Khan, Deafallah Alsadie, Abdul Khader Jilani Saudagar, Mohammed AlKhathami, and Umar Farooq Khattak. 2023. "Symmetry in Privacy-Based Healthcare: A Review of Skin Cancer Detection and Classification Using Federated Learning." Symmetry 15 (7): 1369.

[12]. Alaba, Fadele Ayotunde, Hakeem Adewale Sulaimon, Madu Ifeyinwa Marisa, and Owamoyo Najeem. 2024. "Smart Contracts Security Application and Challenges: A Review." Cloud Computing and Data Science, 15–41.

[13]. Kumar, S N, A Lenin Fred, L R Jonisha Miriam, Ajay Kumar, Parasuraman Padmanabhan, and Balazs Gulyas. 2021. "19 Region of Interest Detection in COVID-19 CT Images Using Neutrosophic Logic." Health Informatics and Technological Solutions for Coronavirus (COVID-19), 19.

[14]. Thillaigovindan, Senthil Kumar, and others. 2023. "An Integrated Accurate-Secure Heart Disease Prediction (IAS) Model Using Cryptographic and Machine Learning Methods." KSII Transactions on Internet \& Information Systems 17 (2).

[15]. Saha, Anindita, Jayita Saha, Manjarini Mallik, and Chandreyee Chowdhury. 2023. "AI Enabled Human and Machine Activity Monitoring in Industrial IoT Systems." In AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications, 29–54. Springer.

[16]. Fernandez-Vazquez, Simon, Rafael Rosillo, David la Fuente, and Javier Puente. 2022. "Blockchain in Sustainable Supply Chain Management: An Application of the Analytical Hierarchical Process (AHP) Methodology." Business Process Management Journal 28 (5/6): 1277–1300.

[17]. Mohammed, Z K, A A Zaidan, H B Aris, Hassan A Alsattar, Sarah Qahtan, Muhammet Deveci, and Dursun Delen. 2023. "Bitcoin Network-Based Anonymity and Privacy Model for Metaverse Implementation in Industry 5.0 Using Linear Diophantine Fuzzy Sets." Annals of Operations Research, 1–41.

[18]. Singh, Anamika, Rajesh Kumar Dhanaraj, Md Akkas Ali, Prasanalakshmi Balaji, and Meshal Alharbi. 2023. "Transfer Fuzzy Learning Enabled Streebog Cryptographic Substitution Permutation Based Zero Trust Security in IIOT." Alexandria Engineering Journal 81: 449–59.

[19]. Morhaim, Lisa. 2019. Blockchain and Cryptocurrencies Technologies and Network Structures: Applications, Implications and Beyond. Infinite Study.

[20]. Sudeep Dey, & Gautam Chandra Ray. (2023). Covering Properties via Neutrosophic b-open Sets. Neutrosophic Systems with Applications, 9, 1–12. https://doi.org/10.61356/j.nswa.2023.66.

Received: April 13, 2023. Accepted: Sep 19, 2023