Multicriteria Algorithms with Applications

Journal Homepage: sciencesforce.com/mawa

SCIENCES FORCE
International Academic Publisher

Multicriteria Algo. Appl. Vol. 4 (2024) 53–68

Paper Type: Original Article

Intervention of Innovative Technologies for Eradicating Tampering in Digital Forensics: Practicing Intelligent Decision Methodologies

Asmaa Elsayed [1,*] and Bilal Arain [2]

[1] Faculty of computers and informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt; aa.ahmed023@eng.zu.edu.eg.

[2] Department of Computer Engineering, University of Sharjah, Sharjah, United Arab Emirates; barain@sharjah.ac.ae.

Received: 31 Jan 2024 **Revised:** 25 May 2024 **Accepted:** 27 Jun 2024 **Published:** 30 Jun 2024

Abstract

The Industrial Internet of Things (IIoT) is one of the popular technologies of Industry 4.0. This technology involves of advanced equipment such as sensors, machines, and analytics platforms in industrial settings. The utilized equipment has been harnessed to improve efficiency, productivity, and safety. IIoT forensics is a specialized field of digital forensics that deals with the investigation of IIoT devices. In terms of digital forensics, there are several open challenges, including the need for more effective data acquisition techniques, the need for better tools and techniques for analyzing IIoT data, and the need for more research on the legal and ethical implications of IIoT forensics. However, the increasing use of IIoT devices and systems is presenting new challenges, including data security, privacy, and safety. These challenges became an incentive for the inclusion of Blockchain technology (BCT) which is considered one of the most famous Industry 4.0 technologies in securing data and transactions. Wherein, BCT offers a solution to some IIoT security challenges, including data integrity, authentication, access control, confidentiality, transparency, scalability, resilience, and provenance. Hence, leveraging BCT in ambiances where tampering is prevalent, and counterfeiting has become imperative. In this light, BCT can be used in digital forensics due to its ability to construct a transparent environment that is characterized by decentralized and immutable in the event of safety accidents or cyber-attacks. Without a doubt, in such an environment, selecting and utilizing an adequate BC application for preventing any data alteration unless there is consensus on that is important. Accordingly, this matter is considered the catalyst in this paper for constructing a robust intelligent appraiser model for appraising the available nominates of BC applications. In the context of selecting and implementing a blockchain-based digital forensic scheme within the IIoT communication architecture, the techniques of Multi-Criteria Decision Making (MCDM) are considered a strong contributor. Wherein these techniques can help balance various criteria that preferences amongst BC applications are based on. Hence, Entropy and Additive Ratio Assessment (ARAS) are contributing to constructing the proposed intelligent appraiser model as techniques of MCDM. As well these techniques are working under the authority of Type-2 neturosophic numbers (T2NN) which are considered one of the popular members of Neutrosophic uncertainty theory.

Keywords: Blockchain, Industrial Internet of Things, IIoT, Forensics, Multi-Criteria Decision Making, Type-2 Neturosophic Numbers.

Corresponding Author: aa.ahmed023@eng.zu.edu.eg

https://doi.org/10.61356/j.mawa.2024.4322

1 | Introduction

The Industrial Internet of Things (IIoT) is crucial to the fourth industrial revolution. The IIoT refers to integrating advanced sensors, machines, and analytics platforms in industrial settings to improve efficiency, productivity, and safety [1]. In the fourth industrial revolution 4.0 context, the IIoT is integral to transforming cyber-physical systems and production processes with big data and analytics [2]. This connectivity allows for data collection, exchange, and analysis, potentially facilitating improvements in productivity, efficiency, and other economic benefits [3]. IIoT applications include predictive maintenance, remote monitoring and control, asset tracking, and process automation [4]. These applications rely on collecting and analyzing large volumes of data from various sources, including sensors, machines, and other devices, then analyzing and exchanging data in real- time, enabling organizations to make informed decisions and optimize their operations [5]. IIoT devices are increasingly used in various industries, generating vast amounts of data that can be crucial in digital investigations [6].

IIoT forensics is a specialized field of digital forensics investigating IIoT devices [7]. In digital forensics, there are several open challenges, including the need for more effective data acquisition techniques, better tools and techniques for analyzing IIoT data, and more research on the legal and ethical implications of IIoT forensics [8]. However, the increasing use of IIoT devices and systems presents new challenges, including data security, privacy, and safety [9]. Blockchain technology can address some of the critical security challenges faced by IIoT, such as data integrity, authentication, access control, confidentiality, transparency, scalability, resilience, and provenance [10]. Blockchain is a decentralized ledger technology operating on a peer-to-peer network, distributing data across multiple nodes. It is known for its unparalleled security, transparency, and immutability [11]. Integrating blockchain technology with IIoT is a promising concept that can revolutionize industries' operations. This can be achieved through various strategies such as developing custom blockchain solutions, optimizing scalability and speed, ensuring interoperability with existing systems, implementing intelligent contracts efficiently, enhancing data privacy, and implementing robust security protocols [12]. By using blockchain, IIoT devices can securely transmit and store data, ensuring that the data is tamper-proof and transparent. This can be particularly useful in manufacturing, logistics, and energy industries, where data integrity and security are critical [13]. However, it also presents challenges such as scalability, interoperability, data privacy, and real-time processing [14].

Blockchain technology can address data integrity and authentication challenges in IIoT by providing a decentralized and secure platform for data storage and sharing [15]. In a blockchain-based system, data is stored in a distributed ledger maintained by multiple network nodes [16]. Each block in the chain contains a cryptographic hash of the previous block, creating a tamper-evident chain of blocks. This ensures data integrity, as any modification to the data would change the hash value, making it easy to detect tampering attempts [17]. In digital forensics, blockchain technology can create a transparent record of evidence collection, analysis, and preservation. This is particularly useful in IIoT environments, where the integrity of data and evidence is crucial [18]. By leveraging blockchain's decentralized and immutable nature, digital forensics investigators can ensure that evidence is collected, analyzed, and stored securely and transparently. This can help to prevent tampering, alteration, or deletion of evidence, which is critical in maintaining the integrity of digital forensic investigations [19]. As such, there is a growing need for robust and secure digital forensics solutions to ensure the integrity and reliability of digital evidence in the event of safety accidents or cyber-attacks. Nan Xiao et al. proposed a novel blockchain-based digital forensics framework to address these challenges by providing a tamper-proof, non-repudiable, and permanent storage of digital forensic data, enabling effective investigation and responsibility determination in the event of safety accidents in IIoT environments [14].

MCDM methods evaluate and prioritize multiple competing criteria to aid decision-making processes [20]. In implementing a blockchain-based digital forensic scheme within the IIoT communication architecture, MCDM methods balance security, scalability, interoperability, cost, and compliance. In this paper, we use the hybrid T2NN-Entropy-ARAS MCDM method that combines the Type-2 neutrosophic numbers (T2NN) technique with the Entropy method and the Additive Ratio Assessment (ARAS) method. The T2NN is a type of neutrosophic number that handles uncertainty and imprecision in decision-making [22]. The Entropy method is an objective MCDM method that uses the concept of Entropy to determine the weights of criteria [24]. The ARAS method is an MCDM method that uses an additive ratio to evaluate and prioritize alternatives [25]. The T2NN-Entropy-ARAS method evaluates and prioritizes blockchain-based digital forensic schemes within IIoT communication architecture based on integrity, immutability, decentralization, and security criteria.

The motivation is to address the growing need for secure digital forensics in IIoT using blockchain technology. The aim is to develop a comprehensive framework that ensures the integrity and reliability of digital evidence in IIoT environments. Additionally, this framework will include a decision-making tool to evaluate and prioritize blockchain-based digital forensic schemes. The paper contributes to the field of IIoT and digital forensics by:

- Investigating the integration of blockchain technology with IIoT to address security and integrity challenges in digital forensics.
- Applying a novel blockchain-based digital forensics framework for IIoT environments.
- Developing a hybrid MCDM method using T2NN, Entropy, and ARAS to evaluate and prioritize blockchain-based digital forensic schemes in IIoT communication architectures.

This paper is organized as follows: Section 2 provides a comprehensive review of the literature on IIoT security, blockchain technology, and digital forensics. It also introduces the MCDM methods used in the paper. Section 3 describes the T2NN-Entropy-ARAS method for evaluating and prioritizing blockchain-based digital forensics. Section 4 presents a case scenario of a safety accident in an IIoT environment and describes how the proposed blockchain-based digital forensics framework can be used to ensure the integrity and reliability of digital evidence. Section 5 applies the T2NN-Entropy-ARAS method to the case scenario and presents a sensitivity and comparative analysis of the results. Section 6 summarizes the findings of the paper and also discusses the implications and limitations of the proposed blockchain-based digital forensics framework.

2 |Literature Review

In this paper, the surveyed literature is divided into three parts. The first part reviews existing studies that explore the application of blockchain technology in IIoT environments. The second part reviews existing studies that utilize the T2NN method in MCDM applications. The third part reviews existing studies that utilize the Entropy and ARAS methods in MCDM applications.

2.1 |Related Studies about IIoT and Blockchain

Blockchain technology can provide a secure and decentralized platform for data storage, sharing, and authentication in IIoT systems, addressing specific security challenges such as data integrity and authentication [11]. Dawei Li et. al, discusses a blockchain-based authentication framework for IIoT devices using Physical Unclonable Functions (PUFs) to ensure the security of data sources [27]. Libo Feng et al. discuss a cross-domain authentication method for the IIoT that combines blockchain technology with a certificateless signature scheme [10]. Yi Li et al. discuss the importance of security provisioning in IIoT, the role of blockchain technology in ensuring trust and transparency, and the concept of digital twins in Industry 4.0 [11]. Feng Zhang et al. present a blockchain-based cloud-edge-end framework and design a trust mechanism based on blockchain consensus for AI-enabled IoT systems [12]. In [21], the Best-Worst Multi-criteria Decision-Making Method (BWM) and the Compromise Ranking Method (VIKOR) is combined for workflow scheduling to handle priority tasks for fault tolerance in IIOT. The scholars in [27] presented a security analysis of IoT systems using digital forensic incident response (DFIR) and discuss the role of DFIR in securing industrial control systems (ICS), cyber-physical systems (CPS), and SCADA systems. Victor R.

Kebande et al. provide a systematic review of digital forensics in the context of IIoT and discuss the challenges and opportunities of digital forensics in IIoT environments [28].

2.2 | Literature of MCDM using T2NN

Mohamed Abdel-Basset et al. proposed the T2NN method and defined some of its operational rules. The T2NN can accurately describe real cognitive information in the decision-making process [22]. Neutrosophic set theory is an extension of fuzzy set theory that deals with incomplete, indeterminate, and inconsistent information. T2NN further extends this concept to handle uncertainty at a deeper level, making it suitable for decision-making in complex and uncertain environments [23]. T2NN can be used in MCDM models to handle uncertain and incomplete information [29]. A T2NN is defined as a set of three membership functions: Truth (T), Indeterminacy (I), and Falsity (F), which are used to represent the degree of truth, indeterminacy, and falsity of a statement, respectively [22]. Pritpal Singh discusses a type-2 neutrosophic-entropy-fusion-based multiple thresholding method for brain tumor tissue structure segmentation [30]. Muhammet Deveci uses T2NN with multi-attributive border approximation area comparison (MABAC) method for offshore wind farm site selection in the USA [29]. Vladimir Simić et al. use T2NN with the ITARA-EDAS model to evaluate sustainable route selection of petroleum transportation [31]. Zeyuan Wang et al. proposes a Type-2 neutrosophic number with modified TODIM for green supplier selection [32].

2.3 | Entropy and ARAS methods

These MCDM methods can be used to solve complex decision-making problems with multiple criteria and alternatives [33]. Entropy is one of the most used methods in decision-making processes to calculate the objective weights of criteria [24]. The method quantifies the uncertainty or disorder within a system [34]. The idea is that a criterion with high entropy (i.e., high uncertainty) is less important, while a criterion with low entropy (i.e., low uncertainty) is more important [35]. After determining the weight for each criterion, another MCDM method is applied to rank alternatives based on these weights. The ARAS method assesses the performance of each alternative in decision-making by calculating the ratio of its weighted sum of the favorable and the weighted sum of non-favorable aspects [25]. This ratio is then used to rank the alternatives [36]. It's a useful tool in decision-making scenarios where there are multiple options and criteria to consider. Note that some literature uses entrpy-ARAS method in different ways. Also, [20] proposed entropy and ARAS for the site selection of a hydroponic geothermal greenhouse. Mishra et al. use the fuzzy ARAS method based on entropy [37]. Shankha Shubhra Goswami et al. implemented the entropy-ARAS for the selection of best engineering materials [38].

3 | Research Methodology

For the sake of brevity, the research methodology is divided into two parts. The first part explains some basic concepts and definitions of T2NN. The second part introduces the hybrid method used to evaluate blockchain-based digital forensics.

3.1 | Preliminaries

Definition 1 [22]. Consider that Z is a limited universe of discourse, and F [0,1] is the set of all triangular neutrosophic numbers on F [0,1].

A Type 2 neutrosophic number set (T2NNS) $\widetilde{U}$ in Z is represented by:

$$\widetilde{U} = \left\langle \left(T_{T_{\widetilde{U}}}(z), T_{I_{\widetilde{U}}}(z), T_{F_{\widetilde{U}}}(z)\right), \left(I_{T_{\widetilde{U}}}(z), I_{I_{\widetilde{U}}}(z), I_{F_{\widetilde{U}}}(z)\right), \left(F_{T_{\widetilde{U}}}(z), F_{I_{\widetilde{U}}}(z), F_{F_{\widetilde{U}}}(z)\right) \right\rangle \tag{1}$$

Where $\check{T}_{\breve{U}}(z) : Z \rightarrow F[0,1]$, $\tilde{I}_{\breve{U}}(z) : Z \rightarrow F[0,1]$, $\check{F}_{\breve{U}}(z) : Z \rightarrow F[0,1]$.

The type -2 neutrosophic number set $\check{T}_{\widetilde{U}}(z) = \left(T_{T_{\widetilde{U}}}(z), T_{I_{\widetilde{U}}}(z), T_{F_{\widetilde{U}}}(z)\right)$, $\tilde{I}_{\widetilde{U}}(z) = \left(I_{T_{\widetilde{U}}}(z), I_{I_{\widetilde{U}}}(z), I_{F_{\widetilde{U}}}(z)\right)$, $\check{F}_{\widetilde{U}}(z) = \left(F_{T_{\widetilde{U}}}(z), F_{I_{\widetilde{U}}}(z), F_{F_{\widetilde{U}}}(z)\right)$ defined as the truth, indeterminacy and falsity member-ships of z in $\widetilde{U}$ respectively.

Definition 2 [22]. Let

$\widetilde{U} = \left\langle \left(T_{T_{\widetilde{U}}}(z), T_{I_{\widetilde{U}}}(z), T_{F_{\widetilde{U}}}(z)\right), \left(I_{T_{\widetilde{U}}}(z), I_{I_{\widetilde{U}}}(z), I_{F_{\widetilde{U}}}(z)\right), \left(F_{T_{\widetilde{U}}}(z), F_{I_{\widetilde{U}}}(z), F_{F_{\widetilde{U}}}(z)\right) \right\rangle$,

$\widetilde{U}_1 = \left\langle \left(T_{T_{\widetilde{U}_1}}(z), T_{I_{\widetilde{U1}}}(z), T_{F_{\widetilde{U1}}}(z)\right), \left(I_{T_{\widetilde{U1}}}(z), I_{I_{\widetilde{U1}}}(z), I_{F_{\widetilde{U1}}}(z)\right), \left(F_{T_{\widetilde{U1}}}(z), F_{I_{\widetilde{U1}}}(z), F_{F_{\widetilde{U1}}}(z)\right) \right\rangle$ and

$\widetilde{U}_2 = \left\langle \left(T_{T_{\widetilde{U}_2}}(z), T_{I_{\widetilde{U}_2}}(z), T_{F_{\widetilde{U2}}}(z)\right), \left(I_{T_{\widetilde{U2}}}(z), I_{I_{\widetilde{U2}}}(z), I_{F_{\widetilde{U2}}}(z)\right), \left(F_{T_{\widetilde{U2}}}(z), F_{I_{\widetilde{U2}}}(z), F_{F_{\widetilde{U}_2}}(z)\right) \right\rangle$ by three T2NN and $\lambda > 0$. Their operations are defined as follow:

- **T2NN Addition:**

$$\widetilde{U}_1 \oplus \widetilde{U}_2 = \left\langle \begin{array}{c} \begin{pmatrix} T_{T_{\widetilde{U}_1}}(z) + T_{T_{\widetilde{U}_2}}(z) - T_{T_{\widetilde{U_1}}}(z).T_{T_{\widetilde{U}2}}(z),\ T_{I_{\widetilde{U1}}}(z) + T_{I_{\widetilde{U2}}}(z) - T_{I_{\widetilde{U1}}}(z).T_{I_{\widetilde{U2}}}(z), \\ T_{F_{\widetilde{U1}}}(z) + T_{F_{\widetilde{U2}}}(z) - T_{F_{\widetilde{U1}}}(z).T_{F_{\widetilde{U2}}}(z) \end{pmatrix}, \\ \left(I_{T_{\widetilde{U1}}}(z).I_{T_{\widetilde{U2}}}(z), I_{I_{\widetilde{U1}}}(z).I_{I_{\widetilde{U2}}}(z), I_{F_{\widetilde{U1}}}(z).I_{F_{\widetilde{U2}}}(z)\right), \\ \left(F_{T_{\widetilde{U1}}}(z).F_{T_{\widetilde{U2}}}(z), F_{I_{\widetilde{U1}}}(z).F_{I_{\widetilde{U2}}}(z), F_{F_{\widetilde{U1}}}(z).F_{F_2}(z)\right) \end{array} \right\rangle \quad (2)$$

- **T2NN Multiplication:**

$\widetilde{U}_1 \otimes \widetilde{U}_2 =$

$$\left\langle \begin{array}{c} \left(\left(T_{T_{\widetilde{U}_1}}(z).T_{T_{\widetilde{U}_2}}(z), T_{I_{\widetilde{U1}}}(z).T_{I_{\widetilde{U2}}}(z), T_{F_{\widetilde{U1}}}(z).T_{F_{\widetilde{U2}}}(z)\right)\right), \\ \left(\left(I_{T_{\widetilde{U1}}}(z) + I_{T_{\widetilde{U2}}}(z) - I_{T_{\widetilde{U1}}}(z).I_{T_{\widetilde{U2}}}(z)\right), \left(I_{I_{\widetilde{U1}}}(z) + I_{I_{\widetilde{U2}}}(z) - I_{I_{\widetilde{U1}}}(z).I_{I_{\widetilde{U2}}}(z)\right), \begin{pmatrix} I_{F_{\widetilde{U1}}}(z) + I_{F_{\widetilde{U2}}}(z) - \\ I_{F_{\widetilde{U1}}}(z).I_{F_{\widetilde{U2}}}(z) \end{pmatrix}\right) \\ \left(\left(F_{T_{\widetilde{U1}}}(z) + F_{T_{\widetilde{U2}}}(z) - F_{T_{\widetilde{U1}}}(z).F_{T_{\widetilde{U2}}}(z)\right), \left(F_{I_{\widetilde{U1}}}(z) + F_{I_{\widetilde{U2}}}(z) - F_{I_{\widetilde{U1}}}(z).F_{I_{\widetilde{U2}}}(z)\right), \begin{pmatrix} F_{F_{\widetilde{U1}}}(z) + F_{F_2}(z) - \\ F_{F_{\widetilde{U1}}}(z).F_{F_2}(z) \end{pmatrix}\right) \end{array} \right\rangle \quad (3)$$

- **Scaler function:**

$$\lambda\widetilde{U} = ((1 - (1- T_{T_{\widetilde{U}}}(z))^{\lambda}, 1 - (1 - T_{I_{\widetilde{U}}}(z))^{\lambda}, 1 - \left(1 - T_{F_{\widetilde{U}}}(z)\right)^{\lambda}),$$

$$(\ (I_{T_{\widetilde{U}}}(z))^{\lambda}, I_{I_{\widetilde{U}}}(z))^{\lambda}, I_{F_{\widetilde{U}}}(z))^{\lambda}\ ), (F_{T_{\widetilde{U}}}(z))^{\lambda}, F_{I_{\widetilde{U}}}(z))^{\lambda}, F_{F_{\widetilde{U}}}(z))^{\lambda})) \quad (4)$$

Definition 3 [22].

Suppose that $\widetilde{U_s} =$

$\left\langle \left(T_{T_{\widetilde{U}s}}(z), T_{I_{\widetilde{U}s}}(z), T_{F_{\widetilde{U}s}}(z)\right), \left(I_{T_{\widetilde{U}s}}(z), I_{I_{\widetilde{U}s}}(z), I_{F_{\widetilde{U}s}}(z)\right), \left(F_{T_{\widetilde{U}s}}(z), F_{I_{\widetilde{U}s}}(z), F_{F_{\widetilde{U}s}}(z)\right) \right\rangle$

Where S = 1, 2, …, m is a group of T2NNs and w = (w_1, w_2, … w_m)^T

Denotes the weight vector of them with $\mathcal{W}_j \in [0,1]$ and $\sum_{m=1}^{m} w_s = 1$ the following equation is used to calculate a Type 2 netrosophic number weighted averaging (T2NNWA) operator: $T2NNWA\left(\widetilde{U_1}, \dots\ \widetilde{U_s}, \dots, \widetilde{U_m}\right) = w_1\widetilde{U_1} \oplus w_s\widetilde{U_s} \oplus \dots .\oplus w_m\widetilde{U_m} = \oplus_{s=1}^{m}\left(w_s\widetilde{U_s}\right)$

$((1 - \prod_{s=1}^{m}(1 - T_{T_{\widetilde{U}s}}(z))^{w_s},\quad 1 - \prod_{s=1}^{m}(1 - T_{I_{\widetilde{U}s}}(z))^{w_s}, 1 - \prod_{s=1}^{m}(1 - T_{F_{\widetilde{U}s}}(z))^{w_s}),$
$\left(\prod_{s=1}^{m} I_{T_{\widetilde{U}s}}(z))^{w_s}, \prod_{s=1}^{m} I_{I_{\widetilde{U}s}}(z))^{w_s}, \prod_{s=1}^{m} I_{F_{\widetilde{U}s}}(z))^{w_s}\right),$

$$(\prod_{s=1}^{m} F_{T_{\widetilde{U}s}}(z))^{w_s}, \prod_{s=1}^{m} F_{I_{\widetilde{U}s}}(z))^{w_s}, \prod_{s=1}^{m} F_{F_{\widetilde{U}s}}(z))^{w_s})). \tag{5}$$

Definition 4 [22]. Suppose that

$\widetilde{U} = \left\langle \left(T_{T_{\widetilde{U}}}(z), T_{I_{\widetilde{U}}}(z), T_{F_{\widetilde{U}}}(z)\right), \left(I_{T_{\widetilde{U}}}(z), I_{I_{\widetilde{U}}}(z), I_{F_{\widetilde{U}}}(z)\right), \left(F_{T_{\widetilde{U}}}(z), F_{I_{\widetilde{U}}}(z), F_{F_{\widetilde{U}}}(z)\right) \right\rangle$ is T2NN

Score function is calculated as follow:

$$S(\widetilde{U}) = \frac{1}{12}\left\langle 8 + \left(T_{T_{\widetilde{U1}}}(Z) + 2\left(T_{I_{\widetilde{U1}}}(Z)\right) + T_{F_{\widetilde{U1}}}(Z)\right) - \left(I_{T_{\widetilde{U1}}}(Z) + 2\left(I_{I_{\widetilde{U1}}}(Z)\right) + I_{F_{\widetilde{U1}}}(Z)\right) - \left(F_{T_{\widetilde{U1}}}(Z) + 2\left(F_{I_{\widetilde{U1}}}(Z)\right) + F_{F_{\widetilde{U1}}}(Z)\right)\right\rangle \tag{6}$$

Table 1. T2NN linguistic variables to distinct experts.

Experiences (years)	Linguistic variables	The type 2 neutrosophic number scale
5 <	Very Bad (VB)	((0.20,0.20,0.10),(0.65,0.80,0.85),(0.45,0.80,0.70))
[5,10]	Bad (B)	((0.35,0.35,0.10),(0.50,0.75,0.80),(0.50,0.75,0.65))
[10,15]	Medium Bad (MB)	((0.50,0.30,0.50),(0.50,0.35,0.45),(0.45,0.30,0.60))
[15,20]	Medium (M)	((0.40,0.45,0.50),(0.40,0.45,0.50),(0.35,0.40,0.45))
[20,25]	Medium Good (MG)	((0.60,0.45,0.50),(0.20,0.15,0.25),(0.10,0.25,0.15))
[25,30]	Good (G)	((0.70,0.75,0.80),(0.15,0.20,0.25,),(0.10,0.15,0.20))
>= 30	Very Good (VG)	((0.95,0.90,0.95),(0.10,0.10,0.05), (0.05,0.05,0.05))

3.2 | The Hybrid T2NN-Entroy-ARAS Method

This model has two Phases. In the first one, the reputation of the experts is determined under the T2NN environment by making the trade-off between their experiences and expertise [39]. Then, in the second phase, the T2NN-Entropy-ARAS method is applied to solve the MCDM problem.

Table 2. T2NN linguistic variable for rank alternatives.

Linguistic variables	The type 2 neutrosophic number scale
Very Bad (VB)	((0.20,0.20,0.10),(0.65,0.80,0.85),(0.45,0.80,0.70))
Bad (B)	((0.35,0.35,0.10),(0.50,0.75,0.80),(0.50,0.75,0.65))
Medium Bad (MB)	((0.50,0.30,0.50),(0.50,0.35,0.45),(0.45,0.30,0.60))
Medium (M)	((0.40,0.45,0.50),(0.40,0.45,0.50),(0.35,0.40,0.45))
Medium Good (MG)	((0.60,0.45,0.50),(0.20,0.15,0.25),(0.10,0.25,0.15))
Good (G)	((0.70,0.75,0.80),(0.15,0.20,0.25,),(0.10,0.15,0.20))
Very Good (VG)	((0.95,0.90,0.95),(0.10,0.10,0.05), (0.05,0.05,0.05))

Phase 1. T2NN expert reputation rating

In this first phase, the reputation of experts is determined under the T2NN environment, which involves making a trade-off between their experiences and expertise. This is a crucial step in evaluating the credibility of the experts.

Let A = {A_1, A_2, …A_m} and a set of criteria is symbolized by C = {C_1, C_2, …, C_n}. Let decision makers = {DM_1, DM_2, … DM_k} (k≥2) be a set of decision makers group. In this phase, T2NN approach is used as follows:

Step 1.1. Construct the T2NN expert reputation matrix $\breve{U}$ as:

$$\begin{array}{cccc} & \mathrm{DM}_1 & \dots & \mathrm{DM}_2 \\ \breve{U} = & \left[\begin{matrix} \left(T_{T_{\tilde{U}_1(1)}}(z), T_{I_{\widetilde{U1}(1)}}(z), T_{F_{\widetilde{U1}(1)}}(z)\right), \\ \langle \left(I_{T_{\widetilde{U1}(1)}}(z), I_{I_{\widetilde{U1}(1)}}(z), I_{F_{\widetilde{U1}(1)}}(z)\right), \rangle \\ \left(F_{T_{\widetilde{U1}(1)}}(z), F_{I_{\widetilde{U1}(1)}}(z), F_{F_{\widetilde{U1}(1)}}(z)\right) \\ \left(T_{T_{\tilde{U}_1(2)}}(z), T_{I_{\widetilde{U1}(2)}}(z), T_{F_{\widetilde{U1}(2)}}(z)\right), \\ \langle \left(I_{T_{\widetilde{U1}(2)}}(z), I_{I_{\widetilde{U1}(2)}}(z), I_{F_{\widetilde{U1}(2)}}(z)\right), \rangle \\ \left(F_{T_{\widetilde{U1}(2)}}(z), F_{I_{\widetilde{U1}(2)}}(z), F_{F_{\widetilde{U1}(2)}}(z)\right) \end{matrix}\right. & \begin{matrix} \\ \dots \\ \\ \\ \dots \\ \\ \end{matrix} & \left.\begin{matrix} \left(T_{T_{\tilde{U}k(1)}}(z), T_{I_{\widetilde{Uk}(1)}}(z), T_{F_{\widetilde{Uk}(1)}}(z)\right), \\ \langle \left(I_{T_{\widetilde{Uk}(1)}}(z), I_{I_{\widetilde{Uk}(1)}}(z), I_{F_{\widetilde{Uk}(1)}}(z)\right), \rangle \\ \left(F_{T_{\widetilde{Uk}(1)}}(z), F_{I_{\widetilde{Uk}(1)}}(z), F_{F_{\widetilde{Uk}(1)}}(z)\right) \\ \left(T_{T_{\tilde{U}k(2)}}(z), T_{I_{\widetilde{Uk}(2)}}(z), T_{F_{\widetilde{Uk}(2)}}(z)\right), \\ \langle \left(I_{T_{\widetilde{Uk}(2)}}(z), I_{I_{\widetilde{Uk}(2)}}(z), I_{F_{\widetilde{Uk}(2)}}(z)\right), \rangle \\ \left(F_{T_{\widetilde{Uk}(2)}}(z), F_{I_{\widetilde{Uk}(2)}}(z), F_{F_{\widetilde{Uk}(2)}}(z)\right) \end{matrix}\right] \end{array} \tag{7}$$

Where$\breve{U}\,_e^{(1)} = \left(T_{T_{\tilde{U}_1(1)}}(z), T_{I_{\widetilde{U1}(1)}}(z), T_{F_{\widetilde{U1}(1)}}(z)\right), \left(I_{T_{\widetilde{U1}(1)}}(z), I_{I_{\widetilde{U1}(1)}}(z), I_{F_{\widetilde{U1}(1)}}(z)\right),$

$$\left(F_{T_{\widetilde{U1}(1)}}(z), F_{I_{\widetilde{U1}(1)}}(z), F_{F_{\widetilde{U1}(1)}}(z)\right)$$

And $\breve{U}\,_e^{(2)} = \left(T_{T_{\tilde{U}_1(2)}}(z), T_{I_{\widetilde{U1}(2)}}(z), T_{F_{\widetilde{U1}(2)}}(z)\right), \left(I_{T_{\widetilde{U1}(2)}}(z), I_{I_{\widetilde{U1}(2)}}(z), I_{F_{\widetilde{U1}(2)}}(z)\right),$

$$\left(F_{T_{\widetilde{U1}(2)}}(z), F_{I_{\widetilde{U1}(2)}}(z), F_{F_{\widetilde{U1}(2)}}(z)\right)$$

are T2NN represent the appraisal of the experiences and expertise of the experts. The T2NN linguistic terms presented in Table 1 are used to distinguish experts according to their experiences and expertise.

Step 1.2. Aggregate the reputation of the experts:

$$\breve{Q}e = T2NNWA\left(\breve{U}\,_e^{(1)}, \breve{U}\,_e^{(2)}\right) = \zeta_1 \breve{U}\,_e^{(1)} \oplus \zeta_2 \breve{U}\,_e^{(2)} = \oplus_{l=1}^{2}\left(\zeta_l \breve{U}\,_e^{(l)}\right)$$

$$((1 - \prod_{l=1}^{2}(1 - T_{T_{\tilde{U}_1(1)}}(z))^{\zeta_l}, 1 - \prod_{l=1}^{2}(1 - T_{I_{\tilde{U}_1(1)}}(z))^{\zeta_l}, 1 - \prod_{l=1}^{2}(1 - T_{F_{\tilde{U}_1(1)}}(z))^{\zeta_l}),$$
$$(\prod_{l=1}^{2} I_{T_{\tilde{U}_1(1)}}(z))^{\zeta_l}, \prod_{l=1}^{2} I_{I_{\tilde{U}_1(1)}}(z))^{\zeta_l}, \prod_{l=1}^{2} I_{F_{\tilde{U}_1(1)}}(z))^{\zeta_l}),$$
$$(\prod_{l=1}^{2} F_{T_{\tilde{U}_1(1)}}(z))^{\zeta_l}, \prod_{l=1}^{2} F_{I_{\tilde{U}_1(1)}}(z))^{\zeta_l}, \prod_{l=1}^{2} F_{F_{\tilde{U}_1(1)}}(z))^{\zeta_l})) \tag{8}$$

In this equation ζ_1, ζ_2 denotes the trade-off parameters of the reputation of the experts, where $\zeta_1, \zeta_2 \in [0,1]\ and\ \zeta_1, +\zeta_2 = 1$.

Step 1.3. Then the score function of the aggregated reputation is calculated as follows:

$$S(\widetilde{Qe}) = \frac{1}{12}\left\langle 8 + \left(T_{T_{\widetilde{Qe}}}(Z) + 2\left(T_{I_{\widetilde{Qe}}}(Z)\right) + T_{F_{\widetilde{Qe}}}(Z)\right) - \left(I_{T_{\widetilde{Qe}}}(Z) + 2\left(I_{I_{\widetilde{Qe}}}(Z)\right) + I_{F_{\widetilde{Qe}}}(Z)\right) - \left(F_{T_{\widetilde{Qe}}}(Z) + 2\left(F_{I_{\widetilde{Qe}}}(Z)\right) + F_{F_{\widetilde{Qe}}}(Z)\right)\right\rangle \tag{9}$$

Step 1.4. Determine the reputation of the experts.

$$\delta_e = \frac{\breve{Q}e}{\sum_{l=1}^{k} \breve{Q}e} \quad \text{e =1,…k} \tag{10}$$

Phase 2. T2NN-Entropy-ARAS

The T2NN-Entropy-ARAS method is applied to solve the MCDM problem. The approach takes into account the entropy in the decision-making process and uses the ARAS to rank alternatives.

Step 2.1. Build the T2NN initial decision matrix as experts express their opinions using linguistic terms in Table 2.

Step 2.2. Aggregate the T2NN decision matrix by using the T2NNWA equation and by using the reputation rate of experts that was calculated in the previous phase.

Step 2.3. The score function is used to convert the T2NN matrix into crisp numbers so decision matrix will be like that

$$\mathcal{M} = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \dots & C_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{bmatrix} \end{array}$$

Step 2.4. Normalize the decision matrix (performance indices) to obtain the feature weight $\mathcal{P}_{ij}$ for the ith alternative and jth criterion

$$\mathcal{P}_{ij} = \frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}} \qquad \text{Where } 1 \le i \ \le m \ , \ 1 \le j \ \le n \tag{11}$$

Step 2.5. The output entropy measure e_j of the jth factor

$$e_j = -k \sum_{i=1}^{m} (\mathcal{P}_{ij} \,.\ln \, \mathcal{P}_{ij}) \ \text{ where } 1 \le j \ \le n \tag{12}$$

k = $^1/_{\ln m}$

Step 2.6. Calculation of variation coefficient of jth factor e_j

$$g_j = |1 - \ e_j| \ \text{ where } 1 \le j \ \le n \tag{13}$$

Step 2.7. Calculation of objective weight of the entropy $\mathcal{W}_j$

$$\mathcal{W}_j = \frac{g_j}{\sum_{i=1}^{m} g_j} \tag{14}$$

Step 2.8. From the decision matrix select x_{0j} is the optimal value for j criteria. When the optimal value of the criteria is unknown, then

$$x_{0j} = \begin{cases} \max x_{ij} \ \ if \ the \ j \ \in B \\ \min x_{ij} \ \ if \ the \ j \ \in C \end{cases} \tag{15}$$

Step 2.9. Normalize the matrix using these two stages:

The criteria, whose preferable values are maxima, are normalized as follows:

$$\overline{\mathcal{X}_{\imath\jmath}} = \frac{x_{ij}}{\sum_{i=0}^{m} x_{ij}} \tag{16}$$

The criteria, whose preferable values are minima, are normalized by applying a two-stage procedure

$$x_{ij} = \frac{1}{x_{ij}^{*}} \ \ ; \qquad \overline{\mathcal{X}_{\imath\jmath}} = \frac{x_{ij}}{\sum_{i=0}^{m} x_{ij}} \tag{17}$$

Step 2.10. Defining the normalized-weighted matrix $\widehat{\mathcal{X}_{\imath\jmath}}$. It is possible to evaluate the criteria with weights 0 < $\mathcal{W}_j$ < 1. Normalized-weighted values of all the criteria are calculated as follows:

$$\widehat{\mathcal{X}_{\imath\jmath}} = \overline{\mathcal{X}_{\imath\jmath}} \,. \mathcal{W}_j \qquad \text{i= 0, …, m} \tag{18}$$

Step 2.11. The following task is determining values of the optimality function $\mathcal{S}_i$:

$$\mathcal{S}_i = \sum_{j=1}^{n} \widehat{\mathcal{X}_{\imath\jmath}} \qquad \text{i=0,…,m ; j=1,…m} \tag{19}$$

Step 2.12. The degree of the alternative utility is determined by a comparison of the variant, which is analyzed with the ideally best one $\mathcal{S}_0$. The equation used for the calculation of the utility degree $\mathcal{K}_i$ of an alternative ai is given below:

$$\mathcal{K}_i = \frac{\mathcal{S}_i}{\mathcal{S}_0} \quad \text{i= 0 ,…,m} \tag{20}$$

where $\mathcal{S}_i$ and $\mathcal{S}_0$ are the optimality criterion values.

Step 2.13. Finally: rank the alternatives based on $\mathcal{K}_i$ values. Note that the calculated values $\mathcal{K}_i$ are in the interval [0, 1] and can be ordered in an increasing sequence, which is the wanted order of precedence. The complex relative efficiency of the feasible alternative can be determined according to the utility function values.

4 | Case Study

The IIoT involves interconnected devices and systems in industrial settings, such as manufacturing, energy, and logistics. These systems generate vast amounts of data and require robust mechanisms to ensure data integrity and security, especially when it comes to digital forensics. A novel blockchain-based digital forensics framework has been proposed to address challenges in digital evidence collection and responsibility determination for industrial safety accidents involving IIoT device nodes [14]. A blockchain-based framework offers a promising solution to meet these criteria by leveraging the properties of blockchain technology to enhance the preservation, security, and reliability of forensic evidence. This scheme can be implemented using a decentralized blockchain storage mechanism to store digital forensic data, smart contract mechanisms to facilitate efficient retrieval and tracing of related evidence chains and a token mechanism for access control to enhance the data security of IIoT device nodes [40]. To enhance the data security of IIoT device nodes, a token mechanism is implemented for access control. Moreover, to meet real-time evidence acquisition requirements in IIoT, an efficient batch consensus mechanism is proposed. Experimental simulations demonstrate the superiority of the novel consensus algorithm compared to the traditional Delegated Proof-of-Stake (DPOS) consensus in the proposed scheme for the IIoT environment [14]. The key criteria for a Blockchain-Based Digital Forensics Framework in IIoT is given by [18, 40-41]:

- C1: Decentralization and Security: Employ a decentralized blockchain network to mitigate the risk of single points of failure and enhance the overall security of data storage and communication.

- C2: Data Integrity and Immutability: Utilize blockchain's immutable ledger to store cryptographic hashes of data and forensic evidence. This ensures that once data is recorded, it cannot be altered, guaranteeing its integrity. Implement robust hashing algorithms to create unique fingerprints for data, which are then stored on the blockchain.

- C3: Transparency and Traceability: Maintain a comprehensive audit trail of all transactions and interactions with forensic data. This includes time-stamped records of data collection, transfer, and analysis.

- C4: Scalability and Efficiency: Integrate edge computing to preprocess and analyze data locally, reducing latency and bandwidth usage. This is critical in handling the high volume of data generated by IIoT devices.

- C5: Interoperability and Integration: Ensure the framework can seamlessly integrate with existing IIoT systems and devices, allowing for real-time data acquisition and evidence collection. Adopt and promote industry standards for data formats and communication protocols to facilitate interoperability among diverse IIoT devices and systems.

Table 3. Experts data.

Experts	Experiences	Expertise	Occupation
DM1	6	Medium Bad	Industry
DM2	4	Very Good	Industry
DM3	11	Good	Industry
DM4	7	Medium Bad	Industry

5 | Research Findings

In this section, the hybrid T2NN-Entropy-ARAS method is applied through a case study. Then the result is obtained and also discussed and sensitivity and comparative analysis is also applied.

5.1 | Application of T2NN-Entropy-ARAS Method

Phase 1. T2NN expert reputation rating

Step 1.1. Four experts are employed to be a part of this application, and their information is shown in Table 3. The T2NN expert reputation rating matrix is calculated using Eq. (7) and Table 1 to express linguistic variables into T2NN, as shown in Table 4.

Step 1.2. The trade-off parameters for the base case are equal, which means that $\zeta_1, = \zeta_2 = 0.5$ using Eq. (8) T2NNWA to aggregate the matrix in Table 6.

Step 1.3. Then calculate the Score function for the aggregated matrix using Eq. (9) and finally using Eq. (10) to determine the reputation rating as shown in Table 5.

Table 4. T2NN reputation rating matrix.

Experts	Experience									Expertise								
	Tt	Ti	Tf	It	Ii	If	Ft	Fi	Ff	Tt	Ti	Tf	It	Ii	If	Ft	Fi	Ff
DM1	0.35	0.35	0.10	0.50	0.75	0.80	0.50	0.75	0.65	0.50	0.30	0.50	0.50	0.35	0.45	0.45	0.30	0.60
DM2	0.20	0.20	0.10	0.65	0.80	0.85	0.45	0.80	0.70	0.95	0.90	0.95	0.10	0.10	0.05	0.05	0.05	0.05
DM3	0.40	0.45	0.50	0.40	0.45	0.50	0.35	0.40	0.45	0.70	0.75	0.80	0.15	0.20	0.25	0.10	0.15	0.20
DM4	0.35	0.35	0.10	0.50	0.75	0.80	0.50	0.75	0.65	0.50	0.30	0.50	0.50	0.35	0.45	0.45	0.30	0.60

Table 5. Expert's reputation rating.

		Score	Reputation
DM1	(0.43, 0.33, 0.33),(0.50,0.51,0.60),(0.47,0.47,0.62)	0.44	0.19
DM2	(0.80, 0.72, 0.79),(0.25,0.28,0.21),(0.15,0.20,0.19)	0.77	0.33
DM3	(0.58, 0.63, 0.68),(0.24,0.30,0.35),(0.19,0.24,0.30)	0.70	0.30
DM4	(0.43, 0.33, 0.33),(0.50,0.51,0.60),(0.47,0.47,0.62)	0.44	0.19

Phase 2. T2NN-Entropy-ARAS

Step 2.1. Our experts express their opinions using Table 2 to build the T2NN initial decision matrix for five criteria and four alternatives as represented in Table 6.

Step 2.2. Use the T2NNWA equation to aggregate the decision matrix by considering the reputation rate of the experts computed in the previous phase in Table 5.

Step 2.3. The score function for the aggregated matrix is computed. By taking into account that beneficial criteria are C1, C2, and C5, and non-beneficial criteria are C3 and C4.

Step 2.4 to 2.7. First, normalize the matrix using Eq. (11) to get a normalized decision matrix as shown in Table 6. Then, compute the output entropy measure e_j of the jth factor using Eq. (12). Calculation of variation coefficient of jth factor e_j by Eq. (13) Finally, calculate the objective weight of the entropy $\mathcal{W}_j$ using Eq. (14) as shown in Table 7.

Step 2.8 to 2.13. Using the decision matrix in Table 6 to select x_{0j} the optimal value for each criterion using Eq. (15), so the modified decision matrix is presented in Table 8. Then, normalize the matrix using the two stages: a) for the beneficial criteria by applying Eq. (16), and b) for the non-beneficial criteria by applying Eq. (17). Defining the normalized-weighted matrix $\widehat{x_{ij}}$ as weight is calculated by the Entropy method in the previous steps and shown in Table 7. The weighted normalized matrix is shown in Table 9. Using Eq. (19) to determine the value of the optimality function $\mathcal{S}_i$ to compute the degree of the alternative utility. The utility degree $\mathcal{K}_i$of an alternative is computed using Eq. (20) as presented in Table 9. Finally: rank the alternatives based on $\mathcal{K}_i$ values.

From these steps the final ranking is ordered as Alt3 > Alt2 > Alt4 >Alt1.

Table 6. Decision matrix.

	C1	C2	C3	C4	C5
Alt1	0.72	0.55	0.39	0.77	0.31
Alt2	0.42	0.58	0.63	0.50	0.65
Alt3	0.82	0.67	0.58	0.64	0.69
Alt4	0.51	0.65	0.49	0.83	0.54

Table 7. Entropy weight.

	C1	C2	C3	C4	C5
Ej	0.974522	0.997614	0.988926	0.987544	0.970966
1-Ej	0.025478	0.002386	0.011074	0.012456	0.029034
Wj	0.316774	0.029668	0.137686	0.154873	0.360999

Table 8. ARAS decision matrix.

	C1 +	C2 +	C3 -	C4 -	C5 +
Alt1	0.72	0.55	0.39	0.77	0.31
Alt2	0.42	0.58	0.63	0.50	0.65
Alt3	0.82	0.67	0.58	0.64	0.69
Alt4	0.51	0.65	0.49	0.83	0.54
X0	0.82	0.67	0.39	0.50	0.69

Table 9. ARAS rank.

weighted Normalized matrix								
	C1 +	C2 +	C3 -	C4 -	C5 +	Si	Ki	Rank
Alt1	0.069618	0.005214	0.033689	0.025072	0.038751	0.172343	0.707278	4
Alt2	0.040061	0.005522	0.020925	0.038208	0.082096	0.186811	0.766656	2
Alt3	0.079181	0.006378	0.022745	0.030197	0.086214	0.224715	0.92221	1
Alt4	0.048734	0.006175	0.02664	0.023189	0.067723	0.17246	0.707759	3
X0	0.08	0.01	0.03	0.04	0.09	0.24	1	

5.2 | Discussion

The hybrid T2NN-Entropy-ARAS method effectively evaluates and ranks alternatives in blockchain-based digital forensics within IIoT, considering multiple criteria and expert opinions. The integration of T2NN enables the handling of uncertainty and vagueness inherent in expert opinions, while the Entropy method provides an objective calculation of criterion weights. The higher the variability, the higher the weight assigned to that criterion. As shown in Table 7, the final weight calculation reveals that criterion C5 is the most important, followed closely by C1, and criterion C2 is deemed the least important. ARAS evaluates and ranks alternatives by calculating their utility degrees, which incorporate both the criteria weights and the performance scores of the alternatives. The results indicate that Alt3 is the top-ranked alternative, followed by Alt2, Alt4, and Alt1, respectively. This ranking is determined by the utility degree of each alternative, which takes into account both the weights of the criteria and the performance of each alternative.

5.3 | Sensitivity Analysis

Sensitivity analysis is conducted to validate the effectiveness of the hybrid T2NN-Entropy-ARAS model, specifically assessing its robustness in the context of blockchain-based digital forensics within the IIoT. This is achieved by changing the trade-off parameters ζ_1 in the base case scenario $\zeta_1 = \zeta_2 = 0.5$. By varying the ζ_1 within the range of [0,1] analyzes the sensitivity. The $\zeta_1 = 0$ indicate the expertise only and $\zeta_1 = 1$ show that experiences only and are shown in Figure 1. The weight of the T2NN-Entropy method was affected by changing the trade-off in nine cases from 0 to 1. Figure 2 shows the T2NN-ARAS rank when weight is chaining according to weight change in the nine cases.

Sensitivity analysis is essential to validate the robustness of the hybrid T2NN-Entropy-ARAS method for evaluating blockchain-based digital forensics in IIoT environments. By varying the trade-off parameter ζ_1 ,ζ_2 which balances expertise and experience, we can assess how variations in this parameter affect the weight calculations and subsequent rankings of alternatives. In the base case $\zeta_1 = \zeta_2 = 0.5$ indicating equal importance. The range ζ_1 varies between 0 and 1, where ζ_1 =0 implies only expertise, and ζ_1 =1 implies only experience. Recalculate the weights using T2NN-Entropy method based on nine cases by changing the value of ζ_1. Figure 1 shows how the weights of the criteria changes as ζ_1 varies from 0 to 1. Each line represents the weight of a specific criterion, demonstrating the sensitivity of weights to the trade-off parameter. Then apply the adjusted weights to the T2NN-ARAS method to recalculate the utility degrees and rankings of the alternatives. Track the rankings for each of the nine cases as shown in Figure 2 which illustrates the rankings of the four alternatives (Alt1, Alt2, Alt3, Alt4) across the nine cases. Each bar or line represents the ranking position of an alternative in each case. The sensitivity analysis confirms the robustness of the hybrid T2NN-Entropy-ARAS method. The top-ranked alternative Alt3, remains consistently high across different trade-off parameter configurations, underscoring its suitability for blockchain-based digital forensics in IIoT environments. The analysis demonstrates the method's ability to handle uncertainty and varying expert opinions effectively, ensuring reliable decision-making.

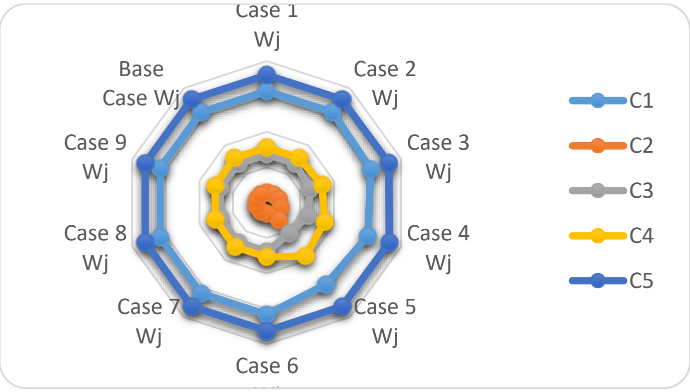

Figure 1. Sensitivity analysis on weight.

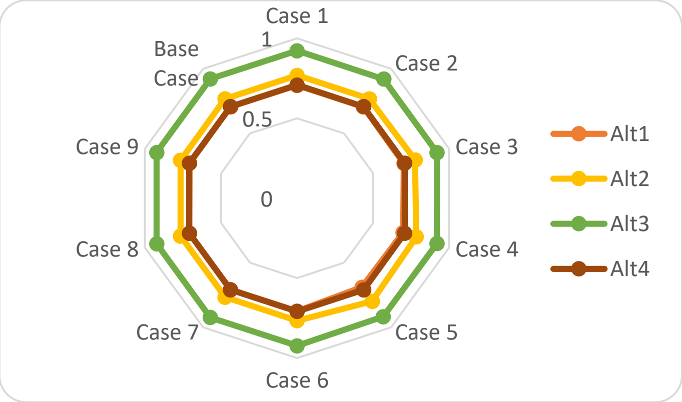

Figure 2. Sensitivity analysis on rank.

5.4 |Comparative Analysis

To further validate the robustness and effectiveness of the proposed hybrid T2NN-Entropy-ARAS method, we perform a comparative analysis using the Entropy-VIKOR method. VIKOR (Vise Kriterijumska Optimizacija I Kompromisno Resenje) is a MCDM method that focuses on ranking and selecting from a set of alternatives in the presence of conflicting criteria, emphasizing the closeness to the ideal solution [42]. Using the Entropy method, the weights are calculated for each criterion, emphasizing their relative importance. These weights are used in both the ARAS and VIKOR methods for consistency. Table 10 shows the final rank using VIKOR method. The VIKOR indices Qj are computed, and the alternatives are ranked accordingly. Using the previously determined weights and criteria, the rankings derived from the ARAS method are compared with those obtained from the VIKOR method.

Table 10. VIKOR rank.

	C1 +	C2 +	C3 -	C4 -	C5 +	Si	Ri	Qj	Rank
Alt1	0.08	0.03	0.00	0.13	0.36	0.59	0.36	0.015609	4
Alt2	0.32	0.02	0.14	0.00	0.03	0.51	0.32	0.201842	3
Alt3	0.00	0.00	0.11	0.06	0.00	0.17	0.11	1	1
Alt4	0.25	0.01	0.06	0.15	0.14	0.61	0.25	0.226738	2

The comparative analysis using the Entropy-VIKOR method supports the findings from the hybrid T2NN-Entropy-ARAS method, demonstrating consistent rankings and validating the robustness of the evaluation framework. The Private Blockchain Deployment (Alt3) is affirmed as the most suitable alternative for blockchain-based digital forensics in IIoT, followed by the Hybrid Blockchain Approach (Alt4), as shown in Figure 3. This consistency across different MCDM methods enhances confidence in the decision-making process, ensuring reliable and effective implementation of blockchain technologies in IIoT digital forensics. Both ARAS and VIKOR methods rank Alt3 as the top alternative. This consistency underscores Alt3's robust performance across multiple criteria and evaluation methods, validating its suitability for blockchain-based digital forensics in IIoT.

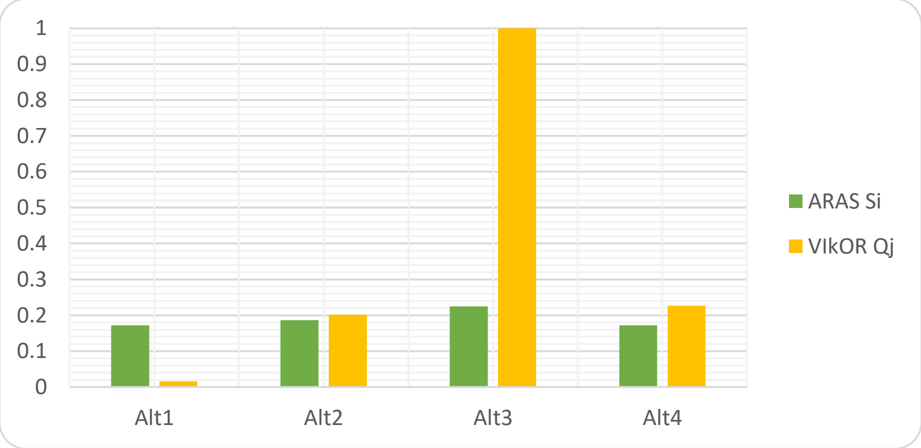

Figure 3. ARAS and VIKOR rank.

6 |Conclusions

Blockchain technology offers significant potential in the context of IIoT forensics. However, the implementation of such systems presents challenges that must be addressed, including scalability, interoperability, data privacy, and real-time processing. These challenges can be overcome through the development of advanced blockchain solutions, the optimization of data processing techniques, and the integration of data privacy and security protocols. By adopting blockchain technology and incorporating MCDM methods, IIoT forensics can provide secure, reliable, and transparent data analysis and evidence preservation. In this paper, we have presented a novel approach to integrating blockchain technology with IIoT digital forensics using a hybrid MCDM method, specifically the T2NN-Entropy-ARAS method. This integration addresses the critical need for data integrity, security, and transparency in IIoT environments. Our approach aims to enhance the reliability and robustness of digital forensic investigations, ensuring that digital evidence remains tamper-proof and traceable. The potential of blockchain technology to mitigate security and integrity challenges in IIoT. The immutable and decentralized nature of blockchain makes it a suitable solution for storing and managing forensic data, ensuring that once data is recorded, it cannot be altered or tampered with. T2NN-Entropy-ARAS method is applied to evaluate and prioritize blockchain-based digital forensic schemes. The T2NN approach effectively handles uncertainty and imprecision in expert opinions, while the ENTROPY method objectively determines the weights of evaluation criteria. The ARAS method then ranks the alternatives based on their utility degrees.

6.1 | Future Considerations

The hybrid T2NN-Entropy-ARAS method has proven effective in evaluating and ranking alternatives based on multiple criteria. However, continuous advancements in blockchain technology and IIoT could shift these evaluations over time. It is crucial for organizations to periodically reassess their choices and stay updated with technological advancements and evolving security standards. Future research could explore integrating additional criteria such as Access Control, Privacy, Legal and Regulatory Compliance, further refining the decision-making process for IIoT digital forensics. Future work could extend this analysis to include additional criteria or explore other hybrid methods to further enhance the robustness of the evaluation process.

Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Author Contributions

All authors contributed equally to this work.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Herbert Endres, Marta Indulska, Arunava Ghosh, 2024,Unlocking the potential of Industrial Internet of Things (IIOT) in the age of the industrial metaverse: Business models and challenges, https://doi.org/10.1016/j.indmarman.2024.03.006

[2] Onu Peter, Anup Pradhan, Charles Mbohwa, 2023, Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies, https://doi.org/10.1016/j.procs.2022.12.282

[3] Shams Forruque Ahmed, Md. Sakib Bin Alam, Mahfara Hoque, Aiman Lameesa, Shaila Afrin, Tasfia Farah, Maliha Kabir, GM Shafiullah, S.M. Muyeen, 2023, Industrial Internet of Things enabled technologies, challenges, and future directions, https://doi.org/10.1016/j.compeleceng.2023.108847

[4] Inam Ullah, Deepak Adhikari, Xin Su, Francesco Palmieri, Celimuge Wu, Chang Choi, 2024,Integration of data science with the intelligent IoT (IIoT): current challenges and future perspectives, https://doi.org/10.1016/j.dcan.2024.02.007

[5] Sharmin Attaran, Mohsen Attaran, Bilge Gokhan Celik, 2024,Digital Twins and Industrial Internet of Things: Uncovering operational intelligence in industry 4.0, https://doi.org/10.1016/j.dajour.2024.100398

[6] F. Casino et al., "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," in IEEE Access, vol. 10, pp. 25464-25493, 2022, doi: 10.1109/ACCESS.2022.3154059.

[7] Victor R. Kebande, 2022, Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0, https://doi.org/10.1016/j.fsir.2022.100257

[8] Zubair A. Baig, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, Paresh Kerai, Ahmed Ibrahim, Krishnun Sansurooah, Naeem Syed, Matthew Peacock, 2017, Future challenges for smart cities: Cyber-security and digital forensics, https://doi.org/10.1016/j.diin.2017.06.015

[9] Yimin Guo, Yajun Guo, Ping Xiong, Fan Yang, Chengde Zhang, 2024, A provably secure and practical end-to-end authentication scheme for tactile Industrial Internet of Things, https://doi.org/10.1016/j.pmcj.2024.101877

[10] Libo Feng, Fei Qiu, Kai Hu, Bei Yu, Junyu Lin, Shaowen Yao, 2024,CABC: A Cross-Domain Authentication Method Combining Blockchain with Certificateless Signature for IIoT, https://doi.org/10.1016/j.future.2024.04.042

[11] Yi Li, Da An Su, Abbas Mardani, 2023, Digital twins and blockchain technology in the industrial Internet of Things (IIoT) using an extended decision support system model: Industry 4.0 barriers perspective, https://doi.org/10.1016/j.techfore.2023.122794

[12] Feng Zhang, Hao Wang, Lu Zhou, Dequan Xu, Liang Liu, 2023, A blockchain-based security and trust mechanism for AI-enabled IIoT systems, https://doi.org/10.1016/j.future.2023.03.011

[13] Spyridon Georg Koustas, Max Jalowski, Tobias Reichenstein, Sascha Julian Oks, 2023, A blockchain-based IIoT traceability system: ERC-721 tokens for Industry 4.0, https://doi.org/10.1016/j.procir.2023.09.163

[14] Nan Xiao, Zhaoshun Wang, Xiaoxue Sun, Junfeng Miao, 2024, A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things, https://doi.org/10.1016/j.aej.2023.12.021

[15] Jin Wang, Jiahao Chen, Yongjun Ren, Pradip Kumar Sharma, Osama Alfarraj, Amr Tolba, 2022, Data security storage mechanism based on blockchain industrial Internet of Things, https://doi.org/10.1016/j.cie.2021.107903

[16] Yash Bobde,Gokuleshwaran Narayanan, Manas Jati ,Raja Soosaimarian Peter Raj, Ivan Cvitić, Dragan Peraković, 2024, Enhancing Industrial IoT Network Security through Blockchain Integration, https://doi.org/10.3390/electronics13040687

[17] R.Lakshmana Kumar, Firoz Khan, Seifedine Kadry, Seungmin Rho, 2022, A Survey on blockchain for industrial Internet of Things, https://doi.org/10.1016/j.aej.2021.11.023

[18] Gulshan Kumar, Rahul Saha, Chhagan Lal, Mauro Conti, 2021, Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications, https://doi.org/10.1016/j.future.2021.02.016

[19] Rejab Hajlaoui, Tarek Moulahi, Salah Zidi, Salim El Khediri, Bechir Alaya, Sherali Zeadally, 2024, Towards smarter cyberthreats detection model for industrial internet of things (IIoT) 4.0, https://doi.org/10.1016/j.jii.2024.100595

[20] G. Nilay Yücenur, Ayça Maden, 2024, Sequential MCDM methods for site selection of hydroponic geothermal greenhouse: ENTROPY and ARAS, https://doi.org/10.1016/j.renene.2024.120361

[21] Md Khalid Jamal, Mohd Muqeem, 2023, An MCDM optimization based dynamic workflow scheduling used to handle priority tasks for fault tolerance in IIOT, https://doi.org/10.1016/j.measen.2023.100742

[22] Mohamed Abdel-Basset, M. Saleh, Abduallah Gamal, Florentin Smarandache , 2019, An approach of TOPSIS technique for developing supplier selection with group decision making under type-2 neutrosophic number, https://doi.org/10.1016/j.asoc.2019.01.035

[23] U. Cali, M. Deveci, S. S. Saha, U. Halden and F. Smarandache, "Prioritizing Energy Blockchain Use Cases Using Type-2 Neutrosophic Number-Based EDAS," in IEEE Access, vol. 10, pp. 34260-34276, 2022, doi: 10.1109/ACCESS.2022.3162190.

[24] Chaouki Ghenai, Mona Albawab, Maamar Bettayeb, 2020, Sustainability indicators for renewable energy systems using multi-criteria decision-making model and extended SWARA/ARAS hybrid method, https://doi.org/10.1016/j.renene.2019.06.157

[25] Edris Soltani, Mostafa Mirzaei Aliabadi, 2023, Risk assessment of firefighting job using hybrid SWARA-ARAS methods in fuzzy environment, https://doi.org/10.1016/j.heliyon.2023.e22230

[26] Dawei Li, Ruonan Chen, Di Liu, Yingxian Song, Yangkun Ren, Zhenyu Guan, Yu Sun, Jianwei Liu, 2022,Blockchain-based authentication for IIoT devices with PUF, https://doi.org/10.1016/j.sysarc.2022.102638

[27] Pranita Binnar, Sunil Bhirud, Faruk Kazi, 2024, Security analysis of cyber physical system using digital forensic incident response, https://doi.org/10.1016/j.csa.2023.100034

[28] Victor R Kebande, Ali Ismail Awad, 2023, Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions, DOI:10.1145/3635030

[29] Muhammet Deveci, Nuh Erdogan, Umit Cali d, Joseph Stekli, Shuya Zhong, 2021, Type-2 neutrosophic number based multi-attributive border approximation area comparison (MABAC) approach for offshore wind farm site selection in USA, https://doi.org/10.1016/j.engappai.2021.104311

[30] Pritpal Singh, 2021, A type-2 neutrosophic-entropy-fusion based multiple thresholding method for the brain tumor tissue structures segmentation, https://doi.org/10.1016/j.asoc.2021.107119

[31] Vladimir Simić, Branko Milovanović, Strahinja Pantelić, Dragan Pamučar, Erfan Babaee Tirkolaee, 2023, Sustainable route selection of petroleum transportation using a type-2 neutrosophic number based ITARA-EDAS model, https://doi.org/10.1016/j.ins.2022.11.105

[32] Zeyuan Wang, Qiang Cai, Guiwu Wei,2023, Modified TODIM method based on cumulative prospect theory with Type-2 neutrosophic number for green supplier selection, https://doi.org/10.1016/j.engappai.2023.106843

[33] Seyyed Shahabaddin Hosseini Dehshiri, Bahar Firoozabadi, 2023, A new multi-criteria decision making approach based on wins in league to avoid rank reversal: A case study on prioritizing environmental deterioration strategies in arid urban areas, https://doi.org/10.1016/j.jclepro.2022.135438

[34] Thu Van Huynh, Sawekchai Tangaramvong, Bach Do, Wei Gao, 2024, A novel decoupled approach combining invertible cross-entropy method with Gaussian process modeling for reliability-based design and topology optimization, https://doi.org/10.1016/j.cma.2024.117006

[35] Ju Junjie, Shi Wenhao, Wang Yuan, 2024,A risk assessment approach for road collapse along tunnels based on an improved entropy weight method and K-means cluster algorithm, https://doi.org/10.1016/j.asej.2024.102805

[36] Selman Karagöz, Muhammet Deveci, Vladimir Simic, Nezir Aydin, 2021, Interval type-2 Fuzzy ARAS method for recycling facility location problems, https://doi.org/10.1016/j.asoc.2021.107107

[37] Mishra, A.R., Rani, P. A q-rung orthopair fuzzy ARAS method based on entropy and discrimination measures: an application of sustainable recycling partner selection. J Ambient Intell Human Comput 14, 6897–6918 (2023). https://doi.org/10.1007/s12652-021-03549-3

[38] Shankha Shubhra Goswami, Dhiren Kumar Behera, 2021, Implementation of ENTROPY-ARAS decision making methodology in the selection of best engineering materials, https://doi.org/10.1016/j.matpr.2020.06.320

[39] Vladimir Simic, Ilgin Gokasar, Muhammet Deveci, Ahmet Karakurt, 2022, An integrated CRITIC and MABAC based type-2 neutrosophic model for public transportation pricing system selection, https://doi.org/10.1016/j.seps.2021.101157

[40] Y. Makadiya, R. Virparia and K. Shah, "IoT Forensics System based on Blockchain," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 490-495.

[41] S. Li, T. Qin and G. Min, "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems," in IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1433-1441, Dec. 2019, doi: 10.1109/TCSS.2019.2927431.

[42] Suwen Luo, Pengrui Yang, 2023, Design and evaluation of a sustainable entropy-weighted and VIKOR-based method for offshore oil collecting, https://doi.org/10.1016/j.heliyon.2023.e21256

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.