Proceedings of Engineering and Technology Innovation, vol. 32, 2026, pp. 85-103

Ranking of Security Factors in Blockchain-Based IoT Paradigm Using AHP-TOPSIS Method

Priyanka Kaushal[1,*], Vipin Saxena[2], Shalini Chandra[3]

Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, India

Received 19 May 2025; received in revised form 06 November 2025; accepted 11 November 2025

DOI: https://doi.org/10.46604/peti.2026.15157

Abstract

The Internet of Things (IoT) connects smart devices for efficient data sharing but faces challenges such as low processing power, limited storage, and security risks. Blockchain technology offers a secure and decentralized solution to these issues. This study prioritizes key security factors in blockchain-based IoT systems using a hybrid approach combining the Analytic Hierarchy Process (AHP) and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). AHP determines the weights and relative importance of security factors, while TOPSIS ranks them based on closeness to the ideal solution. The results demonstrate a strong Spearman correlation (ρ = 0.9916) with individual AHP and TOPSIS outcomes, and sensitivity analysis confirms the stability of the rankings. Data integrity, access control, and authentication are identified as the top three security factors. These findings support the development of secure and scalable blockchain-based IoT systems.

Keywords: IoT, blockchain, AHP, TOPSIS, security

1. Introduction

In recent years, the Internet of Things (IoT) has changed technology by allowing for seamless integration of physical objects, which has transformed ordinary objects into smart systems capable of sensing, processing, and sharing data. This development has resulted in the widespread adoption of smart devices, driving innovation across industries and improving end-user services. IoT networks are typically managed by a centralized authority. Alongside these developments, IoT presents substantial security issues, including unauthorized access, data manipulation, and data breaches. These challenges indicate the critical need for strong security methods to protect the massive amounts of sensitive data created by IoT systems.

Therefore, blockchain technology, characterized by its decentralization and immutable nature, presents an effective way to address various security issues. It provides reliable and transparent databases, which are widely used to track ownership and monitor resources, goods, and services. The distributed database provides a transparent and secure ledger of transactions and data. This significantly reduces the need for central control, minimizes the risk of single points of failure, and enhances security.

Furthermore, the combination of IoT and blockchain technologies boosts innovation by maximizing the advantages of both fields. Fundamental security aspects are crucial in blockchain-based IoT systems. Security in an IoT-blockchain environment involves multiple factors that are essential for securing the overall system. However, determining the proper sequence for handling these security factors remains a significant challenge. To address this, the Multi-Criteria Decision-Making (MCDM) technique is employed. MCDM is used to solve issues involving various attributes and sub-attributes, with

* Corresponding author. E-mail address: priyankakaushal3@gmail.com

the main purpose of identifying the most suitable solution. Numerous MCDM approaches are available for defining objectives and assigning weights to alternatives. One of these approaches is the Analytic Hierarchy Process (AHP), which was proposed in 1970 by Saaty [1]. AHP effectively computes the weights of factors.

In 1981, Hwang and Yoon [2] proposed the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), which is efficient and simple, and is used to rank factors according to their closeness to the optimal solution. However, TOPSIS has some limitations, including the lack of weight computation and consistency testing for assessments. Therefore, the present work integrates these two techniques to form a hybrid approach. This approach provides an effective solution for selecting and ranking security factors in blockchain-based IoT systems. The basic conceptual design of the proposed methodology is shown in Fig. 1.

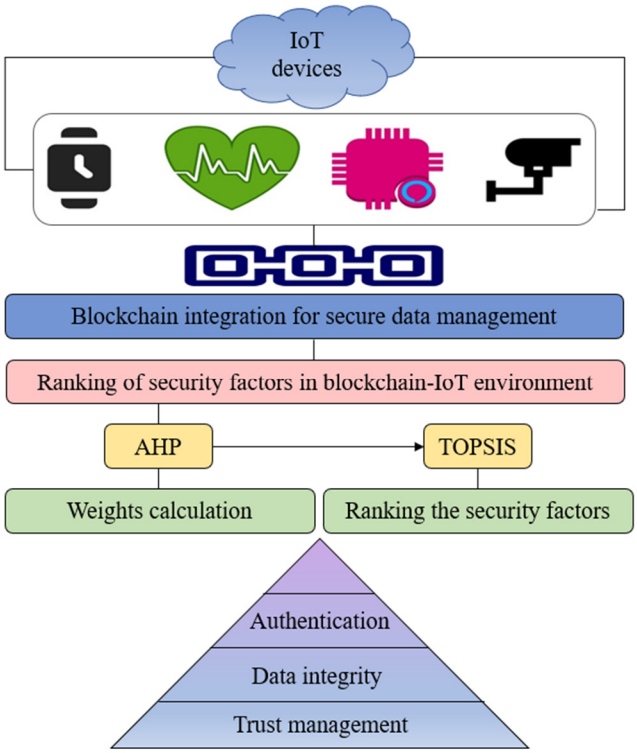

Fig. 1 Basic system model based on integration of AHP and TOPSIS methods

Further, relevant literature from recent studies is discussed here. In 2009, Ashton [3] first proposed the term “Internet of Things.” Since then, IoT devices, including connected vehicles, home automation systems, healthcare wearable devices, and appliances with remote monitoring capabilities, have rapidly evolved. Ferrag et al. [4] provide a comprehensive review of blockchain-IoT, discussing the application domains of blockchain technology in IoT and presenting attack models in five areas: identity-based attacks, manipulation-based attacks, cryptanalytic attacks, reputation-based attacks, and service-based attacks. Ma et al. [5] proposed a Blockchain-based Distributed Key Management Architecture (BDKMA) in fog computing, with the goal of minimizing latency while ensuring scalability and auditability. In 2020, Diesch et al. [6] presented a comprehensive model of Management Success Factors (MSFs) for organizational information security, categorizing them into areas such as physical security, vulnerabilities, infrastructure, access control, and others to evaluate organizational security.

Wang et al. [7] proposed a framework named Identified Security Attributes (ISA), which evaluates security attributes within the Internet of Healthcare Things (IoHT) context. Yohan and Lo [8] utilized a blockchain framework to secure Over the Air (OTA) firmware updates, ensuring integrity and protecting against attacks. Kaur et al. [9] examined the AHP approach in a fog computing environment to rank security attributes. Although AHP is efficient and simple, it is sometimes criticized for failing to address uncertainty in the decision-maker’s perception. IoT is transforming industries by enabling applications in healthcare, transportation, banking, surveillance, and more, but faces device-level vulnerabilities in centralized servers. This

issue is addressed by blockchain, which provides a decentralized architecture [10]. In 2021, Zhou et al. [11] presented a blockchain-based Intelligent Transportation System (ITS) that employs cryptographic primitives, Chinese Remainder Theorem (CRT), and Shamir's scheme, to improve fault tolerance and security.

Panda et al. [12] presented a blockchain-based distributed IoT architecture that uses hash chains for secure and efficient key management. In 2022, Dissanayake et al. [13] presented a review on the management of software security patches, highlighting the main issues, strategies, and resources. Zhou and Chen [14] proposed a hybrid strategy that combines the AHP and Interactive Multi-Criteria Decision Making (TODIM) methods for selecting an appropriate blockchain technology provider in Pythagorean fuzzy situations. Gardas et al. [15] presented a fuzzy-based MCDM approach for identifying the optimal nodes in blockchain-enabled edge IoT systems. In 2023, Alojaiman [16] presented a fuzzy TOPSIS approach for selecting the most reliable and effective IoT application. This approach provides IoT solutions by assessing key factors. Alshahrani et al. [17] presented a review of multi-criteria analysis, focusing on issues related to creating a decentralized ledger platform. The ML-based Proof of Evolutionary Model (PoEM) enables a lightweight consensus for secure data sharing in the IoT context, as presented by Zhao et al. [18].

The growing use of IoT in healthcare creates severe security concerns. To address this issue, a blockchain model based on homomorphic encryption is proposed by Ali et al. [19], which allows secure data sharing and computation without decryption. Haque et al. [20] presented a Delegated Proof of Stake (DPoS) with sharding to address blockchain scalability issues caused by IoT and centralized systems that are unable to manage throughput and latency. The PriMedGuard architecture is proposed by Almotairi et al. [21] to provide robust identity and privacy for sensitive data in the Internet of Medical Things (IoMT). This architecture protects medical data using key generation, encryption, and smart contracts. Furthermore, in 2024, Khan et al. [22] proposed a cloud data security model that incorporates AHP and TOPSIS, providing maximum benefit for the industry and users. Dahiya et al. [23] presented a blockchain-based security architecture to ensure data integrity, privacy, and secure sharing via smart contracts. The model enhances healthcare security while maintaining efficiency and transparency.

Deng et al. [24] proposed a lightweight Blockchain-Based Trust Management (BBTM) scheme to enable secure communication and real-time trust evaluation. This scheme effectively filters malicious nodes and ensures privacy. In 2025, Matey et al. [25] presented a hybrid method to prioritize performance measures and rank enablers that may affect Blockchain in manufacturing sectors. IoT networks face issues with data integrity and traceability due to limited resources. A lightweight blockchain combined with the LoRaWAN protocol to ensure safe data transmission without complex consensus processes [26]. However, while the hybrid AHP-TOPSIS approach has been used in related domains such as IoHT and cloud security, previous research has not systematically prioritized many security factors specific to the blockchain-IoT paradigm. Existing research primarily focuses on limited contexts or uses as a single approach. Hence, the present study addresses this domain-specific need by applying the AHP-TOPSIS hybrid approach.

This approach prioritizes blockchain-IoT security issues using a geometric mean. The results are validated through expert input and provide actionable recommendations for safe system design. Thus, the main contribution of the study is to examine security factors and sub-factors within the Blockchain-IoT paradigm. The security aspects are prioritized based on expert judgment. This study used two MCDM approaches, namely AHP and TOPSIS, which are suitable for systematically ranking and prioritizing security factors and sub-factors. The AHP technique is used to calculate the weights of security factors and prioritize them based on expert opinions, while TOPSIS is used for ranking and validation. The findings, when compared individually using AHP and TOPSIS, demonstrate a very strong correlation. Sensitivity analysis is used to validate the robustness of the results. This innovative approach, which integrates AHP-TOPSIS for decision-making and security evaluation in the blockchain-IoT context, provides valuable information for organizations to focus on the most important security areas.

2. IoT- Blockchain Security

Table 1 Details of security factor and sub-factors

Security factors	References									
	[5]	[6]	[7]	[10]	[18]	[19]	[20]	[21]	[22]	[26]
Node performance (F1)	✓	-	✓	-	-	✓	-	-	-	✓
Computation power (F11)	-	-	-	-	✓	✓	-	✓	-	✓
Storage capacity (F12)	-	-	-	-	-	✓	-	✓	-	✓
Energy efficiency (F13)	-	-	✓	-	✓	✓	✓	✓	✓	✓
Resource allocation (F14)	-	-	✓	-	-	✓	✓	-	✓	✓
Network performance (F2)	✓	-	✓	-	✓	-	✓	✓	-	-
Network bandwidth (F21)	✓	-	✓	-	-	-	-	✓	-	-
Latency (F22)	✓	-	✓	-	-	✓	✓	✓	-	-
Throughput (F23)	✓	-	-	-	-	✓	-	-	✓	-
Load balancing (F24)	✓	-	-	-	-	-	-	-	✓	-
Data integrity (F3)	-	✓	✓	✓	✓	✓	-	✓	✓	✓
Hashing mechanism (F31)	-	-	-	✓	-	✓	✓	✓	-	✓
Proof of work (F32)	-	-	-	✓	-	✓	✓	✓	-	✓
Transparent audit trails (F33)	-	-	-	✓	-	✓	-	-	✓	✓
Tamper detection (F34)	-	-	-	✓	-	✓	-	-	-	-
Access control (F4)	✓	✓	✓	✓	✓	✓	✓	-	✓	✓
Decentralized access control list (F41)	✓	-	-	-	-	-	-	-	✓	✓
Token-based access control (F42)	-	-	-	-	-	-	-	-	✓	✓
Role-based access control (F43)	-	-	-	✓	-	-	✓	-	✓	✓
Attribute-based access control (F44)	-	-	-	✓	-	-	✓	-	✓	-
Authentication (F5)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multi-factor authentication (F51)	-	-	-	-	-	-	-	-	✓	✓
Biometric authentication (F52)	-	✓	-	-	-	-	-	-	-	✓
Digital signature algorithm (F53)	-	✓	-	-	-	-	-	-	-	✓
Zero-knowledge proof (F54)	-	✓	-	-	-	-	-	-	-	✓
Key management (F6)	✓	-	✓	-	✓	✓	✓	-	✓	-
Private key (F61)	-	-	✓	-	✓	✓	-	✓	-	-
Public key (F62)	-	-	✓	-	-	✓	✓	✓	-	-
Asymmetric key pair (F63)	✓	-	-	-	✓	-	-	-	-	-
Nested key (F64)	-	-	✓	-	✓	-	-	✓	-	-
Trust management (F7)	✓	-	✓	-	✓	✓	✓	-	✓	✓
Reputation system (F71)	-	✓	-	-	-	-	-	-	-	✓
Predictability(F72)	✓	-	✓	-	-	-	-	-	✓	✓
Reliability (F73)	✓	✓	✓	-	✓	✓	-	✓	-	✓
Auditability (F74)	✓	✓	✓	✓	-	✓	-	✓	-	✓
Reliable transmission (F8)	-	-	-	-	-	-	-	-	✓	-
Fault tolerance (F81)	-	-	-	-	✓	-	-	-	✓	-
Error detection and correction (F82)	-	-	-	-	-	-	-	-	✓	-
Packet delivery guarantees (F83)	-	-	-	-	-	-	-	-	✓	-
Quality of services (F84)	-	-	-	-	-	-	-	-	✓	-
Firmware update (F9)	-	-	✓	-	✓	-	-	-	✓	✓
Over the air update (F91)	-	-	-	-	✓	-	-	-	-	✓
Rollback mechanism (F92)	-	✓	-	-	✓	-	-	-	✓	✓
Security patching (F93)	-	✓	✓	-	✓	-	-	-	✓	-
Decentralized firmware management (F94)	✓	-	✓	-	✓	-	-	-	✓	-

✓: indicates that the factor is clearly addressed in the cited reference; -: denotes that the factor is not discussed.

In blockchain-integrated IoT systems, security plays a primary role in securing the data and maintaining trust across the network [27]. Security is a combination of several sub-attributes rather than one attribute. The attributes and sub-attributes are responsible for monitoring and addressing the security of the entire system [28]. The main aim of the present work is to reduce

the effort required for the prioritization of the various security factors. In this regard, security factors, along with sub-factors, are identified in the blockchain-based IoT environment. The study finds nine key security factors, and each factor has four additional sub-factors, which are displayed in Fig. 2. The nine key factors and 36 sub-factors were identified through a synthesis of many surveys and research articles, as shown in Table 1, which maps each factor to supporting references. This ensured that the factor set was based on established research rather than selected at random. To offer fair representation, four sub-factors were added under each major factor, guided by their frequency in the literature.

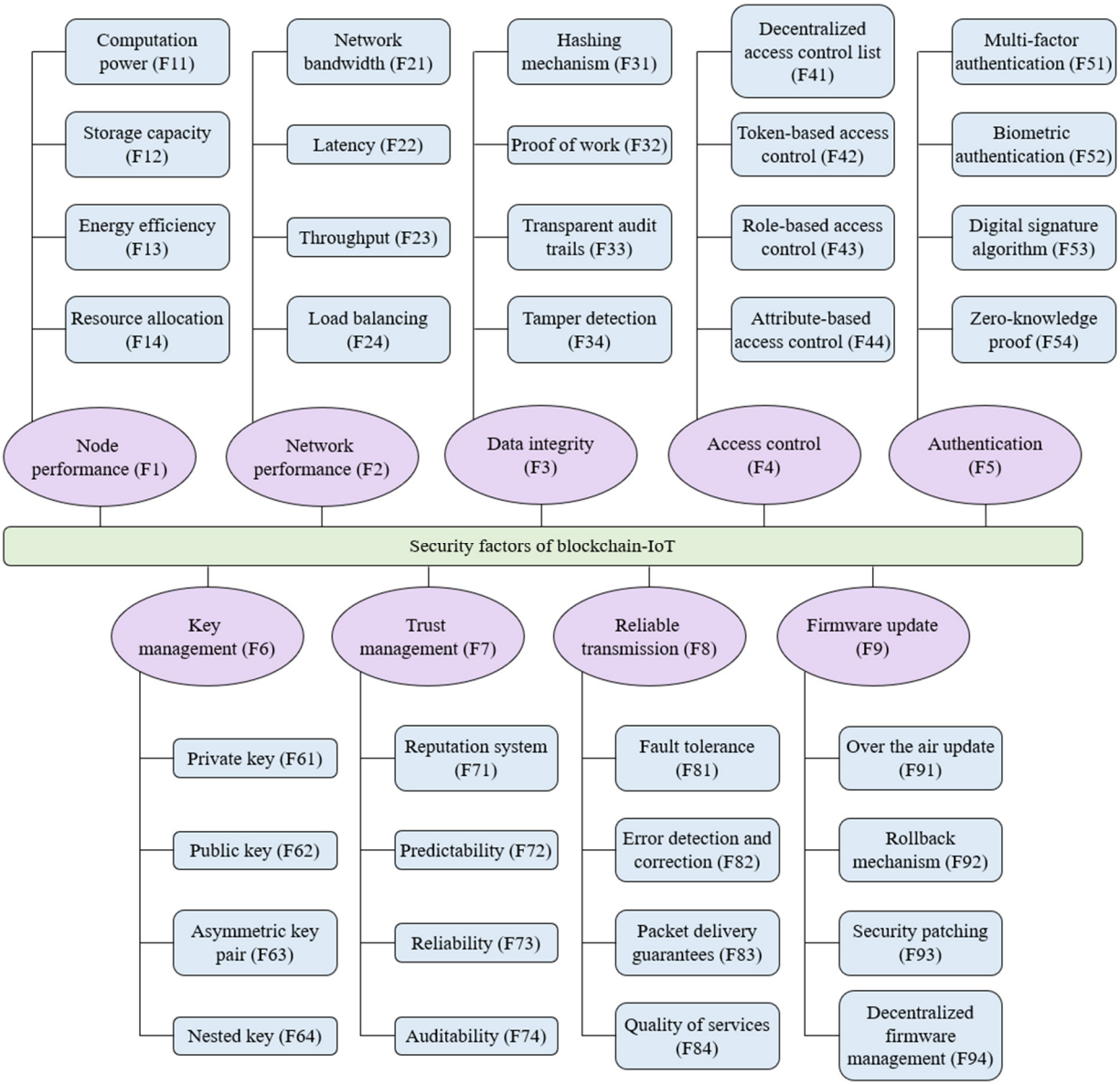

Fig. 2 Security factors of blockchain-IoT

However, Proof of Work is energy-intensive and less ideal for IoT, but it is preserved as a sub-factor under data integrity due to its broad acceptance in blockchain security research. Additionally, authentication and key management were considered as separate factors. Since authentication is about verifying the identity of nodes/devices, while key management is essential for the secure distribution and storage of cryptographic keys, both are important features for blockchain-IoT security. Therefore, the security factors are described below in brief, according to the sequential order:

(1) Node performance (F1) is the crucial component for effective processing in blockchain-based IoT. In the IoT paradigm, it refers to the efficiency of particular IoT devices [5, 7, 19, 26]. In blockchain, it is responsible for ensuring the dependability and scalability of the system. Node performance has four sub-factors, like computation power, storage capacity, energy efficiency, and resource allocation, represented as F11, F12, F13, and F14, respectively.

(2) Network performance (F2) is a factor representing the performance of the network communicated through IoT devices across the blockchain network. It operates in a real-time context, and any delay or latency in communication may influence the network performance [5, 7, 18, 20-21]. Further, it is categorized into four sub-factors: network bandwidth, latency, throughput, and load balancing, represented as F21, F22, F23, and F24, respectively.

(3) Data integrity (F3) ensures that information is not changed from its original state. In a blockchain-IoT architecture, protecting the integrity of data means guaranteeing that once data is captured, it is immutable and unalterable [6-7, 10, 18-19, 21-22]. It has four different sub-factors, including hashing mechanism, proof of work, transparent audit trails, and tamper detection, represented as F31, F32, F33, and F34, respectively.

(4) Access control (F4) is an essential factor that guarantees only authorized people and devices may access certain data or functionalities in the network. In blockchain-based IoT, preventing unauthorized individuals from accessing sensitive data is crucial. This is especially true in healthcare IoT situations, where minor manipulation might endanger someone's life [5-6, 10, 18-19, 20, 22]. It has four sub-factors, such as decentralized access control list, token-based access control, role-based access control, and attribute-based access control, represented as F41, F42, F43, and F44, respectively.

(5) Authentication (F5) checks the identification of users or devices, guaranteeing that only authorized people may access the data or network. Based on several studies [5-6, 10, 18, 22], authentication is recognized as a major security issue. Therefore, a strong authentication method is needed to secure IoT devices. It has four sub-factors: multi-factor authentication, biometric authentication, digital signature algorithm, and zero-knowledge proof, represented as F51, F52, F53, and F54, respectively.

(6) Key management (F6) is a process of managing cryptographic keys, which is crucial for encryption and is widely used for securing data on the blockchain network. It ensures that confidential information is only accessible and decrypted by authorized individuals. Therefore, effective key management is essential for keeping data secure and private [5, 7, 18-20, 22]. It has four sub-attributes, including a private key, public key, asymmetric key pair, and nested keys, represented as F61, F62, F63, and F64, respectively.

(7) Trust management (F7) refers to the determination of node reliability based on previous interactions. Since blockchain technology has no central authority, establishing trust among the devices is important for secure data transactions. Hence, maintaining trust between nodes is critical in a decentralized network to function properly [5, 7, 18-20, 22, 26]. It has four essential sub-factors: reputation system, predictability, reliability, and auditability, represented as F71, F72, F73, and F74, respectively.

(8) Reliable transmission (F8) is the process of guaranteeing that data is transmitted accurately and promptly from one device to another. Since numerous applications depend on it, fast and accurate transmission of data is essential in a blockchain-based IoT environment [22]. It has four essential sub-factors: fault tolerance, error detection and correction, packet delivery guarantees, and quality of services, represented as F81, F82, F83, and F84, respectively.

(9) Firmware update (F9) is required for IoT devices to provide security and keep them up to date. These updates address the security issues and improve device performance [7, 18, 22, 26]. It has four sub-factors: OTA update, rollback mechanism, security patching, and decentralized firmware management, represented as F91, F92, F93, and F94, respectively.

3. AHP-TOPSIS Methodology

Due to the growing use of IoT devices, security has become the top priority for researchers. Several factors help to enhance the overall security of blockchain-IoT systems. In the context of security management, it is highly important to prioritize the factors and sub-factors properly. The proposed approach analyzes the empirical data using both quantitative and qualitative

metrics. Qualitative assessments are suitable for evaluating security, although quantitative measurement of security factors is quite difficult. Therefore, the study focuses on a quantitative assessment of IoT-Blockchain technology security. The study involves two phases: the first uses the AHP technique to assign weights, while the second uses the TOPSIS approach to rank security factors. The general structure of the AHP-TOPSIS hybrid technique for ranking security factors in Blockchain-based IoT is illustrated below.

The AHP method is used for decision-making and was created by Saaty [1]. It is a systematic method employed to evaluate complex decisions by decomposing them into a hierarchy of criteria and subsequently assessing and comparing the elements to reach a decision. The technique is chosen for several reasons, including its emphasis on reducing errors through simplification, segmentation, and comparative analysis of numerous qualities. It is appropriate for comparing both qualitative and quantitative data. Consequently, it offers several features, such as selection, evaluation, resource allocation, prioritization, and ranking. The AHP technique is subjective, which means that experts assign weights depending on their judgment.

The TOPSIS method was first introduced in 1981 by Hwang and Yoon [2]. It is the most widely used MCDM approach because of its computational simplicity. TOPSIS considers both positive and negative ideal solutions, making it highly effective. Factors that are closest to the positive ideal solution are considered the best options. This study employs an integrated approach that combines AHP and TOPSIS to measure the impact of blockchain IoT technologies for ranking the security factors. The step-by-step procedure of the proposed methodology is shown in Fig. 3 and outlined as follows.

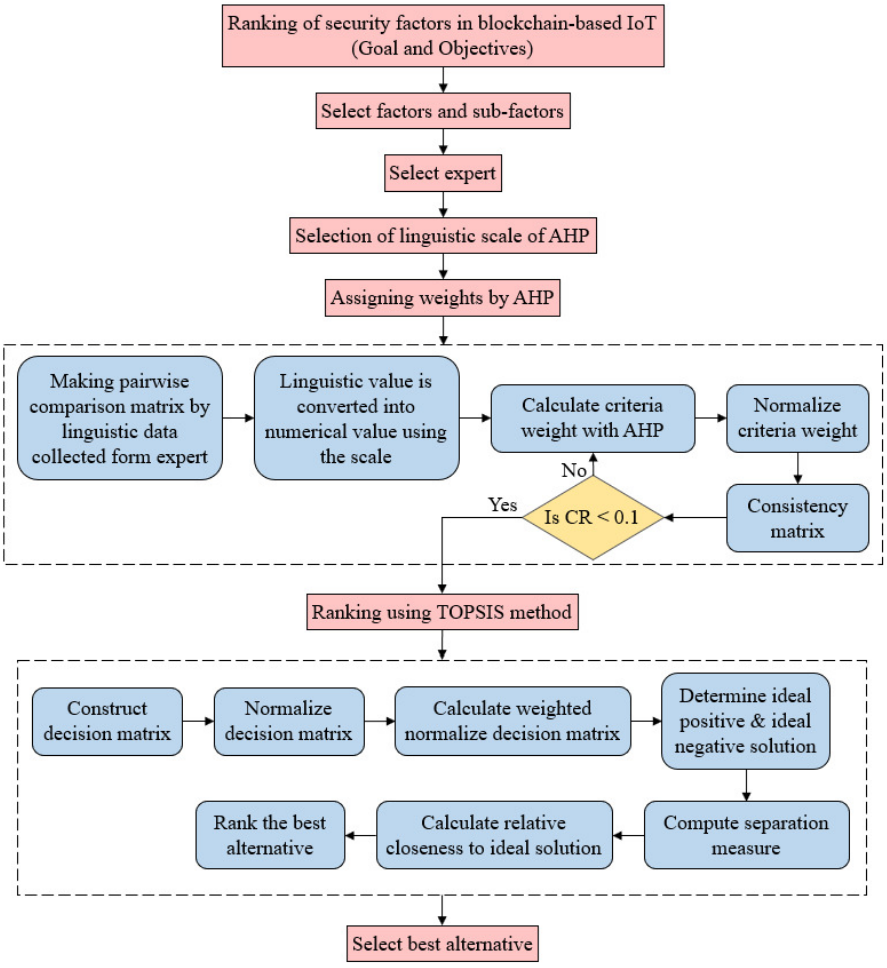

Fig. 3 Methodology procedure for ranking of security factors

Phase 1: *Assigning weights using the AHP method*

The AHP method is used to assign weights to the criteria. This approach is effective for problem-solving involving multiple criteria. According to the literature [1, 7, 9], the AHP method involves the following steps.

Step 1: Data is obtained from experts, such as academicians, researchers, and engineers, in linguistic form using Table 2. A linguistic pairwise matrix is created to analyze the data using the specified scales.

Step 2: The scale shown in Table 2 is used to convert linguistic pairwise comparison matrices into numerical values. Since 75 experts participate in the evaluation, a 9 × 9 pairwise comparison matrix is initially obtained for each expert individually. To aggregate these assessments into a single numerical matrix, the study applies the geometric mean technique across all experts' entries. The geometric mean formula is given below, and an example of the aggregation process is provided in the Appendix for transparency.

$$a_{ij} = \left(\prod_{k=1}^{n} x_{ij}^{k} \right)^{\frac{1}{n}} \tag{1}$$

here x_{ij}^{k} is the k-th expert rating of factor i vs j, and n is the number of experts.

Table 2 Linguistic scale values [1]

Linguistic scale	Linguistic term abbreviation	Numerical value
Absolutely low	AL	1/9
Very low	VL	1/7
Low	L	1/5
Medium low	ML	1/3
Exactly equal	EE	1
Medium-high	MH	3
High	H	5
Very high	VH	7
Absolutely high	AH	9

Step 3: Normalize the numerical values in the pairwise comparison matrix by summing the values in each column. Subsequently, each value in the resulting matrix is divided by the corresponding column sum (a_{ij}). The following formulae are used to compute R_{ij}.

$$\sum_{i=1}^{n} a_{ij} = a_{1j} + a_{2j} + a_{3j} + \ldots + a_{nj} \tag{2}$$

$$R_{ij} = \frac{s_{ij}}{\sum_{i=1}^{m} a_{ij}} \tag{3}$$

where j = 1, 2, ... n and s_{ij} represents the original element in the i-th row and j-th column of the pairwise comparison matrix, while $\sum_{i-1}^{m} a_{ij}$ is the sum of all entries in column j. The normalised value R_{ij} is obtained by dividing s_{ij} by the corresponding column sum.

Step 4: Moreover, priority weight is calculated for each factor, with the help of the following formula:

$$w_j = \frac{a_{1j} + a_{2j} + a_{3j} + \ldots + a_{nj}}{n} \tag{4}$$

where w_j is the average normalised weight of factor j, and n is the total number of criteria taken into account in the analysis.

Step 5: During this stage, the consistency of the pairwise comparison matrix is evaluated. The procedure begins by multiplying all elements of the non-normalized pairwise comparison matrix by the criteria weights, row by row. Next, the weighted sum vector (WSV) is divided by the corresponding criterion weights to calculate the consistency vector (CV). The following formulas are used to calculate the WSV and CV.

$$\mathrm{WSV} = \sum_{j=1}^{n} \left(a_{ij} \times w_j \right) \tag{5}$$

$$\mathrm{CV} = \frac{\mathrm{WSV}}{w_j} \tag{6}$$

Step 6: The average of the CV values is computed to determine λ_{max}. This is done by summing the results of Eq. (6) from the previous step and dividing the total by n, where n denotes the number of attributes.

$$\lambda_{max} = \frac{\sum \mathrm{CV}}{n} \tag{7}$$

Step 7: The Consistency Index (CI) is computed by the formula shown below:

$$\mathrm{CI} = \frac{\lambda_{max} - n}{n-1} \tag{8}$$

where λ_{max} is an eigenvalue, and n represents the number of factors. The next Consistency Ratio (CR) is computed using a Random Index (RI). The value of the RI is obtained from Saaty [1] and is outlined in Table 3. According to Saaty [1], if the CR value is 0.1 or below, it is considered acceptable; otherwise, the entire process must be restarted.

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{9}$$

Table 3 Random Index values

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Phase 2: *TOPSIS method for ranking of security factors*

The second phase is used to determine the best solution using the TOPSIS method. Therefore, the approach is elaborated as follows:

Step 1: Create a decision matrix. For this purpose, the previously normalized decision matrix (R_{ij}) is used to construct the decision matrix for the TOPSIS analysis, ensuring that all criteria are on a similar scale.

Step 2: At this stage, the weighted normalized decision matrix is computed. This is done by multiplying the normalized decision matrix (R_{ij}) by the weights obtained from the AHP, as shown in the following formula:

$$V_{ij} = R_{ij} \times w_j \tag{10}$$

where V_{ij} denotes the element of the weighted normalized decision matrix in row i and column j, and w_j is the priority weight.

Step 3: The positive (A^+) and negative (A^-) ideal solutions are determined using the following formulas. These solutions correspond to the maximum and minimum values, respectively, in the weighted decision matrix.

$$A^+ = \left\{ V_1^+, V_2^+, V_3^+, V_n^+ \right\} = \left\{ \max(V_{ij}) \middle| \imath = 1, 2, \ldots, m \right\} \tag{11}$$

$$A^- = \left\{ V_1^-, V_2^-, V_3^-, V_n^- \right\} = \left\{ \min(V_{ij}) \middle| \imath = 1, 2, \ldots, m \right\} \tag{12}$$

where A^+ denotes the positive ideal solution, A^- denotes the negative ideal solution, is the weighted normalized value, and m denotes the number of rows.

Step 4: The Euclidean distance between each alternative and the positive and negative ideal solutions is calculated using the formula below to determine the separation measures.

$$S_i^+ = \sqrt{\sum_{j=1}^{n} \left(V_{ij} - V^+\right)^2} \tag{13}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n} \left(V_{ij} - V^-\right)^2} \tag{14}$$

where S_i^+, S_i^- is the separation distance of each alternative from the ideal solutions, and V^+, V^- represent positive and negative ideal solutions.

Step 5: At the end, the relative closeness C_i of each factor is computed using the given formula:

$$C_i = \frac{S_i^-}{S_i^+ + S_i^-} \tag{15}$$

Step 6: The security factors are ranked based on the relative closeness C_i. A higher C_i indicates a higher ranking.

4. Data Analysis and Results

The effect of security factors in the blockchain-IoT system was determined using the AHP and TOPSIS techniques. Accordingly, the proposed AHP-TOPSIS was employed as a hybrid strategy for prioritizing security factors. To collect data for analysis, a questionnaire was created to obtain expert opinions. The questionnaire was then distributed to 90 experts with expertise in IoT, cybersecurity, and blockchain. Of the 90 experts, 75 valid responses were received using the scale provided in Table 2, yielding a response rate of 83.3%. Purposive sampling was used to select experts to ensure domain relevance and diversity of experience. The expert panel was composed of academicians (45%), researchers (30%), and industry engineers (25%), all of whom had at least five years of professional or research experience in the relevant field. The entire procedure was implemented and validated step by step using Python 3.10.9 in the Spyder IDE on a system equipped with an Intel Core i5-11260H processor (2.60 GHz), 8 GB RAM, and a 64-bit Windows 11 operating system. This setup ensured reliable and accurate computations. The results of this procedure are presented in Tables 4 to 12.

Step 1: The expert data were obtained in linguistic form, and the resulting linguistic pairwise comparison matrix is presented in Table 4.

Table 4 Linguistic pairwise comparison matrix

Security factors	F1	F2	F3	F4	F5	F6	F7	F8	F9
Node performance (F1)	EE	EE	AL	AL	AL	L	L	ML	VL
Network performance (F2)	EE	EE	AL	AL	AL	L	L	ML	VL
Data integrity (F3)	AH	AH	EE	EE	EE	MH	MH	H	EE
Access control (F4)	AH	AH	EE	EE	EE	EE	MH	H	EE
Authentication (F5)	AH	AH	EE	EE	EE	EE	MH	H	EE
Key management (F6)	H	H	ML	EE	EE	EE	EE	MH	EE
Trust management (F7)	H	H	ML	ML	ML	EE	EE	MH	ML
Reliable transmission (F8)	MH	MH	L	L	L	ML	ML	EE	ML
Firmware update (F9)	VH	VH	EE	EE	EE	EE	MH	MH	EE

Step 2: The scale from Table 2 was used to transform the linguistic matrix into a numerical matrix. The numerical matrix was computed using the geometric mean in Eq. (1), and the resulting aggregated values are presented in Table 5.

Step 3: The Numerical pairwise comparison matrix was further normalized using Eqs. (2) and (3), respectively, and the outcomes are presented in Table 6. It is noted that all values in each row are identical, which is a common result of the AHP normalization process. Each value in the pairwise comparison matrix was divided by the sum of its corresponding column to produce a consistent normalized priority weight for each factor.

Table 5 Numerical pairwise comparison matrix

Security factors	F1	F2	F3	F4	F5	F6	F7	F8	F9
Node performance (F1)	1.0000	0.9285	0.0916	0.1107	0.1109	0.1704	0.2362	0.4827	0.1333
Network performance (F2)	1.0769	1.0000	0.0987	0.1192	0.1194	0.1835	0.2544	0.5198	0.1435
Data integrity (F3)	10.9069	10.1278	1.0000	1.2078	1.2098	1.8590	2.5768	5.2650	1.4542
Access control (F4)	9.0299	8.3849	0.8279	1.0000	1.0016	1.5390	2.1334	4.3589	1.2039
Authentication (F5)	9.0147	8.3709	0.8265	0.9983	1.0000	1.5365	2.1298	4.3516	1.2019
Key management (F6)	5.8670	5.4479	0.5379	0.6497	0.6508	1.0000	1.3861	2.8321	0.7822
Trust management (F7)	4.2326	3.9303	0.3880	0.4687	0.4695	0.7214	1.0000	2.0431	0.5643
Reliable transmission (F8)	2.0715	1.9236	0.1899	0.2294	0.2297	0.3530	0.4894	1.0000	0.2762
Firmware update (F9)	7.5001	6.9644	0.6876	0.8305	0.8319	1.2783	1.7719	3.6205	1.0000

Table 6 Normalized pairwise matrix

Security factors	F1	F2	F3	F4	F5	F6	F7	F8	F9
Node performance (F1)	0.0197	0.0197	0.0197	0.0197	0.0197	0.0197	0.0197	0.0197	0.0197
Network performance (F2)	0.0212	0.0212	0.0212	0.0212	0.0212	0.0212	0.0212	0.0212	0.0212
Data integrity (F3)	0.2151	0.2151	0.2151	0.2151	0.2151	0.2151	0.2151	0.2151	0.2151
Access control (F4)	0.1781	0.1781	0.1781	0.1781	0.1781	0.1781	0.1781	0.1781	0.1781
Authentication (F5)	0.1778	0.1778	0.1778	0.1778	0.1778	0.1778	0.1778	0.1778	0.1778
Key management (F6)	0.1157	0.1157	0.1157	0.1157	0.1157	0.1157	0.1157	0.1157	0.1157
Trust management (F7)	0.0834	0.0834	0.0834	0.0834	0.0834	0.0834	0.0834	0.0834	0.0834
Reliable transmission (F8)	0.0408	0.0408	0.0408	0.0408	0.0408	0.0408	0.0408	0.0408	0.0408
Firmware update (F9)	0.1479	0.1479	0.1479	0.1479	0.1479	0.1479	0.1479	0.1479	0.1479

Step 4: The average was calculated to determine the priority weights using Eq. (4). These priority weights represent the relative significance of each factor. As shown in Table 7, F3 has a higher weight than the other criteria, indicating its importance as recommended by experts. Conversely, F1 and F2 exhibit the lowest values, indicating that both are relatively less essential compared to the other factors.

Step 5: The WSV was computed using Eq. (5), and the CV was calculated using Eq. (6). The results are presented in Table 7.

Table 7 Priority weights, WSV, and CV values

Security factors	Weights	WSV	CV
Node performance (F1)	0.019724	0.177515	9.000000
Network performance (F2)	0.021241	0.191169	9.000000
Data integrity (F3)	0.215127	1.936144	9.000000
Access control (F4)	0.178105	1.602946	9.000000
Authentication (F5)	0.177807	1.600260	9.000000
Key management (F6)	0.115721	1.041489	9.000000
Trust management (F7)	0.083484	0.751355	9.000000
Reliable transmission (F8)	0.040859	0.367735	9.000000
Firmware update (F9)	0.147932	1.331386	9.000000

Step 6: The maximum eigenvalue (λ_{max}) was calculated. Eq. (7) was used to determine λ_{max}, resulting in 81 / 9 = 9.00.

Step 7: The CI was computed using Eq. (8) as (9 − 9) / (9 − 1) = 0.0; and the CR was computed using Eq. (9). The resulting value of 0.00 is less than 0.10, indicating that the matrix is consistent. Consequently, the analysis proceeded to the subsequent security assessment.

Step 8: The TOPSIS technique was used to rank the security factors. Hence, the above-normalized decision matrix, denoted by R_{ij}, was used for further security evaluation.

Step 9: Table 8 presents the weighted normalized decision matrix derived using Eq. (10).

Table 8 Weighted normalized decision matrix

Security factors	F1	F2	F3	F4	F5	F6	F7	F8	F9
Node performance (F1)	0.000388	0.000388	0.000388	0.000388	0.000388	0.000388	0.000388	0.000388	0.000388
Network performance (F2)	0.000450	0.000450	0.000450	0.000450	0.000450	0.000450	0.000450	0.000450	0.000450
Data integrity (F3)	0.046273	0.046273	0.046273	0.046273	0.046273	0.046273	0.046273	0.046273	0.046273
Access control (F4)	0.031720	0.031720	0.031720	0.031720	0.031720	0.031720	0.031720	0.031720	0.031720
Authentication (F5)	0.031614	0.031614	0.031614	0.031614	0.031614	0.031614	0.031614	0.031614	0.031614
Key management (F6)	0.013388	0.013388	0.013388	0.013388	0.013388	0.013388	0.013388	0.013388	0.013388
Trust management (F7)	0.006962	0.006962	0.006962	0.006962	0.006962	0.006962	0.006962	0.006962	0.006962
Reliable transmission (F8)	0.001667	0.001667	0.001667	0.001667	0.001667	0.001667	0.001667	0.001667	0.001667
Firmware update (F9)	0.021879	0.021879	0.021879	0.021879	0.021879	0.021879	0.021879	0.021879	0.021879

Step 10: Additionally, the A^+ was determined using Eq. (11), while the A^- was obtained using Eq. (12). The findings are presented in Table 9.

Step 11: The ideal and non-ideal separation measures were determined by the positive and negative ideal solutions. Eqs. (13) and (14) were used to calculate the values, and the results are presented in Table 9.

Table 9 Ideal solutions with separation measures

Security factors	A^+	A^-	S_i^+	S_i^-
Node performance (F1)	0.046273	0.000388	0.137653	0.000000
Network performance (F2)	0.046273	0.000388	0.137444	0.000186
Data integrity (F3)	0.046273	0.000388	0.000000	0.137655
Access control (F4)	0.046273	0.000388	0.043681	0.093996
Authentication (F5)	0.046273	0.000388	0.043988	0.093678
Key management (F6)	0.046273	0.000388	0.098682	0.039000
Trust management (F7)	0.046273	0.000388	0.117919	0.019722
Reliable transmission (F8)	0.046273	0.000388	0.133817	0.003837
Firmware update (F9)	0.046273	0.000388	0.073177	0.064473

Step 12: Finally, the relative closeness (C_i) was calculated using Eq. (15). The final matrix, which includes the rank of the security factors, was presented in Table 10.

Table 10 Final rank for level 1

Security factors	C_i	Rank
Node performance (F1)	0.000000	9
Network performance (F2)	0.001352	8
Data integrity (F3)	1.000000	1
Access control (F4)	0.682949	2
Authentication (F5)	0.680562	3
Key management (F6)	0.283448	5
Trust management (F7)	0.143321	6
Reliable transmission (F8)	0.027887	7
Firmware update (F9)	0.468678	4

As depicted in Table 10, the top-ranked factors are data integrity, access control, and authentication, which specifically address critical security issues in blockchain-IoT systems. Data integrity guarantees that transactions and logs are tamper-resistant; access control prevents unauthorized transactions, and authentication verifies node identity. Together, these factors mitigate data manipulation, spoofing, and unauthorized access in resource-constrained IoT contexts. Further, the above process was applied to rank the sub-factors at level 2. The determined weights and relative closeness values for each subfactor under the respective main factors were summarized in Table 11.

Table 11 Final rank for level 2 sub-factors

Security factors	Sub-factors	Weights	C_i	Rank
Node performance (F1)	Computation power (F11)	0.560393	1.000000	1
	Storage capacity (F12)	0.257276	0.201523	2
	Energy efficiency (F13)	0.083804	0.015899	4
	Resource allocation (F14)	0.098528	0.026721	3
Network performance (F2)	Network bandwidth (F21)	0.294637	0.527732	1
	Latency (F22)	0.298453	0.472443	2
	Throughput (F23)	0.171713	0.203792	4
	Load balancing (F24)	0.235197	0.362729	3
Data integrity (F3)	Hashing mechanism (F31)	0.384179	0.554926	2
	Proof of work (F32)	0.378486	0.622095	1
	Transparent audit trails (F33)	0.180831	0.158561	3
	Tamper detection (F34)	0.056502	0.000000	4
Access control (F4)	Decentralized access control list (F41)	0.297248	0.522712	1
	Token-based access control (F42)	0.313206	0.500412	2
	Role-based access control (F43)	0.168593	0.197091	4
	Attribute-based access control (F44)	0.220951	0.329442	3
Authentication (F5)	Multi-factor authentication (F51)	0.564445	1.000000	1
	Biometric authentication (F52)	0.208688	0.143385	2
	Digital signature algorithm (F53)	0.182563	0.106869	3
	Zero-knowledge proof (F54)	0.044302	0.000000	4
Key management (F6)	Private key (F61)	0.283129	0.381194	3
	Public key (F62)	0.327123	0.476371	2
	Asymmetric key pair (F63)	0.352028	0.503484	1
	Nested key (F64)	0.037718	0.000000	4
Trust management (F7)	Reputation system (F71)	0.30277	0.512567	2
	Predictability (F72)	0.329317	0.675604	1
	Reliability (F73)	0.169410	0.216195	4
	Auditability (F74)	0.198501	0.301504	3
Reliable transmission (F8)	Fault tolerance (F81)	0.50999	0.923100	1
	Error detection and correction (F82)	0.275750	0.260631	2
	Packet delivery guarantees (F83)	0.145899	0.080771	3
	Quality of services (F84)	0.068352	0.000000	4
Firmware update (F9)	Over the air update (F91)	0.512043	1.000000	1
	Rollback mechanism (F92)	0.193224	0.166453	3
	Security patching (F93)	0.198488	0.170022	2
	Decentralized firmware management (F94)	0.096243	0.015901	4

As indicated in Table 11, proof of work (F32) ranked first under the data integrity factor (F3). This ranking was mainly due to expert assessments that emphasized its security strength and theoretical robustness over its practical impact in IoT contexts. Although proof of work is energy-intensive, making it unsuitable for resource-constrained IoT devices, it remains the most widely used consensus technique for ensuring immutability and trust in blockchain networks. For the practical deployment of energy-efficient security in IoT applications, lightweight alternatives such as proof of stake, proof of authority, and delegated consensus techniques may be considered. Furthermore, the global weights were calculated by multiplying the weights of the main factors by those of the corresponding sub-factors. The obtained global weights were displayed in Table 12.

Table 12 Global weights of factors and sub-factors

Security factors	Weights	Sub-factors	Weights	Global weights	Rank
Node performance (F1)	0.019724	Computation power (F11)	0.560393	0.011053	26
		Storage capacity (F12)	0.257276	0.005074	31
		Energy efficiency (F13)	0.083804	0.001652	36
		Resource allocation (F14)	0.098528	0.019433	20

Table 12 Global weights of factors and sub-factors (continued)

Security factors	Weights	Sub-factors	Weights	Global weights	Rank
Node performance (F1)	0.019724	Computation power (F11)	0.560393	0.011053	26
		Storage capacity (F12)	0.257276	0.005074	31
		Energy efficiency (F13)	0.083804	0.001652	36
		Resource allocation (F14)	0.098528	0.019433	20
Network performance (F2)	0.021241	Network bandwidth (F21)	0.294637	0.006258	29
		Latency (F22)	0.298453	0.006339	28
		Throughput (F23)	0.171713	0.003647	34
		Load balancing (F24)	0.235197	0.004995	32
Data integrity (F3)	0.215127	Hashing mechanism (F31)	0.384179	0.082647	2
		Proof of work (F32)	0.378486	0.081422	3
		Transparent audit trails (F33)	0.180831	0.038901	9
		Tamper detection (F34)	0.056502	0.012155	24
Access control (F4)	0.178105	Decentralized access control list (F41)	0.297248	0.052941	6
		Token-based access control (F42)	0.313206	0.055783	5
		Role-based access control (F43)	0.168593	0.030027	14
		Attribute-based access control (F44)	0.220951	0.039352	8
Authentication (F5)	0.177807	Multi-factor authentication (F51)	0.564445	0.100362	1
		Biometric authentication (F52)	0.208688	0.037106	11
		Digital signature algorithm (F53)	0.182563	0.032461	13
		Zero-knowledge proof (F54)	0.044302	0.007877	27
Key management (F6)	0.115721	Private key (F61)	0.283129	0.032763	12
		Public key (F62)	0.327123	0.037855	10
		Asymmetric key pair (F63)	0.352028	0.040737	7
		Nested key (F64)	0.037718	0.004364	33
Trust management (F7)	0.083484	Reputation system (F71)	0.30277	0.025276	18
		Predictability (F72)	0.329317	0.027492	17
		Reliability (F73)	0.169410	0.014143	23
		Auditability (F74)	0.198501	0.016572	21
Reliable transmission (F8)	0.040859	Fault tolerance (F81)	0.50999	0.020837	19
		Error detection and correction (F82)	0.275750	0.011266	25
		Packet delivery guarantees (F83)	0.145899	0.005961	30
		Quality of services (F84)	0.068352	0.002792	35
Firmware update (F9)	0.147932	Over the air update (F91)	0.512043	0.075747	4
		Rollback mechanism (F92)	0.193224	0.028584	16
		Security patching (F93)	0.198488	0.029362	15
		Decentralized firmware management (F94)	0.096243	0.014237	22

(1) Sensitivity analysis

Table 13 Sensitivity analysis results of AHP weights

Perturbation type	Change applied	Top-1 factor	Top-3 factors	F3 rank	F5 rank	Top-1 changed
Baseline (AHP-TOPSIS)	-	F3	F3, F4, F5	1	3	No
Individual +10% (F1)	+10%	F3	F3, F4, F5	1	3	No
Individual −10% (F5)	−10%	F3	F3, F4, F5	1	3	No
Individual +10% (F7)	+10%	F3	F3, F4, F5	1	3	No
Global +10% (all)	+10%	F3	F3, F4, F5	1	3	No
Global −10% (all)	−10%	F3	F3, F4, F5	1	3	No

A sensitivity analysis was performed on the AHP weights to evaluate the robustness of the resulting ranking. Each weight was adjusted individually by ±10% and renormalized before repeating the TOPSIS process. Furthermore, a global ±10% uniform alteration was applied to all weights. The baseline results identified data integrity (F3) as the highest-ranked factor (C_i = 1.000), followed by access control (F4) and authentication (F5). As shown in Table 13, in every perturbation scenario,

F3 consistently remained the highest-ranked factor, although F4 and F5 occasionally interchanged positions within the top three. These results demonstrate that the hybrid AHP-TOPSIS approach is robust and not sensitive to minor variations in expert-derived weights.

(2) Comparative analysis

The proposed study compares several identical alternatives to test their overall accuracy. The suggested hybrid AHP-TOPSIS methodology is compared with independent AHP and TOPSIS approaches to highlight the relative importance of the outcomes achieved by the presented approach. The questionnaire data are converted into numerical values based on the linguistic scale, and results are calculated using both approaches. In the case of AHP, priority weights are calculated for ranking. In the case of the TOPSIS method, the relative closeness value is computed for factor prioritization. For the comparison, the Spearman correlation (ρ) coefficient is used to compare the three approaches, which is most suitable for ordinal data. The Spearman rank correlation formula is given below:

$$\rho = 1 - \frac{6\sum d_i^2}{n\left(n^2 - 1\right)} \tag{16}$$

where d_i is the variation between in rank, and d_i^2 is the square root of the variation in rank, and n is the number of factors. The range of the correlation ρ is given below:

$0.8 < \rho \leq 1.0$: Very strong correlation;
$0.6 < \rho \leq 0.8$: Strong correlation;
$0.4 < \rho \leq 0.6$: Average correlation;
$0.2 < \rho \leq 0.4$: Weak correlation;
$\rho \leq 0.2$: Very weak correlation.

The Spearman correlation coefficient between the proposed AHP-TOPSIS method and standalone AHP is 0.99166, and with standalone TOPSIS, it is also 0.99166, showing a very strong correlation in both cases. Such high correlation indicates that the hybrid approach does not contradict traditional methods. The goal of hybridization is therefore to address the weaknesses of each approach. AHP ensures that weights are consistently determined from expert judgement and generates normalised linear weights, which result in minimal gaps across criteria. TOPSIS, on the other hand, improves discrimination between close-ranked alternatives by introducing the concepts of ideal and negative-ideal solutions, thereby highlighting performance differences.

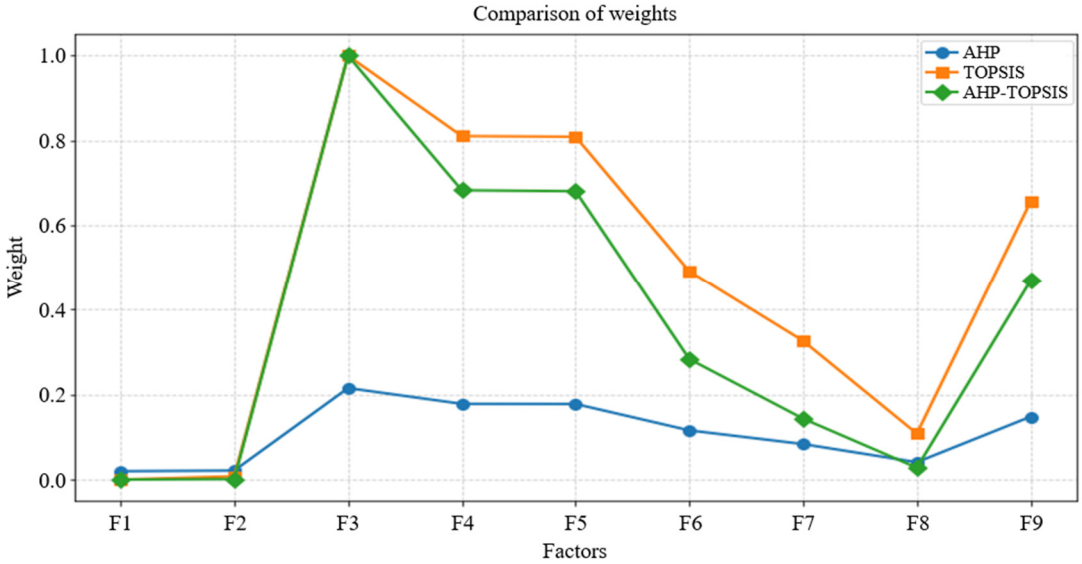

Fig. 4 Comparison of weights by AHP, TOPSIS, and AHP-TOPSIS

The proposed hybrid AHP-TOPSIS method provides flexibility to the system design and improves efficiency compared to the standalone AHP and TOPSIS methods. When AHP is applied alone, the resulting weight distribution may affect ranking precision due to the limitations of subjective judgment. Similarly, when TOPSIS is used alone, the relative closeness values may not accurately reflect the hierarchical importance if the weighting is incorrect, which may affect the resulting ranking. Hence, the hybrid approach combines the strengths of both techniques to enhance the quality, accuracy, and ranking of the selected alternatives. Furthermore, Fig. 4 displays a comparison of the relative weights obtained from different techniques, showing the similarities between the methods, with mid-ranked factors exhibiting clear separation in the hybrid ranking.

5. Discussion

The fusion of blockchain and IoT technologies provides a solid foundation for improving overall network security. By identifying and analyzing major contributing aspects, the study provides a novel perspective on security. It focuses on investigating blockchain-based IoT security factors to support the assessment of security strength. To this end, various security attributes and sub-attributes are identified and hierarchically organized. The data are gathered from domain experts and examined quantitatively using the AHP-TOPSIS approach. Therefore, the advantages of the proposed method are discussed below:

(1) It offers a systematic approach for managing various security issues. The findings of the proposed method will help to estimate the overall Blockchain-IoT security.
(2) The integration of AHP and TOPSIS provides a structured, quantitative strategy for decision-making, as AHP is used for calculating weights, and the TOPSIS technique is used for ranking all the factors.
(3) The combination of AHP and TOPSIS methods gives more accurate, systematic, and unambiguous security assessments.
(4) Security is a continuous concern that requires attention. Thus, the evaluation and prioritization will help developers and industry professionals to develop secure IoT applications.

Although data integrity, access control, and authentication were the top-ranked factors, their implementation in blockchain-IoT systems requires balancing efficacy and feasibility. To ensure that these techniques operate on resource-constrained IoT devices, lightweight cryptographic protocols and optimized access management are required. Furthermore, Addula et al. [29] reported that the key factors, such as authentication and access control, exhibit high performance in advanced anomaly detection, particularly in IoT environments. These top-priority factors are therefore commonly adopted in algorithm-based solutions to combat evolving cyber-attacks. The study assesses security in Blockchain-IoT environments. However, it has some limitations that may be addressed in future work.

(1) IoT and blockchain technologies are continuously evolving, and several new difficulties emerge day by day. Therefore, it is possible that the authors did not take into account other factors while calculating security.
(2) The tools used to collect data may be modified, and future research may employ different techniques that produce better findings.

6. Conclusion

This study addresses significant challenges in blockchain-based IoT systems by identifying and prioritizing essential security factors using a hybrid AHP-TOPSIS approach. The methodology combines AHP to compute factor weights and TOPSIS to rank security factors and sub-factors systematically. Nine main securities factors and thirty-six sub-factors were analyzed. Unlike previous studies that focused only on specific domains, such as IoHT or cloud-centric environments, this study provides a domain-specific and comprehensive ranking of blockchain-IoT security requirements. The findings identify the most important aspects for creating reliable and secure blockchain-enabled IoT infrastructures. Key conclusions of the study are as follows:

(1) Effective hybrid approach: Combining AHP with TOPSIS provides more consistent and reliable prioritization of security factors compared to using each method alone.

(2) Top ranking factors: Data integrity, access control, and authentication are ranked as the most significant factors for enhancing blockchain-IoT security.

(3) Strong methodological correlation: The comparison with standalone AHP and TOPSIS approaches shows a high correlation (0.99166), indicating that the hybrid approach is robust and reliable.

(4) Stability verified by sensitivity analysis: Sensitivity analysis verifies the ranking stability, showing that prioritization remains consistent across different weight conditions.

(5) Practical contribution: The findings present a structured and quantitative security assessment framework that developers may use to address significant security issues in blockchain-IoT systems.

Future research can focus on AI-driven anomaly detection and lightweight consensus techniques to improve IoT scalability. Further studies may include real-world validation via deployment case studies and using fuzzy or grey-based extensions to handle uncertainty in expert judgements.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] R. W. Saaty, "The Analytic Hierarchy Process—What It Is and How It Is Used," Mathematical Modelling, vol. 9, no. 3–5, pp. 161-176, 1987.

[2] C. L. Hwang and K. Yoon, Multiple Attribute Decision Making: Methods and Applications: A State-of-the-Art Survey, Berlin: Springer-Verlag, 1981

[3] K. Ashton, "That 'Internet of Things' Thing", https://www.rfidjournal.com/expert-views/that-internet-of-things-thing/73881/, accessed in 2017.

[4] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188-2204, 2019.

[5] M. Ma, G. Shi, and F. Li, "Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario," IEEE Access, vol. 7, pp. 34045-34059, 2019.

[6] R. Diesch, M. Pfaff, and H. Krcmar, "A Comprehensive Model of Information Security Factors for Decision-Makers," Computers & Security, vol. 92, article no. 101747, 2020.

[7] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods," IEEE Access, vol. 8, pp. 152316-152332, 2020.

[8] A. Yohan and N. W. Lo, "FOTB: A Secure Blockchain-Based Firmware Update Framework for IoT Environment," International Journal of Information Security, vol. 19, no. 3, pp. 257-278, 2020.

[9] J. Kaur, A. Agrawal, and R. A. Khan, "Security Assessment in Foggy Era through Analytical Hierarchy Process," 11th International Conference on Computing, Communication and Networking Technologies, pp. 1-6, 2020.

[10] G. Shrivastava, D. N. Le, and K. Sharma, Cryptocurrencies and Blockchain Technology Applications, Hoboken, NJ: John Wiley & Sons, Inc., pp. 99-127, 2020.

[11] T. Zhou, J. Shen, Y. Ren, and S. Ji, "Threshold Key Management Scheme for Blockchain-Based Intelligent Transportation Systems," Security and Communication Networks, vol. 2021, article no. 1864514, 2021.

[12] S. S. Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Authentication and Key Management in Distributed IoT Using Blockchain Technology," IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12947-12954, 2021.

[13] N. Dissanayake, A. Jayatilaka, M. Zahedi, and M. A. Babar, "Software Security Patch Management - A Systematic Literature Review of Challenges, Approaches, Tools and Practices," Information and Software Technology, vol. 144, article no. 106771, 2022.

[14] F. Zhou and T. Y. Chen, "A Hybrid Approach Combining AHP with TODIM for Blockchain Technology Provider Selection Under the Pythagorean Fuzzy Scenario," Artificial Intelligence Review, vol. 55, no. 7, pp. 5411-5443, 2022.
[15] B. B. Gardas, A. Heidari, N. J. Navimipour, and M. Unal, "A Fuzzy-Based Method for Objects Selection in Blockchain-Enabled Edge-IoT Platforms Using a Hybrid Multi-Criteria Decision-Making Model," Applied Sciences, vol. 12, no. 17, article no. 8906, 2022.
[16] B. Alojaiman, "A Multi-Criteria Decision-Making Process for the Selection of an Efficient and Reliable IoT Application," Processes, vol. 11, no. 5, article no. 1313, 2023.
[17] N. M. Alshahrani, M. L. Mat Kiah, B. B. Zaidan, A. H. Alamoodi, and A. Saif, "A Review of Smart Contract Blockchain Based on Multi-Criteria Analysis: Challenges and Motivations," Computers, Materials & Continua, vol. 75, no. 2, pp. 2833-2858, 2023.
[18] Y. Zhao, Y. Qu, Y. Xiang, Y. Zhang, and L. Gao, "A Lightweight Model-Based Evolutionary Consensus Protocol in Blockchain as a Service for IoT," IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2343-2358, 2023.
[19] A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "Healthlock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications," Sensors, vol. 23, no. 15, article no. 6762, 2023.
[20] E. U. Haque, W. Abbasi, A. Almogren, J. Choi, A. Altameem, A. U. Rehman, et al., "Performance Enhancement in Blockchain Based IoT Data Sharing Using Lightweight Consensus Algorithm," Scientific Reports, vol. 14, article no. 26561, 2024.
[21] S. Almotairi, S. R. Addula, O. Alharbi, Z. Alzaid, Y. M. Hausawi, and J. Almutairi, "Personal Data Protection Model in IOMT-Blockchain on Secured Bit-Count Transmutation Data Encryption Approach," Fusion: Practice and Applications, vol. 16, no. 01, pp. 152-170, 2024.
[22] M. Z. Khan, M. Shoaib, M. S. Husain, K. Ul Nisa, and M. T. Quasim, "Enhanced Mechanism To Prioritize the Cloud Data Privacy Factors Using AHP and TOPSIS: A Hybrid Approach," Journal of Cloud Computing, vol. 13, no. 1, article no. 42, 2024.
[23] R. Dahiya, L. Samal, D. Samal, J. Kumar, V. Sharma, D. K. Sahni, et al., "A Blockchain Based Security System Framework in Healthcare Domain Using IoT," Journal of Electrical Systems, vol. 20, no. 3s, pp. 2039-2050, 2024.
[24] M. Deng, Y. Lyu, C. Yang, F. Xu, M. Ahmed, N. Yang, et al., "Lightweight Trust Management Scheme Based on Blockchain in Resource-Constrained Intelligent IoT Systems," IEEE Internet of Things Journal, vol. 11, no. 15, pp. 25706-25719, 2024.
[25] S. V. Matey, D. N. Raut, R. B. Pansare, and R. Kant, "A Hybrid Framework To Prioritize the Performance Metrics for Blockchain Technology Adoption in Manufacturing Industries," Journal of Modelling in Management, vol. 20, no. 3, pp. 701-731, 2025.
[26] L. García, C. Cancimance, R. Asorey-Cacheda, C. L. Zúñiga-Cañón, A. J. Garcia-Sanchez, and J. Garcia-Haro, "Lightweight Blockchain for Data Integrity and Traceability in IoT Networks," IEEE Access, vol. 13, pp. 81105-81117, 2025.
[27] W. Villegas-Ch, R. Gutierrez, A. M. Navarro, and A. Mera-Navarrete, "Lightweight Blockchain for Authentication and Authorization in Resource-Constrained IoT Networks," IEEE Access, vol. 13, pp. 48047-48067, 2025.
[28] S. A. Mohammed Uveise and S. M. H. Sithi Shameem Fathima, "Efficient Lightweight Blockchain with Hybridized Consensus Algorithm for IoT Networks," IETE Journal of Research, vol. 70, no. 12, pp. 8527-8537, 2024.
[29] S. R. Addula, M. K. Meesala, P. Ravipati, and G. S. Sajja, "A Hybrid Autoencoder and Gated Recurrent Unit Model Optimized by Honey Badger Algorithm for Enhanced Cyber Threat Detection in IoT Networks," Security and Privacy, vol. 8, no. 6, article no. e70086, 2025.

Appendix

This appendix provides a concise demonstration of the conversion of expert responses into a numerical pairwise comparison matrix using the geometric mean method. The values are shown as Saaty [1] numeric equivalents of the linguistic ratings (Table A1). Table A2 shows the worked example of data integrity versus node performance, including per-expert ratios and the geometric mean calculation. For each expert, the pairwise entry of DI and NP is obtained as the ratio of their numeric ratings (DI vs NP).

Their geometric mean is calculated as, GM = $(9 \times 21 \times 25)^{(1/3)}$ = 16.780. When calculated across all 75 experts instead of only three, the aggregated geometric mean for the (DI, NP) pair is equals to approximately 10.907, as reported in Table 5 (Numerical pairwise comparison matrix). The same procedure—computing the ratio followed by the geometric mean— is applied to every factor pair to construct the full aggregated 9 × 9 pairwise comparison matrix.

Table A1 Sample raw numeric ratings (3 experts)

Factor	Expert 1	Expert 2	Expert 3
Node performance	1 (EE)	0.333 (ML)	0.2(L)
Network performance	3 (MH)	5 (H)	3 (MH)
Data integrity	9 (AH)	7 (VH)	5 (H)
Access control	7 (VH)	9 (AH)	7 (VH)
Authentication	9 (AH)	9 (AH)	7 (VH)
Key management	3 (MH)	5 (H)	3 (MH)
Trust management	5 (H)	7 (VH)	5 (H)
Reliable transmission	7 (VH)	5 (H)	3 (MH)
Firmware update	5 (H)	7 (VH)	5 (H)

Table A2 Data integrity (DI) vs node performance (NP)

Expert	DI	NP	DI/NP ratio
Expert 1	9	1	9.000
Expert 2	7	0.333	21.000
Expert 3	5	0.2	25.000