Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Securing Transaction Records over the IoT Network Using Decentralized Distributed Ledger Technology

Ramanakar Reddy Danda, Kiran Kumar Maguluri, Dr. M. Rajesh Khanna, Dr. A Hanumat Prasad, P Jyothi, Dr. S. N. V. Jyotsna Devi Kosuru
IT Architect , CNH, NC ramanakarreddy.danda.eia@gmail.com,
ORCID: 0009-0005-7181-4508
, IT systems Architect, Cigna Plano Texas, kirankumar.maguluri.hcare@gmail.com, ORCID: 0009-0006-9371-058X
Associate Professor
Department of Information Technology
Vel Tech Multi Tech Dr Rangarajan Dr Sakunthala Engineering College, Avadi, Chennai-600062
Rajeshkhanna@Veltechmultitech.Org
Assoc.Prof,
Dept Of CSE- AI &ML
Kallam Haranadhareddy Institute Of Technology, Guntur,
Ap,India
Hanuma.Alahari@Gmail.Com
Assistant Professor, CSE Dept.
VNR Vignana Jyothi Institute Of Engineering And Technology
Hyderabad
Jyothi_P@Vnrvjiet.In
Assistant Professor,
Department Of CSE,
Koneru Lakshmaiah Education Foundation
Vaddeswaram-522302, Guntur, Andhra Pradesh, India
Jyotsnakosuru@Gmail.Com

ARTICLE INFO

Received: 24 Dec 2024
Revised: 16 Feb 2025
Accepted: 24 Feb 2025

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has ushered in a new era of connectivity and data exchange, revolutionizing various industries. However, the inherent vulnerabilities in traditional centralized transaction systems pose significant security challenges, particularly when dealing with sensitive data generated by IoT devices. This paper introduces an ICAA (Integrity Consensus Authorization Algorithm) for securing transaction records over the IoT network by leveraging Decentralized Distributed Ledger Technology (DDL), integrating the PICA (Proof-of-Integrity Consensus Algorithm) and CTAP (Context-Aware Transaction Authorization Protocol). The proposed system addresses the limitations of centralized architectures by employing a decentralized ledger, ensuring transparency, immutability, and tamper-resistant transaction records. The Proof-of-Integrity Consensus Algorithm enhances the security of the network by validating and confirming transactions based on the integrity of the data stored in the distributed ledger. This consensus mechanism minimizes the risk of fraudulent activities and unauthorized modifications, making it well-suited for the dynamic and distributed nature of IoT environments. Furthermore, the integration of the Context-Aware Transaction Authorization Protocol enhances the adaptability of the system to the diverse contexts in which IoT devices operate. The synergy between the Proof-of-Integrity Consensus Algorithm and the Context-Aware Transaction Authorization Protocol creates a comprehensive and secure framework for managing transaction records in IoT networks. . The proposed HGGC is 5.026% better than the ECMQV-MAC, 0.4215% better than QKD, and 0.0843% better than OTP in the nodes 200. The proposed model contributes to the establishment of a trustworthy and resilient infrastructure for the IoT, laying the foundation for secure and transparent transactions in the connected world.

Keywords: establishment, foundation, transactions

1. INTRODUCTION

The increasing significance of digital transformation lies in bridging the gap between the physical and cyber realms, introducing computer-based technologies for both individuals and organizations [1]. One noteworthy aspect is the rising popularity of Internet of Things (IoT)-enabled wireless sensor networks (WSNs), serving as cost-effective and cable-free solutions across diverse applications [2]. Particularly beneficial in environments where installing wires is impractical or too costly, such as oceans, volcanoes, forests, and battlefields, these networks consist of dispersed sensor nodes that monitor and record surrounding conditions [3]. The collected data is then transmitted to a centralized point. IoT-enabled WSNs are adept at monitoring various factors like temperature, sound, pollution levels, humidity, and wind [4]. Their widespread adoption spans across different industries, enhancing day-to-day activities such as real-time video streaming, mobile shopping, and healthcare monitoring. With the growing user base of IoT applications, it becomes imperative for gateways to efficiently manage the increasing volume of traffic [5].

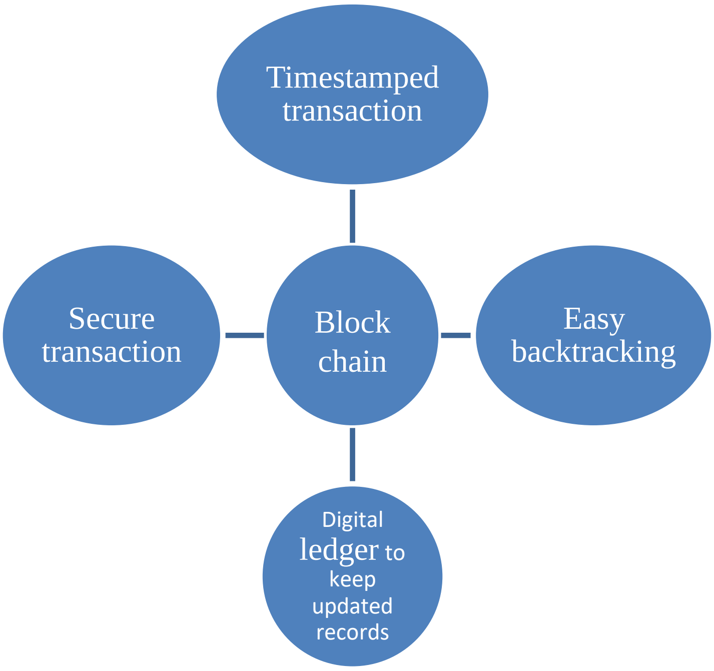

Figure 1. Secure transactions over IoT

IoT-enabled Wireless Sensor Networks (WSNs) constitute a crucial component of technological infrastructure, serving as a primary data source for associated applications [6] [7]. These networks involve user nodes, sensor nodes, and gateway nodes, each playing a pivotal role in the overall architecture. When users seek access to data, secure wireless connections are established among user nodes, sensor nodes, and gateway nodes to facilitate information sharing [8]. Due to resource limitations on sensor nodes, gateway nodes assume the role of intermediaries, offering enhanced processing and communication capabilities [9]. In contrast to traditional networks employing a single gateway, which can lead to bottleneck issues and hinder overall network performance, the adoption of multi-gateway architectures is on the rise [10]. This approach enhances the efficiency and effectiveness of data communication [11]. To ensure the robustness of the communication system, avoiding a single point of failure in the gateway is paramount, as any compromise could render the entire system ineffective [12]. With the emergence of the future 5G mobile network and its stringent standards for energy efficiency, the conventional single gateway design may fall short in meeting network demands, necessitating a transition to a multi-gateway environment [13].

In ongoing conversations, various security breaches such as eavesdropping, unauthorized message modification, replay attacks, and masquerading pose potential threats. To mitigate these risks, mutual authentication between communicating parties is imperative. Establishing a session key agreement between the user and gateway is crucial for maintaining message confidentiality [14]. To safeguard user privacy, it is essential to ensure that successive sessions remain unlinkable and anonymous. Given the susceptibility of IoT-enabled WSNs to diverse malicious attacks, implementing highly efficient security solutions becomes critical [15] [16]. Authentication stands as a crucial element in network security, serving as a means for organizations to safeguard their resources and shield sensitive data from unauthorized access or theft. The significance of authentication has amplified in recent times due to the surge in cyber-attacks and security breaches targeting organizations globally. While various authentication schemes have been proposed over the years, none are entirely impervious to security attacks. As malicious actors continually refine their tactics to circumvent security measures, the demand for more robust and secure authentication methods has grown. Evaluating the security of authentication methods involves employing several criteria. Formal security analysis, a mathematical scrutiny of authentication method security, is one such criterion [17]. Through a thoughtful consideration of the adversary model and system architecture, authentication schemes can be crafted to better withstand potential attacks, ensuring a secure communication environment. Various traditional methods were used such as new hybrid method based on Maritime Transportation System (MTS) [18] map-based user authentication system [19] wireless sensor network (WSN) [20] to resolve the problem, but no proper results were formed. So, a new deep learning method is implemented to improve the performance in this paper.

The key contribution of this paper is given in the following;

1. Initially, the security requirements for transaction records in the IoT network are defined.
2. A novel method Integrity Consensus Authorization Algorithm (ICAA) has been designed by integrating Proof-of-Integrity Consensus Algorithm and the Context-Aware Transaction Authorization Protocol to enhance the security of transaction records within the IoT network.
3. The integration ensures that transactions are validated by the network, promoting data integrity and preventing unauthorized modifications.
4. The testing and simulation of the system is done to identify vulnerabilities and weaknesses.

The following parts of this study are outlined as follows: Section 2 defines the most recent categories of literature; Section 3 explains the system description and problem statement; Section 4 deals with the workflow of the suggested methodology; Section 5 presents the achieved results and discussion; and Section 6 wraps up the research paper.

2. RELATED WORK

Some of the existing works of the securing transaction records over the IOT network is provided below:

Tyagi, A.K., [21] presented promising prospects to address the security challenges inherent in IoT and IIoT applications. This chapter provided an overview of the potential synergies between blockchain and AI within the realm of cybersecurity for IoT and IIoT. Moreover, the noteworthy features such as data integrity, transparency, and resistance to tampering made blockchain well-suited for safeguarding crucial data and transactions. Furthermore, blockchain facilitated secure device identity management, access control, and the establishment of secure communication channels among IoT and IIoT devices. One advantage of secure device identity management was its ability to enhance overall system security by providing a robust and reliable method. However, a disadvantage was the potential complexity and resource demands.

Lin, Q *et al.* [22] executed mutual user authentication through the utilization of the Elliptic curve Menezes–Qu–Vanstone-based message authentication code (ECMQV-MAC) protocol. This occurred within a secure data storage environment using the Deltoid curve-based Pallier cryptosystem (DC-PC), coupled with a key generation mechanism employing Dixon's method-based Blum–Goldwasser cryptosystem (DM-BGC). The protocol ensured legal authentication for users seeking access to the blockchain networking (BCN) while mitigating the need for extensive data storage within the blockchain (BC). Moreover, the key generation method enhanced data privacy resilience against both internal and external threats. Consequently, authorized users could securely upload healthcare data onto the blockchain, with data transfer secured using EKMC-SCP within the BCN. The advantage of this method is its efficient cryptographic operations. The specialized nature of elliptic curve cryptography might require specific hardware or software support.

Dhar, S, *et al.* [23] focused to strengthen the security of multimedia data, encompassing audio, video, and images sourced from IoT devices. Cutting-edge technologies, such as blockchain and quantum cryptography, were explored as promising avenues to enhance multimedia security and uphold privacy. Quantum Key Distribution (QKD) was presented as an alternative to classical encryption and key distribution methods, providing heightened data security. Concurrently, blockchain employed hash functions to bolster the overall security posture. The advantage of this method is its inherent security against certain cryptographic attacks. Factors such as the range limitations of quantum communication channels, the sensitivity of quantum states to environmental conditions, and the requirement for specialized quantum communication infrastructure could be the disadvantage.

Kiran, M, *et al.* [24] introduced the Ownership Transfer Protocol (OTP), which utilized Physically Unclonable Function (PUF) and blockchain technology to ensure the secure transfer of ownership for smart objects in the IoT. The proposed protocol securely tracked and traced smart objects during their movement in the IoT supply chain. In contrast to the traditional Ownership Transfer (OT) architecture, the proposed architecture eliminated the need for a Trusted Third Party (TTP) and supported Partial Ownership Transfer (POT). The innovative use of an immutable blockchain architecture enabled the proposed protocol to effectively support distributed environments and authenticate both the device and involved parties. The advantage is its effective utilization of Physically Unclonable Function (PUF) and blockchain technology to secure the transfer of ownership for smart objects. A disadvantage might have been its potential complexity in implementation and the need for widespread adoption across IoT devices and platforms.

Patil, S.D., *et al.* [25] introduced the challenges associated with electronic health record monitoring and administrations were alleviated through enhancements. Blockchain technology offered a significant advantage in healthcare data management, improving access to monitoring medications, hospital assets, drug systems, patient information, and more. Given the critical need for access to a patient's medical history in dispensing medication, blockchain technology held substantial promise for advancing the healthcare delivery system. Consequently, establishing a secure foundation for medical records based on blockchain technology became of utmost importance. The use of cryptographic techniques and consensus mechanisms contributed to enhanced trust and integrity in various applications, including finance, supply chain, and healthcare. The decentralized nature of blockchain networks and the consensus mechanisms, such as Proof-of-Work, could result in slower transaction processing times and higher resource requirements.

Arazzi, M,,*et al.* [26] initiated investigations into novel mechanisms, wherein a super node (a gateway, hub, or router) analyzed the interactions of the target node with other peers in the network to detect potential anomalies. The most recent strategies involved analyzing the node's behavior fingerprint in an IoT; however, existing solutions failed to address the fully distributed nature of the scenario. This paper contributed to this field by introducing a novel and fully distributed trust model that utilized point-to-point devices' behavioral fingerprints, a distributed consensus mechanism, and Blockchain technology. The advantage is the ability to provide fault tolerance and ensure agreement among nodes in a decentralized network. Moreover, the disadvantage was the potential for increased latency and complexity. The challenges of the existing work are shown in the Table 1.

Table 1. Challenges in the existing work

SI.No	Author name	Methods	Advantages	Disadvantages
1	Tyagi, A.K.,	AI	The ability to enhance overall system security by providing a robust and reliable method.	a disadvantage was the potential complexity and resource demands.
2	Lin, Q *et al.*	Elliptic curve Menezes–Qu–Vanstone-based message authentication code (ECMQV-MAC) protocol	The advantage of this method is its efficient cryptographic operations.	The specialized nature of elliptic curve cryptography might require specific hardware or software support.
3	Dhar, S, *et al.*	Quantum Key Distribution (QKD)	The advantage of this method is its inherent security against certain cryptographic attacks.	The sensitivity of quantum states to environmental conditions, and the requirement for specialized quantum communication infrastructure could be the disadvantage.
4	Kiran, M, *et al.*	Ownership Transfer Protocol (OTP)	The effective utilization of Physically Unclonable Function (PUF) and blockchain technology to secure the transfer of ownership for smart objects.	A disadvantage might have been its potential complexity in implementation.
5	Patil, S.D., *et al.*	cryptography	The use of cryptographic techniques and consensus mechanisms.	The decentralized nature of blockchain networks could result in slower transaction processing times and higher resource requirements.
6	Arazzi, M,,*et al.*	novel mechanism	The ability to provide fault tolerance and ensure agreement among nodes in a decentralized network.	The disadvantage was the potential for increased latency and complexity.

3. SYSTEM MODEL AND PROBLEM STATEMENT

The system comprises a network of interconnected IoT devices, each possessing a unique and secure identity. Transactions generated by these devices are securely recorded on a decentralized distributed ledger, employing blockchain technology. This ledger leverages the Proof-of-Integrity Consensus Algorithm to ensure the validation and immutability of transactions, while the integration of the Context-Aware Transaction Authorization Protocol enhances the system's security by considering contextual information during the transaction approval process. Cryptographic techniques, including encryption and hashing, further secure the transmission and storage of transaction records. Smart contracts, programmed to execute predefined rules, automate transaction processes and contribute to the overall efficiency of the system. The model aims to establish a tamper-resistant, transparent, and decentralized infrastructure for managing transaction records, addressing the unique challenges posed by the IoT environment.

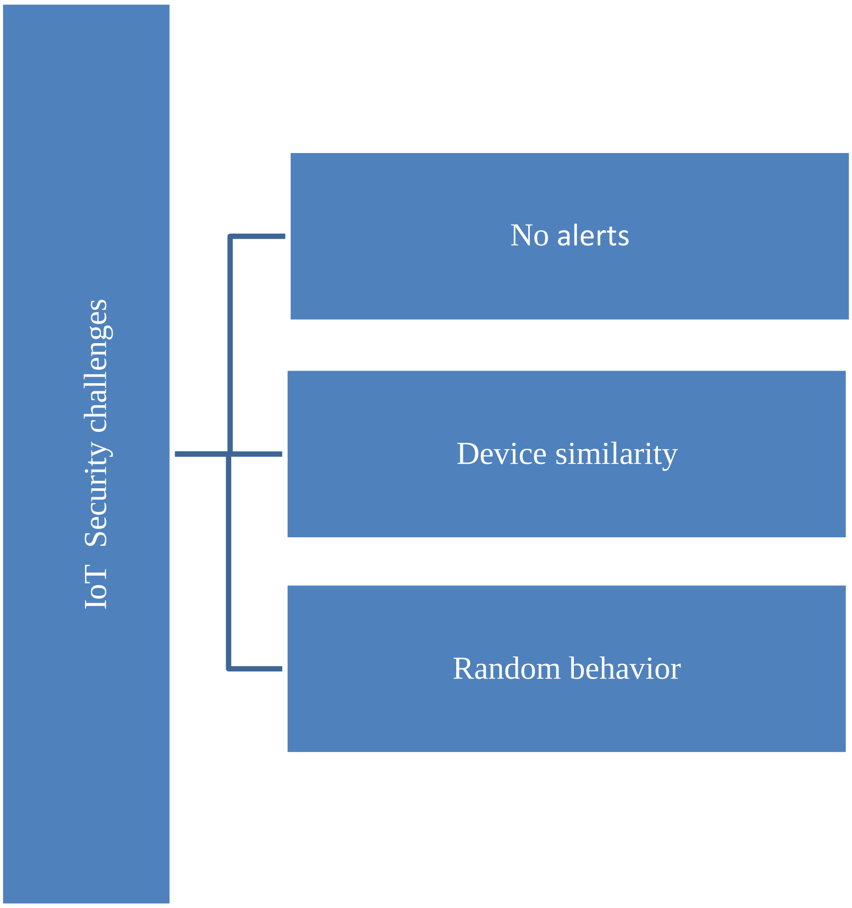

Figure 2. Challenges in the IoT security

The problem addressed by this system model lies in the vulnerability of transaction records within the IoT network to security threats, tampering, and unauthorized access. Traditional centralized approaches may present single points of failure, compromising the integrity of transaction data. Furthermore, the dynamic and interconnected nature of the IoT landscape introduces complexities in ensuring secure and contextually relevant transaction authorization. The proposed system model seeks to address these challenges by integrating decentralized distributed ledger technology, cryptographic mechanisms, and advanced consensus algorithms, providing a comprehensive solution for securing transaction records in the IoT network. The goal is to establish a secure, transparent, and adaptable framework that safeguards the integrity of transactions and ensures the trustworthiness of the overall IoT network.

4. PROPOSED METHODOLOGY

The proposed methodology for securing transaction records over the IoT network through the integration of the Proof-of-Integrity Consensus Algorithm and the Context-Aware Transaction Authorization Protocol involves a systematic and multifaceted approach. Initially, the system architecture will be meticulously designed to accommodate the specific requirements of the IoT environment, ensuring seamless integration of the selected consensus algorithm and authorization protocol. Smart contracts, embodying the predefined rules and conditions for transaction execution, will be developed and deployed onto a decentralized distributed ledger, leveraging blockchain technology. The Proof-of-Integrity Consensus Algorithm will be intricately woven into the fabric of the decentralized ledger to validate and authenticate transactions, promoting an immutable and tamper-resistant transaction history. Simultaneously, the Context-Aware Transaction Authorization Protocol will be seamlessly integrated to enhance the security framework. This protocol will consider contextual information, such as device identity and transaction specifics, during the authorization process, providing a nuanced and adaptive approach to secure transaction approval within the dynamic IoT ecosystem. The architecture of the proposed ICAA is shown in the figure 3.

Subsequently, the secure device identity management system will be implemented, employing cryptographic techniques to uniquely identify and authenticate IoT devices participating in transactions. Encryption and hashing mechanisms will be applied to fortify the transmission and storage of transaction records, ensuring end-to-end security. The methodology will prioritize adaptive security measures, allowing the system to dynamically adjust its parameters based on contextual changes in the IoT environment. Rigorous testing and validation procedures will be conducted, including simulated attacks and scenario-based testing, to identify and address potential vulnerabilities. Continuous monitoring mechanisms will be established to detect and respond to security threats in real-time, and a comprehensive documentation and training program will be developed to ensure the effective implementation and understanding of the secure transaction management processes by administrators, users, and relevant stakeholders. This two-pronged integration approach aims to provide a holistic and resilient security solution tailored to the specific challenges posed by securing transaction records over the IoT network.

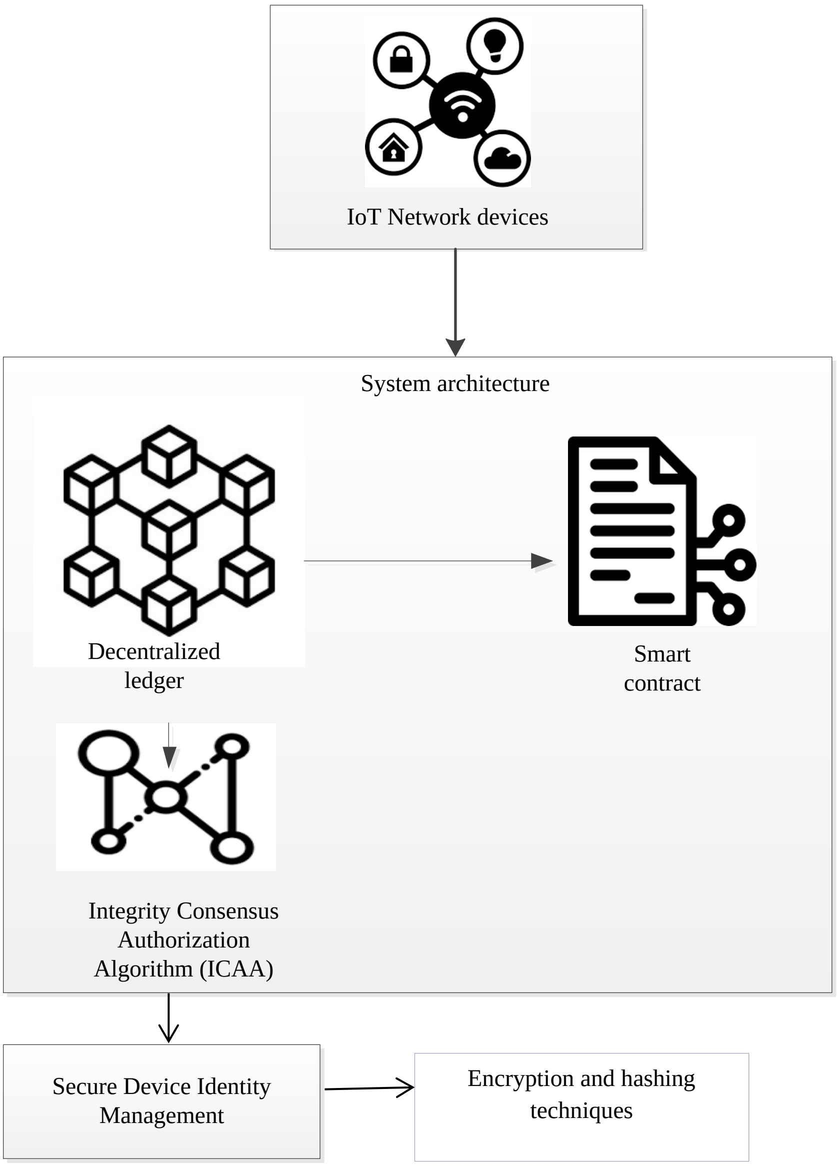
IoT Network devices
System architecture
Decentralized ledger
Smart contract
Integrity Consensus Authorization Algorithm (ICAA)
Secure Device Identity Management
Encryption and hashing techniques

Figure 3. Block diagram for the proposed ICAA

4.1 Process of the ICCA model

The ICCA is employed for achieving agreement, where the block with the shortest allocated time emerges as the winner. Time is assigned to all validator nodes within the block, and the one with the briefest wait time becomes the block leader. The client initiates a request, disseminated to all validator nodes, leading to a consensus among the nodes. Once consensus is reached, the block is committed, and the response is transmitted to the client. This paper explores the latency of the proposed system, assessed through the Blockchain's transaction completion capability. In ICCA, the system model outlines two pivotal steps: block generation and consensus achievement. The suggested methodology employs Consensus Authorization algorithm to facilitate key distribution and the exchange of digital signatures, thereby enhancing security and trust. Additionally, the incorporation of ring signatures fosters trust among users.

$$x^2 \bmod p = (y^3 + by + a) \bmod p \tag{1}$$

The first group of the blockchain was given a specific size as it included the initial blocks until block (y, x). The second group began from block number (Q) and ended at the last transaction block ($v_j + w_j$). The value of T that achieves the best performance will be selected. The first group of the chain used the Consensus Authorization algorithm. When a new block was added to the chain during the experiment, then block number 1 was removed from the second group and added to the first group. Throughout the test, this process was performed during the transactions; the blocks were removed from the second group and added to the first group.

$$H_p = (y, x); b, a, y, x \quad \text{belong to } G_p \tag{2}$$

$$l_Q = Q + Q + ...+ Q \ (l \text{ belong to } Y_p) \tag{3}$$

$$T = \{(v_j + w_j) * H \text{ , if } j \tag{4}$$

ICAA algorithm has been used in the second group of the chain. At the end of the test, groups one and two of the chain were combined and a final hash value was used to validate the transaction. The main purpose of dividing the original blockchain into two groups was to increase the network's efficiency by accelerating the validation execution time required to find the total hash of the blockchain and detect any partial changes. Through this practice, the process of hashing the transactions was performed with high efficiency and speed, allowing the tests to be conducted accurately. L is the time of finalizing the transaction, S_j is the time of transaction initialization, i is blocked generation time, and M is time to achieve consensus. Consensus latency d_j can be measured and given in the following equations

$$L = (v_j H + w_j + u_j) * qij \tag{4}$$

$$S_j = \sum (v_j + u_j) * IP(Q * l_j) \tag{5}$$

$$S_j = \sum v_j * IP(q * l_j) + (v_j + w_j) * j_t \tag{6}$$

$$i = I2(N \,||\, S) \tag{7}$$

$$j = \sum I1\,(i, M1, ...M_n, S1, ...S_n) \sum t \tag{8}$$

$$j = 1E_{ju} = \sum (v_j + w_j) d_j * t_{lj} \tag{9}$$

In the first scenario, the transactions' values were hashed while the chain of transactions was concatenated to form the concatenated hash transactions (CHT). Through this method, the final transaction value was obtained. In the second scenario, the Merkle hash tree (MHT) algorithm was used for hashing the transaction values. MHT is also referred as a hash tree because it is used in data verification and synchronization. Therefore, it is one of the most used methods for hashing the data. MHT has a tree-like structure in which all the nodes are of the same depth and as far left as possible. The input of the tree is mapped onto the fixed output, which is known as a hash. Thus, through this mechanism, ICAA can hash large and complex data with high efficiency. ICAA has also been used by previous researchers to enhance the authentication procedure of the blockchain network. ICAA can be represented mathematically for n blocks as follows:

$$H-n = Hash\,(H-1)(H2-3)(H4-5)....(HK-n) \tag{10}$$

Next, we attempt to modify the sequence of the values of the ICAA algorithm to add complexity to the traditional ICAA algorithm by considering the odd and even value sequences together.

$$D_j = I1(i, Z_1, Z_2, ...Z_s, ...Z_n, ...\beta_1, \beta_2, ...\beta_s, ...\beta_n) \tag{11}$$

$$D_j = I1(i, M_1, M_2, ...M_s, ...M_n, ...S_1, S_2, ...S_s, ...S_n) \tag{12}$$

$$D_V = \sum_U^M D_j \tag{13}$$

4.2 Fitness Function

The fitness function serves as a quantitative measure to guide the optimization process, helping to fine-tune system parameters, algorithms, and protocols to achieve the desired balance between security, accuracy, and efficiency in securing transaction records over the IoT network.

$$F = w_1 * Security\,metric + w_2 * Authorization\ accuracy - w_3 * latency \tag{14}$$

$Security\,metric$ represents the security level of the system, including factors such as transaction integrity, resistance to tampering, and robustness against attacks. $Authorization\ accuracy$ indicates the accuracy of transaction authorization decisions made by the CTAP, reflecting the system's ability to correctly identify and approve legitimate transactions. $latency$ denotes the time taken for transactions to be processed and confirmed within the system, including consensus and authorization delays. $w_1, w_2, and\ w_3$ are weights assigned to each component of the fitness function, reflecting their relative importance.The goal of the fitness function is to maximize F, thereby optimizing the system's performance. Adjusting the weights allows for customization based on specific requirements and priorities. For example, if minimizing latency is paramount, a higher weight may be assigned to w_3 , while ensuring security may involve increasing. Table 2 provides the algorithm of securing transaction records over IoT network.The pseudocode defines three main classes: Block, Transaction, and Blockchain. The Block class represents individual blocks in the blockchain, with attributes such as index, timestamp, transactions, proof, previous hash, and hash. The Transaction class encapsulates the details of a transaction, including sender, recipient, amount, and timestamp. The Blockchain class manages the overall blockchain structure, with methods for initializing the blockchain, implementing the Proof-of-Integrity Consensus Algorithm to validate transaction integrity, adding blocks and transactions, mining new blocks, and executing the Context-Aware Transaction Authorization Protocol for dynamic authorization based on contextual information from IoT devices. The pseudocode provides a modular and clear framework for understanding the integration of security measures into the IoT transaction process, ensuring the robustness and reliability of the distributed ledger system. The example usage at the end illustrates the sequential execution of these operations, showcasing how transactions are added, blocks are mined, and the blockchain is progressively built and secured. The flowchart representation is provided in figure 4. When a transaction is initiated within the IoT network, the relevant information, including transaction details and involved parties, is prepared for processing.The transaction data is submitted to the PICA consensus mechanism for verification and confirmation. Once a consensus is reached among the nodes, the transaction is confirmed as valid.

Table 2. Algorithm for ICAA method

```
Algorithm for ICAA method
Input: empty blockchain
 # Define blockchain structure
            The specific structure of the blockchain is given in the equation 1
                        $x^2 \bmod p = (y^3 + by + a) \bmod p$                    (1)
  {
     # Initialize an empty blockchain
         # Initialize a list to hold pending transactions
                        $L = (v_j H + w_j + u_j) * qij$                    (4)
     }
              Consensus latency $d_j$ can be measured by equation (9)
                        $j = 1E_{ju} = \sum (v_j + w_j) d_j * t_{lj}$                    (9)

                  # Validate the integrity of transactions
                        Hashing is derived by using the equation (10)
                  $H - n = Hash\,(H-1)(H2-3)(H4-5)....(HK-n)$                    (10)
             Fitness function is calculated by using equation (14)
               $F = w_1 * Security\,metric + w_2 * Authorization\,accuracy - w_3 * latency$    (14)
                 # new block with Proof-of-Integrity and Context-Aware Authorization
                     # Repeat the process
            End
     Stop
Output: Secure transaction
```

The decentralized nature of the PICA consensus mechanism ensures that the integrity of the transaction is maintained even if some nodes are compromised. Simultaneously, the transaction details are passed to the CTAP component for contextual analysis. CTAP considers contextual information such as device identity, location, historical behavior, and other relevant parameters. Based on the contextual analysis, CTAP determines the appropriate access permissions for the transaction. CTAP dynamically adjusts authorization levels based on the context of the transaction and the associated devices. Access permissions are granted or denied in real-time, ensuring that only authorized entities can interact with the transaction records. Once both PICA and CTAP processes are successfully completed, the transaction data is added to the decentralized distributed ledger. The ledger is updated across all participating nodes, reflecting the confirmed transaction and maintaining a consistent and secure record of all transactions within the network. The system continuously monitors for any changes in the network or context that may impact the security of transactions. PICA and CTAP work collaboratively to adapt to evolving conditions, ensuring ongoing security and integrity.The transaction process is initiated and the IoT device requests a transaction record. ICAA algorithm is applied to generate a hash for the transaction, ensuring proof of integrity.The generated hash is broadcasted to the decentralized ledger for validation. The decentralized network verifies the transaction through the Proof-of-Integrity Consensus Algorithm. The transaction undergoes approval based on the Context-Aware Transaction Authorization Protocol, considering contextual information. Simultaneously, the transaction details are sent to the CTAP component. CTAP performs a contextual analysis, considering factors such as device identity, location, and historical behavior. If approved, the transaction details are recorded on the decentralized distributed ledger. Confirm that the transaction has been securely recorded and then the transaction process is completed. The integration of PICA and CTAP ensures a comprehensive approach, combining consensus verification for data integrity and context-aware authorization for enhanced access control. The continuous monitoring at the end emphasizes the adaptive nature of the system, capable of responding to changes in real-time to maintain a secure environment for IoT transactions. The system continuously monitors for any changes in the network or context that might impact security. PICA and CTAP collaboratively adapt to evolving conditions to maintain ongoing security and integrity.

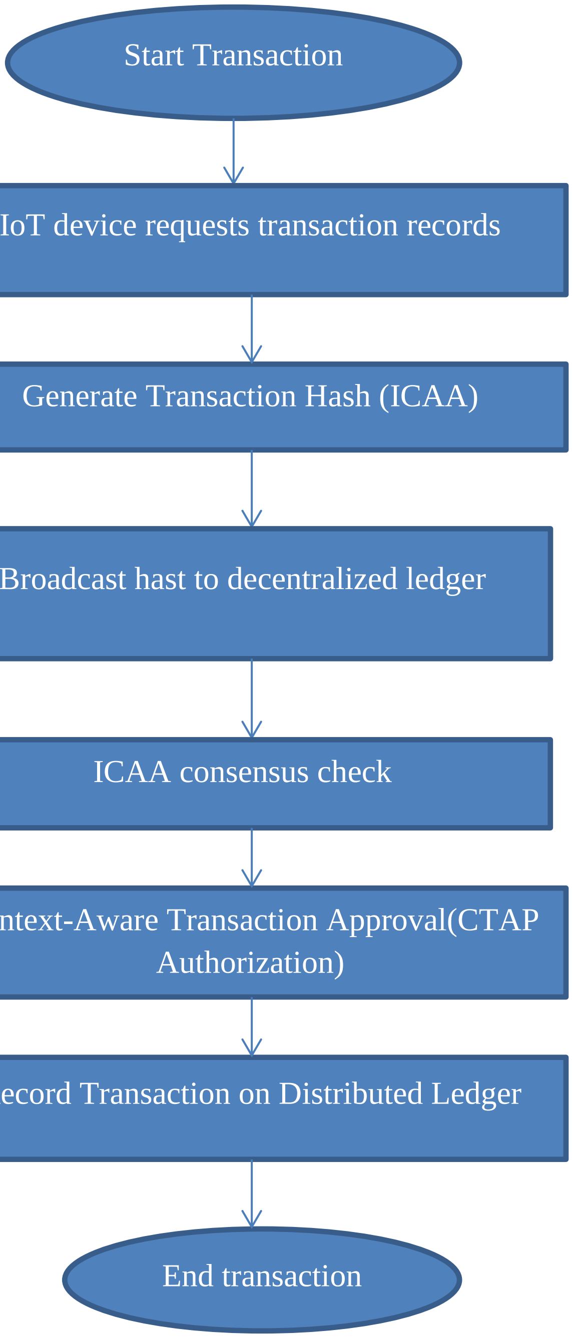
Start Transaction
IoT device requests transaction records
Generate Transaction Hash (ICAA)
Broadcast hast to decentralized ledger
ICAA consensus check
Context-Aware Transaction Approval(CTAP Authorization)
Record Transaction on Distributed Ledger
End transaction

Figure 4. Flowchart representation of the proposed ICAA

5. RESULTS AND DISCUSSION

This section discusses the outcome of the suggested ICAA method. This section provides a comprehensive overview of the conducted simulation and its outcomes. Each result is thoroughly discussed, with a particular focus on comparing the proposed model with a benchmark model to assess its performance. The model efficiently manages required retrievals by utilizing the B+-Tree indexing data structure. Notably, in comparison to existing solutions like SHealth, MedRec, and ECC-Smart, the proposed framework exhibits minimal communication overhead.

5.1 Simulation model

The simulation results, featured in this section, were performed using the Hyperledger Fabric blockchain tool and validated on the Ethereum test net. The dataset used is publicly accessible from UNSW. Additionally, a comparative analysis is presented, focusing on the number of transaction counts and the number of nodes.

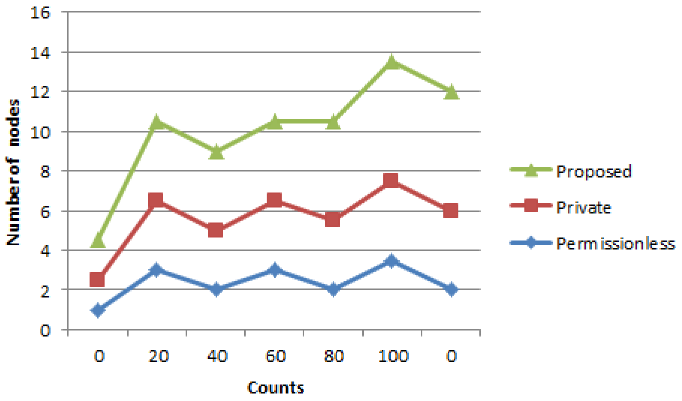

Figure 5. Simulation results based on nodes and counts

The simulation results would need to be conducted in a controlled environment and might vary based on the specific parameters and scenarios defined for the simulation. Actual implementation and real-world testing would provide the most accurate and reliable insights into the performance and security of the integrated PICA and CTAP system. The simulations might involve testing the system's scalability by increasing the number of nodes or transaction volume to evaluate how well the integrated solution handles growing demands. Then, the comparative simulations could be conducted against traditional centralized systems to showcase the advantages of the decentralized approach in terms of security, resilience, and transparency.

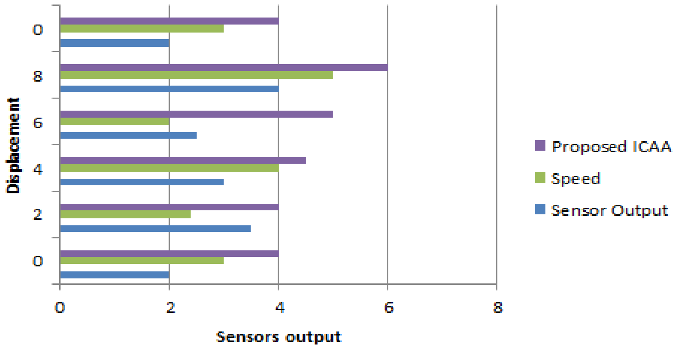

Figure 6. Simulation results based on the number of sensor output nodes

5.2 Comparison of the proposed ICAA with the existing works

The analysis of the accuracy of the proposed ICAA is shown in the Figure 7. The accuracy of the proposed HGGC are 0.95, 0.9654, 0.9522, and 0.9489, which is higher than all the other existing methods.

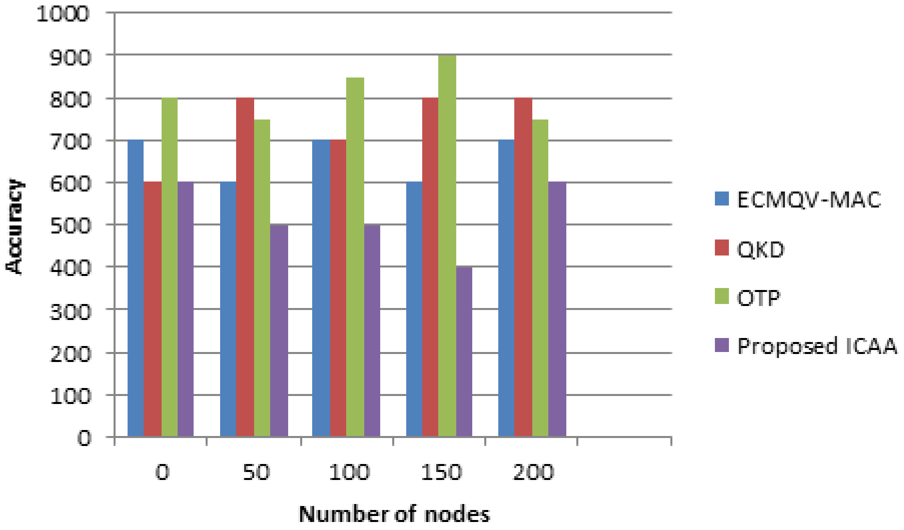

Figure 7. Comparative analysis of the proposed framework vs benchmark model

The contrast between the proposed ICAA and the current techniques in terms of accuracy is given in the Figure 8. In the nodes 50, the proposed ICAA performs 4.83%, 0.48% and 0.1578% better than the ECMQV-MAC, QKD, and OTP. The proposed ICAA is 6.65% better than the ECMQV-MAC, 2.123% better than QKD, and 1.792% better than OTP in the nodes 100. Moreover, for the nodes 150, the performance of the proposed ECMQV-MAC, QKD, OTP and proposed ICAA are 0.9612, 0.9449, 0.9481, and 0.9522. The proposed HGGC is 5.026% better than the ECMQV-MAC, 0.4215% better than QKD, and 0.0843% better than OTP in the nodes 200. Therefore, the proposed ICAA performs better than the other existing methods.

5.3 Comparison with the existing works based on latency

An average latency ranging from 0.4 ms to 0.7 ms on nodes 1, 2, and 4 when handling information or connection requests from other nodes was calculated. Conversely, node 3, utilizing a WiFi-based connection to access the network, experiences average latencies in the range of 13 ms to 50 ms when receiving messages from other nodes. Additionally, nodes 1, 2, and 4 encounter average network latencies ranging from 24 ms to 33 ms when receiving messages from node 3.

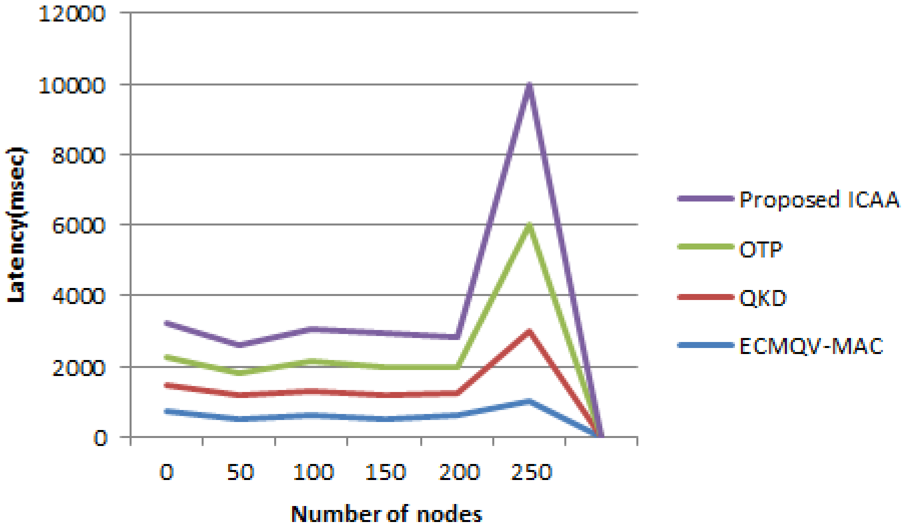

Figure 8. Comparative analysis based on latency

5.4 Effect of network latency

Figure 9 presents a comparison of network latencies when sending ping packets from each node to every other node (designated as Targets 1-3) in the network. Notably, ping queries over Ethernet-connected nodes exhibit significantly lower response times compared to those over WiFi-connected nodes. Furthermore, it is observed that the response time for pings from Node-3 (server) is comparatively lower than responses from resource-constrained nodes (Nodes-1 and 2), even when connected via the same Ethernet-based connection. The relatively higher latencies incurred by resource-constrained nodes (Nodes-1 and 2) are attributed to the time required for packet processing. Continuing, the considerably higher latencies at Node-4 can be ascribed to both its resource-constrained nature, necessitating more time for packet processing, and its mobility, leading to unstable network characteristics. These latencies play a crucial role in estimating the performance of our implemented IoT blockchain and serve as the baseline for network performance. In Proof of Work (PoW) blockchains, elevated network latencies can result in increased block convergence times and the risk of failure to achieve six confirmations. However, in this study, adopting a Proof of Authority (PoA) consensus mechanism, which is notably faster than PoW and PoS mechanisms, minimizes the impact of network latency on blockchain security. In PoA, only reputable validators can approve transactions on the blockchain, making it highly suitable for IoT-based scenarios.

5.5 Comparison of existing methods on encryption time

The encryption throughput is calculated by dividing the encrypted plain-text size (in bytes) by the encryption time (in ms). The proposed ICAA demonstrates one of the shortest encryption times, while ECMQV-MAC requires a comparatively longer computational time. The substantial difference in computational time between these two schemes arises from the size of their search spaces. Figure 9 illustrates the superiority of the proposed ICAA in terms of execution time and enhanced security over other encryption algorithms. Following AES, QKD is the preferred algorithm due to its lower time consumption. Both 3DES and RC2 typically exhibit similar encryption process times, whereas ECMQV-MAC stands out as the slowest. Consequently, the test results clearly indicate that the proposed ICAA is the fastest algorithm for both encryption and decryption processes. This suggests that the ICAA encryption algorithm is well-suited for ensuring IoT data security.

Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

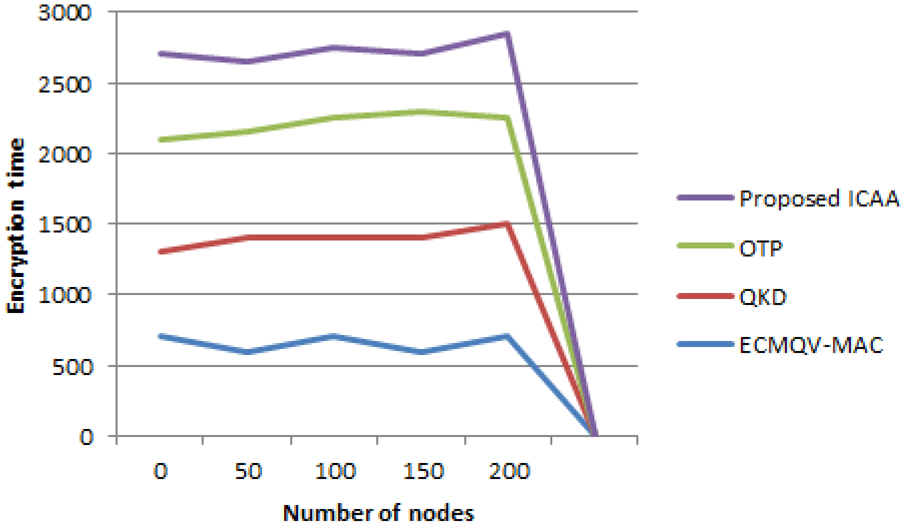

Figure 9. Comparative analysis based on encryption time

5.6 Discussion

The successful implementation of the proposed system heavily depends on the architecture of the blockchain system. Without a highly scalable blockchain infrastructure, deploying the IoT storage system becomes challenging due to the inherent trade-off associated with eliminating centralized servers. Scalability poses a significant challenge in the design of blockchain technology, with ongoing research efforts aimed at addressing this issue. Two extensively studied mechanisms to tackle scalability problems are Sharding and sidechains. Evaluating existing blockchain systems deployed in large networks is essential to identify the most scalable solution. While newer blockchain technologies like Ripple can handle thousands of transactions per second, they often feature partial decentralization. On the other hand, more established decentralized designs like Ethereum might only process thirteen transactions per second. However, emerging blockchain designs, such as those based on Ethereum like Tomochain, boast improved scalability, capable of processing up to one thousand transactions per second. If a blockchain mechanism capable of processing around 1000 transactions per second is adopted, the IoT storage system could handle approximately 10,000 transactions in roughly 10 seconds. A positive outlook is that as blockchain technology advances, it is anticipated that more designs suitable for the proposed IoT storage system will emerge.

6. CASE STUDY

The corporation integrated PICA and CTAP into their existing IoT infrastructure. PICA was implemented to ensure the integrity of transaction records through a consensus mechanism. CTAP was deployed to introduce context-aware transaction authorization for granular access control. A comprehensive testing phase was initiated to verify the functionality and effectiveness of PICA and CTAP. Various scenarios, including normal transactions and potential security threats, were simulated to assess the system's resilience. PICA played a crucial role in validating the integrity of transaction records. Consensus among the distributed nodes ensured that tampering attempts were quickly identified and rejected. CTAP's context-aware approach dynamically adjusted access permissions based on device identity, location, and historical behavior. Unauthorized access attempts were promptly detected and prevented by CTAP. Confirmed transactions were securely added to the decentralized ledger, ensuring a transparent and immutable record across all nodes. The integration of PICA and CTAP significantly enhanced the security of transaction records.

Instances of unauthorized access and tampering were effectively mitigated, contributing to a more resilient and trustworthy IoT ecosystem. The case study highlights the successful integration of PICA and CTAP as an effective security framework for securing transaction records over the IoT network. The implementation not only addressed existing security concerns but also positioned the corporation as a leader in deploying innovative solutions to safeguard IoT data integrity.

7. CONCLUSION

In conclusion, the integration of Decentralized Distributed Ledger Technology, specifically through the amalgamation of the Proof-of-Integrity Consensus Algorithm (PICA) and the Context-Aware Transaction Authorization Protocol (CTAP), stands as a robust and innovative solution for securing transaction records within the IoT network. The Proof-of-Integrity Consensus Algorithm, embodied in PICA, serves as a cornerstone in guaranteeing the integrity of transaction records. By providing a secure consensus mechanism, PICA enhances the trustworthiness of the distributed ledger, ensuring that transactions are validated and confirmed with a high level of reliability. Complementing this, the inclusion of the Context-Aware Transaction Authorization Protocol (CTAP) introduces an additional layer of security. CTAP's context-aware approach considers various factors surrounding each transaction, such as device identity, location, and historical behavior. This contextualization enables a more precise and adaptive authorization process, contributing to the overall resilience of the system against unauthorized access or malicious activities. The combined synergy of PICA and CTAP establishes a comprehensive security framework tailored to the specific challenges presented by the IoT environment. This integrated solution not only addresses the fundamental need for data integrity through PICA's consensus algorithm but also elevates the level of access control by incorporating context-aware authorization via CTAP. As a result, the proposed approach provides a trustworthy, decentralized ledger system capable of meeting the stringent security requirements of IoT transactions. By securing transaction records over the IoT network, the integration of PICA and CTAP paves the way for enhanced data integrity, privacy, and resilience against potential threats, thereby contributing to the advancement and sustainability of secure IoT ecosystems.

REFERENCES

[1] Gill SS, Xu M, Ottaviani C, et al. AI for next generation computing: emerging trends and future directions. Internet Things. 2022;

[2] Siddiqui F, Beley J, Zeadally S, Brought G. Secure and lightweight communication in heterogeneous IoT environments. Internet Things. 2021;

[3] Lee W-K, Schubert MJW, Ooi B-Y, Ho SJ-Q. Multi-source energy harvesting and storage for floating wireless sensor network nodes with long range communication capability. IEEE Trans Ind Appl. 2018

[4] Gupta A, Tripathi M, Muhuri S, Singal G, Kumar N. A secure and lightweight anonymous mutual authentication scheme for wearable devices in medical internet of things. J Inf Secur Appl. 2022;

[5] Panda S, Mondal S, Kumar N. SLAP: a secure and lightweight authentication protocol for machine-to-machine communication in industry 4.0. Comput Electr Eng. 2022;

[6] Chaudhry SA, Irshad A, Yahya K, Kumar N, Alazab M, Zikria YB. Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IoT environment. ACM Trans Internet Technol (TOIT). 2021;21(3):1-19.

[7] Singh D, Kumar B, Singh S, Chand S. SMAC-AS: MAC based secure authentication scheme for wireless sensor network. Wirel Pers Commun. 2019;107(2):1289-1308.

[8] Banerjee S, Chunka C, Sen S, Goswami RS. An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards. Wirel Pers Commun. 2019;107(1):243-270.

[9] . Xie Q, Li K, Tan X, Han L, Tang W, Hu B. A secure and privacy-preserving authentication protocol for wireless sensor networks in smart city. Eurasip J Wirel Commun Netw. 2021;1:2021.

[10] Singh D, Kumar B, Singh S, Chand S. Evaluating authentication schemes for real-time data in wireless sensor network. Wirel Pers Commun. 2020;114(1):629-655.

[11] Singh D, Kumar B, Singh S, Chand S. A secure IoT-based mutual authentication for healthcare applications in wireless sensor networks using ECC. Int J Healthc Inf Syst Inform. 2021;16(2):21-48.

[12] Khalid H, Hashim SJ, Ahmad SMS, Hashim F, Chaudhary MA. Cross-sn: a lightweight authentication scheme for a multi-server platform using IoT-based wireless medical sensor network. Electron. 2021;10(7):790.

[13] Singh D, Kumar B, Singh S, Chand S, Singh PK. RCBE-AS: Rabin cryptosystem–based efficient authentication scheme for wireless sensor networks. Pers Ubiquitous Comput. 2021.

[14] . Shuai M, Yu N, Wang H, Xiong L, Li Y. A lightweight three-factor anonymous authentication scheme with privacy protection for personalized healthcare applications. 33(3):1-18. 22.

[15] Dahia G, Jesus L, Pamplona Segundo M. Continuous authentication using biometrics: an advanced review. Wiley Interdiscip Rev Data Min Knowl Discov. 2020;10(4):

[16] Mansour MM, Salem FM, Saad EM. A secure mutual authentication scheme with perfect forward-secrecy for wireless sensor networks. Adv Intell Syst Comput. 2019;

[17] . Sirisha Uppuluri GL. Secure user authentication and key agreement scheme for IoT device access control based smart home communications. Wirel Netw. 2023;29(3):1333-1354.

[18] Mahmood K, Ferzund J, Saleem MA, Shamshad S, Das AK, Park Y. A provably secure mobile user authentication scheme for big data collection in IoT-enabled maritime intelligent transportation system. IEEE Trans Intell Transp Syst. 2023;24(2):2411-2421.

[19] Mishra KC, Dutta S. A simple and secure user authentication scheme using map street view with usability analysis based on ISO/IEC 25022. Int J Inf Sec. 2023;22(2):403-415.

[20] Wu F, Li X, Xu L, Vijayakumar P, Kumar N. A novel three-factor authentication protocol for wireless sensor networks with IoT notion. IEEE Syst J. 2021;15(1):1120-1129.

[21] Tyagi, A.K., 2024. Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications. In *AI and Blockchain Applications in Industrial Robotics* (pp. 171-199). IGI Global.

[22] Lin, Q., Li, X., Cai, K., Prakash, M. and Paulraj, D., 2024. Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking. *Information Sciences*, *654*, p.119783.

[23] Dhar, S., Khare, A., Dwivedi, A.D. and Singh, R., 2024. Securing IoT devices: A novel approach using blockchain and quantum cryptography. *Internet of Things*, *25*, p.101019.

[24] Kiran, M., Ray, B., Hassan, J., Kashyap, A. and Chandrappa, V.Y., 2024. Blockchain based secure Ownership Transfer Protocol for smart objects in the Internet of Things. *Internet of Things*, *25*, p.101002.

[25] Patil, S.D., Kathole, A.B., Kumbhare, S. and Vhatkar, K., 2024. A Blockchain-Based Approach to Ensuring the Security of Electronic Data. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(11s), pp.649-655.

[26] Arazzi, M., Nicolazzo, S. and Nocera, A., 2024. A novel IoT trust model leveraging fully distributed behavioral fingerprinting and secure delegation. *Pervasive and Mobile Computing*, p.101889.