



Research Article

Improving Network Security: Blockchain-based Authentication and Authorization Scheme in Accordance with Weighted Nodes in a Clustered Network

Bushra Jaber M. Jawad ¹ 
Department of Accounting,
University of Kerbala
Karbala, Iraq
Bushra.j@uokerbala.edu

Saif Mahmood Al-alak ² 
Department of Computer Science
University of Babylon
Babel, Iraq
saif.mahmood@uobabylon.edu.iq

ARTICLE INFO

Article History

Received: 12/12/2024

Accepted: 26/01/2025

Published: 31/5/2025

This is an open-access article under the CC BY 4.0 license:

<http://creativecommons.org/licenses/by/4.0/>



ABSTRACT Addressing concerns related to network security involves protecting a network from various threats, including internal and external risks, such as identity theft, collusion, malicious activities, and other attacks. This study aims to address these challenges by introducing the authentication of the identity of nodes that are connected to a network, utilizing blockchain technology and consensus algorithms as integral elements of its security framework. To improve security and deal with identity theft and spoofing attacks in clustered networks, we suggest implementing a blockchain-based authentication and authorization scheme. This scheme ensures that the authentication of nodes or devices relies on blockchain technology, employing a voting algorithm to validate the eligibility of nodes that are seeking access to a network. A new block is generated for each incoming node, and this block contains essential information about that node. The decision to accept a new node into the network is determined through a voting process that considers individual node weights calculated based on three key factors: initial weight, age, and incentive. Java NetBeans IDE 8.0.2 is used to design and implement the simulator. Experimental results comprise the implementation of consensus algorithms and demonstrate the effect of the highest weight nodes. Moreover, these algorithms will launch attacks on the network and are aware of our scheme's ability to detect such attacks. The simulation results show that our authentication scheme exhibits advantages in terms of security, scalability, and resistance

Keywords: Network security; Blockchain; Consensus algorithms; Node authentication; Trusted degree.

1. INTRODUCTION

Network security involves protecting the underlying network infrastructure and data from security breaches, illegitimate access, and other threats. Authentication is one of the requirements of network security and identity management. Identification refers to the ability to distinguish the user of a system or an application running in that system in a specific and unambiguous manner. To establish the identity of an entity, identification and authentication are combined in a single two-step process. Documents, biometric information, or personal information can be authenticated. Every device on a computer network must have an identity provided by the manufacturer. An ID must be unique and standardized, such as Internet Protocol (IP) addresses, which uniquely identify the device on a network. Barcodes, printed numbers, radio frequency identification, or QR codes are frequently used in device identification [1].

Since 2014, blockchain technology has elicited considerable interest from scientists and members of academia [2]. A blockchain is an organized collection of linked and duplicated data blocks that act as a publicly distributed peer-to-peer ledger [3]. The integrity of a blockchain is maintained by using public-key encryption as the standard method for communicating all network interactions with updated transactions. Given its decentralized structure, security, and immutability aspects, blockchain technology has been implemented in numerous areas and applications, including industry [4], healthcare [5], finance [6], agriculture [7], smart cities [8], forecasting [9], smart contracts [10], and big data [11].

The groundbreaking success of blockchain technology was first observed in bitcoin; thereafter, other blockchains, such as Ethereum and Hyperledger Fabric, emerged [12], [13]. Ethereum can play an important role in a public blockchain, such as bitcoin, or a private one, such as Hyperledger Fabric [14].

Consensus algorithms are special algorithms that are used to maintain the security of a blockchain. They allow for the addition of a new block to a blockchain without violating the integrity of the information stored in the distributed ledger. Different types of consensus algorithms include proof of work (PoW) [15], proof of stake [16], proof of authority [17], practical Byzantine fault tolerance, proof of luck, Ripple, and Raft [18], [19].

The blocks in a blockchain consist of two primary components: 1) the block header and 2) the block body [20]. The body contains transaction records that represent the data that must be stored. These data can encompass various types of transactions, such as currency exchanges, system logs, traffic information, and health data. The block header contains two sets of meta-information [21]. The first set is associated with mining and includes time stamps related to the created time block, difficulty targets, and nonce values [22]. The second set is related to the block itself and includes fields for version numbers and linked parent blocks; that is, the block is hashed and hashed pointers to its previous block, and the Merkle roots that use the SHA256 hash algorithm [23].

Given the characteristics of the aforementioned blockchain technology, the current study proposes an authentication scheme that uses a blockchain to prevent identity theft and spoofing attacks on clustered networks. Despite the transformative potential of a blockchain, it faces several critical challenges. One major issue is scalability. As a network grows, processing and verifying transactions become slower and more resource-intensive, limiting a blockchain's ability to handle high transaction volumes, such as in traditional systems. Energy consumption is another significant concern, particularly with PoW consensus mechanisms [24], which require vast computational power. Security vulnerabilities, such as 51% attacks and smart contract bugs, further threaten the integrity and trustworthiness of blockchain systems. Moreover, data privacy remains a challenge because most public blockchains are transparent by design. Lastly, the complexity of blockchain technology and limited developer expertise slow down innovation and implementation, while user adoption is hampered by poor experience and unclear value propositions. Addressing these challenges requires advancements in consensus algorithms, regulatory frameworks, scalability solutions, and user-centric designs to realize the full potential of a blockchain [25],[26].

Furthermore, blockchain technology is used to authenticate nodes and justify results, and thus, an authentication scheme is proposed. This scheme can reduce the probability of identity-based security violations in a clustered network. Notably, the current study is a continuation of the work in [27].

This paper has five sections. Related work is provided in Section 2. The proposed blockchain-based authentication scheme is described in Section 3. The implementation details and the results are presented in Section 4. Section 5 offers the conclusions drawn from the study.

2. RELATED WORK

Many authentication schemes use blockchain technology in different types of networks and environments. For example, a secure and lightweight blockchain-based Internet of things (IoT) authentication scheme was proposed in [28]. In addition to authentication, the proposed scheme provides integrity and non-repudiation functions. In [29], the authors presented a combined method that integrated quantitative and qualitative analyses to assess the suitability of consensus for a variety of building applications. For a more comprehensive analysis of their appropriateness, blockchain-based applications in the construction industry are classified into four key types: 1) management of construction transactions, 2) management of information, 3) management of construction processes, and 4) monitoring and supervision. Shi et al. presented a blockchain-empowered authentication, authorization, and auditing (AAA) strategy for "LS-HetNet" data security. The processes for AAA were then redefined after the account address of a blockchain was used in identity authentication, and the access control authority of the data was redesigned and stored in the blockchain [30].

A novel scheme was introduced for vehicle group authentication, leveraging the power of blockchain technology. The system was designed for decentralized identification by using secret sharing and a dynamic proxy mechanism. To achieve collaborative authentication, the sub-authentication results were combined through a trust management-based blockchain approach. The tamper-proof blockchain stores data, and an edge computing node with a superior reputation is responsible for uploading the aggregated authentication result to the central server. This process ensures a secure

and decentralized authentication process for vehicles [31]. A self-sovereign identification and authentication method based on a blockchain was proposed to prevent fraud, identity theft, and spoofing in distributed energy networks. In this work, a paradigm for IoT device identification and authentication based on blockchain technology and a Merkle tree architecture was discussed. With focus on identity-based security, the implementation of identification and authentication was also described [1].

An innovative approach for decentralized authentication by using blockchain technology is introduced. The authentication process is optimized by organizing IoT devices into clusters based on their computational capability, energy reserve, and location. Each cluster undergoes authentication through a hierarchical structure of interconnected blockchains [32]. A consensus protocol is proposed to reduce processing load. This protocol relies on verifying the identity-based encryption key signature of the device and its corresponding cluster. This model describes how to use the immutability feature of a blockchain to address serious issues in the area of decentralized ad-hoc networks. In particular, we demonstrate how a comprehensive solution that includes mechanisms for authentication and trust evaluation may be created in a self-organized, evolving network [33].

In [34], a model that used a blockchain was proposed for detecting malicious nodes. However, network resources could be accessed and used by nodes without authorization if they were not authenticated. Kim et al. presented a blockchain-based trust model based on the behavior of nodes and data-based trust. However, recommender nodes were employed to evaluate indirect trust. The network obtained incorrect information about trustworthy nodes when recommender nodes were malicious [35]. Accordingly, we proposed our schemes to overcome the aforementioned problems and issues.

A blockchain-based decentralized authentication modeling scheme (called BlockAuth) was proposed for edge and IoT environments to provide a strong fault tolerance solution, in which each edge device was regarded as a node to form a blockchain network. A registration and authentication strategy was designed, and the blockchain consensus, smart contract, was developed [36].

3. PROPOSED SYSTEM

In the current study, a new scheme for authentication and authorization that uses blockchain technology is presented. The proposed authentication and authorization scheme is based on the weights of nodes. It implements a new method for achieving numerous goals related to authorization and authentication mechanisms with the trust values of nodes. A blockchain is used as a database to store security information for each node in the network. Scalability is one of the features that has been selected as the focus of this study. To prevent malicious nodes from joining a network by using the voting principle based on the weights of nodes, a new node that has been added must be accepted by the other nodes in the cluster with the highest weight. Therefore, all nodes have calculated weights based on three factors: 1) initial weight, 2) profit or incentive, and 3) age.

The cluster structure is used in the proposed authentication and authorization scheme. The cluster head is the first node that builds the cluster network, and it plays a major role in the management of the cluster. However, the cluster head performs the collected votes and the most related consensus process. It does not exceed half of the total number of nodes, considering the weight of each node in the network. The weight value is represented as the ratio of the trust weight of each participating node in the voting process, and each node that is participating for the first time in the network will have an initial value as the minimum value of weight. This value is used as a measure to indicate the weights of nodes. Fig. 1 illustrates the network structure for the authentication scheme.

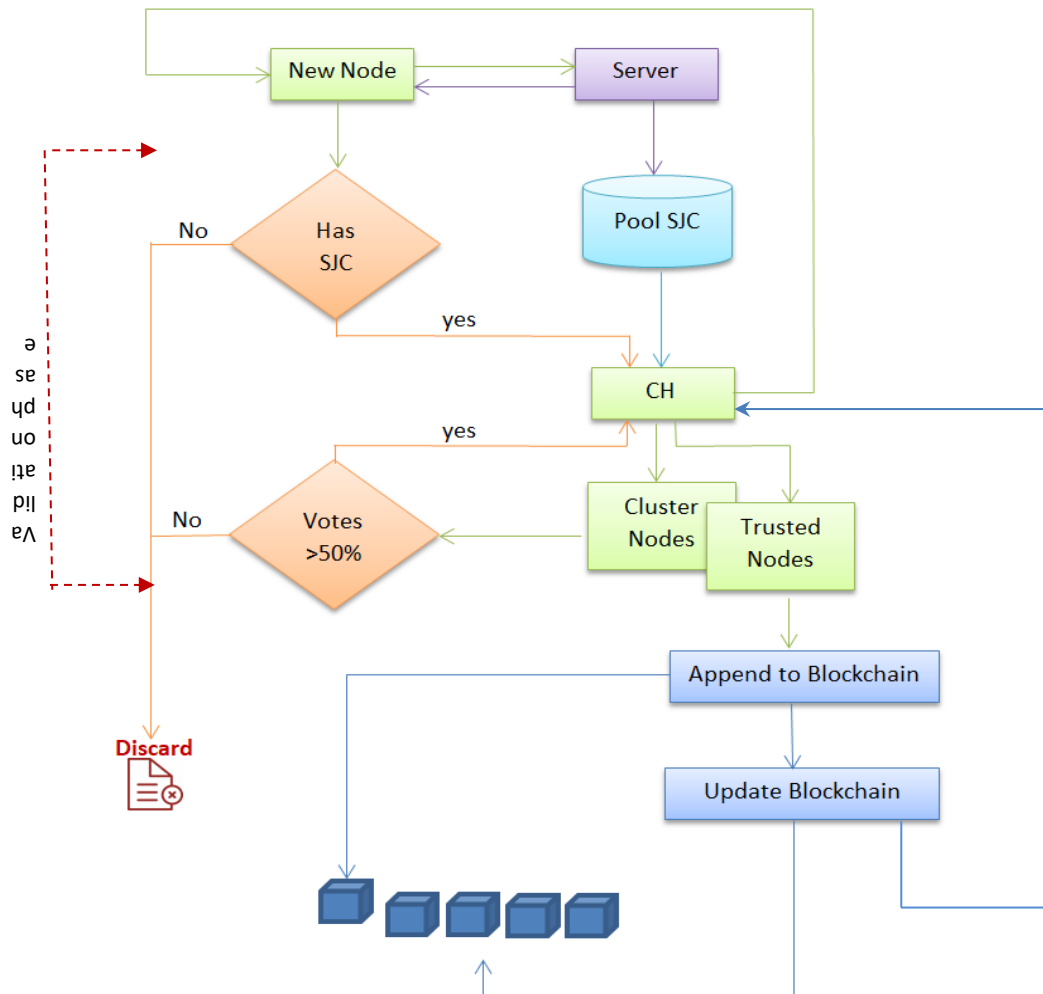


Fig. 1. Block of the proposed authentication and authorization scheme.

The initial weight is segmented into five levels of trust. As indicated in Equation 1, where the joining level refers to the degree of trust and depends on the time that the node is added to the network, the five levels will indicate the value of trust for a new node. By updating the nodes through the server and obtaining their secret joining card (SJC), these levels minimize the chance of illegitimate nodes joining the cluster.

$$\text{Joining level} = (\text{joining}_{Time} - \text{system}_{InitialTime}) \text{ Mode } 5 \quad (1)$$

The votes of nodes can be calculated using the following equation, where the weight of each node is multiplied by its vote:

$$v_i = k * w_i, \quad (2)$$

where $k = 1, 0$; w_i is the weight of each node; $i = 1$ to n ; and n is the number of nodes.

Equation 3 can find the impact node via the weight of nodes.

$$Impact\ node_i = \frac{w_i}{\sum_{i=1}^n w_i}, \quad (3)$$

where i is the node that votes, and w_i is the weight of nodes that are considered voters.

$$Result = \frac{\sum_{i=1}^m wi}{\sum_{j=1}^n wj} * 100\%, \quad (4)$$

where m is the number of voters, w_i is the weight of each voter, n is the total number of nodes, and w_j is the weight of the total nodes. Weight, which is equivalent to a trusted degree, depends on many factors. These factors include the following. 1) The initial weight of each node represents the time when a node arrives in the network and sends the request to connect to the network. 2) Age represents the time spent by a node in a network—from its arrival in the network and its connection until the present. 3) Incentive or profit refers to scores or degrees as a reward given to nodes that build a block. As depicted in Fig. 1, our schemes consist of four stages to authenticate new nodes—starting from the stage in which a new node wants to join a network to the stage of acceptance and building new blocks in the blockchain network for the new node.

During the initial stage, a new node sends a request to the server to obtain a unique identity, which includes a secret identity and an SJC. The SJC includes a matrix that represents a number of rows equivalent to the number of nodes in the cluster. Each row of the matrix contains the node identity and secret identity encrypted by the public key of a node, as described in Table 1. The SJC supports the new node's decision to join the cluster by asking all the members of the cluster to vote on its authenticity.

TABLE I. Sjc

No. of Nodes	Secret Identity
1	Encryption(PK _{Node1} (r600e984Fd47645489202329t898393B2))
2	Encryption(PK _{Node2} (7eregvs34511753984732g32880263523e))
3	Encryption(PK _{Node3} (87he6534876492098h33s736290973524))
..
N	Encryption(PK _{Noden} (87he653482909984634325d4362337524))

The request sent by the new node must be encrypted by the server's public key after being sent to the server. The side of the server responds to a new node request for providing SJC with an encrypted code called SJC, which is explained in the following steps in Algorithm (1).

<i>Algorithm (1): Sending of and Responding to Request and Generating SJC</i>	
Input (info _{NewNode} , Request)	
Output (Card[SJC _i])	
1. For i = 1 to n do	
2. New Node Send Request to Join	
3. Server Receive Request	
4. Server Generate SJC _{NewNode} (info _{NewNode})	
5. Append Card[SJC _i]	
6. End for	
7. Send (Card[SJC _i])	// to cluster head for update it and to new node

In the second stage, as explained in Algorithm (2), a new node sends a request to the cluster head to join a network. Such request includes the SJC. The new node also sends all its information to be stored later on the blockchain. This information is required to confirm the legitimacy of the new node. It comprises an ID node, name, time stamp, public key, IP address, and location. This information must be correct and accurate.

After the new node sends the request to join the network and the cluster head receives the request, the new node's SJC is checked. If it exists, then the cluster head will broadcast the request to all the nodes in the cluster; otherwise, the cluster head will ignore it.

Algorithm (2): Sending a Request to the Cluster Head

```

Input (Card[SJCi])
Output (RequestNewNode to all nodes)

1.      New Node Sends Request to Cluster Head
2.      Cluster Head Receives (RequestNewNode)
3.      if SJCNewNode  $\subset$  (Card[SJCi]) then           // checking SJCNN if existing
4.      Broadcast(RequestNewNode)                 // send request for voting
5.      end if

```

As shown in Algorithm (3), after the cluster head broadcasts the new node's SJC to validate it, each node receives a request and, if ready, compares the SJC with its card, and then votes.

Algorithm (3): Validating SJC

```

Input n, Card[SJCi]                                //n: number of members in the cluster
Output(validation of SJCNewNode)

1:  Begin  $v_i * \text{Weight}_i$ 
2:  for i = 1 to n
3:      if SJCNewNode  $\subset$  (card[SJCi]) then
4:           $v_i \square$  yes votes
5:           $M_i = v_i * \text{Weight}_i$                      // votes multiply weight of each
node
6:          Sum = Sum +  $M_i$ 
7:          if Sum > 50% of total number of nodes then
8:              Result voting  $\square$  Sum                     // if sum > 50 accepted
9:              Send (Result voting to the cluster head)
10:             else reject NewNode
11:         end if
12:     end if
13: end for
14: End

```

When the total number of votes exceeds half of the total number of nodes in the cluster, the voting result is calculated by multiplying each node's weight by its vote, as shown in Equation 2. Then, the node is accepted if the voting conditions are met, as illustrated in the steps of Algorithm (3).

The weights of the nodes are calculated and updated by the cluster head after each node is added to the blockchain and a new block is built for this new node. Members who participate in building the new block receive an incentive or reward, and thus, their weight is increased. Accordingly, they can represent an increase in miner's effectiveness or trust values.

Suppose the total number of votes exceeds more than half of the total number of nodes in the cluster and the vote result. Then, it will be calculated by multiplying the weight of each node by its vote, as shown in Equation 2. The vote will be accepted if the voting conditions are met, as shown in the steps of Algorithm (4).

After validating the SJC of the new node by voting for it to join the network, the seventh phase will enter. In this phase, the cluster head multicasts information about the node to the trusted nodes to build a block.

Meanwhile, in the eighth phase, as illustrated in Fig. 1, the role of trusted nodes includes adding a new block to the blockchain for the new node, in which the block contains the previously mentioned node information (i.e., ID, name,

IP address, time stamp). In turn, the trusted nodes perform the necessary steps, which include building a new block and updating the blockchain.

4. RESULTS AND DISCUSSION

4.1 Programming Environment

The application is implemented on a laptop with an Intel i7 core processor, 16 GB of RAM, and Windows 11 Pro operating system. The application is developed on NetBeans IDE 8.0.2, JDK 8, and Apache 8.0.15. The proposed scheme estimates the reliability of nodes in the network, which exhibits a cluster structure with the management of cluster members via the cluster head.

4.2 Experiments

To analyze and evaluate the scheme, the values of many factors were set to prove their effects. To measure the effectiveness of the proposed scheme, we suggested the initialized values and set them to obtain the best choice, making the system's security more robust and effective.

TABLE II: Input Parameters of the Experiments

Parameters	No.
Member nodes	25 to 500
Server	1
Admin	1
Cluster head	1
Privilege admin	- Providing ID - Configuring server and pool
Privilege server	- Providing SJC, updating SJC poll - Interconnection with the admin and cluster head
Privilege cluster head	- Calculating the weight of nodes, updating the blockchain

To investigate the effect of the weight on each member node and how weight is affected by the values of the parameters, the suggested values of the parameters are provided in Table II for the three tests (RSM,HSM, and LSM).

TABLE III: Parameters and values for the three tests RW, HW, and LW

Test No.	Profit	Initial Weight
1	0.1	0.01
2	0.5	0.05
3	0.1	Rang(0.01 to 0.09)
4	0.5	Rang(0.01 to 0.09)

Three algorithms are used in our study. The first algorithm is the random weight algorithm (RW), which randomly chooses the member that will build the new block for the new node. The second algorithm is the highest weight algorithm (HW), which depends on the nodes with the highest weights. The third algorithm is the lowest weight algorithm (LW), which depends on the nodes with the lowest weights. The last two algorithms were chosen randomly among the members.

When analyzing the results and giving the initial values for the factors (age, profit, and initial weight), as indicated in Table 3, and the set values of these factors are as follows: age and profit (0.5) and initial weight (0.01), the results will be as follows. The highest levels of the weights of the nodes are located within the range of 0.20–0.40 when HW is used. When RW is used, the highest level of weights is within the range of 0.15–0.40. For LW, the lowest value, as illustrated in Fig. 2, starts from the maximum value of 0.20 and below.

When the values of age and profit are reduced to 0.01, the initial weight remains at 0.01. The results in Fig. 3 are as follows. The highest weights of nodes are achieved when RW is used. Meanwhile, HW provides the highest level of weights, ranging from 0.15 to 0.38. LW obtains the least weight of nodes. Therefore, the results will be more satisfying when they are considerably less than the previous experience.

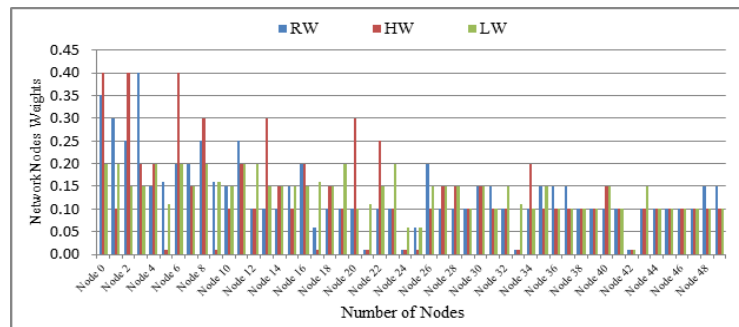


Fig. 2. The impact of two factors age and profit with consensus algorithms.

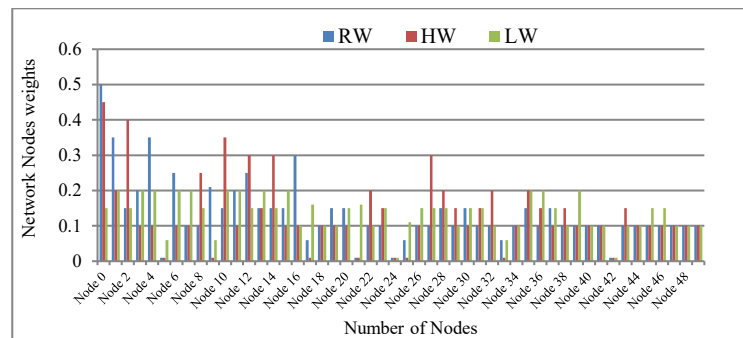


Fig 3: Effect of reducing age and profit.

When age is set to a value of 0.05, the result is nearly similar to the previous results presented in Fig. 3. If the profit value is increased to 0.05, then the results will be closer to those shown in Fig. 2. Finally, if the initial weight is increased gradually, then the weights of the nodes will be affected.

The next results of the study are for the effect of the initial weight of each node. As mentioned earlier, each node obtains a trust degree based on the time during which it sends a request to join the network. The age and profit values will be 0.01 or 0.05. Fig. 4 illustrates the result of randomly setting the initial weight values. Meanwhile, Fig. 5 depicts the values of the initial weight by using Equation 1.

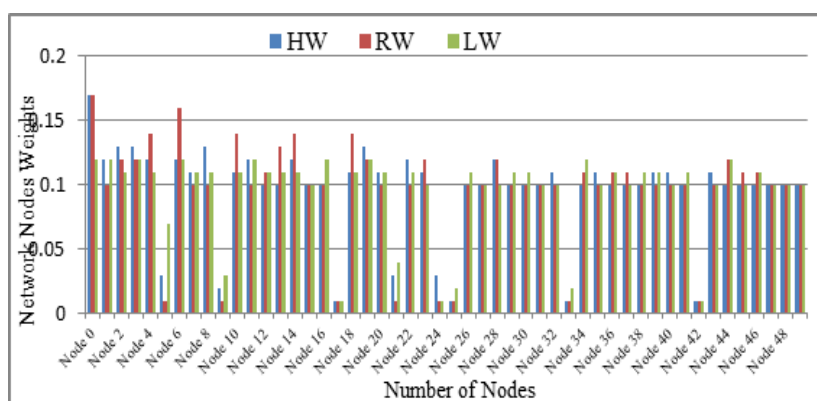


Fig. 4. The impact of random values of initial weight on weights of node.

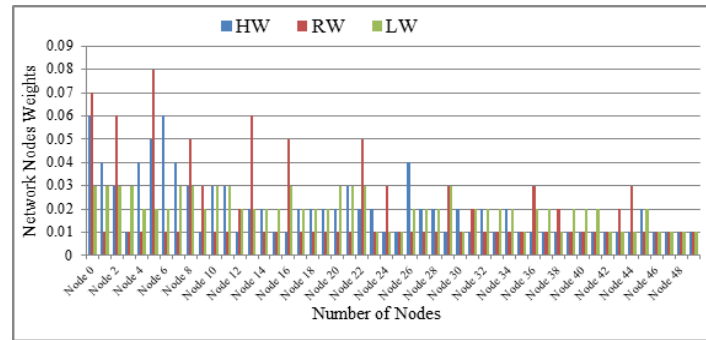


Fig. 5. Effect of varied values of initial weight through Equation 1.

In general, when the value of age is increased in the above experiments, the final results of node weights will change slightly and increase. However, when the value of profit is increased, the change in weight and impact ratio will be more significant. Moreover, when the initial weight values are calculated in accordance with Equation (1) (or the inverse values), the results will be more satisfying and considerably lower than in the previous experiments. Thus, the summary of the above results is as follows:

HW: proves its performance in terms of weight and acceptance rate; most effective for secure and efficient networks.

RW: balances fairness and security, but its random nature may not be as efficient as that of HW.

LW: underperforms due to its focus on low-trust nodes, increasing risk.

HW with RW may further enhance network fairness and security.

4.3 Security Analysis

This section discusses how secure the suggested solution is and how well it can resist common attacks directed against blockchain networks. The comprehensive system is evaluated based on its ability to satisfy the security requirements for authorization and authentication. A comparison of the proposed system's security features with those of related centralized and decentralized authentication techniques is provided in Table 4.

4.3.1 Management Identities of nodes

In our proposed system, possessing a distinct identifier (i.e., SJC) is essential for each node. The identifier is assigned by the server, and it is used to authenticate a node's legitimacy. The details of the identity are recorded on the blockchain, while the SJC is stored within the server-provided SJC's (trusted third party) for verification. A node is considered valid unless its SJC corresponds to one of the stored identities in the pool of SJC's, ensuring the reliability of the new identity. Communication between two nodes is safeguarded by the private key, which is linked to the node's confidential identity, generating the SJC. Consequently, entities within our model can be readily identified.

4.3.2 Secure Authentication

Authentication is crucial for ensuring that data originate from a legitimate and registered source. In the context of node authentication within a cluster, a set of voting principles is employed to incorporate a new node into the network and blockchain. Before transmitting any data, verifying the authenticity of the new node is essential to thwart impersonation attacks that can introduce manipulated or falsified data.

In centralized-level communication, the server provides identity and SJC to the new node. The blockchain initially confirms the legitimacy of each new node in decentralized communication. Each new node has an SJC.

If a node receives agreement from most nodes during the voting stage, and its SJC is matched, then the validating stage is completed. Thereafter, the new node is accepted by the members of the cluster, and thus, authentication is confirmed. The SJC of the new node is accepted, and a new block is built and added to the blockchain.

4.3.3 Resistance Attacks

The proposed authentication system is resistant against spoofing and Sybil attacks. In the case of a spoofing attack, when an attempt is made to mimic the identity of a legitimate node for a malicious activity, the suggested scheme incorporates authentication measures. The cluster head and other nodes do not endorse any attempts to manipulate messages in the system, because the authentication mechanism relies on a node's private key to encrypt the secret identity and SJC. Therefore, data delivered across networks in communication scenarios are resistant to spoofing attempts and cannot be altered.

A Sybil attack involves the creation of several fake identities by the attacker in an attempt to compromise and disrupt system functionality. Every node in the network is only allowed to have one secret identity and one SJC registered on the system. Node creation of multiple identities is prohibited. Furthermore, only one SJC and key pair may be associated with each identity. Each communication that is sent out must be signed by the sender's identification keys in addition to their signature. Fig. 3.1 illustrates how to define and store identities in the pool SJC of the server and blockchain, preventing a malicious node from creating new identities to launch a Sybil attack.

TABLE VI: Comparing the suggested system's security properties with those of related models

Features		Zhaofeng et al. (2021) [36]	Selvaraj et al. (2022) [37]	Proposed scheme
Authentication type:		Decentralized blockchain-based	Centralized blockchain-based	Centralized and decentralized blockchain-based
Secure authorization:		Strong	Poor	Strong
Resistance attacks:	Identity theft	Moderate	Moderate	Strong
	Spoofing attack			
	Sybil attack			
	Malicious nodes			

6. CONCLUSION

In this study, we propose an authentication scheme based on the principles of blockchain technology. This scheme validates network nodes through a voting mechanism. The voting process relies on the degree of trust assigned to each node, as represented by their weights. These weights are determined based on three factors: the age of the node, its profit or incentive, and the duration for which the node has been part of the system. In addition, the scheme identifies and monitors potential attackers based on their relevant identities. The three proposed algorithms depend on the weight of the nodes to assess their effect on system effectiveness and robustness. Consequently, the nodes with the highest weights and the greatest influence are prioritized in the voting process and the acceptance of new nodes to join the network. The implementation of this scheme was achieved using Java, and the experimental results indicate that our approach effectively detects malicious nodes and attacks, regulates the integration of new nodes, and protects the network, ensuring security and supporting scalability.

References

- [1]. V. Dehalwar, M. L. Kolhe, S. Deoli, and M. K. Jhariya, "Blockchain-based trust management and authentication of devices in smart grid," *Clean. Eng. Technol.*, vol. 8, no. March, p. 100481, Jun. 2022, doi: <https://doi.org/10.1016/j.clet.2022.100481>.
- [2]. H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain Res. Appl.*, vol. 3, no. 2, p. 100067, 2022, doi: [10.1016/j.bcr.2022.100067](https://doi.org/10.1016/j.bcr.2022.100067).
- [3]. B. Tavares, F. Figueiredo Correia, and A. Restivo, "A survey on blockchain technologies and research," *J. Inf. Assur. Secur.*, vol. 14, pp. 118–128, 2019, [Online]. Available: www.mirlabs.net/jias/index.html

-
- [4]. J. Lee, M. Azamfar, and J. Singh, "A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems," *Manuf. Lett.*, vol. 20, no. October, pp. 34–39, 2019, doi: 10.1016/j.mfglet.2019.05.003.
- [5]. C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthc.*, vol. 7, no. 2, 2019, doi: 10.3390/healthcare7020056.
- [6]. A. Polyviou, P. Velanas, and J. Soldatos, "Blockchain Technology: Financial Sector Applications Beyond Cryptocurrencies," p. 7, 2019, doi: 10.3390/proceedings2019028007.
- [7]. G. Mirabelli and V. Solina, "Blockchain and agricultural supply chains traceability: Research trends and future challenges," *Procedia Manuf.*, vol. 42, no. 2019, pp. 414–421, 2020, doi: 10.1016/j.promfg.2020.02.054.
- [8]. S. Meikandasivam, R. Thirumalaivasan, M. Janaki, P. Rath, and A. Shanmuganaathan, "Smart home energy management system," *Int. J. Appl. Eng. Res.*, vol. 10, no. 19, pp. 39970–39974, 2015, doi: 10.4018/978-1-7998-1230-2.ch011.
- [9]. H. Jang and J. Lee, "An Empirical Study on Modeling and Prediction of Bitcoin Prices with Bayesian Neural Networks Based on Blockchain Information," *IEEE Access*, vol. 6, no. c, pp. 5427–5437, 2017, doi: 10.1109/ACCESS.2017.2779181.
- [10]. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
- [11]. C. Xu *et al.*, "Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 4, pp. 870–882, 2019, doi: 10.1109/TPDS.2018.2871449.
- [12]. C. Cachin, "Architecture of the Hyperledger Blockchain Fabric*," *Work. Distrib. cryptocurrencies Consens. ledgers*, vol. 310, 2016.
- [13]. K. Cho and Y. Cho, "Hyper ledger fabric-based proactive defense against inside attackers in the WSN with trust mechanism," *Electron.*, vol. 9, no. 10, pp. 1–17, 2020, doi: 10.3390/electronics9101659.
- [14]. A. Anoaica and H. Levard, "Quantitative Description of Internal Activity on the Ethereum Public Blockchain," *2018 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc.*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/NTMS.2018.8328741.
- [15]. S. Zhang and J. H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, 2020, doi: 10.1016/j.icte.2019.08.001.
- [16]. S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," 2012, [Online]. Available: <http://www.peercoin.net>
- [17]. Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.
- [18]. D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," *Proc. 2014 USENIX Annu. Tech. Conf. USENIX ATC 2014*, pp. 305–319, 2014.
- [19]. M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *J. Netw. Comput. Appl.*, vol. 182, no. July 2020, p. 103035, 2021, doi: 10.1016/j.jnca.2021.103035.
- [20]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.
- [21]. N. Arunkumar and P. Sivaprakasam, "Blockchain Technology in Data Management," *Proc. 4th Int. Conf. Comput. Methodol. Commun. ICCMC 2020*, no. Iccmc, pp. 199–206, 2020, doi: 10.1109/ICCMC48092.2020.ICCMC-00039.
- [22]. M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.
- [23]. T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.
- [24]. G. Tripathi, M. A. Ahad, and G. Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," *Decis. Anal. J.*, vol. 9, no. October, p. 100344, 2023, doi: 10.1016/j.dajour.2023.100344.
- [25]. S. Velliangiri and P. Karthikeyan Karunya, "Blockchain technology: Challenges and security issues in consensus algorithm," *2020 Int. Conf. Comput. Commun. Informatics, ICCCI 2020*, 2020, doi:
-

- 10.1109/ICCCI48352.2020.9104132.
- [26]. N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," *ICOSST 2018 - 2018 Int. Conf. Open Source Syst. Technol. Proc.*, no. May 2020, pp. 54–63, 2019, doi: 10.1109/ICOSST.2018.8632190.
- [27]. B. M. Jawad and S. Al-Alak, "Node authentication using the voting scheme for clustered network," *Int. Conf. Electr. Comput. Commun. Mechatronics Eng. ICECCME 2022*, no. November, pp. 16–18, 2022, doi: 10.1109/ICECCME55909.2022.9988052.
- [28]. S. Hong, "P2P networking based internet of things (IoT) sensor node authentication by Blockchain," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 579–589, 2020, doi: 10.1007/s12083-019-00739-x.
- [29]. Y. Xu *et al.*, "Suitability analysis of consensus protocols for blockchain-based applications in the construction industry," *Autom. Constr.*, vol. 145, no. June 2022, p. 104638, 2023, doi: 10.1016/j.autcon.2022.104638.
- [30]. N. Shi, L. Tan, W. Li, X. Qi, and K. Yu, "A blockchain-empowered AAA scheme in the large-scale HetNet," *Digit. Commun. Networks*, vol. 7, no. 3, pp. 308–316, 2021, doi: 10.1016/j.dcan.2020.10.002.
- [31]. H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain Empowered Cooperative Authentication with Data Traceability in Vehicular Edge Computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4221–4232, 2020, doi: 10.1109/TVT.2020.2969722.
- [32]. M. T. Al Ahmed, F. Hashim, S. Jahari Hashim, and A. Abdullah, "Hierarchical blockchain structure for node authentication in IoT networks," *Egypt. Informatics J.*, vol. 23, no. 2, pp. 345–361, 2022, doi: 10.1016/j.eij.2022.02.005.
- [33]. A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," pp. 1–6, 2017, [Online]. Available: <http://arxiv.org/abs/1706.01730>
- [34]. W. She, Q. Liu, Z. Tian, J. Sen Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019, doi: 10.1109/ACCESS.2019.2902811.
- [35]. T.-H. Kim *et al.*, "A Novel Trust Evaluation Process for Secure Localization Using a Decentralized Blockchain in Wireless Sensor Networks," *IEEE Access*, vol. 7, no. December, pp. 184133–184144, 2019, doi: 10.1109/ACCESS.2019.2960609.
- [36]. M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2116–2123, 2021, doi: 10.1109/JIOT.2020.3037733.
- [37]. P. Selvaraj and V. B. Srinivasan, "Capture Based Trust Dependence framework for authorized node identification in mobile agent systems," *Meas. Sensors*, vol. 24, no. July, p. 100471, 2022, doi: 10.1016/j.measen.2022.100471.