sustainability

Article

Critical Controlling for the Network Security and Privacy Based on Blockchain Technology: A Fuzzy DEMATEL Approach

Firuz Kamalov [1], Mehdi Gheisari [2,3,4], Yang Liu [2,5,*], Mohammad Reza Feylizadeh [6,*] and Sherif Moussa [1]

[1] Department of Electrical Engineering, Canadian University Dubai, Dubai 144534, United Arab Emirates; firuz@cud.ac.ae (F.K.)

[2] Department of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China; mehdi.gheisari61@gmail.com

[3] Department of Cognitive Computing, Institute of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, India

[4] Department of Computer Science, Islamic Azad University of Tehran, Tehran 1468763785, Iran

[5] Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies, Shenzhen 518055, China

[6] Department of Industrial Engineering, Shiraz Branch, Islamic Azad University, Shiraz 7473171987, Iran

* Correspondence: liu.yang@hit.edu.cn (Y.L.); mo.feylizadeh@iau.ac.ir (M.R.F.)

Abstract: The Internet of Things (IoT) has been considered in various fields in the last decade. With the increasing number of IoT devices in the community, secure, accessible, and reliable infrastructure for processing and storing computed data has become necessary. Since traditional security protocols are unsuitable for IoT devices, IoT implementation is fraught with privacy and security challenges. Thus, blockchain technology has become an effective solution to the problems of IoT security. Blockchain is an empirical data distribution and storage model involving point-to-point transmission, consensus mechanism, asymmetric encryption, smart contract, and other computer technologies. Security and privacy are becoming increasingly important in using the IoT. Therefore, this study provides a comprehensive framework for classifying security criteria based on blockchain technology. Another goal of the present study is to identify causal relationship factors for the security issue using the Fuzzy Decision-Making Trial-and-Evaluation Laboratory (FDEMATEL) approach. In order to deal with uncertainty in human judgment, fuzzy logic is considered an effective tool. The present study's results show the proposed approach's efficiency. Authentication (CR6), intrusion detection (CR4), and availability (CR5) were also introduced as the most effective and essential criteria, respectively.

Keywords: network security and privacy; blockchain technology; cause and effect; fuzzy DEMATEL

check for updates

Citation: Kamalov, F.; Gheisari, M.; Liu, Y.; Feylizadeh, M.R.; Moussa, S. Critical Controlling for the Network Security and Privacy Based on Blockchain Technology: A Fuzzy DEMATEL Approach. *Sustainability* **2023**, *15*, 10068. https://doi.org/10.3390/su151310068

Academic Editors: Yan Yan and Shanwu Tian

Received: 3 March 2023
Revised: 26 May 2023
Accepted: 31 May 2023
Published: 25 June 2023

1. Introduction

The increasing complexity of today's networks makes it more challenging to keep track of all the devices, services, users, and other network entities [1,2]. Even network and system administrators may lose track of assets under their control in vast and diverse networks with thousands of devices and users [3,4]. In a computer network, various services and protocols are installed and configured in order to provide services to users. Some services are ready for all kinds of attacks, and in the first stage and during their installation and configuration, it is necessary to be careful about safety issues. Additionally, in the second stage, unnecessary services and protocols should be avoided [5–8]. Therefore, it can be acknowledged that the network's security should be considered whenever the network and communications are discussed. Further, as the Internet and information grow, the need for Network Security (NS) becomes more important [9,10]. Therefore, creating reliable infrastructure in computer networks is a necessity. In other words, users should be aware of the hazards of online social networks, such as privacy, in this technologically advanced day [11–15].

Some studies focused on traditional security measures to secure communication across devices, such as authentication, privacy, and trust management [16–18]. They are, however, insufficient since data must be safely transmitted to the correct location, at the proper time, and in a valid format [19–21]. Others focus on the literature surrounding the use of blockchains. Blockchain Technology (BT) and traditional security measures can neutralize all hostile threats posed by real-world physical equipment [22–24]. The ability of a user to keep their confidential information private or choose the level of information disclosure in a shared context is known as privacy. The term "privacy" describes two elements in blockchain networks. The following are two types of transaction privacy in blockchains [25]:

1. **Privacy of Users (Anonymity):** User privacy refers to transforming a blockchain user's genuine identity into something that cannot be traced while ensuring that the original identity remains untraceable. It masks the user's identity by replacing their genuine network address with a computer-generated one [26];
2. **Personal Data Privacy (Confidentiality):** The privacy of blockchain data is maintained by hiding the contents of a transaction. Confidentiality is another term for data privacy. Data confidentiality ensures that the contents of transactions are protected from illegal access, manipulation, and alteration [27].

Today, BT attracts much interest from academics and scientists for various reasons, including access control, data security, privacy, and wireless network decentralization. Though blockchain has multiple advantages, such as peer-to-peer technology, anonymity, enhanced capacity, and improved security, its immutable structure is the primary reason for its popularity. The BT is an efficient technology for data protection and privacy. Blockchain works because it uniquely has a decentralized and distributed structure and cryptographic features. The network's top priority is information security and confidentiality, so BT is preferred [28–30].

The blockchain is a strong security system that relies on encryption, communication technologies, and consensus. Blockchain is changing the IoT system in various ways. The IoT can attain high-security standards for blockchain properties. Some of these properties are decentralized peer-to-peer networks and open and transparent multiparty consensus. BT can be used in various applications, including identity management, Supply Chain Management (SCM), and the IoT [22]. Blockchain and related technologies can tackle several of the Internet's most serious security challenges. Some examples include [31,32]:

- Consensus processes in blockchain maintain Internet security;
- Blockchain is a solution to Internet's insecurity.
- Blockchain can dramatically lower equipment costs while improving Internet infrastructure's effectiveness;
- Blockchain has the potential to extend the life of products and services.

As mentioned above, the network and Internet services are the fastest and most accessible communication tools. Therefore, with the increasing growth of the Internet and electronic communication, electronic security and information secrecy have become more apparent. Given the importance of the issue and the studies conducted in this field, we found criteria to assess the security level and achieve security goals. However, no systematic classification of security criteria based on BT is available. We propose a systematic framework for identifying security criteria based on BT to address this. In the first step, a set of security criteria was collected through surveys within the proposed framework. In the next step, effective and influential factors for security were considered using the FDEMATEL method as a decision-making tool. Then, using the FDEMATEL approach, causal relationships are evaluated. In the proposed framework, fuzzy logic has been used to deal with the inherent ambiguities in human judgment.

2. Literature Review

Jakeri and Hassan [33] introduced the adaptive security activity selection model as a Multi-criteria Decision Making (MCDM) problem. The results of this study were used to select security activities. Zhou et al. [34] identified practical scenarios and technological barriers to BT in trade. Then, using the DEMATEL method, they investigated the degree of impact and analyzed the causal mechanism of the identified factors. Karuppiah et al. [35] developed a framework for identifying and evaluating the challenges in accepting the blockchain in S.C.M. First. They identified 40 challenges for obtaining the blockchain using the fuzzy Delphi technique. The challenges were then assessed using the grey DEMATEL method. Varshney et al. [36] discussed the blockchain with its key features. They also outlined various security principles such as confidentiality, integrity, availability, attacks on the network, and countermeasures. Schlecht et al. [37] created a study based on the Delphi approach to identify the potential for the future value of the blockchain for organizations by 2030. This research also helped in technological forecasting and strategic planning by providing indications for blockchain developments and practical advice to managers. Schwerin [38] expressed the opportunities, limitations, and suggestions using the Delphi approach and with the help of a panel of 25 experts. Therefore, it was found that blockchains can lead to more friendly privacy if enabled.

Kamalov et al. [39] developed an automatic intrusion detection system using a fusion machine-learning approach. They utilized the orthogonal variance decomposition technique to identify the most pertinent features in network traffic data, which were then used to construct a deep neural network for intrusion detection. The proposed algorithm was able to detect DDoS attacks with 100% accuracy. The results of the tests showed that the proposed method has great potential. Kamalov et al. [40] conducted a study to identify the most important features of network traffic data that could be used for intrusion detection and developed efficient machine-learning-based detection systems.

Furthermore, they proposed a novel feature selection technique that considers continuous input features and discrete target values. Their results indicated that their method outperformed existing benchmark selection methods. The authors concluded that their findings could benefit experts looking to create automated intrusion detection systems. Thabtah and Kamalov [41] conducted a study to assess the effectiveness of predictive models with rules for phishing detection. To do this, they tested four different rule-based classifiers from greedy, associative classification, and rule induction categories on real phishing datasets and measured their performance using various metrics.

Wang et al. [42] proposed a blockchain-distributed data integrity audit scheme. This scheme provides a brand-new method that allows customers to store data safely without relying on any specific Third-Party Auditor and protect users' privacy at a lower cost. For this new concept, this paper points out the problems of the existing scheme and puts forward system and security models. Additionally, in other research, Wang et al. [43] proposed a scheme to solve this problem. However, in this paper, we show their scheme is not secure. Concretely, the adversary can easily forge tags for outsourced data. Thus, the correctness of the group sum evaluation cannot be guaranteed any more.

Mohammad and Pradhan [44] proposed a Machine-Learning-Assisted Cloud Computing Model with big data analytics to enhance security and boost data transmission speeds. Their experiments revealed that the Machine-Learning-Assisted Cloud Computing Model had a data transmission rate of 96.4%, efficient data management of 94.3%, a computational time of 35.2%, an accuracy of 91.7%, and a performance of 95.2%. Gheisari et al. [45] initially proposed a federated machine-learning approach for a privacy-preserving edge intelligence model.

Iqbal et al. [46] presented an outline of critical issues and challenges of the IoT and Chines blockchain that demonstrated the safety requirements for the IoT and blockchain design. They then used the DEMATEL technique to categorize these challenges. Si et al. [47] proposed a security framework for sharing IoT information based on BT. The results showed that the framework is secure, practical, and feasible, and verifying system spatial information for secure storage devices is possible. Azizi et al. [1] aimed to create an intelligent SCM using the IoT and the blockchain for the first time. This study identified IoT and blockchain indicators as causes based on the DEMATEL method. Kabak et al. [48] proposed a three-step process for finding critical success factors for an industrial sector. They highlighted Critical Success Factors (CSFs) using the FDEMATEL and Delphi methods.

Guo et al. [49] proposed a new conceptual network approach for the intelligent diagnosis of medical device defects. The relationships between the common people were identified to minimize the effect of uncertain factors using the FDEMATEL method.

Han et al. [50] used Hesitant Fuzzy Linguistic Term Sets (HFLTSs) to streamline the specialists' statements concerning a direct effect level between elements. This research provided an algorithm for the multi-granular scaled assessment. Two configurable possibility thresholds are incorporated into the algorithm.

Suzan and Yavuzer [51] presented a FDEMATEL technique for assessing the most prevalent diseases. When examining the findings, it was revealed that dyspepsia, hyperlipidemia, and anemia were essential factors. The results show that they successfully employed these strategies to uncover the cause–effect relationship in the current investigation.

Lin et al. [52] used a hybrid methodology to determine the most influential criteria by combining fuzzy logic and DEMATEL. The results suggest that service quality, customer relationships, bank performance, and COVID-19 are in order of influence. The most critical factors are customized investment information, switching behavior, fee income, and the number of confirmed cases in the top five nations affected by COVID-19.

A dynamic group DEMATEL technique based on HFLTSs was developed by Xie et al. [53]. Additionally, it thoroughly considers the impact of expert weight on hesitation and fuzziness in expert preference representation.

Today, the Internet's demand is rapidly expanding, with attractive technologies. With the expansion and development of Internet use, its users face many security problems. The resulting issues become more severe as the Internet becomes more common in technology. Designing and implementing a safe and secure environment on the Internet is one of today's significant challenges. Several studies have been conducted to identify security standards on social and Internet networks, and researchers from various aspects have considered this issue. Traditional databases have always had shortcomings that have caused much damage. This defect is due mainly to their centralization. In case of system failure, all the organization's information is lost. Maintaining and creating stable conditions for traditional information systems has high costs. BT is a secure, reliable, distributed, and transparent enterprise-system database. In addition to increasing security in data storage, BT can better organize information and reduce error rates.

The present study is based on the need expressed in recent articles in this field. This study provides a comprehensive framework for security standards based on the new Chinese BT. The proposed research solution is designed in a three-step approach using conventional multi-criteria decision-making tools. In this framework, the FDEMATEL method is used to investigate the direct effects of the criteria and form a conceptual model of these effects. The combination of DEMATEL's approach and fuzzy logic deals with the ambiguities and uncertainties in human judgment. Identifying effective security criteria using BT shows the need to apply this technique in NS. This issue is a strength of the current research and leads to operational transparency. Accordingly, the innovations of this research are as follows:

- Identifying effective security criteria using BT shows the need to apply this technique in NS;
- Provides a comprehensive framework for security standards based on the new Chinese BT;
- The proposed research solution is designed in a three-step approach using conventional multi-criteria decision-making tools.

3. Research Methodologies

In this section, we introduce fuzzy logic, FDEMATEL, and the research methodology of this study.

3.1. Fuzzy Logic

In ordinary linguistic variables, many statements are expressed in numerical terms, such as short, good, young, and hot, and it is essential for understanding to take these scales into account. In this procedure, however, the main problem is that numerical data are generally not accurate enough or fluctuate excessively [54–56]. A syntactic representation is required to account for the fact that some information does not fall within the numeric realm. Since verbal expressions accept fuzzy variables as quantities, they are more precise than fuzzy expressions. There may be synthetic or natural variables, sentences, or words in a language and their quantities. As an example, the temperature of a liquid may be considered a fuzzy variable when it assumes values such as cold, cool, warm, and hot. In addition, the term 'old' or 'young' can also be considered fuzzy when referring to a specific age. As a result of their capability to provide an approximate and optimal explanation for complex phenomena, fuzzy variables are widely recognized as an effective tool for doing so.

Definition 1 (Fuzzy relation). *Let X, Y be two universes of discourse, and a fuzzy subset R of $X \times Y = \{(x,y)|x \in X, y \in Y\}$ is considered a fuzzy relationship from X to Y:*

$$R = \{(x,y), \mu_R(x,y)|\,(x,y) \in X \times Y\},\ \mu_R(x,y) = \begin{cases} 1, (x,y) \in R \\ 0,\ (x,y) \notin R' \end{cases}$$

The degree of R relationship between X and Y is reflected by the $R(x,y)$ function, in which $\mu_R(x,y)$ represents the membership function.

Definition 2 (Max–min composition). *Considering $R_1(x,y)$ and $R_2(y,z)$ as two fuzzy relations of $(x,y) \in X \times Y$ and $(y,z) \in Y \times Z$, max–min composition $R_1 \circ R_2$ is presented as follows:*

$$R_1 \circ R_2 = \{(x,z), Max_y\{Min\{\mu_{R_1}(x,y), \mu_{R_2}(y,z)\}\}|\,x \in X, y \in Y, z \in Z\}$$

Definition 3 (Fuzzy equivalence relations). *The fuzzy relation R on $X \times X$ indicates a fuzzy equivalence relation by meeting the three conditions as described below:*

(1) *Reflexive: $\mu_R(x,x) = 1; \forall x \in X$.*
(2) *Symmetric: namely, $R(x,y) = R(y,x); \forall x \in X, y \in Y$.*
(3) *Transitive: $R \circ R \subseteq R\ (R^2 \subseteq R)$.*

Definition 4 [57] *(α-cut).* *The α-cut set of the fuzzy relation (R_α) is:*

$$R_\alpha = \{(x,y), \mu_{R_\alpha}(x,y)|\,\mu_R(x,y) \geq \alpha, (x,y) \in X \times Y\}$$

The n α-cut of an original relation is further represented in trees; each level represents a representative relation of a finite number of elements. Several researchers use Triangular Fuzzy Numbers (TFNs) and Trapezoidal Fuzzy Numbers (TrFNs) in Multi-criteria Decision Making. Our study uses TrFNs [58,59]. A TrFN (Figure 1) has the advantage that it is a general case over a TFN. Hence, TFNs can be regarded as specific cases of TrFNs. Since a general case provides more helpful information than a particular case, we prefer to use TrFNs [60]. Additionally, the model of this research can also be used when TFNs are necessary because the model can easily be applied by equating two middle parameters in a TrFN. Meanwhile, the parameters a, b, c and d are shown in Figure 1 for better understanding the TrFN.

Definition 5 (The distance of TrFNs). *Regarding the algorithm mentioned above, the distance between the two TrFNs are considered; namely, $A_i = (c_i, a_i, b_i, d_i)$ and $A_k = (c_k, a_k, b_k, d_k)$, which is denoted by $d_p(A_i, A_k)$ as follows:*

$$d_p(A_i, A_k) = \begin{cases} [0.25(|c_i - c_k|^p + |a_i - a_k|^p + |b_i - b_k|^p + |d_i - d_k|^p)]^{\frac{1}{p}}, 1 \leq p < \infty \\ max\{|c_i - c_k|, |a_i - a_k|, |b_i - b_k|, |d_i - d_k|\}, p = \infty \end{cases}$$

It is important to note that the Manhattan distance is calculated for $(p = 1)$, Euclidean distance for $(p = 2)$, and Chebyshev distance for $(p = \infty)$. The Euclidean distance is employed in this paper to calculate the TrFNs' $(p = 2)$ distance.

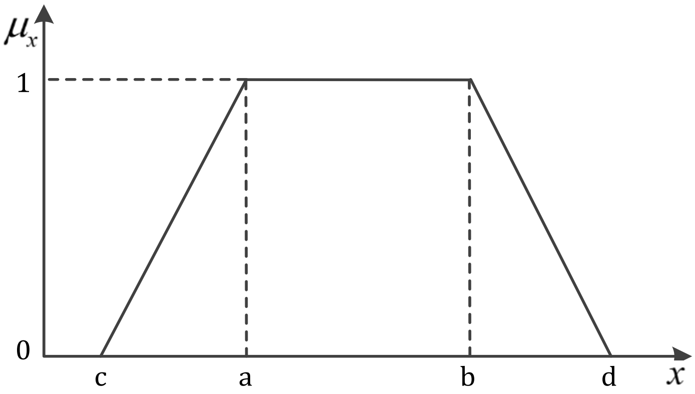

Figure 1. Membership function of a TrFN.

3.2. Fuzzy DEMATEL

To analyze a system's causal relationships and the status of its elements, A. Gabus and E. Fontela developed the DEMATEL method based on graph and matrix theory [61]. A research system's components are analyzed according to their type and severity, and their direct and indirect relationships are visualized using this method. Using DEMATEL, we can more fully understand the relationships between structural components in a research system as well as organize elements in the form of cause-and-effect groups. Solving complex system problems requires the discovery of the ideal solution. However, DMs generally make judgments based on their abilities and experiences rather than addressing specific values or addressing them in their judgments [62,63].

Consequently, the DEMATEL method cannot be used to determine the long-term impact of factors on BT at the HSC level. As a result, the DEMATEL method requires modification using fuzzy set theory [64]. For decision-making in an uncertain environment, this method uses linguistic evaluation. This section briefly overviews the fuzzy DEMATEL method developed by Wu and Lee [64] and Hiete et al. [65]. The following are the steps involved in the implementation of fuzzy DEMATEL:

Step 1. An expert determines the degree to which the factors are directly related.

This step aims to design a suitable fuzzy linguistic scale and associated fuzzy numbers to obtain a collective perspective from experts regarding the intended outcome. As a result, these opinions are collected and registered as fuzzy numbers, which are then merged. Fuzzy aggregation methods facilitate the maximization of dispersed opinions due to their ability to maximize the number of dispersed opinions; nevertheless, there are disadvantages associated with such methods. Therefore, Lin et al. [66] suggested using methods with smaller fuzzy sets for such applications. Expert opinions can be fused using the fuzzy average. For n TrFNs $(F_{ave}) \cong (c, a, b, d)$, the fuzzy average is calculated as follows:

$$\widetilde{F_{ave}} = \left(\frac{\sum_i^n c}{n}, \frac{\sum_i^n a}{n}, \frac{\sum_i^n b}{n}, \frac{\sum_i^n d}{n} \right).$$

Step 2. The subsequent step in the fuzzy DEMATEL method is centered on extracting the fuzzy direct relation matrix. This $n \times n$ matrix $(\widetilde{U})$ describes the relationships among the influential factors $F_1, F_2, \ldots, F_n$, as follows:

$$\widetilde{U} = \left[\widetilde{u}_{ij}\right]_{n \times n} \ (i, j = 1, 2, 3, \ldots, n),$$

TrFN $\widetilde{u}_{ij} = \left(c_{ij},\ a_{ij},\ b_{ij},\ d_{ij}\right)$ indicates the direct relationship between factors F_i and Fj according to the fuzzy direct relation matrix's fuzzy measurement scale. Where $i = j$, we have all cases $\widetilde{u}_{ij} = (0,\ 0,\ 0,\ 0)$.

Step 3. The normalization of the fuzzy direct relation matrix is this step of the fuzzy DEMATEL method. A normalized fuzzy direct relation matrix, $\widetilde{N}$, can be expressed as follows concerning the initial fuzzy direct relation matrix $U \cong [\widetilde{u}_{ij}]_{(n\times n)}$ $(i, j = 1, 2, 3, \ldots, n)$:

$$\widetilde{N} = \left[\widetilde{n}_{ij}\right]_{n\times n} (i,j = 1,2,3,\ldots,n),\ \widetilde{n}_{ij} = \frac{\left(\widetilde{u}_{ij} - \underset{1\le i\le n}{min} c^t_{ij}\right)}{max^n_{i=1} d^t_{ij} - min^n_{i=1} c^t_{ij}},$$

In each column of the matrix $\widetilde{U}$, $min\ c^t_{ij}$ and $max\ d^t_{ij}$ are the lowest lower and the highest upper bounds.

Step 4. Defuzzifying the normalized fuzzy direct relation matrix is the objective of this step. A method for converting fuzzy numbers into relevant, crisp values has been proposed by Opricovic and Tzeng [60]. Compared to conventional methods, such as the center of the area and the center of gravity, CFCS can distinguish between different versions of fuzzy equivalents for two identical crisp values. Here is a detailed explanation of the CFCS technique [67].

3.2.1. Calculation of the Left and Right Bounds of Normal Values

Definition 6. *Assume that N $\cong [\widetilde{n}_{ij}]_{(n\times n)}$ (i,j = 1, 2, 3, …, n) represents a normalized fuzzy direct relation matrix, and that$\widetilde{N}_{ij} = \left(c_{ij},\ a_{ij},\ b_{ij},\ d_{ij}\right)$is a TrFN that describes the matrix (Table 1). Equations (1) and (2) can be used to calculate both the left and right bounds of normal values:*

$$c^s_{ij} = \frac{a^x_{ij} + b^x_{ij}}{\left(1 + a^x_{ij} + b^x_{ij} - c^s_{ij}\right)} \tag{1}$$

$$d^s_{ij} = \frac{d^x_{ij}}{\left(1 + d^x_{ij} - a^s_{ij} - b^s_{ij}\right)} \tag{2}$$

There are two bounds to normal values, left and right, denoted by c^s_{ij} and d^s_{ij}, respectively.

Table 1. Fuzzy linguistic scale used in the present research.

Preference in Terms of Score	Description of the Linguistic Variable	Equivalent Trapezoidal Fuzzy Numbers (TrFN)
0	No Influence (No)	(0, 0, 0.1, 0.2)
1	Very Low Influence (VL)	(0.1, 0.2, 0.3, 0.4)
2	Low Influence (L)	(0.3, 0.4, 0.5, 0.6)
3	High Influence (H)	(0.5, 0.6, 0.7, 0.8)
4	Very High Influence (VH)	(0.7, 0.8, 0.9, 1)

3.2.2. Calculation of Crisp Normalized Values

By applying Equation (3), we can obtain the crisp normalized values for the right and left bounds of normal values:

$$Y_{ij} = \frac{c^s_{ij}\left(1 - c^s_{ij}\right) + (d^s_{ij})^2}{\left(1 - c^s_{ij}\right) + d^s_{ij}} \tag{3}$$

3.2.3. Computation of Final Crisp Values

In the final phase of the CFCS algorithm, Equation (4) calculates the final crisp direct relation matrix:

$$Z_{ij} = \left(Y_{ij} \times \left(max\ d_{ij}^{t} - min\ c_{ij}^{t}\right)\right) + \underset{1\,\leq\,i\,\leq\,n}{min}\ c_{ij}^{t} \tag{4}$$

Step 5. This step calculates the crisp total relation matrix.

Equation (5) computes the crisp total relation matrix $T = \left[t_{ij}\right]_{n\times n}\ (i, j = 1, 2, 3, \ldots, n)$:

$$T = \lim_{k\to\infty}\left(Z + Z^2 + \cdots + Z^k\right) = Z(I - Z)^{-1} \tag{5}$$

In Equation (5), the identity matrix is shown by I.

Step 6. The row and column sums of the matrix T are R_j (j = 1, 2, . . . , n) C_i (i = 1, 2, . . . , n) and are computed as follows:

$$T = \left[T_{ij}\right]_{n\times n}\ (i, j = 1, 2, 3, \ldots, n) \tag{6}$$

$$R_j = \left[\sum_{j=1}^{n} T_{ij}\right]_{1\times n} = \left[r_j\right]_{1\times n} \tag{7}$$

$$C_i = \left[\sum_{i=1}^{n} T_{ij}\right]_{1\times n} = \left[c_i\right]_{1\times n} \tag{8}$$

- The sum of rows and columns of matrix Z's crisp values yields Rj and Ci vector representations. Summing rows and columns can determine a barrier's influence and influenceability. Using the $(R_j - C_i)$ index, it is possible to explain the causal–effect relationship between the barriers. In terms of influence power, this index represents the barrier's total effects. The $(R_j - C_i)$ index explains how barriers are related causally using the relation map as a cause-and-effect category. Positive index values indicate that the factor has influenced other factors, whereas negative values indicate that other factors have affected the factor. Figure 2 depicts the procedures implicated in the fuzzy DEMATEL method.

3.3. Important Factors

In this part, the nine selected factors are described as follows:

- **Reliability (CR1)**: Reliability would fulfill IoT device safety, auditing, and inspection [67];
- **Prevention (CR2)**: A technique to enhance IoT cyber security against attacks that consume bandwidth in modern IoT devices [68];
- **Network access management (CR3):** Related to IoT access management, which is occasionally developed by the Internet Engineering Task Force or the Open Mobile Alliance [69];
- **Intrusion detection (CR4)**: Intrusion Detection Systems (IDS) are used in cloud systems to detect cyberattacks [70];
- **Availability (CR5)**: The blockchain's persistence property causes availability. Once an update is included in a valid block on the blockchain, it is impossible to remove it [71];
- **Authentication(CR6)**: The authentication mechanism ensures that only authorized users can exchange data and access resources [72];
- **Privacy (CR7)**: The blockchain concept encompasses the user's and transactions' privacy [73];
- **Integrity (CR8)**: Any change or error will prevent correct decryption, ensuring integrity. Using private keys provides security [74,75];

- **Confidentiality (CR9)**: To be considered private, payments must have two properties: (a) confidentiality, i.e., concealing the transferred amounts, and (b) anonymity, i.e., concealing the identities of the sender and receiver in a transaction [76,77].

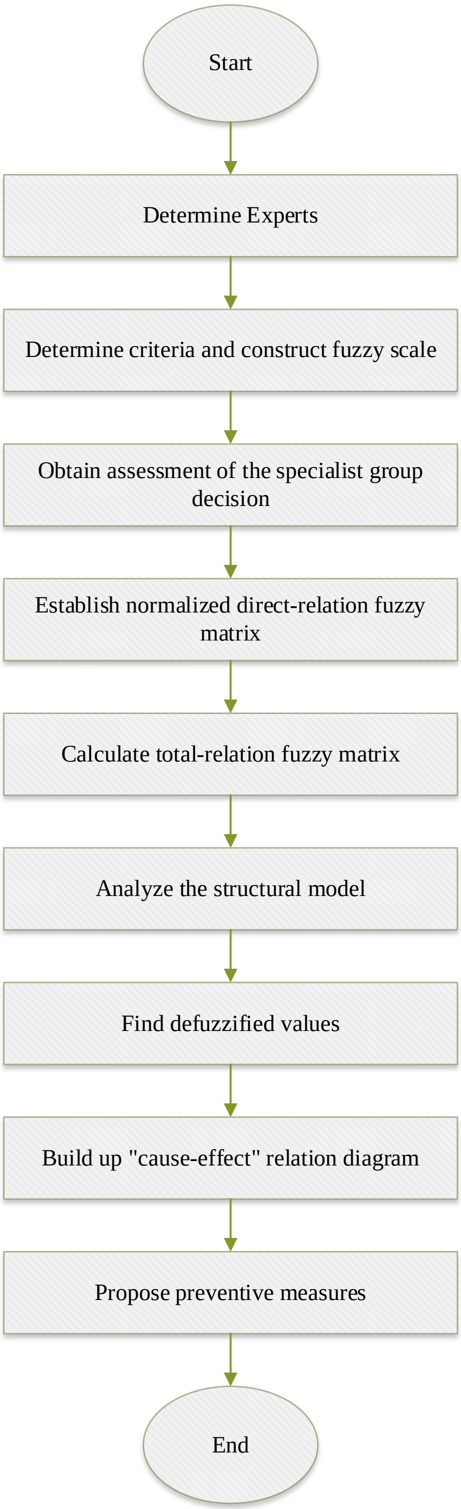
Start
Determine Experts
Determine criteria and construct fuzzy scale
Obtain assessment of the specialist group decision
Establish normalized direct-relation fuzzy matrix
Calculate total-relation fuzzy matrix
Analyze the structural model
Find defuzzified values
Build up "cause-effect" relation diagram
Propose preventive measures
End

Figure 2. Application order of the fuzzy DEMATEL Method.

4. An Illustrative Case Study of Fuzzy DEMATEL

In a blockchain, there is no need to control access to networks; the protocols of these networks allow anyone to enter the network and access and participate in it. In contrast, specific blockchains require appropriate security controls to protect network access. An ideal assumption is that LANs and systems, because of their private nature, are protected behind security layers such as firewalls, VPNs, VLANs, intrusion detection and prevention systems, and through a strategy known as in-depth defense. However, security scenarios in the ideal world are very dreamy, and relying on these security control methods will not be effective in the real world. Organizations must identify their change risk profile and determine acceptable cyber risk. This issue is addressed according to the priorities of each organization and the amount of their investment. Organizations and stakeholders in the blockchain network should be aware that in-house employees, suppliers, and trusted partners may cause errors or take actions that could lead to sabotage. Therefore, paying attention to the weaknesses of end-to-end user processes seems necessary. Resolving such challenges requires the relevant organizations to implement a comprehensive cybersecurity program. This comprehensive plan should include an organizational and governance framework that defines objectives, processes, accountability criteria, performance criteria, and, most importantly, a corporate change in people's mindsets. Advanced security controls can be performed with the help of blockchain.

Data encryption in blockchain protects the confidentiality of organizations' information and controls data access. For example, implementing secure communication protocols in blockchain (taking into account the latest security standards and implementation guidelines) safeguards against middleman attacks. By implementing such protocols, if an attacker intends to attack maliciously, they will still be unable to impersonate the audience or reveal information being traded and transmitted. Protecting user information, maintaining data privacy, personal authentication, and authentication to access and log in to the network are just a few of the actual uses of private keys.

The National Institute of Standards and Technology defines integrity as "protection against undue destruction or distortion of information and ensuring that information is accurate and non-denial". Maintaining the data's integrity and ensuring its accuracy throughout the life cycle of information systems is essential. Data encryption, hash comparison (or so-called data digestion), and digital signatures allow system owners to ensure the validity of their data, regardless of where the system is (running, resting, or storing). Blockchain technology can be considered a secure technology because its users can ensure the accuracy of transaction data. Using a combination of hash encryption and link encryption along with the decentralized structure of blockchain poses a severe challenge to those who intend to intervene in the technology's databases. This issue makes organizations that use blockchain technology more confident in the accuracy of their data. In addition, protocols based on the consensus model of this technology provide a higher level of security for organizations' data.

Given that the data are immutable, examining how it complies with the privacy policy will be essential. Implementing the right to forgetting in blockchain technology, which ensures that nothing will be erased, is an exciting challenge; fortunately, several solutions exist. One of these solutions is to encrypt personal information written in the system. Each transaction added to a public or private blockchain is digitally signed and dated. This issue means that organizations can, when needed, refer to a specific period to track each transaction and identify the parties involved (via the public blockchain address). This feature is related to one of the essential information security features, non-denial. The non-denial feature ensures that no one will copy their signature confirmation from a file or transaction they participated in. This extraordinary feature of blockchain greatly increases the system's reliability (by detecting aggressive attempts and fraudulent transactions) because each transaction is encrypted and linked to a specific user.

With the increasing attacks on computer networks on the one hand and the high dependence of the activities of various industrial, commercial, military, medical, and educational fields on the services provided by computer networks, efforts to prevent, detect, and infiltrate networks are significant. Intrusion detection detects and responds to malicious activity that attacks network resources. Therefore, efficient intrusion detection systems to ensure network security are essential. Methods such as user authentication, data encryption, firewall, etc., have been used to establish security in computer networks. Intrusion detection systems are critical elements in security infrastructure in many organizations. Intrusion detection systems use analytical methods to detect attacks, identify attack sources, and send alerts to network administrators.

Regarding those mentioned above and based on the information in Figure 3, among the examined criteria, authentication (CR6), intrusion detection (CR4), availability (CR5), integrity, and privacy, respectively, are the most effective and, the most important criteria. Additionally, the highest intensity of impact is related to the power of the effect of the authentication criterion (4.71), then associated with the intensity of the impact of intrusion detection (2.91), which indicates that the highest intensity of the effect is on the two criteria being imported that are most important in the system. Additionally, the existence of two-way communication, according to Table 2, among two of the nine criteria examined, clearly indicates the simultaneous and reciprocal effects of the criteria affecting network security and the appropriate use of the DEMATEL method in this study. It should also be noted that the impact intensity numbers listed on each bow are listed in Table 3. The criteria that affect some other criteria are indicated by the number one (highlighted cells), and those that are not affected are indicated by the number zero (Table 3).

Table 2. Crisp value of criteria.

Criteria	R	C	R + C	R − C	Cause/Effect
CR1	−1.07	−0.81	−1.87	−0.26	Effect
CR2	−1.05	−0.78	−1.82	−0.27	Effect
CR3	−2.69	−0.50	−3.19	−2.19	Effect
CR4	1.86	−1.05	0.82	2.91	Cause
CR5	1.15	0.47	1.62	0.68	Cause
CR6	1.16	−3.56	−2.40	4.71	Cause
CR7	−1.03	1.08	0.06	−2.11	Effect
CR8	−0.43	2.33	1.90	−2.75	Effect
CR9	−2.23	−1.51	−3.74	−0.71	Effect

Table 3. Relation matrix of values.

Criteria	CR1	CR1	CR1	CR1	CR1	CR1	CR1	CR1	CR1
CR1	1	0	0	0	0	0	0	1	0
CR2	0	1	1	0	0	1	1	0	0
CR3	0	0	1	1	0	0	1	1	1
CR4	1	0	1	1	1	1	1	1	0
CR5	0	1	0	1	1	0	1	1	1
CR6	0	1	1	0	1	1	1	1	0
CR7	1	1	1	0	1	1	1	1	0
CR8	0	0	0	1	0	0	1	1	1
CR9	1	0	1	0	1	1	0	0	1

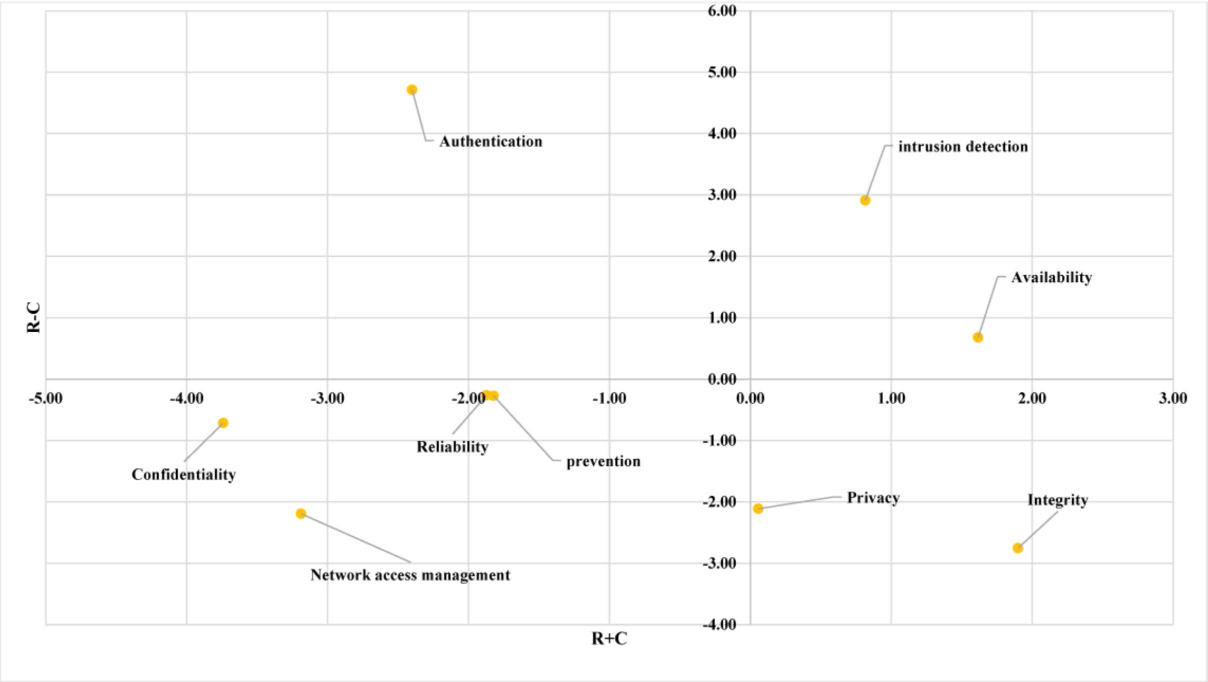

Figure 3. Cause–Effect Relation Diagram.

5. Conclusions

Blockchain technology is missing in solving security, scalability, privacy, and reliability on the Internet. Due to the properties of blockchain, it can be a good option for solving these issues. The key benefits of using blockchain technology in network security can be expressed in three points: building trust, reducing costs, and speeding up transactions. As a result, the network needs light, scalable, distributed security and privacy protection. Blockchain technology, the basis of Bitcoin as the first cryptocurrency system, has the potential to overcome the challenges listed due to its distributed, secure, and private nature. Its overall framework relies on a hierarchical structure that builds trust for blockchain security and privacy, making it more suited to the specific needs of the Internet. This issue is the case with a smart home, but the framework can be applied to other areas of network security.

Regarding the results, and based on the information in Figure 3, among the examined criteria, authentication (CR6), intrusion detection (CR4), availability (CR5), integrity, and privacy, respectively, are the most effective and, at the same time, the most important criteria. Additionally, the highest intensity of impact is related to the intensity of the impact of the authentication criterion (4.71), then associated with the intensity of the effect of intrusion detection (2.91), which indicates that the highest intensity of impact is on the two criteria being imported that are most important in the system. Further, according to Table 2, among two of the nine criteria examined, two-way communication indicates the existence of simultaneous and reciprocal effects of the criteria affecting network security and the appropriate use of the DEMATEL method in this study.

It should also be noted that the impact intensity numbers listed on each bow are listed in Table 3. As shown in Table 3, the criteria are represented by the numbers one and zero for effective and non-effective criteria.

Author Contributions: Conceptualization, M.G.; Investigation, Y.L.; Writing—original draft, M.R.F.; Visualization, S.M.; Funding acquisition, F.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by National Key Research and Development Program of China (No. 2020YFB1005805), Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies (2022B1212010005), Shenzhen Stable Supporting Program (General Project) (No. GXWD20201230155427003-20200821160539001), and China Southern Power Grid Technological Project (No. GDKJXM20201922).

Data Availability Statement: The authors state that data is unavailable due to privacy.

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

References

1. Azizi, N.; Malekzadeh, H.; Akhavan, P.; Haass, O.; Saremi, S.; Mirjalili, S. IoT–Blockchain: Harnessing the Power of Internet of Thing and Blockchain for Smart Supply Chain. *Sensors* **2021**, *21*, 6048. [CrossRef] [PubMed]
2. Kia, M.M.; Alzubi, J.A.; Gheisari, M.; Zhang, X.; Rahimi, M.; Qin, Y. A novel method for recognition of Persian alphabet by using fuzzy neural network. *IEEE Access* **2018**, *6*, 77265–77271. [CrossRef]
3. Ashourian, M.; Gheisari, M.; Hashemi Talkhoncheh, A. An improved node scheduling scheme for resilient packet ring network. *Majlesi J. Electr. Eng.* **2015**, *9*, 43–50.
4. Hassija, V.; Ratnakumar, R.; Chamola, V.; Agarwal, S.; Mehra, A.; Kanhere, S.S.; Binh, H.T.T. A Machine Learning and Blockchain Based Secure and Cost-Effective Framework for Minor Medical Consultations. *Sustain. Comput. Informatics Syst.* **2022**, *35*, 100651. [CrossRef]
5. Stephan, T.; Sharma, K.; Shankar, A.; Punitha, S.; Varadarajan, V.; Liu, P. Fuzzy-Logic-Inspired Zone-Based Clustering Algorithm for Wireless Sensor Networks. *Int. J. Fuzzy Syst.* **2021**, *23*, 506–517. [CrossRef]
6. Zanna, P.; Radcliffe, P.; Kumar, D. Preventing Attacks on Wireless Networks Using SDN Controlled OODA Loops and Cyber Kill Chains. *Sensors* **2022**, *22*, 9481. [CrossRef]
7. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT Security: Challenges and Solution Using Machine Learning, Artificial Intelligence and Blockchain Technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
8. Hendalianpour, A. Mathematical Modeling for Integrating Production-Routing-Inventory Perishable Goods: A Case Study of Blood Products in Iranian Hospitals. In Proceedings of the International Conference on Dynamics in Logistics, Breman, Germany, 20–22 February 2018; pp. 125–136.
9. Du, Y.W.; Sun, X.L. Influence Paths of Marine Ranching Ecological Security in China Based on Probabilistic Linguistic Term Sets and Qualitative Comparative Analysis. *Int. J. Fuzzy Syst.* **2021**, *23*, 228–242. [CrossRef]
10. Oktian, Y.E.; Le, T.-T.-H.; Jo, U.; Kim, H. RealPrice: Blockchain-Powered Real-Time Pricing for Software-Defined Enabled Edge Network. *Sensors* **2022**, *22*, 9639. [CrossRef]
11. Kumar, C.; Bharati, T.S.; Prakash, S. Online Social Network Security: A Comparative Review Using Machine Learning and Deep Learning. *Neural Process. Lett.* **2021**, *53*, 843–861. [CrossRef]
12. Wu, W.W. Mining Significant Factors Affecting the Adoption of SaaS Using the Rough Set Approach. *J. Syst. Softw.* **2011**, *84*, 435–441. [CrossRef]
13. Miglani, A.; Kumar, N. Blockchain Management and Machine Learning Adaptation for IoT Environment in 5G and beyond Networks: A Systematic Review. *Comput. Commun.* **2021**, *178*, 37–63. [CrossRef]
14. Liu, P.; Hendalianpour, A.; Hafshejani, M.F.; Yaghoobi, F.; Feylizadeh, M. System Dynamics Model: Developing Model for Supplier Selection with a Focus on CSR Criteria. *Complex Intell. Syst.* **2023**, *9*, 99–114. [CrossRef]
15. Hendalianpour, A.; Razmi, J.; Gheitasi, M. Comparing Clustering Models in Bank Customers: Based on Fuzzy Relational Clustering Approach. *Accounting* **2017**, *3*, 81–94. [CrossRef]
16. Yontar, E. Critical Success Factor Analysis of Blockchain Technology in Agri-Food Supply Chain Management: A Circular Economy Perspective. *J. Environ. Manag* **2023**, *330*, 117173. [CrossRef]
17. Singh, R.; Khan, S.; Dsilva, J.; Centobelli, P. Blockchain Integrated IoT for Food Supply Chain: A Grey Based Delphi-DEMATEL Approach. *Appl. Sci.* **2023**, *13*, 1079. [CrossRef]
18. Liu, P.; Hendalianpour, A.; Fakhrabadi, M.; Feylizadeh, M. Integrating IVFRN-BWM and Goal Programming to Allocate the Order Quantity Considering Discount for Green Supplier. *Int. J. Fuzzy Syst.* **2022**, *24*, 989–1011. [CrossRef]
19. Ge, H.; Yue, D.; Xie, X.; Deng, S.; Hu, S. Security Control of Networked T–S Fuzzy System Under Intermittent DoS Jamming Attack with Event-Based Predictor. *Int. J. Fuzzy Syst.* **2019**, *21*, 700–714. [CrossRef]
20. Alabool, H.; Kamil, A.; Arshad, N.; Alarabiat, D. Cloud Service Evaluation Method-Based Multi-Criteria Decision-Making: A Systematic Literature Review. *J. Syst. Softw.* **2018**, *139*, 161–188. [CrossRef]
21. Zhang, Y.; Chen, Y.; Miao, K.; Ren, T.; Yang, C.; Han, M. A Novel Data-Driven Evaluation Framework for Fork after Withholding Attack in Blockchain Systems. *Sensors* **2022**, *22*, 9125. [CrossRef]
22. Liu, P.; Hendalianpour, A.; Hamzehlou, M.; Feylizadeh, M.R.; Razmi, J. Identify and Rank the Challenges of Implementing Sustainable Supply Chain Blockchain Technology Using the Bayesian Best Worst Method. *Technol. Econ. Dev. Econ.* **2021**, *27*, 656–680. [CrossRef]

23. Jan, M.A.; Cai, J.; Gao, X.C.; Khan, F.; Mastorakis, S.; Usman, M.; Alazab, M.; Watters, P. Security and Blockchain Convergence with Internet of Multimedia Things: Current Trends, Research Challenges and Future Directions. *J. Netw. Comput. Appl.* **2021**, *175*, 102918. [CrossRef] [PubMed]
24. Siddiqui, Z.A.; Haroon, M. Application of Artificial Intelligence and Machine Learning in Blockchain Technology. In *Artificial Intelligence and Machine Learning for EDGE Computing*; Academic Press: Cambridge, MA, USA, 2022; pp. 169–185, ISBN 9780128240540.
25. Bailur, R.P.; Rao, S.; Iyengar, D. Use of Blockchain Partnerships to Enable Transparency in Supply Chain Digitization. In *The Oxford Handbook of Supply Chain Management*; Choi, T.Y., Li, J.J., Rogers, D.S., Schoenherr, T., Wagner, S.M., Eds.; Oxford University Press: Oxford, UK, 2020.
26. Amponsah, A.A.; Adekoya, A.F.; Weyori, B.A. A Novel Fraud Detection and Prevention Method for Healthcare Claim Processing Using Machine Learning and Blockchain Technology. *Decis. Anal. J.* **2022**, *4*, 100122. [CrossRef]
27. Junejo, A.Z.; Hashmani, M.A.; Memon, M.M. Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges. *Appl. Sci.* **2021**, *11*, 7013. [CrossRef]
28. Errampalli, M.; Patil, K.S.; Prasad, C.S.R.K. Evaluation of Integration between Public Transportation Modes by Developing Sustainability Index for Indian Cities. *Case Stud. Transp. Policy* **2020**, *8*, 180–187. [CrossRef]
29. Patil, P.; Sangeetha, M.; Bhaskar, V. Blockchain for IoT Access Control, Security and Privacy: A Review. *Wirel. Pers. Commun.* **2021**, *117*, 1815–1834. [CrossRef]
30. Gaur, R.; Prakash, S.; Kumar, S.; Abhishek, K.; Msahli, M.; Wahid, A. A Machine-Learning–Blockchain-Based Authentication Using Smart Contracts for an IoHT System. *Sensors* **2022**, *22*, 9074. [CrossRef]
31. Xu, L.D.; Lu, Y.; Li, L. Embedding Blockchain Technology into IoT for Security: A Survey. *IEEE Internet Things J.* **2021**, *8*, 10452–10473. [CrossRef]
32. Shen, B.; Xu, X.; Yuan, Q. Selling Secondhand Products through an Online Platform with Blockchain. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102066. [CrossRef]
33. Jakeri, M.M.; Hassan, M.F. Criteria Prioritization in Adaptive Security Activities Selection, ASAS Model Using Analytic Network Process, ANP. In Proceedings of the 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia, 19–21 November 2019; IEEE: Manhattan, NY, USA; pp. 6–11.
34. Zhou, J.; Wu, Y.; Liu, F.; Tao, Y.; Gao, J. Prospects and Obstacles Analysis of Applying Blockchain Technology to Power Trading Using a Deeply Improved Model Based on the DEMATEL Approach. *Sustain. Cities Soc.* **2021**, *70*, 102910. [CrossRef]
35. Karuppiah, K.; Sankaranarayanan, B.; Ali, S.M. A Decision-Aid Model for Evaluating Challenges to Blockchain Adoption in Supply Chains. *Int. J. Logist. Res. Appl.* **2023**, *26*, 257–278. [CrossRef]
36. Varshney, T.; Sharma, N.; Kaushik, I.; Bhushan, B. Authentication Encryption Based Security Services in Blockchain Technology. In Proceedings of the 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 18–19 October 2019; IEEE: Manhattan, NY, USA; Volume 2019, pp. 63–68.
37. Schlecht, L.; Schneider, S.; Buchwald, A. The Prospective Value Creation Potential of Blockchain in Business Models: A Delphi Study. *Technol. Forecast. Soc. Chang.* **2021**, *166*, 120601. [CrossRef]
38. Schwerin, S. Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study. *J. Br. Blockchain Assoc.* **2018**, *1*, 1–77. [CrossRef]
39. Kamalov, F.; Moussa, S.; El Khatib, Z.; Mnaouer, A.B. Orthogonal Variance-Based Feature Selection for Intrusion Detection Systems. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021; pp. 1–5.
40. Kamalov, F.; Moussa, S.; Zgheib, R.; Mashaal, O. Feature Selection for Intrusion Detection Systems. In Proceedings of the 2020 13th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China, 12–13 December 2020; pp. 265–269.
41. Thabtah, F.; Kamalov, F. Phishing Detection: A Case Analysis on Classifiers with Rules Using Machine Learning. *J. Inf. Knowl. Manag.* **2017**, *16*, 1750034. [CrossRef]
42. Wang, H.; Wang, X.A.; Xiao, S.; Liu, J. Sen Decentralized Data Outsourcing Auditing Protocol Based on Blockchain. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 2703–2714. [CrossRef]
43. Wang, X.A.; Liu, Y.; Sangaiah, A.K.; Zhang, J. Improved Publicly Verifiable Group Sum Evaluation over Outsourced Data Streams in IoT Setting. *Computing* **2019**, *101*, 773–790. [CrossRef]
44. Panda, S.; Modak, N.M.; Pradhan, D. Corporate Social Responsibility, Channel Coordination and Profit Division in a Two-Echelon Supply Chain. *Int. J. Manag. Sci. Eng. Manag.* **2016**, *11*, 22–33. [CrossRef]
45. Gheisari, M.; Wang, G.; Chen, S.; Seyfollahi, A. A method for privacy-preserving in IoT-SDN integration environment. In Proceedings of the 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), Melbourne, VIC, Australia, 11–13 December 2018; pp. 895–902. [CrossRef]
46. Iqbal, A.; Amir, M.; Kumar, V.; Alam, A.; Umair, M. Integration of next Generation IIoT with Blockchain for the Development of Smart Industries. *Emerg. Sci. J.* **2020**, *4*, 1–17. [CrossRef]
47. Si, H.; Sun, C.; Li, Y.; Qiao, H.; Shi, L. IoT Information Sharing Security Mechanism Based on Blockchain Technology. *Futur. Gener. Comput. Syst.* **2019**, *101*, 1028–1040. [CrossRef]

48. Kabak, Ö.; Ülengin, F.; Çekyay, B.; Önsel, Ş.; Özaydın, Ö. Critical Success Factors for the Iron and Steel Industry in Turkey: A Fuzzy DEMATEL Approach. *Int. J. Fuzzy Syst.* **2016**, *18*, 523–536. [CrossRef]
49. Guo, X.; Liu, A.; Li, X.; Xiao, Y. Research on the Intelligent Fault Diagnosis of Medical Devices Based on a DEMATEL-Fuzzy Concept Lattice. *Int. J. Fuzzy Syst.* **2020**, *22*, 2369–2384. [CrossRef]
50. Han, W.; Sun, Y.; Xie, H.; Che, Z. Hesitant Fuzzy Linguistic Group DEMATEL Method with Multi-Granular Evaluation Scales. *Int. J. Fuzzy Syst.* **2018**, *20*, 2187–2201. [CrossRef]
51. Suzan, V.; Yavuzer, H. A Fuzzy Dematel Method To Evaluate The Most Common Diseases In Internal Medicine. *Int. J. Fuzzy Syst.* **2020**, *22*, 2385–2395. [CrossRef]
52. Lin, A.J.; Chang, H.-Y.; Huang, S.-W.; Tzeng, G.-H. Improving Service Quality of Wealth Management Bank for High-Net-Worth Customers During COVID-19: A Fuzzy-DEMATEL Approach. *Int. J. Fuzzy Syst.* **2021**, *23*, 2449–2466. [CrossRef]
53. Xie, H.; Ren, Q.; Duan, W.; Sun, Y.; Han, W. New Dynamic Group DEMATEL Decision-Making Method Based on Hesitant Fuzzy Linguistic Term Sets. *Int. J. Fuzzy Syst.* **2021**, *23*, 2118–2131. [CrossRef]
54. Xu, X.; Su, P.; Wang, F.; Chen, L.; Xie, J.; Atindana, V.A. Coordinated Control of Dual-Motor Using the Interval Type-2 Fuzzy Logic in Autonomous Steering System of AGV. *Int. J. Fuzzy Syst.* **2021**, *23*, 1070–1086. [CrossRef]
55. Li, H.; Wang, W.; Fan, L.; Li, Q.; Chen, X. A Novel Hybrid MCDM Model for Machine Tool Selection Using Fuzzy DEMATEL, Entropy Weighting and Later Defuzzification VIKOR. *Appl. Soft Comput.* **2020**, *91*, 106207. [CrossRef]
56. Jana, S.H.; Jana, B. Application of Random Triangular and Gaussian Type-2 Fuzzy Variable to Solve Fixed Charge Multi-Item Four Dimensional Transportation Problem. *Appl. Soft Comput.* **2020**, *96*, 106589. [CrossRef]
57. Liu, P.; Hendalianpour, A.; Hamzehlou, M.; Feylizadeh, M. Cost Reduction of Inventory-Production-System in Multi-Echelon Supply Chain Using Game Theory and Fuzzy Demand Forecasting. *Int. J. Fuzzy Syst.* **2022**, *24*, 1793–1813. [CrossRef]
58. Parmar, P.S.; Desai, T.N. Evaluating Sustainable Lean Six Sigma Enablers Using Fuzzy DEMATEL: A Case of an Indian Manufacturing Organization. *J. Clean. Prod.* **2020**, *265*, 121802. [CrossRef]
59. Dutta, P. Mathematics of Uncertainty: An Exploration on Semi-Elliptic Fuzzy Variable and Its Properties. *SN Appl. Sci.* **2020**, *2*, 111. [CrossRef]
60. Hendalianpour, A.; Fakhrabadi, M.; Zhang, X.; Feylizadeh, M.R.; Gheisari, M.; Liu, P.; Ashktorab, N. Hybrid Model of IVFRN-BWM and Robust Goal Programming in Agile and Flexible Supply Chain, a Case Study: Automobile Industry. *IEEE Access* **2019**, *7*, 71481–71492. [CrossRef]
61. Jiang, S.; Shi, H.; Lin, W.; Liu, H.-C. A Large Group Linguistic Z-DEMATEL Approach for Identifying Key Performance Indicators in Hospital Performance Management. *Appl. Soft Comput.* **2020**, *86*, 105900. [CrossRef]
62. Opricovic, S.; Tzeng, G.H. Defuzzification within a Multi-criteria Decision Model. *Int. J. Uncertain. Fuzziness Knowl. Based Syst.* **2003**, *11*, 635–652. [CrossRef]
63. Mohammadfam, I.; Mirzaei Aliabadi, M.; Soltanian, A.R.; Tabibzadeh, M.; Mahdinia, M. Investigating Interactions among Vital Variables Affecting Situation Awareness Based on Fuzzy DEMATEL Method. *Int. J. Ind. Ergon.* **2019**, *74*, 102842. [CrossRef]
64. Amirghodsi, S.; Naeini, A.B.; Makui, A. An Integrated Delphi-DEMATEL-ELECTRE Method on Gray Numbers to Rank Technology Providers. *IEEE Trans. Eng. Manag.* **2020**, *69*, 1348–1364. [CrossRef]
65. Chen, L.; Hendalianpour, A.; Feylizadeh, M.R.; Xu, H. Factors Affecting the Use of Blockchain Technology in Humanitarian Supply Chain: A Novel Fuzzy Large-Scale Group-DEMATEL. *Gr. Decis. Negot.* **2023**, *32*, 359–394. [CrossRef]
66. Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards Decentralized IoT Security Enhancement: A Blockchain Approach. *Comput. Electr. Eng.* **2018**, *72*, 266–273. [CrossRef]
67. Choudhary, S.; Kesswani, N. Detection and Prevention of Routing Attacks in Internet of Things. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing, New York, NY, USA, 1–3 August 2018; pp. 1537–1540.
68. Novo, O. Scalable Access Management in IoT Using Blockchain: A Performance Evaluation. *IEEE Internet Things J.* **2019**, *6*, 4694–4701. [CrossRef]
69. Alkadi, O.; Moustafa, N.; Turnbull, B. A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions. *IEEE Access* **2020**, *8*, 104893–104917. [CrossRef]
70. Boudguiga, A.; Bouzerna, N.; Granboulan, L.; Olivereau, A.; Quesnel, F.; Roger, A.; Sirdey, R. Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain. In Proceedings of the 2nd IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017; IEEE: Manhattan, NY, USA; pp. 50–58.
71. Khan, M.A.; Salah, K. IoT Security: Review, Blockchain Solutions, and Open Challenges. *Futur. Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
72. Zhang, R.; Xue, R.; Liu, L. Security and Privacy on Blockchain. *ACM Comput. Surv.* **2019**, *52*, 51. [CrossRef]
73. Gheisari, M.; Ebrahimzadeh, F.; Rahimi, M.; Moazzamigodarzi, M.; Liu, Y.; Dutta Pramanik, P.K.; Heravi, M.A.; Mehbodniya, A.; Ghaderzadeh, M.; Feylizadeh, M.R.; et al. Deep learning: Applications, architectures, models, tools, and frameworks: A comprehensive survey. *CAAI Trans. Intell. Technol.* **2023**. [CrossRef]
74. Thakore, R.; Vaghashiya, R.; Patel, C.; Doshi, N. Blockchain—Based IoT: A Survey. *Procedia Comput. Sci.* **2019**, *155*, 704–709. [CrossRef]
75. Jivanyan, A. Lelantus: Towards Confidentiality and Anonymity of Blockchain Transactions from Standard Assumptions. Available online: https://lelantus.io/lelantus.pdf (accessed on 1 March 2023).

76. Ghaderzadeh, M.; Aria, M. Management of COVID-19 Detection Using Artificial Intelligence in 2020 Pandemic. In Proceedings of the 5th International Conference on Medical and Health Informatics, Kyoto, Japan, 14–16 May 2021; pp. 32–38.
77. Hosseini, A.; Eshraghi, M.A.; Taami, T.; Sadeghsalehi, H.; Hoseinzadeh, Z.; Ghaderzadeh, M.; Rafiee, M. A mobile application based on efficient lightweight CNN model for classification of B-ALL cancer from non-cancerous cells: A design and implementation study. *Inform. Med. Unlocked* **2023**, *39*, 101244. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.