

SECURE USER AUTHENTICATION AND KEY AGREEMENT IN SMART NETWORKS WITH BLOCKCHAIN GATEWAYS

DURVASI GUDIVADA¹, M. KAMESWARA RAO²

¹Research Scholar, Koneru Lakshmaiah Educational Foundation, Department of Computer Science and Engineering, Guntur, India

²Professor, Koneru Lakshmaiah Educational Foundation, Department of Electronics and Communication Engineering, Guntur, India

E-mail: ¹kiran.durvasi@gmail.com, ²dr.ramakoteswarao@gmail.com

ABSTRACT

As IoT-driven smart environments such as intelligent cities, buildings, and industries develop quickly, user authentication is becoming increasingly important to guard against illegal access and guarantee data security. Because of issues such as device heterogeneity, computing resource limitations, and potential single points of failure, conventional and current authentication methods frequently fail to overcome security issues such as impersonation, replaying, and denial-of-service attacks in IoT networks. With the goal of offering lightweight, secure, and decentralized user authentication and key agreement in smart settings, this study suggests a blockchain-based user authentication and secure key agreement protocol for smart networks. In this case, gateway nodes are permitted to create a blockchain to authenticate users and IoT nodes by integrating cryptographic hash algorithms. The AVISPA tool is used to formally verify a protocol's security. The comparison analysis reveals that our protocol has an execution time of 0.0858 ms, confirming its performance against more recent research efforts.

Keywords: *IoT, User Authentication, Smart Contract, AVISPA*

1. INTRODUCTION

Smart environments, which combine many of networked devices to form automated and responsive systems, have rapidly developed as a result of the Internet of Things [1]. By continuously gathering and analysing vast amounts of data, smart networks seek to increase convenience, security, and efficiency [2]. [3] predicts that by 2025, 30.9 billion IoT devices will be connected globally. However, privacy and security are becoming increasingly vulnerable, especially with respect to user authentication [4]. Poor processing and storage make conventional security measures difficult for IoT devices. This restriction, added to the vast diversity of devices, undermines user authentication and access control in smart environments [5].

User authentication plays a crucial role in ensuring that only legitimate user access IoT systems and devices [6]. Classical systems employ a centralized server to store and maintain user credentials for the authentication process, but this results in single points of failure, leaving devices open to identity theft, data breaches, and distributed

denial-of-service assaults [7]. It also poses difficulties in scaling and conflicts with the device's decentralized nature, where devices are scattered and often disconnected from the network. This emphasizes the necessity of efficient, reliable, secure, decentralized authentication systems that protect user identities without compromising them. Furthermore, many modern user authentication methods have been designed and developed by researchers on the basis of various kinds of cryptographic systems, such as symmetric, asymmetric, and cryptographic hashes, to overcome single points of failure but remain exposed to attacks such as denial-of-service, replay, impersonation, and man-in-the-middle (MITM) [8, 9]. Blockchain offers secure authentication, but limited research on lightweight protocols for smart networks. This study proposes an efficient blockchain-based solution for smart environments.

Blockchain, initially designed for cryptocurrencies, proposed a decentralized, unchangeable digital ledger to record and secure transactions without any central authority in the network. Its transparency, immutability, and

distributed consensus make it appropriate for robust authentication procedures [10]. It is possible to create a secure and scalable decentralized user authentication system for smart networks via blockchain technology for secure data exchange among nodes and users [11].

A blockchain-based user authentication protocol designed for IoT smart environments is proposed in this study. This work will be of particular interest to many researchers, developers, and practitioners in the fields of cybersecurity, IoT, and distributed systems. As traditional and modern methods struggle many security and privacy issues, blockchain offers a promising alternative. The main goals are to restrict unwanted access, secure user authentication, and provide key distributions among users and IoT nodes for the exchange of sensed data from smart ecosystems. For that, we have research questions: How blockchain integrated into smart environments for effective user authentication? What methods enable secure key agreement without central authority? Outcome of this study is the blockchain-based user authentication protocol that improves security, scalability, and robustness by removing the need for a central authority for user authentication through the decentralized nature of the blockchain.

2. RELATED WORKS

To prevent unwanted user access, many authentication techniques utilizing either blockchain or non-blockchain technologies have been presented and extensively used in IoT networks for years. A review of some schemes suggested within the literature will be provided in this section.

2.1 Blockchain in Authentication

To authenticate users and issue tokens to access data from IoT nodes without relying upon reliable third-parties, Almadhoun *et al.* [12] suggested a decentralized user authentication approach for IoT networks that uses blockchain-enabled fog nodes. The system functionality is verified in Remix IDE with entities such as end users, IoT devices, and fog or cloud nodes. Similarly, Khalid *et al.* [13] proposed a blockchain authentication protocol to enable secure communication between devices within and across IoT systems. In this, all fog nodes collectively form a blockchain network. The authors used the elliptic curve digital signature algorithm (ECDSA) to generate key pairs and digital signatures for the devices and fog nodes, which are then used for storage and authentication. The identity of the IoT

device is stored as a block in the nearest blockchain-enabled fog nodes. Later, they are distributed across all connected blockchain-enabled fog nodes. To access data from devices in other networks, devices need to provide credentials, which are authenticated via blockchain.

To address the security challenges posed by the vast number of IoT devices, Lua *et al.* [14] proposed an authentication model leveraging blockchain technology. In this, blockchain is used to securely join and store structured data and files by assigning a unique digital identity to each device. To enable secure communication between IoT devices, the cloud server, and the base station of IoT safe communication by the device, Tian *et al.* [15] proposed an IoT identity authentication framework. The authors adopted Ripple consensus algorithm to ensure the authenticity and reliability of new nodes, whereas the Public Key Infrastructure is used to distribute keys each communication entity securely.

To secure communication between miners and IoT devices within the IoT network, Hameed *et al.* [16] implemented a blockchain-based authentication scheme using token mechanism. The time for authentication of the IoT device is less than 1.5s. To continue operating effectively even when certain components of blockchain malfunction, Zhaofeng *et al.* [17] proposed BlockAuth, a password-based verification scheme that leverages blockchain to establish a secure, decentralized, and fault-tolerant identification system for edge-based IoT environments.

To enable secure communication between IoT devices and external systems, Hwaitat *et al.* [18] proposed a novel authentication method that employs a permission-based blockchain to maintain and validate device identification data in a distributed manner. The authors also included homomorphic encryption to encrypt data at the user's end before uploading it to the cloud.

Lee *et al.* [19] proposed a data access control and key agreement scheme for IoT, using ciphertext-policy attribute-based encryption (CP-ABE) and blockchain. It ensures data integrity, supports data auditing, and allows only authorized users to decrypt data, providing nonrepudiation, accountability, and verification.

To avoid unnecessary calculations by vehicles, Son *et al.* [20] designed a handover authentication system based on blockchain for vehicular ad-hoc networks (VANETs) using hash and xor operations. The system identifies irregular behavior and reports revocation through blockchain to resist various attacks. For securing patient information in the healthcare domain against known

attacks, Idrissi *et al.* [21] proposed a dynamic and decentralized attribute-based access control (ABAC) authentication and authorization mechanism that integrates mobile agents and blockchain technology. The scheme employs elliptic curve cryptography (ECC) for mutual authentication and uses a challenge-response mechanism to securely exchange secret keys.

To ensure mutual authentication among remote users and IoT nodes Guo *et al.* [22] proposed blockchain-based secure remote authentication (BSRA), which uses a piggyback authentication process to prevent desynchronization attacks in fog computing environments and continue operation even if the fog node is compromised. To secure group communication within IoT systems, Singh *et al.* [23] and Alsaeed *et al.* [24] proposed blockchain-based authentication protocol. Singh *et al.* [23] integrated blockchain, ECC, and bilinear pairing to create a lightweight, secure and efficient key agreement protocol, which was tested with the NS-3 tool. For the internet of Medical Things (IoMT), Alsaeed *et al.* [24] designed a method that combines Shamir's Secret Sharing (SSC) and ECC with blockchain to increase security and efficiency.

To balance security and performance, Yang *et al.* [25] proposed a blockchain-based authentication scheme for fog-cloud smart homes, which uses only xor and hash functions. In this case, federated chain smart contracts are used to ensure that access is granted only to authorized nodes.

2.2 Non-Blockchain in Authentication

To enable automated access control and authenticate users and devices mutually in a smart home, Alshaharni *et al.* [26] proposed a scheme based on cumulative keyed-hash chains and temporary identities. It uses challenge and response mechanisms to enforce security policies and fog computing principles among nodes to enhance identity verification. In the same way, Fakroon *et al.* [27] proposed a secure, anonymous, and remote user authentication system to overcome clock synchronization and table verification in the authentication process.

Using xor and hash operations, Lee *et al.* [28] proposed a scheme to address vulnerabilities, such as impersonation attacks, stolen device attacks and compromised user private keys, identified in [29] for the IoT. The system was verified by the ProVerif tool to ensure security, user anonymity, and robustness against various security threats. Chang *et al.* [30] identified a total of five flaws in [28] and suggested an enhanced version using ECC. Later, Li *et al.* [31]

reported several shortcomings in system phases, including susceptibility to MITM and impersonation attacks on the scheme [28]. As a result, the authors further proposed an enhanced version with an execution time of 4.337 ms using only the xor and hash functions.

To enable secure mutual authentication via gateway among users and IoT devices, Rahnama *et al.* [32] proposed a lightweight and anonymous user identification protocol for IoT networks using hash and XOR functions. Kumar *et al.* [33] proposed a hybrid model combining ECC with the moth search algorithm (MSA) for session key generation and DNA computing technique for encryption and decryption to store and access data in a multi-tenant cloud environment. The system uses smaller keys to enhance data integrity and authentication in cloud storage while reducing attacks.

For device authentication, a situation-aware protocol was proposed by Xiang and Zheng [34] proposed a situation aware authentication scheme for smart grid-enabled home area networks (SG-HANs), using two levels of threat assessment, low and high, via a home automation network. Their scheme proved efficient for mutual authentication and strong against MITM, impersonation and replay attacks. Later, Oh *et al.* [35] identified issues in [34] and suggested a lightweight mutual authentication scheme that enhances security while reducing computational overhead in user to device communication.

To ensure anonymity, privacy and untraceability in IoT-based digital health networks, Masud *et al.* [36] designed a lightweight user verification technique with low computational and communication costs. Mohammed *et al.* [37] proposed an anonymous identification technique for 5G vehicular fog networks, where vehicles receive a temporary secret key to verify digital signatures. The ProfVerif tool revealed that the overall transmission cost is 108 bytes, and the time for a single signature is 2.0158 ms. To prevent patient privacy and provide faster, flexible, and more services, Faraj *et al.* [38] proposed an authentication and key agreement scheme for the Telecare Medical Information System (TMIS). Nyangaresi *et al.* [39] proposed a lightweight protocol using hash and XOR operations, ensuring secure session key, user anonymity, authentication, key secrecy, and resistance to various attacks, with improved communication and computation overheads of 31.56% and 33.33%, respectively. The table 1 gives the summary of related works in the literature.

Table 1: Summary of Related Works In The Literature

Scheme	Methodology/Platform	Advantages	Limitations/Drawbacks
Blockchain Authentication Schemes			
[12]	Ethereum Smart Contracts	- Resistant to eavesdropping, reply, and denial-of-service attacks	- Scalability increases system complexity and adds additional resources for execution and continuous maintenance
[13]	Ethereum Blockchain and tokens	- Lightweight - Resistant to various types of attacks	- Miners are not elected based on trust values to avoid more energy consumption
[14]	Public Blockchain	- Security enhanced	- Computational and storage cost are more to transfer data from devices to blockchain
[15]	Ripple consensus mechanism and PKI	- Prevent joining of malicious node	- Processing speed reduced due to authentication requests increases
[16]	Ethereum Blockchain	- Reduces communication, computational, and financial costs	- Managing identification of IoT devices by a single miner creates scalability issues - Lack of process to detect authenticated device that launches attacks
[17]	BlockAuth based on Hyperledger Fabric 1.4	- Avoids single-side risk	- Not addressed dynamic change in network - Fails to ensure efficiency of analysis and performance requirements
[18]	Blockchain with Homomorphic encryption	- Lightweight - Optimized storage	- Efficiency of the scheme with consensus is not evaluated
[19]	Ciphertext-policy and attribute-based policy with blockchain	- Secure against attacks	- Unable to provide secure services due to rising computational cost of bi-linear operations when either number of users or attributes increases
[21]	Blockchain Hyperledger Fabric 1.4 and ECC	- Low latency - Robust security	- Missing big data analytics and miner algorithm
[22]	Hash and Physically Unclonable Functions (PUF)	- Lightweight - Resistant against various attacks	- Communication costs are slightly high compared with few schemes
Non-Blockchain Authentication Schemes			
[26]	Cumulative Keyed-hash chains	- Lightweight - Minimal computational overhead	- Susceptible to replay and time synchronization attacks
[27]	Hash and xor operations	- Lightweight - Ensures user anonymity	- Suffers scalability and performance issues when more users and IoT devices are included
[28]	Xor and hash functions	- Proper session key agreement	- Registration and authentication phases are weak - Vulnerable to user impersonation and man-in-the-middle attacks
[32]	Xor and hash functions	- Low computational and communicational loads	- Registration and initial setup phases are unclear
[33]	MSA, DNA and ECC	- Optimized for key size, throughput, and encryption and decryption time.	- Not immune to DDoS attacks.
[34]	Xor, and hash functions	- Reduced computation and communication costs	- Susceptible to stolen device attack
[35]	Xor and hash functions	- Secure against various attacks	- Higher computational cost - Prone to DoS attack
[36]	Nonce, xor, and hash	- Mutual authentication	- Not included zero-knowledge proof and PUF
[38]	Hash and ECC	- Secure against various attacks	- Consumes more energy

Despite numerous advancements in user authentication protocols for the IoT and related applications, several limitations persist in the existing literature. Blockchain-based authentication schemes focus primarily on IoT device authentication and often neglect user-IoT interactions. While non-blockchain schemes address both, they frequently encounter security challenges and inefficiencies. Moreover, the analysis shows that many schemes face challenges in terms of security, strength, scalability, computational efficiency, communication overhead, storage efficiency, and integration with IoT systems. To address these gaps, we propose a blockchain-based user authentication and key agreement protocol that enables gateway nodes to form a blockchain and ensures secure data exchange between users and IoT nodes.

3. PROPOSED METHOD

This work proposes a secure lightweight mutual authentication protocol for IoT-based smart environments. It integrates blockchain technology with an IoT network to utilize unique features of blockchain. The proposed method aims to ensure secure data exchange and user anonymity.

3.1 System Architecture

Figure 1 illustrates the system architecture, which comprises five main components: users, IoT nodes, blockchain of gateways, blockchain, and smart contracts. Users and IoT nodes act as endpoints that register and interact with the system through nearby gateway nodes. The gateway nodes belong to different networks, forming the blockchain network, with each maintaining a copy of the blockchain ledger, and are responsible for

tasks such as user and IoT node registration, identity authentication, and key generation and distribution in blockchain consensus. The blockchain itself ensures a secure, immutable, and decentralized system that stores records of all identities along with secret keys and specific codes used for authentication. A block in the blockchain stores identities, secret keys and specific codes along with hashes of these values, the current time, and the previous block's hash. Smart contracts on top of gateway nodes automate and enforce the rules for user authentication and key distribution, enabling seamless and secure exchanges among users and IoT nodes.

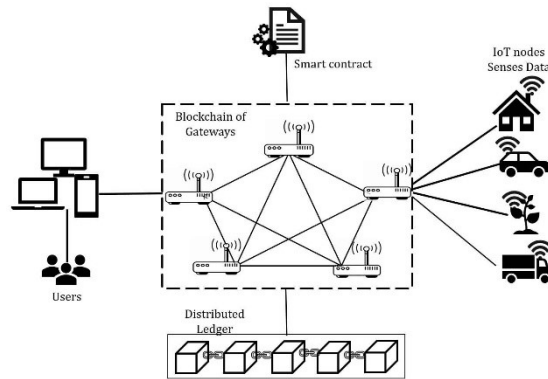


Figure 1: System Architecture Of Blockchain Over IoT

The proposed protocol uses hash functions, XOR and symmetric encryption for the implementation which includes system initialization, user registration, IoT node registration, authentication and key agreement and update password phases. The figure 2 describes about the overview of the proposed authentication protocol using blockchain of gateways. Table 2 provides descriptions of the symbols in the proposed scheme.

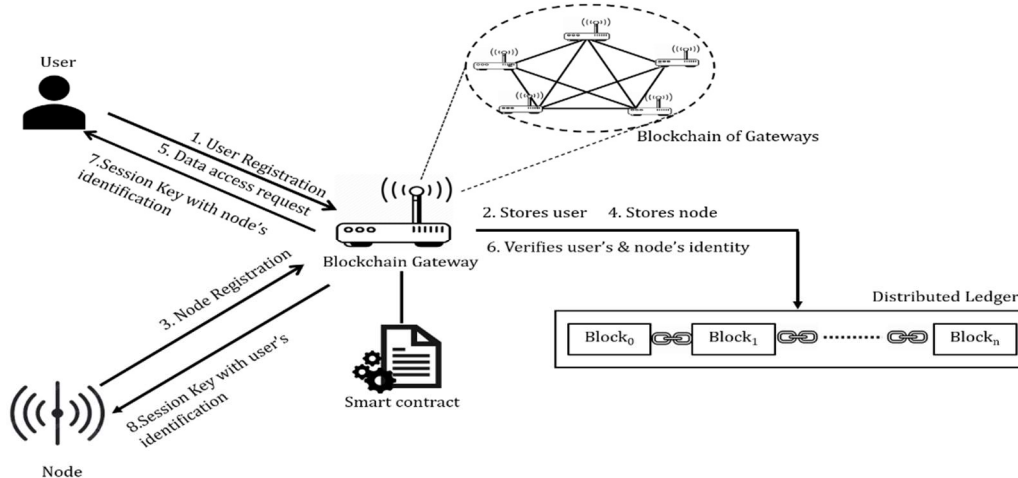


Figure 2: Overview Of The Registration and Authentication Process Using Blockchain

Table 2: Symbols And Their Descriptions

Symbol(s)	Description
U_i, ND_i, GW_i	i^{th} user, node and gateway respectively
Id_u, Pw_u	Identity and password of user
Id_n, Pw_n	Identity and password of node
Id_g, K_g	Identity and master key of the gateway
K_{gu}, K_{gn}	Keys shared by user and node with gateway
N_i, R_i	Nonces and random numbers
V_u, V_n	Specific codes of the user and node
$H(\cdot), \oplus, E_{k_i}/D_{k_i}$	Hash function, XOR, and symmetric encryption
S_k	Session Key
$Ts_i, Tc, \Delta T$	Timestamp i , current time, and maximum delay

3.2 System Initialization

Assumes that gateways from different systems with unique identities and master keys, form a blockchain network to serve as a distributed ledger for recording user and node registrations and updating credentials. Additionally, it is assumed that gateways assign identities to nodes within the system.

3.3 User registration

The user U_i registers with a nearby gateway node in the network as follows:

- User U_i saves the current time Ts_1 , chooses unique Id_u and Pw_u , creates nonce N_1 , computes $M_u = H(Id_u || Pw_u)$, $MId_u = H(Id_u || N_1 || M_u || Ts_1)$, $RN_1 = (N_1 \oplus H(Id_u || MId_u || Ts_1))$ and writes $\langle Id_u, M_u, MId_u, RN_1, Ts_1 \rangle$ to the nearby gateway GW_i .
- Gateway GW_i receives the message and terminates if either $|Tc - Ts_1|$ is greater than ΔT or Id_u exists. Else, computes $N_1^* = RN_1 \oplus H(Id_u || M_u || MId_u || Ts_1)$, $MId_u^* = H(Id_u || N_1^* || M_u || Ts_1)$, verifies whether MId_u^* is equal to MId_u and terminates if not; otherwise, N_1 is considered fresh and GW_i generates secret key K_{gu} , $V_u = H(M_u || Id_g || K_{gu} || K_g)$, $MV_u = V_u \oplus H(M_u || N_1^* || K_{gu} || Ts_2)$, $K_{gu} = H(K_{gu} || M_u || H(K_{gu} || N_1^* || MV_u || Ts_2))$ and $RK_{gu} = K_{gu} \oplus H(MK_{gu} || N_1^* || Ts_2)$. Finally, GW_i constructs a block with (Id_u, V_u, K_{gu}) , $H(Id_u || V_u || K_{gu})$, the current time, and the previous block's hash, and stores it in the blockchain and writes $\langle MV_u, MK_{gu}, RK_{gu}, Ts_2 \rangle$ to U_i .

- User U_i accepts the message if $|Tc - Ts_2| \leq \Delta T$ and calculates $K_{gu}^* = RK_{gu} \oplus H(MK_{gu} || N_1 || MV_u || Ts_2)$, $MK_{gu}^* = H(K_{gu}^* || M_u || H(K_{gu}^* || N_1 || MV_u || Ts_2))$, compares MK_{gu}^* and MK_{gu} to validate K_{gu} and $V_u^* = MV_u \oplus H(M_u || N_1 || K_{gu}^* || Ts_2)$ and stores $\{M_u, V_u, K_{gu}\}$ in secure memory.

3.4 IoT Node registration

Node ND_i registers with the gateway as follows:

- Node ND_i saves the current timestamp Ts_3 and chooses Pw_n , generates a nonce, N_2 computes $M_n = H(Id_n || Pw_n)$, $RN_2 = (N_2 \oplus H(M_n || Id_n || Ts_3))$ and sends $\langle Id_n, M_n, RN_2, Ts_3 \rangle$ to the gateway.
- Gateway GW_i receives the message and terminates if either $|Tc - Ts_3|$ is greater than ΔT and Id_n exists. Else, computes $N_2^* = (RN_2 \oplus H(M_n || Id_n || Ts_3))$, creates secret key K_{gn} , $V_n = H(M_n || Id_g || H(Id_n || K_{gn} || K_g))$, $MV_n = V_n \oplus H(M_n || N_2^* || K_{gn} || Ts_4)$, $MK_{gn} = H(K_{gn} || M_n || H(K_{gn} || N_2^* || MV_n || Ts_4))$, $RK_{gn} = (K_{gn} \oplus H(MK_{gn} || N_2^* || MV_n || Ts_4))$ and stores (Id_n, V_n, K_{gn}) , $H(Id_n || V_n || K_{gn})$, current time and previous block's hash as a block in the blockchain. Later, $\langle MV_n, MK_{gn}, RK_{gn}, Ts_4 \rangle$ is sent to node ND_i .
- Node ND_i verifies Ts_4 and computes $K_{gn}^* = RK_{gn} \oplus H(MK_{gn} || N_2^* || MV_n || Ts_4)$, $MK_{gu}^* = H(K_{gn}^* || M_n || H(K_{gn}^* || N_2^* || MV_n || Ts_4))$, maps MK_{gn}^* with MK_{gn} , and $V_n^* = MV_n \oplus H(M_n || N_2^* || K_{gn} || Ts_4)$ and stores $\{M_n, V_n, K_{gn}\}$ in memory.

The user and node register with a gateway, and their blocks are stored in the blockchain. The figure 3 demonstrates the user and node registration.

3.5 Authentication and key agreement

Figure 4 shows the authentication and key agreement processes.

- User U_i enters Id_u , and Pw_u to login. The system computes $M_u^* = H(Id_u || Pw_u)$ and verifies M_u^* with stored M_u . If not, terminate; otherwise, generate nonce N_3 , and compute $D_q = H(Id_u || K_{gu} || H(K_{gu} || V_u || N_3 || Ts_5))$, $Md_q = (D_q \oplus H(N_3 || Ts_5 || H(V_u || K_{gu} || Id_u)))$, $Mu_1 = (N_3 \oplus H(Md_q || Ts_5))$, $Mid_u = (Id_u \oplus H(Md_q || H(Mu_1 || N_3 || Ts_5) || Ts_5))$, $Mid_n = (Id_n \oplus H(H(N_3 || Id_u || D_q) || Ts_5))$ and sends $\langle Ts_5, Mu_1, Mid_u, Md_q, Mid_n \rangle$ to the nearby gateway.

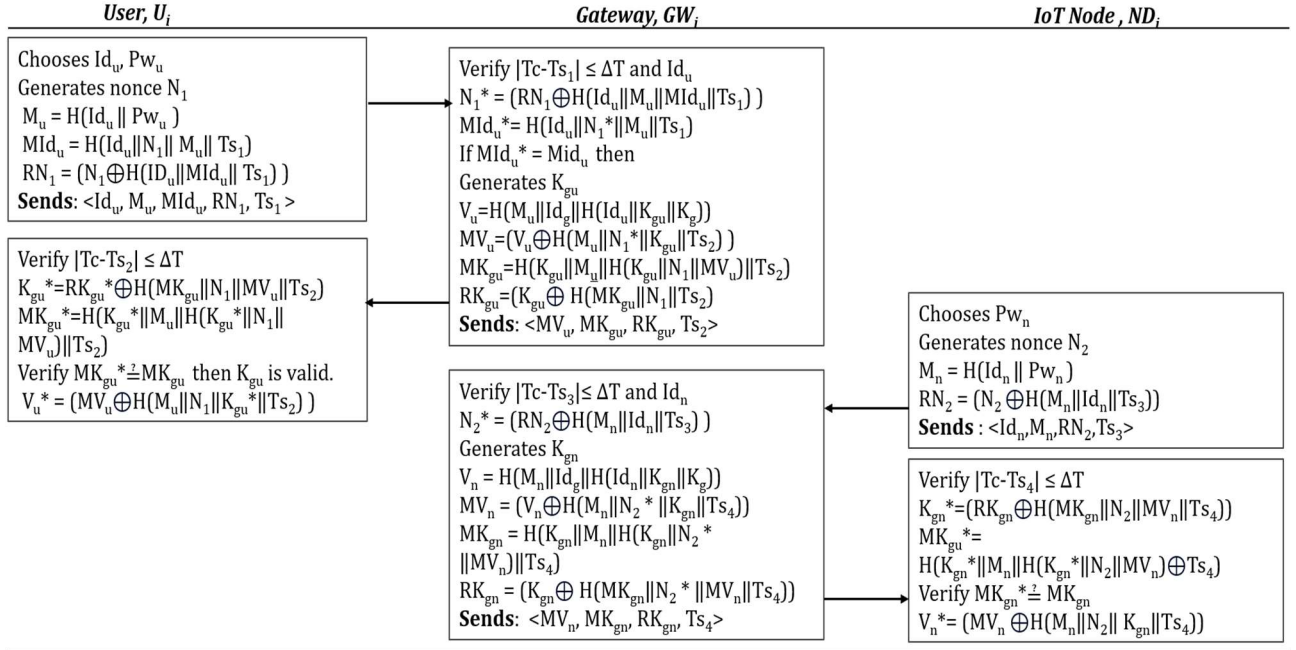


Figure 3: User And Node Registration

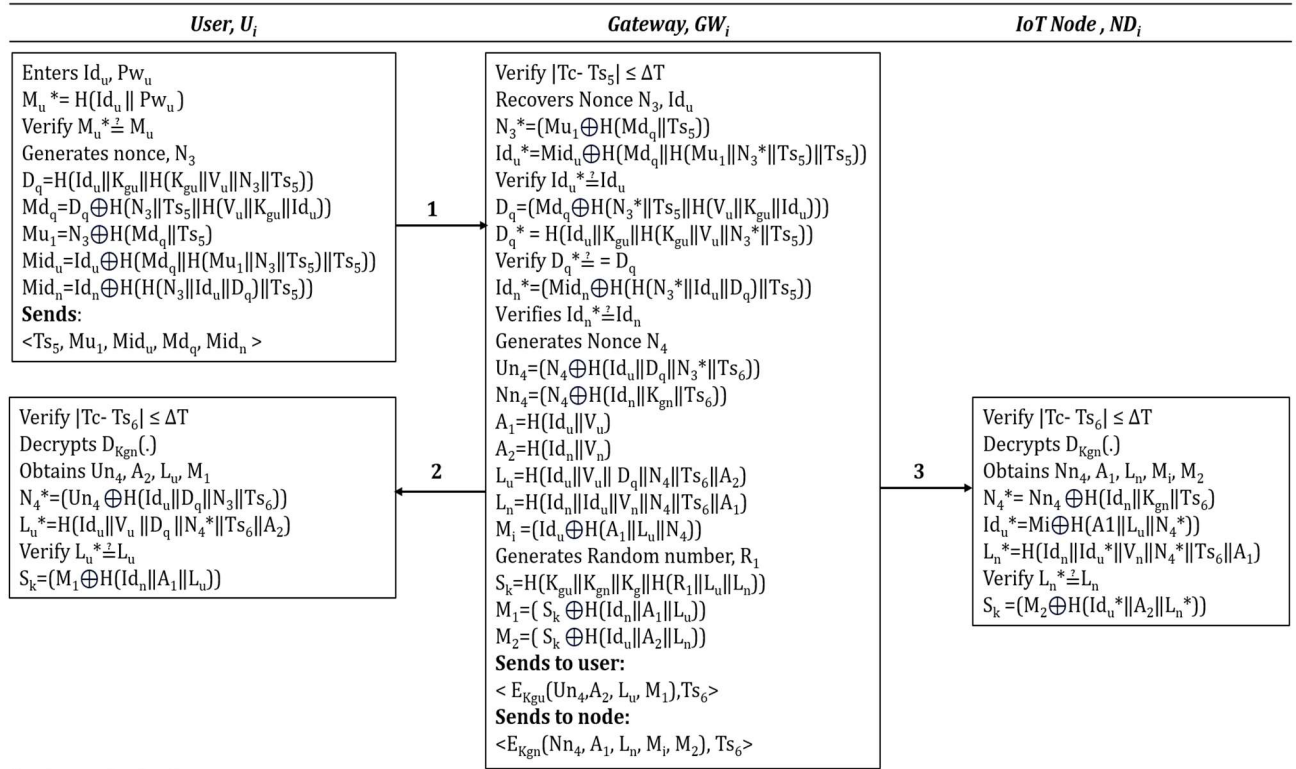


Figure 4: Authentication and Key agreement

2. If not, terminate. Otherwise, GW_i continues to compute $N_3^* = (Mu_1 \oplus H(Md_q || Ts_5))$, $Id_u^* = (Mid_u \oplus H(Md_q || H(Mu_1 || N_3^* || Ts_5) || Ts_5))$, and maps Id_u^* with Id_u in blockchain. If not, terminates; else recover $D_q = (Md_q \oplus H(N_3^* || Ts_5 || H(V_u || K_{gu} || Id_u)))$ and compute $D_q^* = H(Id_u || K_{gu} || H(K_{gu} || V_u || N_3^* || Ts_5))$. If $D_q^* = D_q$, this means a valid nonce, legitimate

identity, and fresh request. Now, the user is authenticated by a gateway via blockchain. Now, the gateway GW_i recovers $Id_n=(Mid_n \oplus H(H(N_3 * Id_u || D_q) || Ts_5))$, then verifies it in the blockchain. If Id_n exists, then generates nonce N_4 , calculates

$Un_4=(N_4 \oplus H(Id_u || D_q || N_3 * Ts_6))$,
 $Nn_4=(N_4 \oplus H(Id_n || K_{gn} || Ts_6))$, $A_1=H(Id_u || V_u)$,
 $A_2=H(Id_n || V_n)$, $L_u=H(Id_u || V_u || D_q || N_4 || Ts_6 || A_2)$,
 $L_n=H(Id_n || V_n || D_q || N_4 || Ts_6 || A_1)$, and $M_1=(Id_u \oplus H(A_1 || L_u || N_4))$. Later, random number R_1 is generated, and $S_k=H(K_{gu} || K_{gn} || K_g || H(R_1 || L_u || L_n))$,
 $M_1=(S_k \oplus H(Id_n || A_1 || L_u))$, $M_2=(S_k \oplus H(Id_u || A_2 || L_n))$ are computed, $\langle E_{K_{gn}}(Un_5, A_2, L_u, M_1), Ts_6 \rangle$ is sent to the user, and $\langle E_{K_{gn}}(Nn_5, A_1, L_n, M_1, M_2), Ts_6 \rangle$ is sent to the IoT node.

3. User U_i , verifies whether $|Tc-Ts_6| \leq \Delta T$. If it is, decrypts $D_{K_{gn}}(.)$ to obtain Un_4, A_2, L_u , and M_1 . Compute $N_4^*=(Un_4 \oplus H(Id_u || D_q || N_3 || Ts_6))$ and $L_u^*=H(Id_u || V_u || D_q || N_4 || Ts_6 || A_2)$. If $L_u^*=L_u$, then the node is legitimate one. Then, the shared key, $S_k=(M_1 \oplus H(Id_n || A_1 || L_u))$ is computed to access data from the IoT node.
4. IoT node ND_i verifies if $|Tc-Ts_6| \leq \Delta T$. If it is, decrypts $D_{K_{gn}}(.)$ to obtain Nn_4, A_1, L_n, M_1 , and M_2 .
 $N_4^*=(Nn_4 \oplus H(Id_n || K_{gn} || Ts_6))$,
 $Id_u^*=(M_1 \oplus H(A_1 || L_u || N_4^*))$, and $L_n^*=H(Id_n || Id_u^* || V_n || N_4^* || Ts_6 || A_1)$ are computed. If $L_n^*=L_n$, then the user is legitimate. Recovers the secret key, $S_k=(M_2 \oplus H(Id_u^* || A_2 || L_n^*))$.

3.6 Update password

Figure 5 illustrates password update process of user U_i . Password updates are mandatory after accessing data from IoT node. Along with password Pw_u, K_{gu} and V_u are also updated. The process is as follows:

1. User U_i chooses a new password Pw_u , generates nonce N_5 and computes $M_u=H(Id_u || Pw_u)$ and $M_3=H(V_u || S_k || N_5 || M_u || Ts_7)$ and sends $\langle E_{K_{gu}}(M_u, N_5, M_3), Ts_7 \rangle$ to the gateway GW_i .
2. Gateway GW_i checks for Ts_7 . If it is, $D_{K_{gu}}(.)$ to obtain M_u, N_5 , and M_3 . Later, it computes $M_3^*=H(V_u || S_k || N_5 || M_u || Ts_7)$. If $M_3^*=M_3$, then generates new K_{guN} and random number R_2 and computes $V_{uN}=H(M_u || R_2 || H(Id_u || K_{guN} || K_g))$,
 $M_4=H(K_{guN} || V_{uN} || N_5)$ and sends $\langle E_{K_{gu}}(K_{guN}, V_{uN}, M_4), Ts_8 \rangle$ to the user U_i .
3. Upon receiving, the user verifies Ts_8 and decrypts to obtain K_{guN}, V_{uN} , and M_4 . Now, compute $M_4^*=H(K_{guN} || V_{uN} || N_5)$ and compares $M_4^*=M_4$. If yes, then update K_{gu} and V_u with new values K_{guN} and V_{uN} respectively.

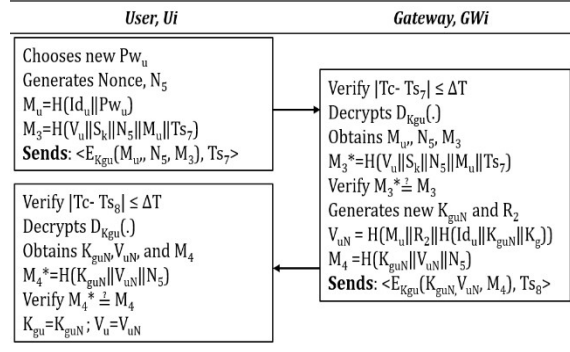


Figure 5: Password Update Phase

4. RESULTS AND DISCUSSION

Informal analysis of standard security parameters and formal analysis with the AVISPA tool are discussed to evaluate the security of the proposed protocol.

4.1 Informal Analysis

4.1.1 Anonymity

In this scheme, identities are replaced by $Mid_u=(Id_u \oplus H(Md_q || H(Mu_1 || N_3 || Ts_5) || Ts_5))$, and $Mid_n=(Id_n \oplus H(H(N_3 || Id_u || D_q) || Ts_5))$ for transmission. Even if the attacker intercepts both Mid_u and Mid_n , it is impossible to find identities because of the one-way property of the hash function and dynamic inputs, such as nonces and timestamps. Hence, the protocol ensures anonymity.

4.1.2 Resistance to replay attacks

Each exchange in the protocol includes timestamps Ts_i and nonces, N_i , to ensure the freshness of the message. Moreover, masked nonces only exchanged and were reconstructed after ensuring timestamps. If either the timestamp is invalid or the reconstructed nonces do not match, the replayed message will fail. It is clear that, in this protocol, it is not possible to replay old messages.

4.1.3 Resistance to spoofing attacks

To cover user login from the gateway, the attacker must master identities Id_u and Id_n ; secret values K_{gu}, V_u , and Pw_u ; and a dynamic value N_3 to send $\langle Ts_5, Mu_1, Mid_u, Md_q, Mid_n \rangle$ to the gateway. Moreover, the secret values are updated after every secure data access. It is impossible for an attacker to master all these values. Thus, the scheme is resistant to spoofing attacks.

4.1.4 Resistance to impersonation attacks

To mimic another entity, an attacker must intercept messages exchanged. However, messages are secured by either masking (Mu_1, Mid_u, Md_q, Mid_n) or encryption ($E_{K_{gu}}(Un_5, A_2, L_u, M_1)$) and

$E_{K_{gn}}(N_{n5}, A_1, L_n, M_i, M_2)$), which prevents impersonation. Moreover, blockchain is used to validate users and nodes via a gateway. Thus, the scheme is resistant to impersonation attacks.

4.1.5 Resistance to man-in-the middle attacks

The scheme uses hash-based masking and encrypted communications to secure messages in transit, ensure that even if the message is intercepted, it remains unreadable. Various dynamic inputs, such as nonces, N_i , random integers, R_1 , and user/node-specific values A_1 and A_2 , are used to derive session keys, S_k . An attacker can manipulate the verification process to create uneven hashes or keys, which would result in rejection. Thus, the protocol efficiently avoids an opponent from secretly intercepting or modifying data.

4.1.6 Forward secrecy

This is ensured by deriving session keys, S_k , dynamically for each communication from K_{gu} , K_{gn} and K_g , random session-specific values R_1 , and N_i and other parameters. Moreover, updates to user details, such as Pw_u , K_{gu} , and V_u , after each session ensure the confidentiality of past session keys. Even if a secret key, either K_{gu} or K_{gn} , is compromised, past session keys remain secure.

4.1.7 Resistance to insider attacks

Nonces and hash functions are used to transmit sensitive data, such as passwords and keys. One user or node cannot access another’s sensitive data because of transparency in blockchain. An insider attempting to misuse stored data, such as, $M_u = H(Id_u || Pw_u)$, cannot compute the actual password due to the irreversibility of the hash function. Mitigates threats from compromised gateway or node administrators.

4.1.8 Resistance to key compromise

Session keys, S_k , are generated by the gateway and securely distributed both the user and node via encryption. After each session, any update to user’s password, Pw_u , results an automatic update of the secret key, K_{gu} , and secret code, V_u . It ensures that

even if a session key is compromised, future updates render a key outdated, thereby reducing the risk of damage.

4.1.9 Secure session key agreement

The session key, $S_k = H(K_{gu} || K_{gn} || K_g || H(R_1 || L_u || L_n))$, is derived dynamically for each session via random inputs. Both the user and the IoT node verify the legitimacy of S_k by independently computing and matching it. Ensures secure communication between the user and the IoT node

4.1.10 Mutual authentication

The user calculates $L_u^* = H(Id_u || V_u || D_q || N_4^* || Ts_6 || A_2)$ and compares it with received L_u . If same, node is authenticated and user proceeds to recover session key. The IoT node calculates $L_n^* = H(Id_n || Id_u^* || V_n || N_4^* || Ts_6 || A_1)$ and compares with received L_n . If same, user is authenticated by node. This protocol guarantees mutual trust between the user and IoT node.

Table 3 demonstrates the comparison of security parameters our protocol with related works [20, 22, 25, 30, 35, 39].

4.2 Formal Analysis

The Automated Validation of Internet Security Protocols and Applications (AVISPA) and Security Protocol Animator (SPAN) is a tool used to validate proposed protocol coded as a role-based model in High-Level Protocol Specification Language (HLPSL) to determine whether it is safe, unsafe, or inconclusive [40]. Authentication and key agreement are implemented with specific roles, sessions and goals to defend against attacks, including impersonation, replay, and MITM. Figures 6 and 7 shows the results from AVISPA’s OFMC and CL-AtSe back-ends its SPAN simulations, respectively.

Table 3: Comparison Of Security Parameters With Related Works

Security Parameter	[20]	[22]	[25]	[30]	[35]	[39]	Proposed
Anonymity	√	√	√	√	√	√	√
Resistant to replay attack	√	√	√	√	√	√	√
Resistant to Impersonation Attacks	√	√	√	√	√	√	√
Resistant to MITM attacks	√	√	√	X	√	√	√
Forward Secrecy	√	√	√	X	√	√	√
Resistant to Insider attacks	√	√	√	X	√	√	√
Resistant to Key Compromise	X	X	X	X	√	√	√
Mutual Authentication	√	√	√	X	√	X	√
Provides Blockchain-based solution	√	√	√	X	X	X	√

√: secured; X: not secured

<pre>% OFMC % Version of 2006/02/13 SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS PROTOCOL /home/span/span/testsuite/results/FINAL-BIO-KEY-MANAGEMENT.if GOAL as_specified BACKEND OFMC COMMENTS STATISTICS parseTime: 0.00s searchTime: 0.00s visitedNodes: 4 nodes depth: 2 plies</pre>	<pre>SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS TYPED_MODEL PROTOCOL /home/span/span/testsuite/results/FINAL-BIO-KEY-MANAGEMENT.if GOAL As Specified BACKEND CL-AtSe STATISTICS Analysed : 1 states Reachable : 1 states Translation: 0.00 seconds Computation: 0.00 seconds</pre>
---	---

Figure 6: AVISPA Results Of Proposed Protocol Using OFMC And CL-AtSe

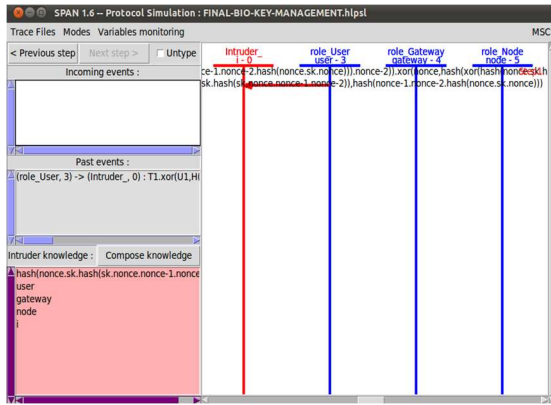


Figure 7: AVISPA results using SPAN

4.3 Performance Evaluation

The performance of our protocol is demonstrated through comparisons with similar studies based on blockchain [20, 22, 25] and non-blockchain [30, 35, 39] technologies in IoT smart environments.

4.3.1 Computation cost

For execution times, we refer to [41, 42]. The XOR operation is negligible. During mutual authentication and key agreement, user U_i executes $9T_H$ and $1T_{SY}$; gateway GW_i runs $15T_H$ and $2T_{SY}$; and the IoT node performs $4T_H$ and $1T_{SY}$. The proposed protocol involves $28T_H$ and $4T_{SY}$ operations. The estimated execution time of the proposed protocol is 0.0858 ms (refer table 4). A comparison of the computational costs with those of other related methods is shown in table 5.

Table 4: Computation Cost Of Cryptographic Operations

Operation (Notation)	Duration (milli seconds)
One-way hash function (T_H)	0.0026
Symmetric encryption/decryption (T_{SY})	0.00325
ECC point multiplication (T_{EM})	1.989
Fuzzy extractor (T_{FE})	1.989
Symmetric polynomial (T_P)	0.416
PUF function (T_{PUF})	0.0023

Table 5: Computational Cost Comparison

Scheme	Total cost	Estimated Execution Time (milli seconds)
Son <i>et al.</i> [20]	$33T_H+4T_{EM}$	8.0418
Guo <i>et al.</i> [22]	$27T_H+2T_P+1T_{PUF}$	0.0754
Yang <i>et al.</i> [25]	$30T_H+1T_{FE}$	2.067
Chang <i>et al.</i> [30]	$31T_H+3T_{EM}$	6.0476
Oh <i>et al.</i> [35]	$42T_H$	0.1092
Nyangaresi <i>et al.</i> [39]	$34T_H$	0.0884
Proposed	$28T_H+4T_{SY}$	0.0858

4.3.2 Communication cost

In [41], the lengths of identity, hash value, nonce, random number, XOR, timestamp and

symmetric encryption/decryption are 32bit, 160bit, 128bit, 128bit, 160bit, 32bit, and 128bit respectively. Our protocol takes 992 bits as the total communication cost by exchanging three messages during authentication and key agreement. Table 6 shows the comparison details of communication cost with other related works.

Table 6: Communicational Cost comparison

Scheme	Messages exchanged	Total bits
Son <i>et al.</i> [20]	4	2368
Guo <i>et al.</i> [22]	4	2656
Yang <i>et al.</i> [25]	4	2368
Chang <i>et al.</i> [30]	4	2400
Oh <i>et al.</i> [35]	5	1824
Nyangaresi <i>et al.</i> [39]	5	2656
Proposed	3	992

5. CONCLUSIONS

The growing adoption of smart environments has increased the risk of unauthorized access to sensitive data. Existing authentication methods are vulnerable to attacks such as MITM, impersonation, and data modification. The proposed protocol uses blockchain with smart contract to increase security and privacy in IoT environments. When validated via the AVISPA tool, the protocol is lightweight, efficient, and robust, as it uses hash functions and XOR operations and has an execution time of 0.0858 ms, making it ideal for resource constrained devices. Future work includes real-world implementation with real-time data for dynamic and accurate user authentication

REFERENCES:

- [1] S. Nizetic, P. Soli, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart sustainable future", *Journal of cleaner production*, Vol. 274, 2020, pp. 1-32.
- [2] Y. Hajjaji, W. Boulila, IR. Farah, I. Romdhani, and A. Hussain, "Big data and IoT-based applications in smart environments: A systematic review", *Computer Science Review*, Vol. 39, 2021.
- [3] M. Balega, W. Farag, X.W. Wu, S. Ezekiel, and Z. Good, "Enhancing IoT Security: Optimizing Anomaly Detection through Machine Learning", *Electronics*, Vol. 13, No. 11, 2024.
- [4] A.A. Patwary, R.K. Naha, S. Garg, S.K. Battula, M.A. Patwary, E. Aghasian, M.B. Amin, A. Mahanti, M. Gong, "Towards secure fog computing: A survey on trust management, privacy, authentication, threats and access control", *Electronics*, Vol. 10, No. 10, 2021.
- [5] M. Aqeel, F. Ali, M.W. Iqbal, T.A. Rana, M. Arif, and M.R. Auwal, "A review of security and privacy concerns in the internet of things (IoT)", *Journal of Sensors*, Vol. 2022, No. 1, 2022.
- [6] S. Uppuluri & G. Lakshmeeswari, "Secure user authentication and key agreement scheme for IoT device access control based smart home communications", *Wireless Networks*, Vol. 29, No. 3, 2023, pp. 1333-1354.
- [7] G.J. Ra, & I.Y. Lee, "A study on KSI-based authentication management and communication for secure smart home environments" *KSI Transactions on Internet and Information Systems (TIIS)*, Vol. 12, No. 2, 2018, pp. 892-905.
- [8] A. Khan, A. Ahmad, M. Ahmed, J. Sessa, & M. Anisetti, "Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends", *Complex & Intelligent Systems*, Vol 8, No. 5, 2022, pp. 3919-3941.
- [9] E. Ebrahimpour, & S. Babaie, "Authentication in Internet of Things, protocols, attacks, and open issues: a systematic literature review", *International Journal of Information Security*, Vol. 23, No. 3, 2024, pp. 1583-1602.
- [10] S. Dong, K. Abbas, M. Li, & J. Kamruzzaman, "Blockchain technology and application: an overview", *PeerJ Computer Science*, Vol. 9, 2023.
- [11] F. Chen, Z. Xiao, L. Cui, Q. Lin, J. Li, & S. Yu, "Blockchain for Internet of things applications: A review and open issues", *Journal of Network and Computer Applications*, Vol. 172, 2020.
- [12] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, & K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes", *IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, IEEE, October 28 – November 1, 2018, pp. 1-8.
- [13] U. Khalid, M. Asim, T. Baker, P.C. Hung, M. A. Tariq, & L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems", *Cluster Computing*, Vol. 23, No. 3, 2020, pp. 2067-2087.
- [14] CH. Lau, KH. Alan, and F. Yan, "Blockchain-based authentication in IoT networks" *Conference on Dependable and Secure Computing (DSC)*, IEEE, December 10-13, 2018, pp. 1-8.

- [15] Tian Z, Yan B, Guo Q, Huang J, Du Q. Feasibility of identity authentication for IoT based on blockchain. *Procedia Computer Science*, Vol. 174, 2020, pp. 328-332.
- [16] K. Hameed, S. Garg, M.B. Amin, and B. Kang, "A formally verified blockchain-based decentralised authentication scheme for the internet of things", *The Journal of Supercomputing*, Vol. 77, No. 12, 2021, pp. 14461-501.
- [17] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and IoT environment", *IEEE Internet of Things Journal*, Vol. 8, No. 4, 2020, pp. 2116-23.
- [18] A.K. Al Hwaitat, M.A. Almaiah, A. Ali, S. Al-Otaibi, R. Shishakly, A. Lutfi, and M. Alrawad, "A new blockchain-based authentication framework for secure IoT networks", *Electronics*, Vol. 12, No. 17, 2023.
- [19] J. Lee, M. Kim, K. Park, S. Noh, A. Bisht, A.K. Das, and Y. Park, "Blockchain-based data access control and key agreement system in iot environment" *Sensors*. Vol. 23, No. 11, 2023.
- [20] S. Son, J. Lee, Y. Park, Y. Park, and A.K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET" *IEEE Transactions on Network Science and Engineering*, Vol. 9, No. 3, 2022, pp. 1346-58.
- [21] H. Idrissi and P. Palmieri, "Agent-based blockchain model for robust authentication and authorization in IoT-based healthcare systems", *The Journal of Supercomputing*, Vol. 80, No. 5, 2024, pp. 6622-60.
- [22] Y. Guo, Z. Zhang, Y. Guo, P. Xiong. "Bsra: Blockchain-based secure remote authentication scheme for the fog-enabled internet of things", *IEEE Internet of Things Journal*, Vol. 11, No. 2, 2023, pp. 3348-61.
- [23] A. Singh, H. Chandra, S. Rana, and D. Chhikara, "Blockchain based authentication and access control protocol for IoT" *Multimedia Tools and Applications*, Vol. 83, No. 17, 2024, pp. 51731-53.
- [24] N. Alsaeed, F. Nadeem, and F. Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing", *Future Generation Computer Systems*, Vol. 151, 2024, pp. 162-81.
- [25] H. Yang, Y. Guo, and Y. Guo, "Blockchain-based cloud-fog collaborative smart home authentication scheme", *Computer Networks*, Vol. 242, 2024.
- [26] M. Alshahrani, and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain", *Journal of information security and applications*, Vol. 45, 2019, pp. 156-75.
- [27] M. Fakroon, M. Alshahrani, F. Gebali, I. Traore, "Secure remote anonymous user authentication scheme for smart home environment" *Internet of Things*, Vol. 9, 2020.
- [28] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments", *Journal of Information Security and Applications* Vol. 52, 2020
- [29] PK. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for Internet of Things environments", *International Journal of Communication Systems*, Vol. 30, No. 16, 2017.
- [30] Y.F. Chang, W.L. Tai, P.L. Hou, and K.Y. Lai, "A secure three-factor anonymous user authentication scheme for internet of things environments", *Symmetry*, Vol. 13, No. 7, 2021
- [31] A. Li, B. Kang, Y. Huo, X. Zuo, and S. Niu, "Analysis and Improvement on a Three-Factor Authentication Scheme in IoT Environment", *Frontiers in Computing and Intelligent Systems*, Vol. 4, No. 2, 2023, pp. 81-9.
- [32] A. Rahnama, M. Beheshti-Atashgah, T. Eghlidos, and M.R. Aref, "A lightweight anonymous authentication protocol for IoT wireless sensor networks", *16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, IEEE, August 28-29, 2019.
- [33] P. Kumar and A. Kumar Bhatt. "Enhancing multi-tenancy security in the cloud computing using hybrid ECC-based data encryption approach", *IET Communications*, Vol. 14, No. 18, 2020, pp. 3212-22.
- [34] A. Xiang and J. Zheng, "A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks", *Electronics*, Vol. 9, No. 6, 2020.
- [35] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A secure and lightweight authentication protocol for IoT-based smart homes", *Sensors*, Vol. 21, No. 4, 2021.
- [36] M. Masud, G.S. Gaba, K. Choudhary, M.S. Hossain, M.F. Alhamid, G.Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare", *IEEE Internet of Things Journal*, Vol. 9, No. 4, 2021, pp. 2649-56.

- [37] B.A. Mohammed, M.A. Al-Shareeda, S. Manickam, Z.G. Al-Mekhlafi, A.M. Alayba, A.A. Sallam, “Anaa-fog: A novel anonymous authentication scheme for 5g-enabled vehicular fog computing”, *Mathematics*, Vol. 11, No. 6, 2023.
- [38] G.H. Faraj, K. Shahtalebi, and H. Mala. “An Anonymous Authenticated Key Agreement Scheme for Telecare Medical Information Systems”, *Cryptography*, Vol. 8, No. 4, 2024.
- [39] V.O. Nyangaresi and G.K. Yenukar, “Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks”, *High-Confidence Computing*, Vol. 4, No. 2, 2024. 2024.
- [40] T. Genet, “A short span+avispa tutorial” (Doctoral dissertation, IRISA). 2015. <https://inria.hal.science/hal-01213074>
- [41] W. Huang, “ECC-based three-factor authentication and key agreement scheme for wireless sensor networks”, *Scientific Reports*, Vol. 14, No. 1, 2024.
- [42] Y. Guo, Z. Zhang, and Y. Guo, “Fog-centric authenticated key agreement scheme without trusted parties”. *IEEE Systems Journal*, Vol. 15, No. 4, 2020, pp. 5057-66.