Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.sciencedirect.com/journal/computers-in-industry

Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks

Abbas Yazdinejad [a,*], Ali Dehghantanha [a], Reza M. Parizi [b], Gautam Srivastava [c,e,f], Hadis Karimipour [d]

[a] *Cyber Science Lab, School of Computer Science, University of Guelph, Ontario, Canada*
[b] *Decentralized Science Lab, College of Computing and Software Engineering, Kennesaw State University, GA, USA*
[c] *Department of Math and Computer Science, Brandon University, Manitoba, Canada*
[d] *School of Engineering, Department of Electrical and Software Engineering, University of Calgary, Alberta, Canada*
[e] *Research Centre for Interneural Computing, China Medical University, Taichung, Taiwan*
[f] *Department of Computer Science and Math, Lebanese American University, Beirut 1102, Lebanon*

ARTICLE INFO

Keywords:
Threat detection
Fuzzy blockchain
IoT
Fuzzy DNN
ANFIS
Fuzzy matching

ABSTRACT

Integrating blockchain into the Internet of Things (IoT) for security is a new development in computational communication systems. While security threats are changing their strategies and constructing new threats on blockchain-based IoT systems. Also, in combining blockchain with IoT networks, malicious transactions and active attacks deliver more vulnerabilities, privacy issues, and security threats. The concept of blockchain-based IoT attacks is a hot topic in both IoT and blockchain disciplines. Network attacks are a type of security and privacy threat and cover the exact scope of threats related to the combination of IoT and blockchain. Even though blockchain has potential security benefits, new cyberattacks have emerged that make blockchain alone insufficient to deal with threats and attacks in IoT networks since vagueness and ambiguity issues are unavoidable in IoT data. The heterogeneous nature of IoT sources has made uncertainty a critical issue in IoT networks. Deep Learning (DL) models have difficulty dealing with uncertainty issues and cannot manage them efficiently as an essential tool in security techniques. Thus, we need better security, privacy, and practical approaches, such as efficient threat detection against network attacks in blockchain-based IoT environments. Also helpful to consider fuzzy logic to tackle deterministic issues when DL models face uncertainty. This paper designs and implements a secure, intelligent fuzzy blockchain framework. This framework utilizes a novel fuzzy DL model, optimized adaptive neuro-fuzzy inference system (ANFIS)-based attack detection, fuzzy matching (FM), and fuzzy control system (FCS) for detection of network attacks. The proposed fuzzy DL applies the fuzzy Choquet integral to have a powerful nonlinear aggregation function in the detection. We use metaheuristic algorithms to optimize the attack detection error function in ANFIS. We also validate transactions via FM to tackle fraud detection and efficiency in the blockchain layer. This framework is the first secure, intelligent fuzzy blockchain framework that identifies and detects security threats while considering uncertainty issues in IoT networks and having more flexibility in decision-making and accepting transactions in the blockchain layer. Evaluation results verify the efficiency of the blockchain layer in throughput and latency metrics and the intelligent fuzzy layer in performance metrics (Accuracy, Precision, Recall, and F1-Score) in threat detection on both blockchain and IoT network sides. Additionally, FCS demonstrates that we obtain an effective system (stable model) for threat detection in blockchain-based IoT networks.

1. Introduction

The Internet of Things (IoT) is one of the fastest growing technologies. It is undeniable how important and applicable IoT has become in our everyday lives. IoT turns any device through its existing network infrastructure empowering physical resources into intelligent entities. IoT networks aim to develop a complex information system with sensor data acquisition and efficient data exchange through networking, artificial intelligence (AI), machine learning (ML), clouds, and big data (Barrios et al., 2022; Yazdinejad et al., 2020c). At this time, due to

[*] Corresponding author.
E-mail addresses: ayazdine@uoguelph.ca (A. Yazdinejad), adehghan@uoguelph.ca (A. Dehghantanha), rparizi1@kennesaw.edu (R.M. Parizi), srivastavag@brandonu.ca (G. Srivastava), hadis.karimipour@ucalgary.ca (H. Karimipour).

https://doi.org/10.1016/j.compind.2022.103801
Received 7 June 2022; Received in revised form 22 October 2022; Accepted 26 October 2022
Available online 8 November 2022

ever-growing security threats, malicious attacks, and criminal activities, investigating cyber-attacks has become a critical issue, especially in IoT environments. IoT security is an ongoing concern since IoT networks and applications leave plenty of room for hacking. This lack of security can be a real concern when considering IoT networks in financial tasks, smart homes, and smart car applications.

Many industrial sectors and organizations utilizing IoT networks seek solutions to enhance their security. In this regard, there are many security recommendations for IoT networks. One well-known and potential security solution in IoT networks is blockchain. Blockchain has been integrating with IoT, especially in network design, financial transactions, device authentication, and identification (Wu et al., 2022).

Applying blockchain in IoT is necessary since the IoT architecture is centralized and applies a third-party central authority. The central authority controls all data without imposing clear restrictions on its use (Da Xu et al., 2021). On the other hand, blockchain technology delivers a decentralized, autonomous, trustless, and distributed environment. Unlike centralized systems, which have problems with single points of failure, trust, and security, blockchains use the processing capacities of all the participating users, providing greater efficiency and eliminating the single point of failure. Furthermore, blockchain offers better security and data integrity due to its immutable and unchangeable features.

In computational communication systems, the integration of blockchain and IoT are essential developments (Šarac et al., 2021). Blockchain and IoT both have the meaning of connection and are two dimensions of the information processing system. At this time, we have been faced with a blockchain-based IoT concept. Based on IBM's definition, IoT enables devices via the internet to forward data to the blockchain to create immutable records of transactional data in blockchain-based IoT systems. Blockchain as a service layer is considered a layer between the application and network layers in the typical IoT architecture. Several blockchain IoT projects have influenced the business and industry such as IoTA, Waltonchain, IoTex, Ambrosus, Moeco, and Atanomi. Also, we can mention some real-world implemented blockchain-based IoT items such as Telstra, Mediledger, NetObjex, Slock.it, and Drone on the Volga.

Despite the potential blockchain security benefits in IoT, there are significant cyberattacks on IoT networks seen when applying blockchain. Also, security issues are still a significant concern for blockchain-based IoT systems due to the vulnerabilities of IoT and blockchain. Depending on the characteristics of the blockchain, attackers change their strategies and construct new attacks on blockchain-based IoT system (Da Xu et al., 2021). There are some blockchain-based IoT security attacks, including distributed denial-of-service (DDoS), injection, abandon, denial-of-service (DoS), falsifying, public block modification, link modification, and time interval destruction (Da Xu et al., 2021). To explain some blockchain-based IoT attacks, **Abandon** is an auditing node that discards its members' transactions and isolates them, DoS is the target node by sending too many transactions to it, exceeding its processing capabilities, DDoS attacks use more than one node, Equipment Injection allows an attacker to gain unauthorized access to private data by injecting a fake node into the network, and Link, by using the same ID, the attacker can find real-world identifiers corresponding to anonymous nodes. As a real example, IOTA was attacked by DDoS and Trinity (IOTA, 2020).

Therefore, blockchain alone is not enough and cannot be a complete security solution to tackle intrusion attacks and make valid transactions on IoT networks. Intrusion attacks and fraud transactions on IoT networks have grown exponentially at the device level. Malicious actors threaten IoT networks by malicious transactions in blockchain Singh et al. (2020b). They can attempt to determine a particular user by finding links between the user's anonymous transactions and other publicly available information. Malicious transactions have behavioral patterns and even show different patterns during various attacks. Malicious actors can also attempt to pass themselves off as legitimate users to gain access to data.

Also, in addition to some common attacks in blockchain (such as 51% attacks, eclipse attacks, Sybil attacks, Finney attacks, decentralized autonomous organization (DAO) attacks, DDoS race attack, and routing attack (Aggarwal and Kumar, 2021; Anon, 2021)), we can mention some recent ways that they have exposed vulnerabilities and attacks in blockchain-based IoT networks. Active attacks, like, jamming and impersonation, are emerging on blockchain due to multiple active malicious nodes (Mujtaba Buttar et al., 2022). These active attacks lead to the failure of the consensus process responsible for verifying the transactions in the blockchain. In addition, a spam Destination Oriented Directed Acyclic Graph (DODAG) Information Solicitation (DIS) attack is a novel attack that consumes the energy of IoT devices in blockchain frameworks, resulting in a Denial of Service (DoS) vulnerability (Alsirhani et al., 2022). These attacks prove that IoT devices and networks are vulnerable to security threats, and blockchain is not a sufficient safeguard for IoT security (Yazdinejad et al., 2022a).

From a structural and functional perspective, we can analyze blockchain-based IoT security issues, as shown in Fig. 1. Structural security has included devices, networks, and application layers that the blockchain improves security; nevertheless, different attacks on these layers are associated with IoT and blockchain. Function-based security includes upgrades to devise safety, access control, anti-DDoS mechanisms, authentication of identities, privacy protection, data assurance, and self-regulation of IoT networks. Due to the heterogeneous nature of converged networks, IoT has faced security issues at functional security. Blockchain also involves these challenges while it can solve some of them, like access control. Da Xu et al. (2021), Singh et al. (2021).

According to IoT security taxonomy based on blockchain networks (Da Xu et al., 2021), there are mainly two types of threats in blockchain-based IoT systems. First, blockchain-related privacy threats in the blockchain layer. Second, IoT security threats in the IoT layer. Hence, network attacks are a type of security and privacy threat related to IoT and blockchain. In this paper, network attacks cover both threats in both IoT and blockchain, especially the most prominent attacks in this regard, including Denial of Service (DoS), probing, Remote to Local (R2L), transaction privacy leakage, and phishing (Bahaa et al., 2021).

Another challenge we should mention here is the uncertainty and vagueness of data issues in IoT networks that are unavoidable (Yazdinejad et al., 2020b). Taking into account the heterogeneous nature of IoT sources, uncertainty has become a vital issue in IoT networks since data may not be measured accurately or capable of being understood in either of two or more possible senses. At the same time, DL models are widely used in security techniques since they can efficiently process any piece of information in the cybersecurity datasets by defying attacks. However, DL models have difficulty dealing with uncertainty issues. They cannot manage uncertainty issues efficiently, while blockchain-based IoT networks need more security and practical approaches, such as efficient threat detection.

In both IoT and blockchain research, the blockchain-based IoT attack area is a hot topic, and we need to tackle the security threats in this area more effectively. As a result, it is a more pressing concern to consider practical security approaches such as efficient threat detection in blockchain-based IoT networks. Due to ever-rising security threats in IoT networks (Singh et al., 2020b; Yazdinejad et al., 2020c) while applying blockchain and its benefits, our motivation has been formed to provide an effective security approach in blockchain-based IoT networks. Our main innovation is designing and implementing a secure intelligent fuzzy blockchain framework that can effectively detect security threats in IoT networks while providing more efficiency in the blockchain layer. We apply deep learning (DL) and fuzzy logic concepts in this framework. DL has shown good performance in improving cybersecurity attack detection, and it is a critical part of modern cybersecurity strategies. DL also is capable of analyzing attack patterns and learning to prevent similar attacks and respond to

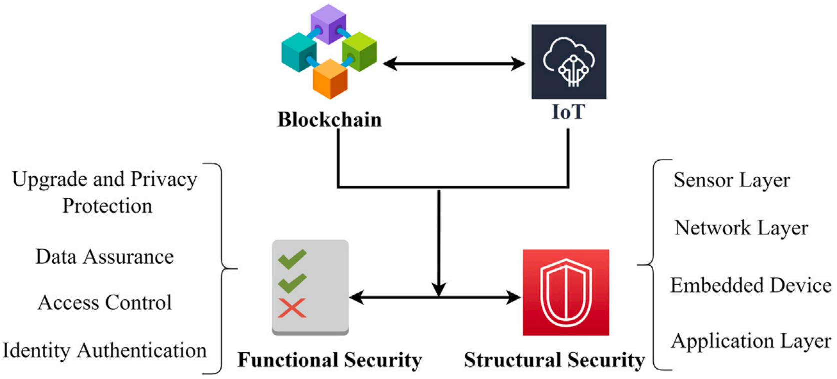

Fig. 1. IoT security taxonomy based on blockchain.

changing behaviors. The fuzzy logic approach can help make reasonable decisions concerning threat detecting and makes DL works with indeterministic assumptions (Makkar et al., 2021) in IoT networks that utilize blockchain.

In addition, fuzzy learning in the proposed framework can mitigate the problem of uncertainty issues during the decision-making process for threat detection, as well as allow more flexibility in decision-making and transaction acceptance in the blockchain layer. It seems too superior to use a combination of fuzzy logic, DL, and blockchain in detecting cyber threats (Yazdinejad et al., 2020a). In summary, the paper makes the following contributions:

- The design and implementation of a secure intelligent fuzzy blockchain framework. This framework applies threat detection (TD), ANFIS, fuzzy control system (FCS), and fuzzy matching (FM) modules in the intelligent fuzzy layer to monitor IoT devices, activities, and real-time processing during connection with IoT and blockchain layer toward detecting security and privacy threats.
- Proposed a novel fuzzy DL model for threat detection in the proposed framework. This fuzzy DL model consists of fuzzy layers, neural representation, defuzzy layer, and fuzzy Choquet integral to have a powerful nonlinear aggregation function to detect threats.
- Design the optimized ANFIS-based attack detection system for the IoT networks. We use metaheuristic algorithms such as genetic algorithm (GA), differential evolution (DE) and particle swarm optimization (PSO) in our design instead of the classic ANFIS training algorithm.
- Using the FM method to validate transactions to obtain fraud detection features in the proposed framework.
- Providing FCS in the proposed framework that utilizes the power of fuzzy logic principles. FCS based on the level of security threat (low, medium, high), can present our system effectively in threat detection.

Table 1 gives the descriptions and nomenclatures that are used throughout the rest of the paper.

Following is a breakdown of the rest of the paper. In Section 2, we discuss work related to IoT networks integrated with blockchain and fuzzy machine learning. Section 3 describes the proposed framework. In Section 4, the evaluation results and comparison of the proposed model with other models are presented, and in Section 5, conclusions are drawn, and research is suggested going forward.

2. Related work

Although a lot of works apply blockchain in IoT as a security solution and mention blockchain-based IoT terms (Dwivedi et al., 2019; Singh et al., 2020a). In these works, the relevant anti-measures against attacks on IoT are described along with how blockchain can be integrated into the IoT security system (r4, 2021; Da Xu et al., 2021). It is worth noting that a few limited research works provide examples of attacks on IoT security under the blockchain (Zolfaghari et al., 2022). There is finite research on attacks and threats in blockchain-based IoT systems and mentions vulnerabilities in combining blockchain with IoT networks. Blockchain-based IoT attacks are a hot topic in both IoT and blockchain disciplines. Blockchain-based IoT environments are susceptible to a wide range of new security threats and vulnerabilities. Also, due to the heterogeneous nature of IoT sources, uncertainty has become a vital issue in IoT networks. It will provide difficulties during decision-making for attacks, threats, and validating transactions in blockchain-based systems, especially when applying DL and ML models since they are based on deterministic assumptions and will not work well with uncertain and vague data. This section discusses research on threat detection, especially concerning blockchain and IoT networks, while applying fuzzy logic, DL, and ML.

Table 1
Summary of nomenclature.

Parameters	Description
AI	Artificial intelligence
DL	Deep learning
ML	Machine learning
DoS	Denial-of-service
DDoS	Distributed denial-of-service
DAO	Decentralized autonomous organization
TD	Threat detection
ANFIS	Adaptive neuro-fuzzy inference system
FM	Fuzzy matching
FCS	Fuzzy control system
GA	Genetic algorithm
PSO	Particle swarm optimization
DE	Differential evolution
IoT	Internet of Things
CSF	Cognitive spammer framework
FIS	Fuzzy inference system
FL	Fuzzy logic
MF	Membership function

By and large, fuzzy logic is used to solve several problems involving uncertainties in deciding about cyber threats; In Thonnard et al. (2009), Thonnard et al. proposed a model based on knowledge discovery and fuzzy decision-making for identifying attacks. Their model generates fuzzy clusters in different attack dimensions. Every attack has four dimensions in this model: geolocation Internet Protocol (IP) subnet, targeted platform, and port sequences. They used the Sugeno inference model for fuzzy rule generation, but they could not explain attacks in IoT networks. Moreover, In Thonnard et al. (2010), the authors proposed a multi-criteria culturing method for addressing attack detection on cloud-based platforms. In the proposed model, clusters of IP addresses were analyzed unsupervised to find the real source of the attack. Another research, Haddadpajouh et al. (2020), proposed a multi-view fuzzy consensus clustering model for malware threat attribution. In this work, cyber-threat payloads are attributed to actors based on their consensus clustering model. They carried out over 4000 experiments for the attribution task to find the best combinations of all 12 extracted views. Moreover, Pitropakis et al. (2018) has proposed a framework as an enhanced cyber-attack detection (NEON), which performs the detection of malicious parties behind APT campaigns. The goal of NEON is to increase societal resiliency to APTs that focus on adversarial machine learning and privacy considerations in mind. Similarly, in Sahoo (2022), the authors proposed cyber threat detection with multi-view heuristic analysis. This work via multi-view analysis helps attribute the malware to its source with higher accuracy. However, these works neglected to address the IoT and Blockchain issues, especially threat detection in blockchain-enabled IoT networks.

Blockchain offers a wide range of security protections, including allowing trusted devices to manage designated smart watering systems. To make smart decisions, individuals are encouraged to such blockchain and fuzzy logic approaches since they are associated with multiple successes in IoT. The utilization of the two methods can also guide a study focused on developing a smart watering system (Munir et al., 2019). For blockchain-based IoT networks, the concept of threat detection has been neglected. In another study that considered IoT and blockchain integration (Namasudra et al., 2022a), the authors proposed generating and verifying medical certificates using blockchain technology for IoT-based healthcare systems. Though this work suffers from fuzzy logic, its proposed architecture provides an interface between users and healthcare centers to generate and maintain health records, while the scheme ensures security by setting up rules through smart contracts.

In Marsh and Gharghasheh (2022), Marsh et al. considered fuzzy Bayesian learning for cyber threat hunting in industrial control systems. The authors integrate fuzzy logic with Bayesian inference to deliver an optimized fuzzy model for identifying threats in cybersecurity datasets. Their algorithm gained a viable accuracy for malware classification while not considering the blockchain vulnerability. Similarly, the authors in Sahoo and Upadhyay (2022) proposed scalable fair clustering machine learning methods for threat hunting. Applying the fair k-median clustering technique in their work allows for high accuracy to obtain fairness criteria in IoT-based cyber–physical systems. It suffers from a fuzzy perspective and blockchain vulnerability.

In another work, an integrated blockchain-IoT-big data platform is available called Di-ANFIS (Bamakan et al., 2021). Adaptive network-based fuzzy inference systems (ANFIS) are used to evaluate service supply chains in this framework. Although they introduced a distributed blockchain-based framework in response to ANFIS's reliance on big data and a lack of trust and security in the supply chain, they failed to focus on threat detection issues in blockchain-based IoT networks. Furthermore, in another framework (Jamil et al., 2021), based on blockchains and machine learning, the authors propose a peer-to-peer energy trading system for a smart grid that is sustainable. The proposed blockchain-based platform consists of energy trading modules that use smart contracts and predictive analytics modules that use blockchain technology. Contrary to this, it would be wonderful if security threats could be detected and hunted.

Makkar et al. presented a fuzzy-based approach to enhance the cybersecurity of next-generation IoT in Makkar et al. (2021). They provide a cognitive spammer framework (CSF). A combination of fuzzy rule-based and machine learning classifiers is used to detect web spam in their CSF. These classifiers produce a quality score for each webpage. According to the evaluation, CSF is 97.3% accurate. Also, in de Miranda Rios et al. (2021) has been proposed detection of DDoS attacks using machine learning algorithms and fuzzy logic. The authors use a technique known as the Reduction of Quality (RoQ) attack in this study. This approach detects attacks based on Euclidean Distance (ED), Fuzzy Logic (FL), and MLP. Nevertheless, this work suffers from a longer execution time.

According to related works, no solid research has been conducted using fuzzy logic, ML, and blockchain in threat detection, especially in blockchain-based IoT networks. Considering the continuous rise of security threats in IoT networks and blockchain, there is no denying the importance of threat detection in blockchain-based IoT areas. To reach our goal in this study, our primary motivation was to move in this direction, to tackle blockchain-based IoT attacks.

3. Proposed secure intelligent fuzzy blockchain framework

Our proposed framework creates effective threat detection in network attacks on blockchain-enabled IoT environments. IoT systems are susceptible to various cyberattacks, where the common attacks on IoT systems are in the network layers, such as Denial of Service (DoS) and Remote to local (R2L). Furthermore, phishing attacks and abnormal and fraudulent transactions are common in blockchain, threatening users' privacy. These threats have motivated us to select network attacks in blockchain-based IoT systems. As shown in Fig. 2, an overview of the proposed framework includes three main layers: the IoT layer, intelligent fuzzy layer, and blockchain layer. To show the simple abstract of the overview of the proposed framework, we divided it into 3-layer. Therefore, this framework is designed with blockchain security support and fuzzy logic to track and trace IoT device transactions and perform threat detection in IoT networks. In the workflow, blockchain has integrated into the IoT layer like Dai et al. (2019), Agarwal (2021) while the fuzzy layer has a control plane role concerning this layer, integrated blockchain, and IoT . In addition to providing more security, this capability would also improve the efficiency of the blockchain layer in terms of latency and throughput. As illustrated in Fig. 2, all these layers interact to provide secure communication and detect security threats for blockchain-enabled IoT networks. The IoT layer includes all the smart devices and hardware devices such as drones, cell phones, sensors, and actuators that connect and communicate with each other in the blockchain environment. The blockchain layer handles IoT device management, cloud storage and the blockchain-based security module. Blockchain provides safe channels for the transmission of data and transactions between IoT devices. The most important and operational layer in the proposed framework is the intelligent fuzzy layer which is our major discussion in this paper. This layer has some components to tackle security issues, detecting processes, and the blockchain layer's efficiency.

3.1. *Role of intelligent fuzzy layer*

In the proposed framework, the intelligent fuzzy layer has been placed between IoT and blockchain layers that play an important role in real-time processing and security management. Fig. 3 presented the relationship between the main components of this layer, such as TD, ANFIS, FCS, and FM. We will examine the functionality of these components in more detail and discuss their performance during run-time in the following.

3.1.1. *Threat detection module*

Since common DL models are deterministic, they cannot be used to deal with uncertainty in IoT environments. Additionally, existing fuzzy classifiers and fuzzy DL models are not designed and efficient (Yazdinejad et al., 2019) for classification in nonlinear tasks, such as threat detection, which is the focus of this paper. In the TD component, we design and implement a novel fuzzy DL model for threat detection in the blockchain layer in the proposed framework. Although blockchain enhances security by its design, it is not immune to attacks. For example, existing attacks and vulnerabilities on the Ethereum Blockchain. Therefore, the TD component can play a vital role in the detection process by considering signs and patterns of attacks and threats with

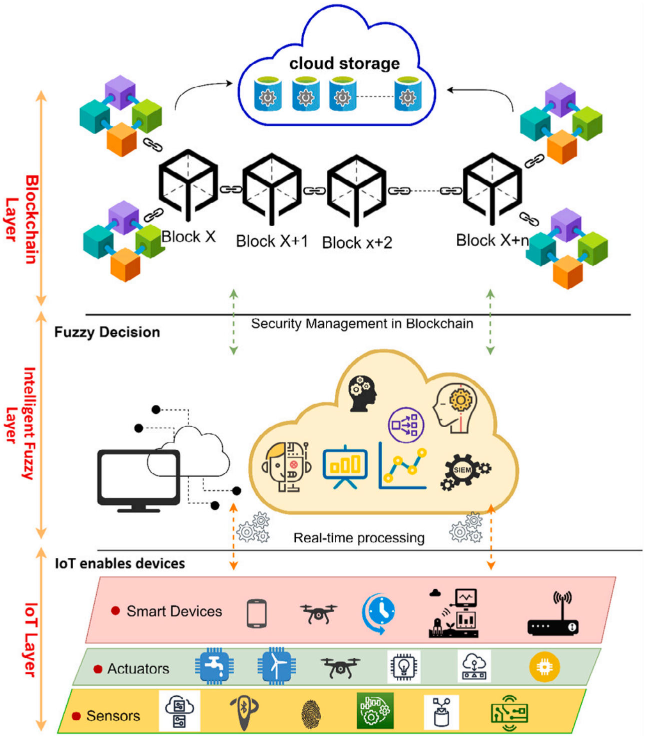

Fig. 2. General overview of the proposed framework.

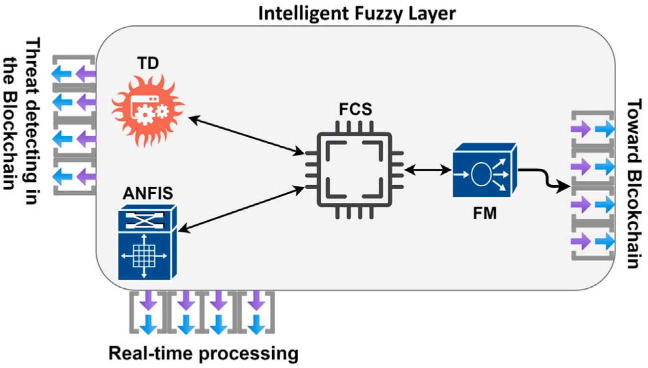

Fig. 3. Component of the intelligent fuzzy layer.

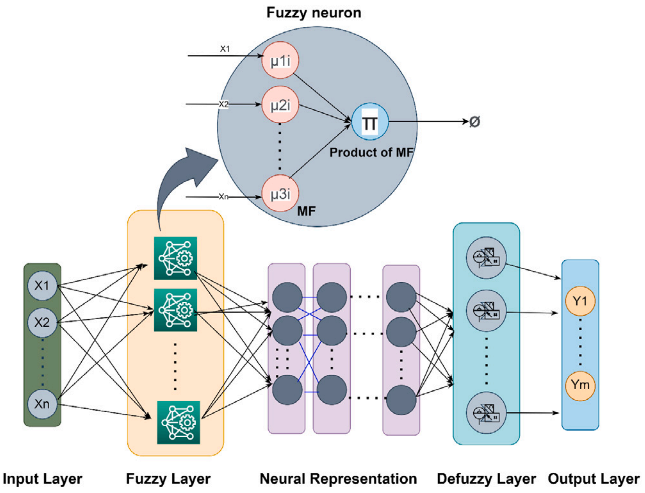

Fig. 4. Structure of Fuzzy DL model.

human reasoning. As shown in Fig. 4, the fuzzy DL model consists of an input layer, fuzzy layer, neural representation, defuzzy layer, and output layer.

Layer 1 is the input layer, so there is an input vector as $X_i = [x_1, x_2, \dots, x_n]$ that each neuron in this layer represents an input variable, X_i, $i = 1, 2, \dots, n$. Next layer, the fuzzy layer, each neuron (as mentioned in the fuzzy neuron in Fig. 4) in this layer represents an if-part of a fuzzy rule. The outputs of neurons in the fuzzy layer are computed by-products of the grades of membership functions (MFs). Each MF is in the form of m as shown in Eq. (1).

$$\lambda(x, s, m) = e^{-\sum_{i=0}^{dim} \frac{1}{4} \frac{(xi-si)}{mi^2}} \tag{1}$$

When x is an input vector of dim length, s is the centroid of the ith membership function, and m represents the scaling factor. The fuzzy layer is suitable for cases when you are working with data that can be clustered into interpretable groups, e.g. spatial coordinates, multi-function values.

The neural representation layer transforms the input into some high-level representations using the neural learning concept. The layers are fully-connected implying each node on the $(r)th$ layer is connected to all the nodes on the $(r-1)th$ layer with parameters $\omega(r) = \{w(r), b(r)\}$, and ei is Euler's number.

$$Q_i^l = \frac{1}{1 - e_i^{-m}}, m_i^l = w_i^l Q_i^{l-1} + b_i^l \tag{2}$$

The weights and bias of node i on layer lth are represented by $w(r)_i$ and $b(r)_i$. By reducing the uncertainty and noise of the input data, neural parts attempt to make better representations.

The Defuzzy layer is the fourth layer. Each neuron in this layer represents an output variable caused by the summation of signals received from the neural representation layer. The output of a neuron in layer 4 is based on Eq. (3) where $k = input - dim$.

$$d(x, f) = \sum_{i=1}^{k} x_i f_i \tag{3}$$

The defuzzy layer can be trained to transform the output of a model to continuous values. In other words, this layer can be interpreted as a ruleset and input to this layer.

In the last layer, the output layer, the Fuzzy Choquet integral, has been considered since it is objective evidence supplied by each information source and the expected worth of each subset of information source in its decision-making process. Fuzzy Choquet integral, a powerful nonlinear aggregation function, can be represented as a multi-layer network.

The Fuzzy Choquet integral of observation h on X is shown in Eq. (4).

$$\int hog = C_g(h) = \sum_{j=1}^{N} h_{\pi(j)}(g(A_{\pi(j)}) - g(A_{\pi(j-1)})) \tag{4}$$

For $A_{\pi(j)} = \{X_{\pi(1)}, \dots, X_{\pi(j)}\}$, $g(A_{\pi(0)}) = 0$ and premutation π such as that $h_{\pi(1)} \geq h_{\pi(2)} \geq h_{\pi(3)} \dots \geq h_{\pi(N)}$.

In other words, the output layer utilizes the fuzzy Choquet integral as an aggregation function to combine and integrate the classification results of several classifiers. The final part is the classification task that assigns the representation to its corresponding category.

3.1.2. Optimized adaptive neuro-fuzzy inference system model

We design an ANFIS-based attack detection system for IoT networks. The goal is to design an optimal fuzzy system using intelligent optimal algorithms. We use metaheuristic algorithms such as Particle Swarm Optimization (PSO), Genetic Algorithm (GA), and Differential Evolution (DE) in our design instead of the classic ANFIS training algorithm. The optimized ANFIS is a security tool that allows authorized access to the desired system by examining the IoT network traffic. Fig. 5 shows the ANFIS model, a feed-forward neural network, for detecting the

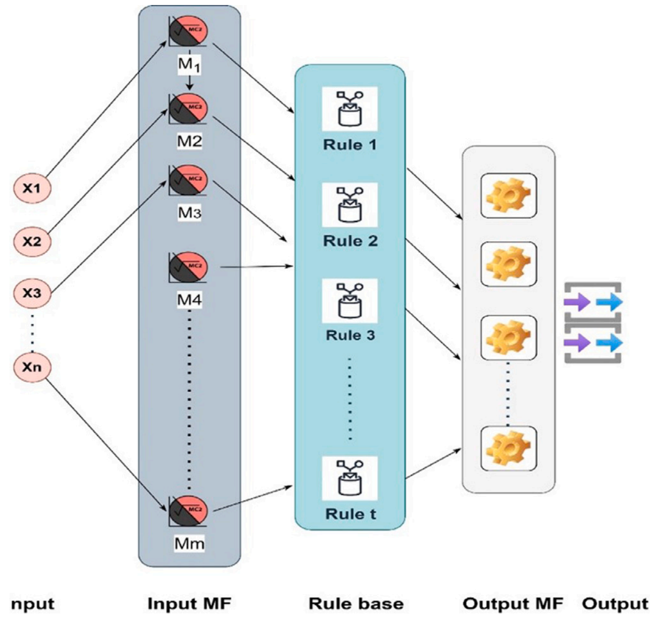

Fig. 5. General structure of ANFIS.

attack of blockchain-enabled IoT networks. The ANFIS model is crucial as it outlines input membership functions and output membership functions. Doing that lays a foundation for what input and output should look like. The input's first layer contains values converted into fuzzy sets. The above parameters progress after learning processes that result in additional membership sets. The above process uses metaheuristic algorithms based on the selected error criteria, ANFIS changes, and input member constraints. The selected criteria follow the formula (sum of the squared difference between actual and desired outputs). The ANFIS model is effective in showcasing various membership functions in different categories.

Assuming vector P is the parameters of fuzzy inference system (FIS), then $[p_1, p_2, p_3, \dots, p_n]$ are the basic values of FIS. $P^* = [P^*1, P^*2, P^*3, \dots, P^*n]$ is the optimal value here since it is derived from optimal algorithms in ANFIS. To answer how this optimal Pi^* will be obtained, we can mention it by generating xi by optimal algorithms, Eq. (1). The PSO, GA, and DE algorithms adjust fuzzy system parameters according to the error function.

3.1.3. Fuzzy matching module

textcolorblackFM module is part of the Fuzzy Intelligent layer that utilizes fuzzy string matching and has a relationship with the blockchain layer. In general, fuzzy string matching is a technique used in computer-assisted translation as a special case of record linkage. It works with matches that may be less than 100% perfect when finding correspondences between text segments and entries in a database of previous translations. A fuzzy string matching algorithm can provide fraud detection (Kumar et al., 2019). A good example is "Spam Detection in Twitter" by fuzzy string matching. Therefore, applying this technique to the FM module can be viable when considering transactions in the blockchain layer in the proposed framework.

The main question here is what FM's role in the proposed framework is. In response to this question, first, we should know how a transaction gets into the blockchain. Furthermore, how blockchain transactions are validated must be determined. Consensus algorithms such as Proof of Work (PoW) usually do blockchain transactions and add blocks. Finally, all participants in the network must agree on the ledger's state. Conversely, we consider the blockchain validator approach with the FM method as the proposed framework since a major technical issue exists in the current blockchain system.

Validation and consensus are two different concepts. A blockchain validator is responsible for diverse actions, including verifying if transactions are legal and verifying transactions conducted in a blockchain. Conversely, a consensus involves ordering events and ensuring that such orders agree in a blockchain. To a much greater extent, a consensus consists in coming to terms with orders of validated transactions. Therefore, from the above explanation, it is evident that the validation precedes the agreement. In some instances, some elements are "valid," and the network fails to "agree" upon them.

As is known, authentication and authorization are required before a transaction can be added to the blockchain. In this section, we validate transactions via FM using cryptographic keys (public and private keys) in authentication and node ID in the authorization. Fuzzy matching remove problems of consensus algorithms such as PoW for blockchain enable IoT networks. This approach will provide time efficiency and more security. Each user has their ID, private key and public key. They can be used to create a secure digital identity for authenticating the user via digital signatures and unlocking the transaction they want to complete (authentication). As soon as the transaction is completed between users, it must be authorized or approved before it can be added to a block in the chain (authorization).

During fuzzy string matching in FM, the most probable similarity of string matching for the validation transaction is determined by Eq. (5).

$$argmax_{c} \in candidates P(c)P(w|c) \tag{5}$$

Computing the $P(c)$ highlights how c employ. The above aspect can be recorded by considering the number of times it appears on a corpus string. $P(w|c)$ highlights that the word w has existed instead of appearing as c. The use of the word $P(w|c)$ depends on the severity of the error.

Using the thorough approach, finding the appropriate word is fulfilled by finding possible valid words with distances. The distance is considered in terms of the number of insertions or deletions required to upgrade a string from one to the other. Then, the error model determines that words at an edit distance of 1 are more likely than those at an edit distance of 2. Having both $P(c)$ and $P(w|c)$ is crucial. A Levenshtein distance is used to compare string sequences. The Levenshtein distance can be calculated mathematically based on Zhang et al. (2017). Levenshtein distance is a string metric used in information theory, linguistics, and computer science.

The above process is efficient as it illustrates how different probability theories are utilized to generate simple methods of transaction validation in the blockchain layer. In Algorithm 1, fuzzy string matching is used to describe the overall process of the FM module.

Algorithm 1 The role of FM in the proposed framework

```
Require: $PairKey(P, Q), IDs$ (Get all public and private keys and node's ID)
Ensure: $Match✓ \Rightarrow Valid \rightarrow transaction$
  $N \leftarrow n$ (Num Transaction)
  $Match$ == False
  Get Transaction list: $T \rightarrow []$
  while $N \neq 0$ do
      For  i in T:
        Extract $Pi, Qi, IDi \leftarrow Ti$
         Do Fuzzy Matching ()
           if $M = 1$
            $Match$ == True, $\Rightarrow Valid \rightarrow transaction$
           else $M = 0$
            $Invalid \rightarrow transaction$
  end while
   Function: Fuzzy Matching
    $M = 0$
    Get S1, & S2 (String)
     Comput  → lev(S1,S2) (Levenshtein distance)
      if $S1.size == 0$
       return S2.size()
      if $S2.size == 0$
       return S1.size()
      else
       return Min[ lev(S1.substr(1), S2)+1, lev(S2.substr(1), S1)+1),lev(S1.substr(1), S2.substr(1),)))
       $M = 1$
    End Function
   End
```

3.1.4. Fuzzy control system module

FCS works as a proactive security search in the proposed framework. FCS is the heart of the intelligent fuzzy layer that communicates with TD, ANFIS, and FM components while considering the efficiency of these components during threat detection. FCS utilizes the power of fuzzy logic principles to overcome complex decisions. In the FCS component, we consider the security threat level such as low, medium, and high for the performance of TD, ANFIS, and FM. FCS refers to the proposed framework's efficiency in threat detection based on the security threat level.

For instance, there are three inputs, TD, ANFIS, and FM, and one output as the security threat level. Therefore, we consider three fuzzy states as $high$, $medium$, and low and create membership functions for inputs and output variables. The fuzzy relationship between inputs and output variables create via applying the fuzzy membership function, triangular. In FCS, the number of rules will be S^N, N, the number of inputs, and S, the number of fuzzy states. Therefore, when $N = 3$, and $S = 3$, these 27 rules. D, the direction of influence for each metric $(TD, ANFIS, FM)$, a positive relationship ($D = 1$), or a negative relationship ($D = 0$). For example, $D = 1$ means input has a direct relationship with output, while $D = 0$ means input has an inverse relationship with output. W, there should be a weight for each input ($wi, i = 1, \dots, N$), and the sum of the importance weights should be 1. Consider 1for all inputs and $W_{TD} = 0.4, W_{ANFIS} = 0.3$, and $W_{FM} = 0.3$. We can consider below rules based on our assumption ($N = 3, S = 3, W = \{0.4, 0.3, 0.3\}, D = \{1, 1, 1\}$):

1. **If** TD ($High$) **AND** $ANFIS$ (Low), **AND** FM (Low) **Then** security threat ($High$)
2. **If** TD (LoW) **AND** $ANFIS$ ($medium$), **AND** FM (Low) **Then** security threat ($medium$)
3. **If** TD ($High$) **AND** $ANFIS$ ($High$), **AND** FM (Low) **Then** security threat ($High$)
4. **If** TD (Low) **AND** $ANFIS$ (Low), **AND** FM (Low) **Then** security threat (Low)

Though the rules are fuzzy, most experts agree to consider them to explain a system's behavior. Here, we may face the challenge of mapping the rules into a security threat level that fuzzy logic is the best way to tackle. In the intelligent fuzzy layer, FCS determines the security threat level in blockchain-enabled IoT networks. During the detecting process, TD, ANFIS, and FM results determine the security threat level, ranging from 0 to 10. Low, Medium and High are the three levels within the range (0–10). Based on these values from TD, ANFIS, and FM, FCS let us know the level of security threat we are facing in the blockchain-enable IoT network that maps the level of security threat between zero and one hundred percent. Formulating this issue is as follows:

- Antecedents (Inputs) : TD, ANFIS, FM
  - TD: Fuzzy set : low, $medium$, $high$
  - ANFIS: Fuzzy set: low, $medium$, $high$:
  - FM: Fuzzy set: low, $medium$, $high$
- Consequents (Outputs): level of detecting
  - Fuzzy set: low, $medium$, $high$
- Rules
  - $R_1, R_2, R_3, \dots, R_{27}$
- Usage
  - If tell FCS that rated:
    - The $TD = 9.8$, ANFIS = 7.8 and $FM = 6.5 \rightarrow R_i$ (Check with relevant rule)
  - it would recommend detecting:
    - 79.2% .

Finally, Algorithm 2 presents the overall workflow of the proposed secure intelligent fuzzy blockchain framework in threat detection. The training strategies in TD, ANFIS, and FM for this framework have been summarized that cover inputs, initialization, fuzzy levels (low, $medium$, $high$), FCS behavior, and outputs.

Algorithm 2 Workflow of the proposed framework

```
Input:
  Get training samples and their labels → TD, ANFIS, FM
  Determine fuzzy states: ($low$, $medium$, $high$) ⇒ NS = 3
Output :
  Report security threat by FCS
  The well-trained framework
Initialization:
  TD:
    Initialize weights of layer $i$ → wdi
    Training epoch → ep
    Input vector as $X_i = [x_1, x_2, \dots, x_n]$ → Input layer
    MF for each fuzzy neuron in fuzzy layers: $\lambda(x, s, m) = e^{-\sum_{i=0}^{dim} \frac{1}{4} \frac{(xi-si)}{mi^2}}$
    $h = \int hog = C_g(h) = \sum_{j=1}^{N} h_{\pi(j)}(g(A_{\pi(j)}) - g(A_{\pi(j-1)}))$ // Fuzzy Choquet integral
  ANFIS:
    Parameters of FIS → $P = [P1, P2, P3, \dots, Pn]$
    Get metaheuristic algorithms ⇒ PSO, GA, and DE
  FM:
    Similarity of string matching → $argmax_c \in candidates P(c)P(w|c)$
  FCS:
    Get → N, S, D, W
    Calculate number of rules→ $N^S$
$Well\_Train = 0$
 While  $Well\_Train == 0$ do  :
  TD → Threat detection in blockchain side
    $etd = 1000$ // train epoch in TD
     For  i in $etd$ :
      $Fi(xi, yi)$ → Forward all training samples
      $e_{training}$ →Minimize fitting error ⇒ Adam optimizer
      Updating parameters → $P_{fuzzy}$
    Apply test sample → $Ti(xi, yi)$
    $eva_{model}$ → Evaluate the performance ⇒ Map to range (0–10) ⇒ $R_{TD}$
  ANFIS → Threat detection in IoT side
    Get → $P^* = [P^*1, P^*2, P^*3, \dots, P^*n]$ // Optimal values of FIS by metaheuristic algorithms
    $eanfis = sample\_size$
     For  j in $eanfis$ :
      $Ai(xj, yj)$ → Forward all training samples
      Tranin ⇒based on $PSO, GA, DE$, and standard $ANFIS$ algorithm
      Rules and membership functions ⇒ adjusted
      ANFIS updates
    ANFIS tests → statistical amount of error
        MSE, RMSE, mean and std based on ⇒based on $PSO, GA, DE$, and standard $ANFIS$ algorithm
    Apply model with the best performance in attack detection
    $eva_{Anfis}$ → Evaluate the performance ⇒ Map to range (0-10) ⇒ $R_{ANFIS}$
  FM → Considering transactions validation in the blockchain side
     Apply Algorithm 1
      T → Get Transaction list
     For  k in $T$ :
      Check transaction $k$ with all transactions in T → Do Fuzzy Matching ()
       IF valid == 1:
          Accept transaction $k$ → $valid$ list
       Else Add to $Un\_valid$ list
    $eva_{FM}$ → Evaluate the performance ⇒ Map to range (0-10) ⇒ $R_{FM}$// valid and $Un\_valid$ list →
Refer to malicious transactions
  FCS → Efficiency of the framework during threat detection in the blockchain-based IoT systems
    for l in $S^N$:
      $Rl$ → Generate fuzzy rules()
  Get fuzzy states ⇒ $high$, $medium$, and $low$
  Map $R_{TD}$, $R_{ANFIS}$, $R_{FM}$ → R // Generated all rules ⇒ Fuzzy inference
  Return security threat level
  End while
  $Well\_Train = 1$
End
```

4. Evaluation of the proposed framework

This section evaluates the performance of the secure Intelligent fuzzy blockchain framework. First, we introduce the proposed framework's experimental setup, which leverages blockchain technology and fuzzy concept in IoT networks. In the next step, we will go in-depth with the details of applying datasets and a detailed discussion of results and evaluation metrics of a secure Intelligent fuzzy blockchain framework. Lastly, a comparison of the proposed model with peer works is discussed.

4.1. Experimental setup

In our experimental environment, Intel(R) Core(TM) i7-10700KF CPUs at 3.80 GHz 3.79 GHz, Linux64-bit operating system (Ubuntu 20.04), and 16 GB DDR4 memory with a secure fuzzy blockchain framework is used. For proper implementation and evaluation of our components in the fuzzy intelligence layer in the blockchain enable IoT environment, Python 3.8.4, fuzzy libraries (e.g., fylearn, ANFIS, and

Table 2
Fuzzy framework parameters.

Parameters	Description
Simulators	BlockSim, VS code
libraries	fylearn, ANFIS, and Scikit-Fuzzy
IoT devices	6000
Size of block	1 MB up to 16 MB
Miners	16, 32, 64
Algorithms	GA, PSO, DE
Batch size	16
Error function	MSE, RMSE
Epoch	1000
loss	binary_crossentropy
momentum	0.9
optimizer	SDG
ANFIS system	Takagi Segueno
ANFIS step size	0.01
ANFIS Epoch	1000
MF	Gaussian,triangular
PSO_pop	50
PSO_Iteration	1000
DE_pop	20
DE_Iteration	1000
GA_pop	100
GA_Iteration	500
Mutation	0.01
Gama_cross_over	0.2

Scikit-Fuzzy), and BlockSim are applied as in Alharby and van Moorsel (2020). BlockSim is an extensible simulation tool for Blockchain systems. The implementation details of the proposed framework in a blockchain enable IoT network is presented in Table 2. The details of the fuzzy DL model, ANFIS, Fuzzy match, and FCS, in the Blockchain network have mentioned in Table 2.

4.2. Datasets

A robust framework for analyzing whether these features are related to blockchain-based IoT attacks can be provided by fuzzy logic, which allows for handling uncertain and imprecise knowledge. A fuzzy DL model and other fuzzy modules used in the intelligent fuzzy layer take attack features from the dataset defined by the correlation between protected and unprotected attributes to deal with uncertainty issues.

To assess intelligent fuzzy layer, TD and ANFIS components, we consider three datasets as Ethereum transaction dataset (Al-E'mari et al., 2020), Ethereum Fraud Detection (Jung et al., 2019) and NSL-KDD (Bala and Nagpal, 2019) dataset. From 2017-to 2019, Ethereum transactions have been associated with 71,250 normal and suspicious attacks. In such instances, datasets are classified according to scamming and phishing types. Phishing attacks are based on extracting critical and sensitive information from various users. Phishing also involves the creation of fake websites that result in adding up to the Ethereum wallet key. Other forms of attack, such as scamming, are associated with acts such as counterfeit ICOs. Secondly, Ether Fraud Detection includes rows of fraudulent and valid Ethereum transactions. The dataset is highly imbalanced in that 17.8% of samples are fraud (7662 none fraud samples and 2179 fraud samples), and It has 9841 samples, each of which has 50 features.

NSL-KDD datasets are superior to the KDDCup99 dataset, which is widely applied in IoT network intrusion detection. There are 41 network features and five types of network attacks (Normal (No intrusion), U2R, R2L DoS, and Probe). These intrusion types are Normal = 67,343, DoS = 45927, R2L = 995, U2R = 52, Prob = 11,656.

4.3. Threat model

As mentioned, not only IoT but also blockchain environments are at risk of leaking transactional information and privacy due to their public nature and structure. In addition, several security vulnerabilities have been reported to blockchain-based IoT environments (Singh et al., 2021; Da Xu et al., 2021). In blockchain-based IoT environments, security and privacy issues remain a concern. Because blockchain transactions can be traced, the privacy of users' transactions is a problem. In addition, malicious IoT users threaten the security and privacy of blockchain transactions. This subsection aims to design a threat model in blockchain-based IoT environments. Here, a threat model identifies the most likely threats in security and privacy for network attacks. To protect the whole environment against every attack(er), we consider the most probable ones. Threat modeling involves systematically identifying and analyzing security threats within our proposed framework. According to Fig. 2, there are mainly two types of threats: blockchain-related privacy threats in the blockchain layer and IoT security threats in the IoT layer (Yazdinejad et al., 2022b).

- **Privacy**: Data privacy involves both identity and data privacy from the perspective of data holders. By intercepting or eavesdropping on broadcasted messages, attackers attempt to steal the private information of data holders.
- **Security**: From an IoT security threats perspective, attacks that can cause the network to fail at learning accurate predictive models are considered system security threats. Assumption: our work mainly focuses on IoT network attacks (U2R, R2L DoS, and Probe).

We formulate threat modeling based on network attacks in blockchain-based IoT systems, covering attacks in both IoT and blockchain.

4.3.1. Formulation

We formulate our threat model in three stages:

1. Modeling the system
2. Identifying threats
3. Threats are identified for each subsystem

To begin developing the threat model, we focus on threats to blockchain and IoT environments. In the second stage, threats from the first stage are updated and assessed using an expert's assessment of the probability of damage resulting from implementing a threat to blockchain-based IoT attacks and then calculating the likelihood of security and privacy threats occurring. Following that, threats were identified for each subsystem (IoT and blockchain) as well as for the environment in which each subsystem operated.

To create a threat model exclusively for IoT and blockchain environments, we consider sets of IoT devices as $V = \{v_1, v_2, v_3, v_4, \dots, v_n\}$ and $B = \{b_1, b_2, b_3, b_4, \dots, b_n\}$ is a set of blocks related to them. In the graph, IoT devices are vertices, and blocks are edges. When linking these elements, we get an information flow as $g = \{v_i, b_l, v_j\}$ where v_i, v_j are IoT devices, and b_l is a related block. Therefore, If a subset of IoT devices v_1, v_2, v_3 and blocks related to them have been considered, we obtain streams as $G = \{g_1, g_2, g_3, g_4\}$, where $g_1 = \left\{v_1^i, b_3, v_1^j\right\}, g_2 = \left\{v_2^i, b_4, v_2^j\right\}, g_3 = \left\{v_3^i, b_1, v_2^j\right\}, g_4 = \left\{v_3^i, b_4, v_2^j\right\}$.

Threats to IoT and blockchain are considered to create a threat model, and this article discusses threats to Blockchain-based IoT systems. Let us designate the set of possible typical threats to Blockchain-based IoT systems in terms of security and privacy as $T = \{t_1, t_2, t_3, t_4, \dots, t_n\}$, and $Z = \{z_1, z_2, z_3, z_4, \dots, z_n\}$, respectively. s_i refers to privacy threats, and z_i refers to security threats. We can map each type of security and privacy threat to $t_1, t_2, \dots, t_n$ and $z_1, z_2, \dots, z_n$. The cartesian product of the original sets consists of combinations of flows and their threats since each threat applies to each flow. In our case, such a result set has the following cardinality in Eq. (6):

$$|G \times T \times Z| = |G| \times |T| \times |Z| \tag{6}$$

The proposed threat model considers all of the above security and privacy threats. At the same time, the model we developed includes

Table 3
The threat to flow g_1.

Threat	Description	Consequences	Item name in graph
T1	The attacker sends so many transactions to the target node	Denial of service (DoS)	g1t1
T2	An attack that tries to get information from a network	Prob Attack	g1t2
Z1	An attacker uses the same ID to link transactions in multiple transactions	Link Attack	g1z1
Z2	Malicious transactions in the blockchain	Linking transactions	g1z2

a detailed description of threats concerning each IoT and blockchain area based on the datasets in this paper, which indicates that the proposed model considers the types of blockchain-based IoT attacks. For example, threats to the flow $g_1 = \left\{ v_1^i, b_3, v_1^j \right\}$ are presented in Table 3.

4.4. Experimental analysis

Experimental and evaluation procedures of the proposed model are presented next. In the following subsection, we focus on the goal of the proposed framework in threat detection via evaluating implemented fuzzy DL model, ANFIS, fuzzy matching in blockchain, and FIS.

4.4.1. Threat detection by fuzzy deep learning

As fuzzy systems and neural networks are both effective, we implement a deep fuzzy model for threat detection in the Ethereum blockchain. In this section, we will discuss the performance evaluation of fuzzy DL. In pre-processing, we address data cleaning, Filtering and Drop features. During the Filtering step, we find the features with 0 variances, and then during the Drop features step, we remove the features with 0 variances since they do not contribute to the model's performance. Next, we make feature selection (such as hash, nonce, value, gas, gas_price, receipt_gas_used, block_number, receipt_cumulative_gas_used) based on Ethereum transaction and Ethereum Fraud. Finally, the standard scaler was adopted. The model was trained at epoch = 1000 and batch size = 16. We used 80% of the datasets for training and 20% for testing. In implemented fuzzy deep model, 10 neurons are for input and 1 neuron is for output. Also, between fuzzy and defuzzy layers there are four dense layers with 64, 32, 16, and 8 neurons. For the first three layers, we apply ReLu activation and for the last dense layer, we use sigmoid activation. The Adam optimizer was used to minimize the error while training the model and the stochastic gradient descent function. During compiling our model, we use binary cross-entropy as a loss function. To evaluate the performance of our implemented fuzzy model, we have used the standard evaluation metrics such as True Negative (TN), False Negative (FN), False Positive (FP), and True Positive (TP) to meet performance metrics, such as F1-score, precision, recall, and accuracy as follows.

In Table 4 and Table 5 respectively, the following values were obtained after training and testing the proposed fuzzy model on the Ethereum blockchain dataset and Ethereum Fraud detection dataset as the best possible accuracy, precision, F1-score, and recall. Our model utilized efficient fuzzy design, fine-tuning parameters in dense layers, optimization, and fuzzy integral. To present the efficiency of the proposed fuzzy DL model when applying Ethereum blockchain, we implement fuzzy classifiers such as Fuzzy Pattern classifiers, fuzzy Pattern Tree Top-Down classifiers, Multimodal Evolutionary classifiers, Fuzzy pattern Classifier GA, and Fuzzy Reduction Rule Classifier with Fylearn library. Furthermore, several heuristic search methods are implemented in these fuzzy classifiers like Pattern Search Optimizer, GA Search in parameters for modification and scaling, and search parameters from the discrete universe. These are used in the learning algorithms for parameter assignment. Moreover, we compared our results with some common ML models like LogisticRegression, SVM, and GaussianNB.

Table 4
Comparison performance of models based on Ethereum blockchain dataset.

Model	Accuracy	Precision	F1-Score	Recall
Proposed fuzzy model	0.964	0.994	0.96	0.991
Fuzzy Pattern	0.77	0.9	0.83	0.79
Multimodal Evolutionary	0.88	0.86	0.82	0.62
fuzzy Pattern Tree Top Down	0.9	0.89	0.92	0.69
Fuzzy Reduction Rule	0.89	0.89	0.91	0.9
Fuzzy pattern Classifier GA	0.89	0.92	0.69	0.93
LR	0.88	0.84	0.63	0.51
GaussianNB	0.37	0.69	0.4	0.76
SVM	0.88	0.83	0.53	0.75

Table 5
Comparison performance of models based on Ethereum fraud detection dataset.

Model	Accuracy	Precision	F1-Score	Recall
Proposed fuzzy model	0.928	0.94	0.93	0.95
Fuzzy Pattern	0.61	0.89	0.69	0.66
Multimodal Evolutionary	0.65	0.9	0.7	0.62
fuzzy Pattern Tree Top Down	0.76	0.79	0.87	0.92
Fuzzy Reduction Rule	0.79	0.8	0.88	0.91
Fuzzy pattern Classifier GA	0.83	0.92	0.78	0.9
LR	0.77	0.8	0.89	0.92
GaussianNB	0.37	0. 85	0.35	0.66
SVM	0.76	0.81	0.89	0.93

Table 6
Accuracy of attack detection based on NSL-KDD dataset.

Class	Accuracy (%)
Normal	99.7
Probe	99.6
DoS	100
U2R	99.8
R2L	99.8

4.4.2. Assess optimized adaptive neuro-fuzzy inference system model

This section discusses the numerical results of the proposed ANFIS model considering network attack categories based on the NSL-KDD dataset for blockchain-enabled IoT networks. We assess the ANFIS model when monitoring IoT traffic in the proposed framework. An FIS editor that has an ANFIS interface creates a simulation model under MATLAB. After loading ANFIS parameters, its classifier initially identifies membership function, error rate, and learning methods that correspond to its features. The training approach is then continued until input/output membership functions and their constraints are customized. In such instances, conventional ANFIS algorithms are abandoned, and PSO, GA, and DE are utilized. The next process involves ANFIS tests which continue until rules and membership functions are adjusted. The last method involves ANFIS updates that include its stores and attributes.

Figs. 6, 7, 8, and 9 illustrate the statistical amount of error in terms of MSE, RMSE, mean, and std based on PSO, GA, DE, and standard ANFIS algorithm, respectively. PSO has better performance, and DE has weaker performance in this regard. Therefore, we finally apply PSO in our optimized ANFIS model on the NSL-KDD dataset.

Table 6 shows the attack detection in IoT networks. To identify the different types of attacks, accuracy is used as a statistical characteristic. Using the optimized ANFIS model, DoS attacks are detected very accurately, while all other types of attacks are also detected very accurately.

4.4.3. Assess fuzzy matching

To highlight the effect of proposing fuzzy matching during transaction validating and show its efficiency in blockchain enable IoT network, In this section, we evaluate our secure intelligent fuzzy blockchain framework with a BlockSim toolkit (Alharby and van Moorsel, 2020). To evaluate the performance of this framework, the simulation

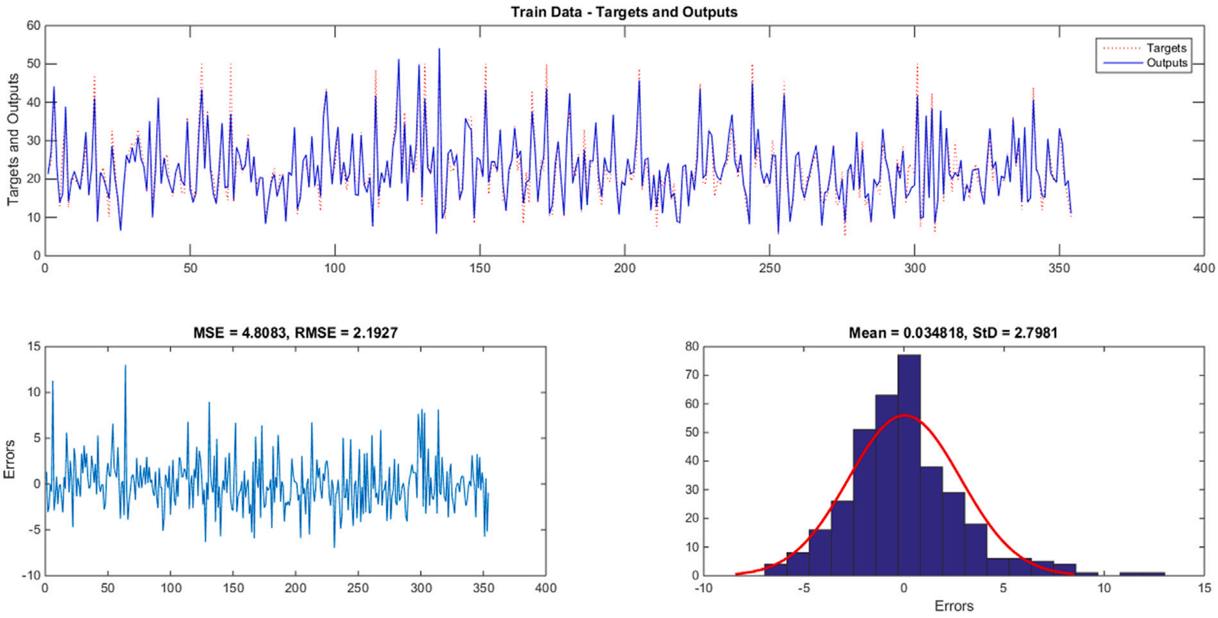

Fig. 6. Result of ANFIS.

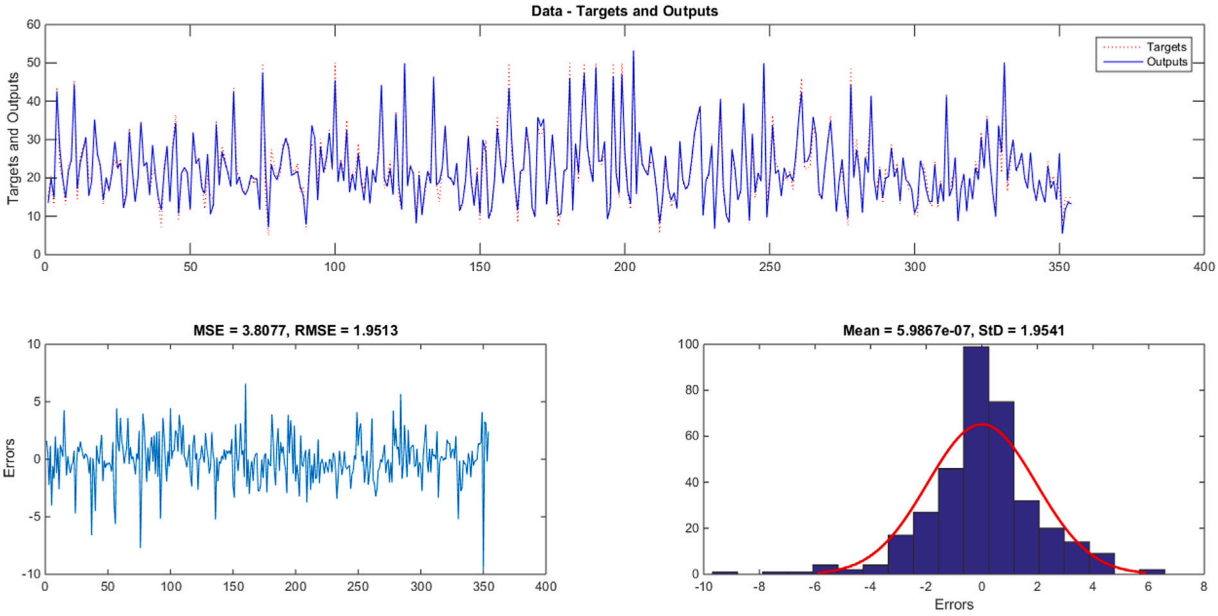

Fig. 7. Result of ANFIS with GA.

parameters are presented in Table 2. To accomplish more realistic results, we did the simulation 50 times and compared it with 2 peer works as BMCGV (Namasudra et al., 2022b) and a non-fuzzy model during the simulation. BMCGV is blockchain-based medical certificate generation and verification for IoT-based healthcare systems and a Non-fuzzy model has been considered another scenario that uses a common consensus algorithm, PoW for transaction validation with the standard blockchain network model. A non-fuzzy model has no features such as fuzzy matching. The thing that needs to be highlighted here is that these parameters, such as transaction number, number of blocks, nodes, and relay network, directly affect the model's performance metrics, such as latency and throughput. The delay experienced between transaction appearances and transaction requests in a blockchain network is referred to as latency. The proposed architecture contains 200 transactions needed to calculate the latency experienced between similar conditions. In this instance, transactions are defined separately to evaluate approximate time, as indicated in Fig. 10. The designated BlockSim toolkit further analyzes the delay for each set, and then the typical latency is calculated. Although there is an increase in latency with an increase in the number of transactions, the efficiency of the proposed model is more than the BMCGV and none-fuzzy model due to utilizing fuzzy matching during the validation process. The main benefit of FM, as presented in Algorithm 1, is that it used fuzzy string matching with Levenshtein distance to valid transactions while peer works in the BlockSim utilize consensus model like proof-of-work (PoW) to validate transactions that need more time.

In Fig. 11, all transactions done per a time frame are represented. In the figure, the blockchain network is analyzed by considering a set of transactions that are calculated throughout the proposed network. To calculate the entire transaction, a group of 20 transactions is used, and for each mockup, the number of transactions that are increased is set, and then the typical values are analyzed. In general, the number of

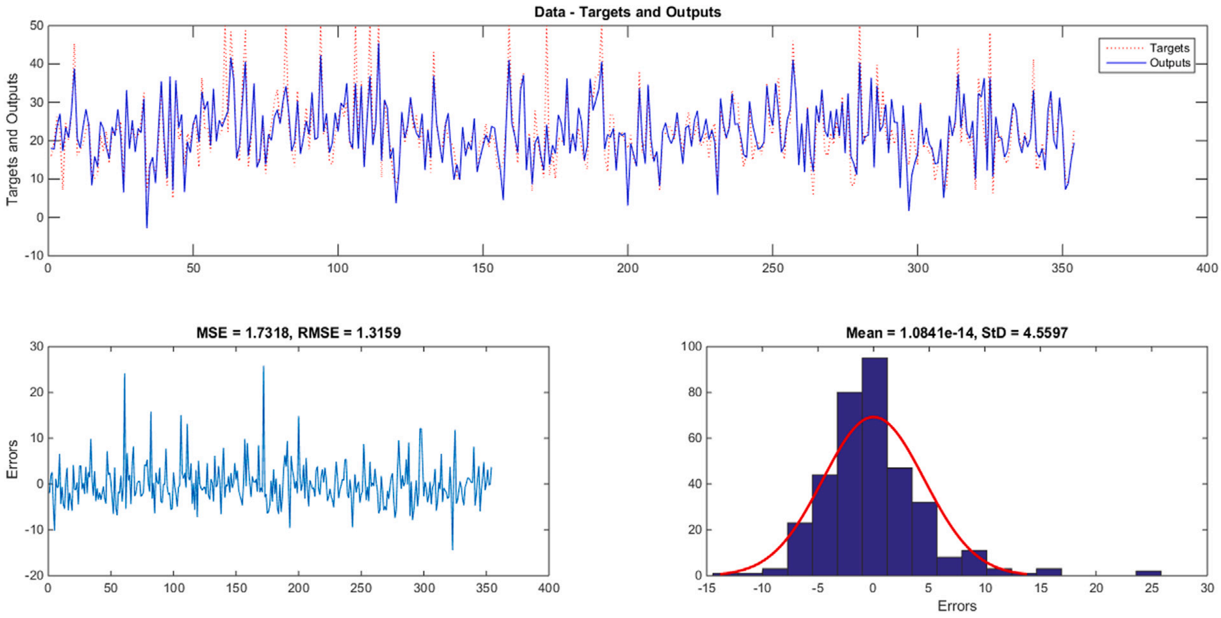

Fig. 8. Result of ANFIS with PSO.

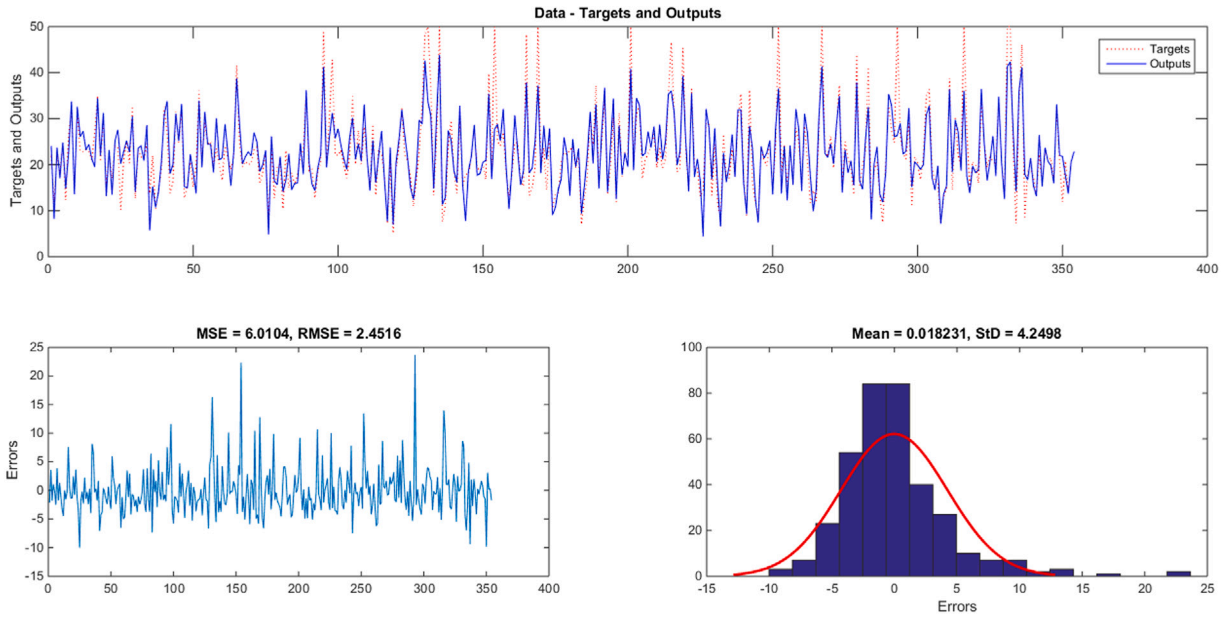

Fig. 9. Result of ANFIS with DE.

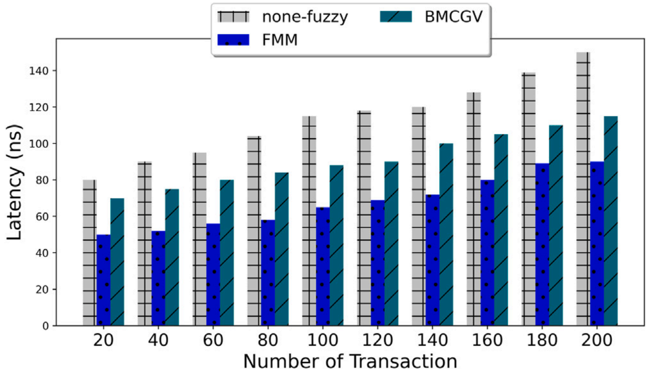

Fig. 10. Comparison of latency.

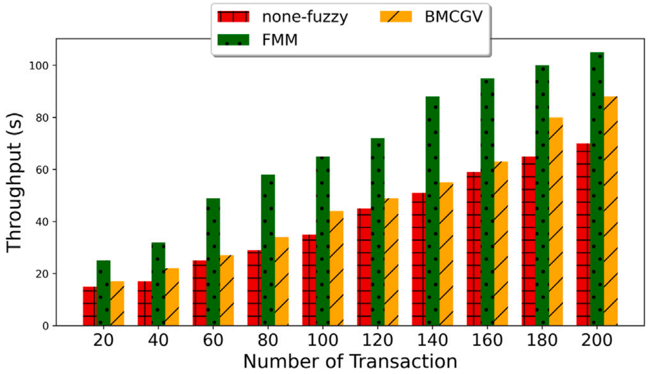

Fig. 11. Comparison of Throughput.

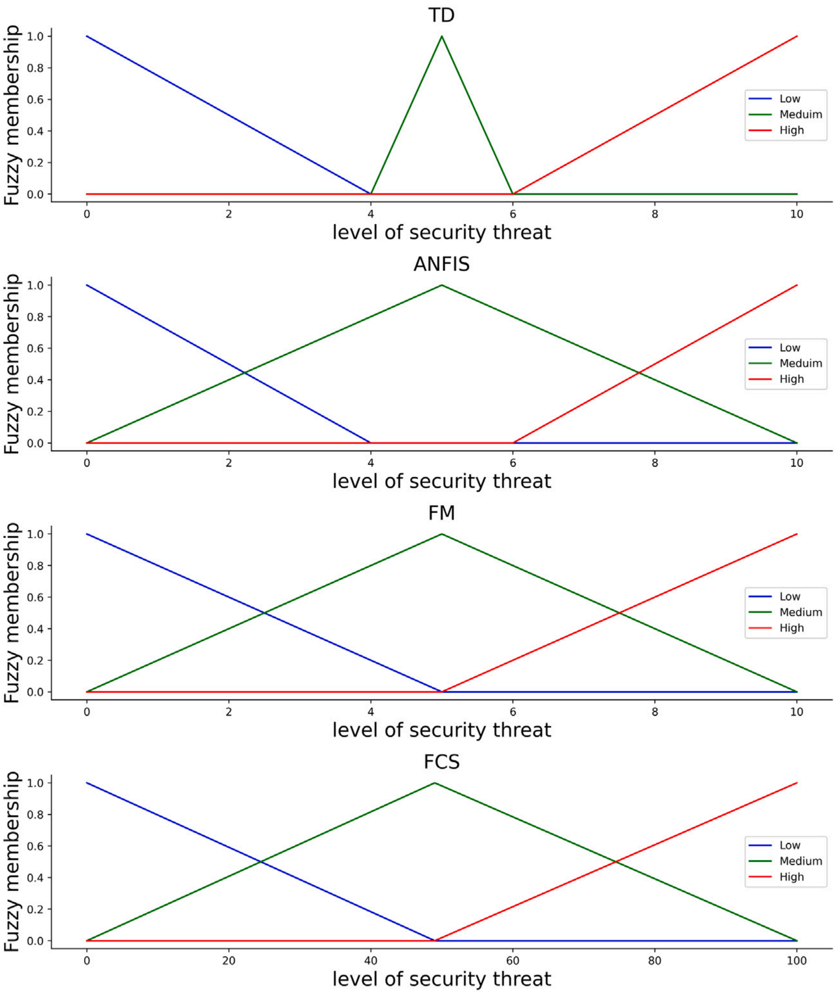

Fig. 12. Output of the membership functions.

transactions increases throughout the session. As expected, the fuzzy-based model performs better in the proposed framework because of applying the fuzzing matching approach in network communication, transaction validation, and minimized delay.

4.4.4. *Assess fuzzy matching*

In this section, we assess our FCS as the key element of the fuzzy intelligent layer in the proposed framework, which is a nonlinear controller. FCS considers the situation of other components to tackle in a complex security state. To assess our FCS in the detecting process, it should understand the threat detection and security level based on TD, ANFIS, and FM components. Fig. 12 shows universes and membership functions for FCS based on our components in the fuzzy layer. The triangular membership function converts the crisp input to the fuzzy inference system.

After considering our rules and applying them in FCS, the output of the membership function is in Fig. 13. The activity membership of each output must be combined. The above aspect is fulfilled as described to achieve aggregation. Aggregation is performed by using the maximum operator. Accumulation, in this case, means combining several elements into a cluster, and here, several membership outputs are combined into a single set of outputs. Aggregation is conducted to gather all possible outputs and use the medium to gain the outcome.

Finally, we return to crisp logic from the fuzzy world of membership functions to obtain a meaningful result. Based on fuzzy rules, the security threat level result would be 79% if TD = 9.8 (high), ANFIS = 7.8, and FM = 6.5 (low), Fig. 14 illustrates effective threat detection in the proposed framework.

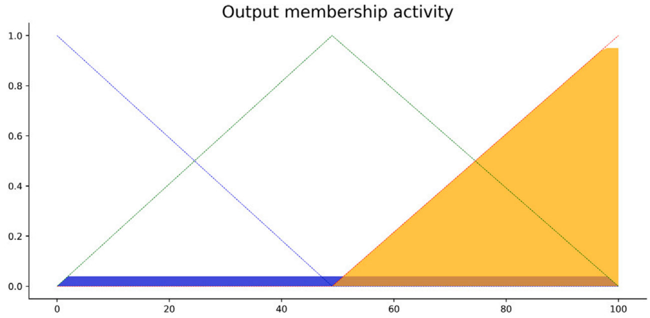

Fig. 13. Level of FCS based on inputs if they were high.

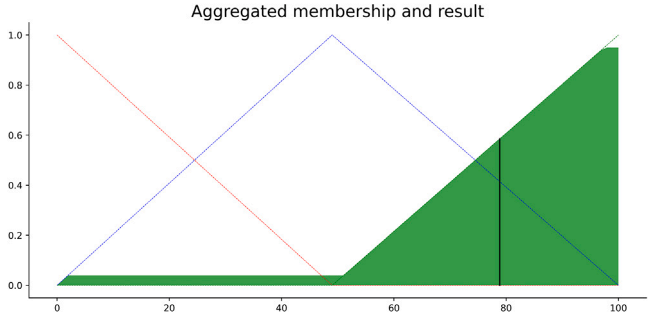

Fig. 14. Show results of FCS based on TD and FM.

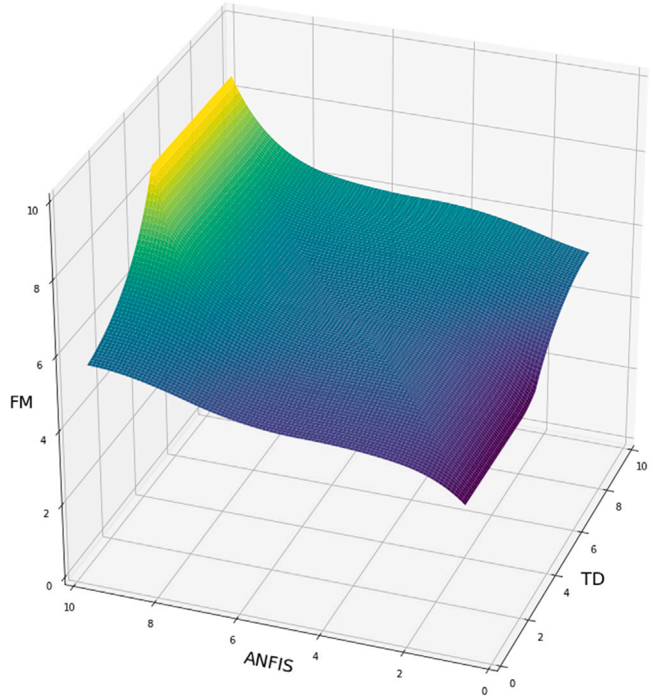

Fig. 15. Present 3D efficiency of FCS.

To show that our FCS works appropriately, and our design is correct, we draw the 3D surface of our FCS as presented in Fig. 15, which shows all inputs and output that the smoother surface proves we have a good design (stable) to consider the detecting process. Designed smooth fuzzy models provide sufficient conditions of stability for the model. Also, this issue has been proved that smoother fuzzy designs have a higher tolerance to the noises and disturbances for returning to stability rather than non-smoother models (Sadjadi et al., 2020).

5. Conclusion

This paper proposed and developed a secure intelligent fuzzy blockchain framework to detect security threats in blockchain-enabled IoT networks using threat detection, adaptive neuro-fuzzy inference system, fuzzy control system, and fuzzy matching modules. This framework utilized a novel fuzzy deep learning model and optimized neuro-fuzzy inference system-based attack detection system via metaheuristic algorithms such as genetic algorithm, differential evolution and particle swarm optimization to detect threats and attacks. We have assessed these models and compared their results with fuzzy classifiers (such as Fuzzy Pattern Classifiers, Fuzzy Pattern Tree Top-Down Classifiers, Multimodal Evolutionary Classifiers, Fuzzy pattern Classifier GA, and Fuzzy Reduction Rule Classifiers), and standard adaptive neuro-fuzzy inference system algorithm. Furthermore, the fuzzy string-matching algorithm has been applied to transaction validation to obtain fraud detection features. The proposed framework is efficient in terms of latency and throughput. Fuzzy control system presented our method effectively in threat detecting in Blockchain-enabled IoT networks based on the level of security threat (low, medium, high). In the future, we could propose a fuzzy blockchain framework model that could be used to detect and hunt cyber threats. To improve transparency, explainability, and analyst understanding of attacks, extract fuzzy if-then rules from the fuzzy deep learning model. It would be good to apply federated learning to design a secure, intelligent fuzzy blockchain framework, then compare it with our results to understand the impact of federated learning on threat detection and hunting.

CRediT authorship contribution statement

Abbas Yazdinejad: Conceptualization, Methodology, Software, Validation, Data curation, Writing – original draft, Writing – review & editing. **Ali Dehghantanha:** Conceptualization, Methodology, Validation, Data curation, Writing – review & editing. **Reza M. Parizi:** Methodology, Software, Validation, Writing – original draft. **Gautam Srivastava:** Methodology, Validation, Writing – original draft, Writing – review & editing. **Hadis Karimipour:** Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgment

All authors approved the version of the manuscript to be published.

References

2021. Blockchain-enabled cyber-physical smart modular integrated construction. Comput. Ind. 133, 103553. http://dx.doi.org/10.1016/j.compind.2021.103553.

Agarwal, N., 2021. Framework for Integration of Blockchain with IoT Devices, Mphasis. https://www.mphasis.com/content/dam/mphasis-com/global/en/downloads/whitepaper/framework-for-integrating-blockchain-with-iot-devices-whitepaper.pdf (31-Mar-2021).

Aggarwal, S., Kumar, N., 2021. Attacks on blockchain. In: Advances in Computers, Vol. 121. Elsevier, pp. 399–410.

Al-E'mari, S., Anbar, M., Sanjalawe, Y., Manickam, S., 2020. A labeled transactions-based dataset on the ethereum network. In: International Conference on Advances in Cyber Security. Springer, pp. 61–79.

Alharby, M., van Moorsel, A., 2020. Blocksim: An extensible simulation tool for blockchain systems. Front. Blockchain 3, 28.

Alsirhani, A., Khan, M.A., Alomari, A., Maryam, S., Younas, A., Iqbal, M., Siqqidi, M.H., Ali, A., 2022. Securing low-power blockchain-enabled IoT devices against energy depletion attack. ACM Trans. Internet Technol..

Anon, 2021. Detecting cyberattacks using anomaly detection in industrial control systems: A federated learning approach. Comput. Ind. 132, 103509. http://dx.doi.org/10.1016/j.compind.2021.103509.

Bahaa, A., Abdelaziz, A., Sayed, A., Elfangary, L., Fahmy, H., 2021. Monitoring real time security attacks for IoT systems using DevSecOps: a systematic literature review. Information 12 (4), 154.

Bala, R., Nagpal, R., 2019. A review on kdd cup99 and nsl nsl-kdd dataset. Int. J. Adv. Res. Comput. Sci. 10 (2).

Bamakan, S.M.H., Faregh, N., ZareRavasan, A., 2021. Di-ANFIS: an integrated blockchain–IoT–big data-enabled framework for evaluating service supply chain performance. J. Comput. Des. Eng. 8 (2), 676–690.

Barrios, P., Danjou, C., Eynard, B., 2022. Literature review and methodological framework for integration of IoT and PLM in manufacturing industry. Comput. Ind. 140, 103688. http://dx.doi.org/10.1016/j.compind.2022.103688.

Da Xu, L., Lu, Y., Li, L., 2021. Embedding blockchain technology into IoT for security: A survey. IEEE Internet Things J. 8 (13), 10452–10473.

Dai, H.-N., Zheng, Z., Zhang, Y., 2019. Blockchain for internet of things: A survey. IEEE Internet Things J. 6 (5), 8076–8094. http://dx.doi.org/10.1109/JIOT.2019.2920987.

Dwivedi, A.D., Malina, L., Dzurenda, P., Srivastava, G., 2019. Optimized blockchain model for internet of things based healthcare applications. In: 2019 42nd International Conference on Telecommunications and Signal Processing. TSP, IEEE, pp. 135–139.

Haddadpajouh, H., Azmoodeh, A., Dehghantanha, A., Parizi, R.M., 2020. MVFCC: A multi-view fuzzy consensus clustering model for malware threat attribution. IEEE Access 8, 139188–139198.

IOTA, 2020. Trinity Attack Incident. https://blog.iota.org/trinity-attack-incident-part-1-summary-and-next-steps-8c7ccc4d81e8/.

Jamil, F., Iqbal, N., Ahmad, S., Kim, D., et al., 2021. Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid. IEEE Access 9, 39193–39217.

Jung, E., Le Tilly, M., Gehani, A., Ge, Y., 2019. Data mining-based ethereum fraud detection. In: 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, pp. 266–273.

Kumar, A., Singh, M., Pais, A.R., 2019. Fuzzy string matching algorithm for spam detection in twitter. In: International Conference on Security & Privacy. Springer, pp. 289–301.

Makkar, A., Ghosh, U., Sharma, P.K., Javed, A., 2021. A fuzzy-based approach to enhance cyber defence security for next-generation IoT. IEEE Internet Things J.

Marsh, K., Gharghasheh, S.E., 2022. Fuzzy Bayesian learning for cyber threat hunting in industrial control systems. In: Handbook of Big Data Analytics and Forensics. Springer, pp. 117–130.

de Miranda Rios, V., Inácio, P.R., Magoni, D., Freire, M.M., 2021. Detection of reduction-of-quality DDoS attacks using fuzzy logic and machine learning algorithms. Comput. Netw. 186, 107792.

Mujtaba Buttar, H., Aman, W., Rahman, M., Abbasi, Q.H., 2022. Countering active attacks on RAFT-based IoT blockchain networks. ArXiv E-Prints, arXiv-2204.

Munir, M.S., Bajwa, I.S., Cheema, S.M., 2019. An intelligent and secure smart watering system using fuzzy logic and blockchain. Comput. Electr. Eng. 77, 109–119.

Namasudra, S., Sharma, P., Crespo, R.G., Shanmuganathan, V., 2022a. Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. IEEE Consum. Electron. Mag..

Namasudra, S., Sharma, P., Crespo, R.G., Shanmuganathan, V., 2022b. Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. IEEE Consum. Electron. Mag..

Pitropakis, N., Panaousis, E., Giannakoulias, A., Kalpakis, G., Rodriguez, R.D., Sarigiannidis, P., 2018. An enhanced cyber attack attribution framework. In: International Conference on Trust and Privacy in Digital Business. Springer, pp. 213–228.

Sadjadi, E.N., Menhaj, M.B., Zadeh, D.S., Moshiri, B., 2020. Stability analysis of smooth positive fuzzy systems. In: 2020 IEEE Canadian Conference on Electrical and Computer Engineering. CCECE, pp. 1–6. http://dx.doi.org/10.1109/CCECE47787.2020.9255694.

Sahoo, D., 2022. Cyber threat attribution with multi-view heuristic analysis. In: Handbook of Big Data Analytics and Forensics. Springer, pp. 53–73.

Sahoo, D., Upadhyay, A., 2022. Evaluation of scalable fair clustering machine learning methods for threat hunting in cyber-physical systems. In: Handbook of Big Data Analytics and Forensics. Springer, pp. 141–158.

Šarac, M., Pavlović, N., Bacanin, N., Al-Turjman, F., Adamović, S., 2021. Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture. Energy Rep. 7, 8075–8082.

Singh, R., Dwivedi, A.D., Srivastava, G., 2020a. Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. Sensors 20 (14), 3951.

Singh, S., Hosen, A.S., Yoon, B., 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access 9, 13938–13959.

Singh, S.K., Rathore, S., Park, J.H., 2020b. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Gener. Comput. Syst. 110, 721–743.

Thonnard, O., Mees, W., Dacier, M., 2009. Addressing the attack attribution problem using knowledge discovery and multi-criteria fuzzy decision-making. In: Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics. pp. 11–21.

Thonnard, O., Mees, W., Dacier, M., 2010. On a multicriteria clustering approach for attack attribution. ACM SIGKDD Explor. Newsl. 12 (1), 11–20.

Wu, L., Lu, W., Xue, F., Li, X., Zhao, R., Tang, M., 2022. Linking permissioned blockchain to internet of things (IoT)-BIM platform for off-site production management in modular construction. Comput. Ind. 135, 103573. http://dx.doi.org/10.1016/j.compind.2021.103573.

Yazdinejad, A., Bohlooli, A., Jamshidi, K., 2019. Performance improvement and hardware implementation of open flow switch using FPGA. In: 2019 5th Conference on Knowledge Based Engineering and Innovation. KBEI, IEEE, pp. 515–520.

Yazdinejad, A., Dehghantanha, A., Parizi, R.M., Hammoudeh, M., Karimipour, H., Srivastava, G., 2022a. Block hunter: Federated learning for cyber threat hunting in blockchain-based IIoT networks. IEEE Trans. Ind. Inf. 1. http://dx.doi.org/10.1109/TII.2022.3168011.

Yazdinejad, A., HaddadPajouh, H., Dehghantanha, A., Parizi, R.M., Srivastava, G., Chen, M.-Y., 2020a. Cryptocurrency malware hunting: A deep recurrent neural network approach. Appl. Soft Comput. 96, 106630.

Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Karimipour, H., Srivastava, G., Aledhari, M., 2020b. Enabling drones in the internet of things with decentralized blockchain-based security. IEEE Internet Things J. 8 (8), 6406–6415.

Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Zhang, Q., Choo, K.-K.R., 2020c. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Trans. Serv. Comput. 13 (4), 625–638.

Yazdinejad, A., Zolfaghari, B., Dehghantanha, A., Karimipour, H., Srivastava, G., Parizi, R.M., 2022b. Accurate threat hunting in industrial internet of things edge devices. Digit. Commun. Netw. http://dx.doi.org/10.1016/j.dcan.2022.09.010, URL https://www.sciencedirect.com/science/article/pii/S2352864822001857.

Zhang, S., Hu, Y., Bian, G., 2017. Research on string similarity algorithm based on levenshtein distance. In: 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference. IAEAC, IEEE, pp. 2247–2251.

Zolfaghari, B., Yazdinejad, A., Dehghantanha, A., 2022. The dichotomy of cloud and IoT: Cloud-assisted IoT from a security perspective. arXiv preprint arXiv:2207.01590.