International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 12, December, 2025, pp. 2589-2602
Journal homepage: http://iieta.org/journals/ijsse

A Blockchain-Biometric Lightweight Mutual Authentication Protocol for IoT Security

Durvasi Gudivada*, Kameswara Rao Manchiraju

Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Guntur 522302, India

Corresponding Author Email: gdurvasi@gmail.com

https://doi.org/10.18280/ijsse.151215

Received: 16 October 2025
Revised: 15 December 2025
Accepted: 24 December 2025
Available online: 31 December 2025

Keywords:
lightweight mutual authentication, blockchain-based security, biometric hashing, smart contract, decentralized authentication, Internet of Things, secure access control

ABSTRACT

The swift growth in the number of Internet of Things (IoT) devices in smart environments has facilitated more automation, data-driven decision-making, and service efficiency; at the same time, it has caused serious security and privacy issues, especially in user and device authentication. To overcome these limitations, the paper presents a blockchain and biometric-enhanced lightweight mutual authentication protocol to provide secure IoT environments. The model proposed combines the biometric hashing of privacy-related identity checking and blockchain technology to provide decentralized and tamper-resistant credential management. Light cryptographic primitives are used to make them suitable for resource-constrained IoT devices, and smart contracts are used to automate authentication and key distribution. The proposed method covers secure steps for registering users and IoT devices, verifying identities, managing credentials using blockchain, and updating keys with minimal overhead. Experimental analysis was based on a simulation-based environment of the IoT with the same system parameters, and the proposed protocol was contrasted with other lightweight authentication protocols. The findings indicate that the suggested strategy can obtain a low mean execution time of around 2.06 ms, and it has a great impact in lowering the cost of computation and communication in comparison to the protocols of the baseline. These results prove the effectiveness and applicability of the suggested authentication scheme to the resource-constrained IoT.

1. INTRODUCTION

The Internet of Things (IoT) is transforming the way the physical and digital worlds interact with one another by interconnecting diverse IoT devices, from domestic appliances and wearable sensors to industrial equipment and autonomous systems, through the internet-enabled wireless sensor networks [1-3]. Chataut et al. [4] proposed that the increasing number of IoT devices compared to humans creates an astonishing level of interconnectivity. This increase presents a twofold impact. One that allows smooth communication, real-time data collection, and intelligent automation in a wide range of smart application domains, including smart homes, healthcare, transportation, and industrial control systems [5]. Two, due to the limited capabilities, security challenges faced are data security, user privacy, and system integrity in situations where devices are under-monitored [6].

To overcome security challenges faced by smart, distributed, and dynamic applications, the authentication process acts as a protection layer by not only identifying the legitimacy of the IoT devices that collect and share the data but also users before granting access to sensed data [7]. Despite having a huge number of authentication methods proposed in the literature, from traditional to advanced, user authentication remains a challenging issue since they often prove inefficient or insecure for many IoT use cases [8-11]. These mechanisms typically require substantial processing power, centralized management, and constant network availability, all of which may not be feasible in IoT deployments that involve low-power, intermittently connected, or physically unprotected devices [12-14]. Furthermore, many existing authentication schemes are exposed to sophisticated cyberattacks, comprising phishing, malware, brute force, and numerous other attacks [15]. The increase in cyberattacks is not only based on the limited capabilities of IoT devices but also on their deployment in insecure environments where the devices operate under minimal supervision [16]. The risk of exposing the user's sensitive identity information while sharing it over an insecure channel raises serious privacy concerns when personal or confidential data is involved [17].

To address these problems, it requires developing a robust, decentralized, lightweight, and secure authentication protocol for the specific needs of the IoT ecosystems. This study aims to provide a secure, privacy-aware, mutual authentication and secret key agreement protocol to validate identities of trusted entities and establish secure communication in IoT environments between the user and device by integrating blockchain technology and biometric hashing with IoT.

By identifying trusted individuals, biometric qualities like fingerprints, iris patterns, faces, etc., provide a dependable, practical, and suitable solution to enhance the usability and security of the IoT environment [18, 19]. In contrast to traditional authentication methods, biometric traits cannot be easily duplicated and require the actual presence of the individual, thereby offering a secure and efficient means of user identification. The selection of a biometric trait generally depends on the necessities of the authentication system [20]. However, storing raw biometric data creates privacy risks since biometric traits cannot be changed if compromised [21]. To address this, the proposed authentication method applies biometric hashing, which converts original biometric data into irreversible hash templates that conceal the original biometric features while still enabling reliable matching. These hashes behave like access tokens that protect users' privacy and reduce the risk of data leakage and improve identity protection.

Simultaneously, blockchain technology is integrated to create a decentralized, tamper-resistant, immutable, and distributed ledger for recording and managing authentication credentials such as username, password, etc., as identity records [22]. Decentralized architecture of blockchain guarantees that these records cannot be tampered with or forged, while its consensus mechanisms eliminate the dependency on centralized trust authorities [23, 24]. This increases transparency, enhances resistance to single points of failure, and enables robust authentication across the smart network. The benefits of integrating blockchain technology and biometric hashing with IoT networks are shown in Figure 1.

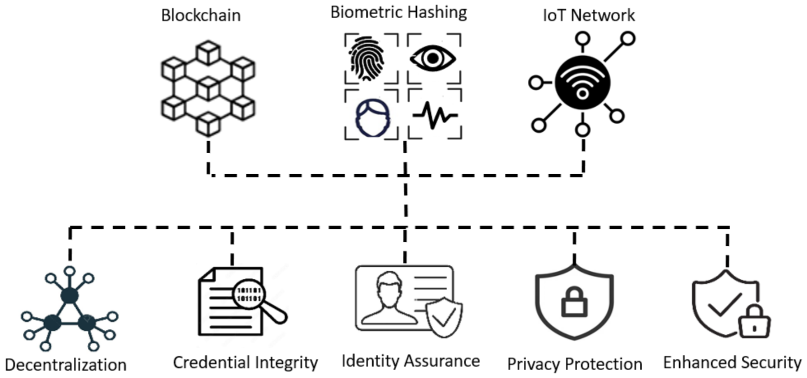


Figure 1. Benefits of integrating blockchain technology and biometric hashing with IoT networks

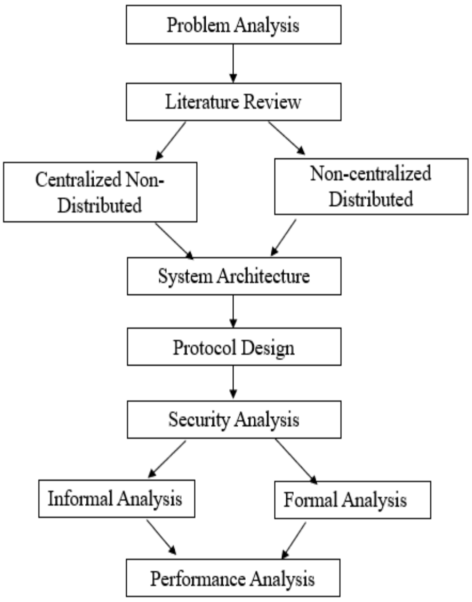


Figure 2. Research study and design

Blockchain technology combined with biometric hashing creates a secure, reliable, and effective authentication method for IoT-based networks. Biometric hashing guarantees unique and difficult to forge user identities, while blockchain ensures the immutability and integrity of stored biometric hashes, preventing unauthorized access and protecting against various security attacks. The research study and design process is depicted in Figure 2. Therefore, we propose a robust solution by merging the realistic and privacy-preserving nature of biometric hashing with the reliability and decentralization of blockchain technology to overcome issues raised in authentication. It supports lightweight functions suitable for constrained devices, resists a wide range of security threats, and ensures both user secrecy and secure access control. This work presents the system architecture, protocol description, and security analysis to show how the proposed solution effectively secures identity and communication within IoT ecosystems.

1.1 Research gaps

Although much has been studied on the authentication and access control of the IoT, the current solutions usually deal with security, identity protection, or decentralization alone, and thus result in trade-offs between the efficiency of computation, identity protection, and management of trust. The lightweight authentication schemes commonly use centralized authority and do not have a high level of resistance against identity compromise, and using biometric schemes poses a privacy issue because of the exposure of templates and storage weaknesses. On the other hand, authentication methods implemented using blockchains improve decentralization and trust, but are often computationally and communicationally expensive, which is not suitable for IoT devices that have limited resources.

Thus, an urgent research void is still present in the creation of a lightweight, decentralized, and privacy-preserving mutual authentication system that can at once be a biometric identity protection system and enable trust management using blockchain technology without causing excessive burdens to IoT nodes. To pinch this gap, the proposed protocol combines biometric hashing with smart contract based decentralized authentication to provide secure mutual authentication at low computational cost and with small communication overhead. It is this combined approach that makes the proposed work stand out from the previous research and offers a viable solution that suits the actual IoT environment.

1.2 Problem statement

The deployment of IoT devices in open as well as limited smart networks has brought forth serious security and privacy issues, particularly in authentication. Since most of the devices are installed in resource-limited environments and operate in physically insecure environments, it becomes hard to guarantee secure and reliable communication. Conventional and modern authentication mechanisms are either too computationally expensive for resource constrained devices or make heavy use of centralized infrastructures that introduce scalability and single point of failure risks [25, 26]. Moreover, IoT networks are dynamic and made up of heterogeneous types of devices with limited communication, processing, and power consumption capabilities. This increases the attack vector, including spoofing, man-in-the-middle, denial-of-service, and replay attacks [27, 28]. Beyond these attacks, the storage and transmission of sensitive identity information, particularly biometric data, pose severe privacy issues [29]. Once biometric data is compromised, it cannot be revoked or updated like traditional credentials, making privacy-preserving mechanisms essential.

Thus, the need for an authentication method that is secure and lightweight, able to protect user identity and device integrity, and remain appropriate for resource constraint and decentralized networks.

1.3 Research objectives

This research aims to design, develop, and evaluate a secure, lightweight, and efficient authentication and secure key distribution protocol for IoT environments by integrating biometric hashing with blockchain technology. The specific objectives of the study are as follows:

1. To analyze the vulnerabilities of authentication protocols suggested for IoT networks in the literature, particularly in terms of computational overhead, scalability, and vulnerability to attacks.
2. To design and develop a privacy-preserving lightweight user authentication protocol for IoT environments by combining biometric hashing and blockchain technology.
3. To assess the performance of the recommended protocol with related works in the literature.

The paper is organized as follows: Section 2 reviews the extensive literature on the topic, Section 3 outlines the proposed methodology, Section 4 presents the results, Section 5 compares the performance of the proposed method, and Section 6 concludes the research and discusses future directions.

2. RELATED WORKS

Numerous studies have proposed authentication and key management techniques to ensure security and privacy in IoT networks. This section presents a brief overview of centralized on-distributed and non-centralized distributed user authentication and secure key management methods proposed for IoT-based smart networks in the literature.

2.1 Centralized non-distributed authentication

Centralized and non-distributed authentication mechanisms depend on a single trusted authority responsible for managing and verifying the identities of trusted individuals in the network and issuing keys for secure data exchange, thereby preserving privacy and security.

Vernam and Bhardwaj [30] proposed a centralized three-way authentication protocol for fog-enabled dynamic topological smart networks to overcome authentication challenges faced by devices moving across unprotected and resource-constrained IoT environments. In this, cloud and fog servers serve as resource rich elements that maintain global and local databases of original identities of resource constrained IoT devices, respectively. Digital certificates are used for mutual authentication between the fog and cloud servers, while devices are authenticated by the fog node when it is in a cluster and by the cloud server when it moves between clusters. Lansky et al. [31] developed a centralized five-stage identification framework for fog-driven networks. In this, initially, a Trusted Third Party (TTP) obtains registration details of devices, fog nodes, and cloud servers. Mutual authentication and key generation between the cloud server, fog node, and device are ensured by asymmetric cryptographic techniques, digital certificates, and lightweight hashing algorithms. However, the storage overhead of this model is higher when compared with existing methods.

Höglund et al. [32] implemented PKI4IoT, an automated certificate enrolment protocol for IoT networks to address the issues related to device enrolment and certificate management in Public Key Infrastructure (PKI). This protocol provides secure communication among Certificate Authorities (CA) and devices where CAs issue X.509 certificates while minimizing overhead. In the same way, to resolve issues of compromised CAs and mismanagement of certificates in authentication methods based on public key cryptography and identity-based encryption, Gupta and Varshney [33] designed and developed a prototype on the ESP32 platform using Physically Unclonable Functions (PUF), bitwise Exclusive OR (XOR), and a hash function. In this approach, devices do not need to store secrets in memory and can perform authentication autonomously without relying on a server, thereby improving computing power. This approach is appropriate for environments utilizing ZigBee, BLE, RFID, and other wireless technologies, as it eliminates the need for an active internet connection for the device to communicate with the server during the authentication phase.

To provide security exchange among various individuals in healthcare IoT, Alruwaili et al. [34] proposed two authentication and key agreement methods, IoT Device to Cloud Server (IoTD-2-CS) and User to Cloud Server (UX-2-CS). This approach includes gathering healthcare data from devices and making it accessible to users via the cloud. To minimize the processing and storage power of the IoT device, PUFs are utilized. The implementation was executed using Raspberry Pi 3 B+ devices and evaluated with the Scyther tool. The results indicate that the framework is secure and efficient.

Das et al. [35] proposed an advanced lightweight authentication scheme for healthcare IoT using PUF and symmetric encryption to resolve issues in device authentication, storage, and processing power of healthcare devices. This scheme achieves mutual authentication and secure key exchange between wearable devices and the server with a low computational cost while preserving device privacy by not storing any sensitive data in memory, including temporary identity. However, it is susceptible to anonymity and replay attacks.

Wu et al. [36] proposed a lightweight validation scheme to enhance user privacy and security in complex and open wireless environments, where both the users and cloud servers register with a control server for authorization and session key generation; subsequently, users utilize IoT devices to access cloud services securely. The proposed protocol was formally verified by the ProVerif tool, and the results demonstrated its resistance to several common attacks. However, Ju and Park [37] later revealed that the scheme [36] remains exposed to verification table leakage, impersonation, and privileged insider attacks. To address these security flaws, Ju and Park [37] proposed an improved protocol for authenticating and exchanging secret keys in Cloud-IoT networks by integrating user biometric information with the cloud server's confidential key, thereby preventing leakage of key factors. Experimental results showed that the proposed scheme achieves a 6% improvement in performance.

Rana et al. [38] proposed a lightweight and secure authentication method for the 6G/IoT infrastructure to avoid insecurities and heavy computations in password based and smartcard authentication. However, it requires a massive exchange of messages and hence has increased computational overhead. Darman et al. [39] designed enhanced remote user identification and key maintenance for 6G networks used in industrial IoT, called the Improved User Authenticated Key Management Scheme Network in a Box (iUAKMS-NIB). This approach enables self-recovering and self-configuring network infrastructure to ensure uninterrupted and real-time communication between affected individuals and responders during a disaster.

2.2 Non-centralized distributed authentication

Distributed non-centralized authentication mechanisms remove the dependence on a single control server. Instead, authentication responsibilities are shared across multiple nodes in the network.

Tahir et al. [40] proposed a lightweight authentication and authorization method for a healthcare system that integrates cloud-IoT environments with blockchain to remotely monitor patients, establish secure connections among diverse health-tracking devices for exchanging raw patient data and diagnostic results, and enhance the privacy of smart medical informatics through a probabilistic model that incorporates random numbers. Furthermore, Yu et al. [41] presented BAKMP, a blockchain-assisted authentication and key management protocol for medical IoT environments using a private blockchain. The protocol aims to securely store and transmit patient data and medical reports between medical implanted or wearable smart medical devices and authorized users, including doctors, care-providers, and medical test centres. In this network, a trusted authority registers all network nodes; the cloud server acts as a miner in blockchain, and stores patient data received from the personal server; and authorized users, such as doctors and care takers access data securely from the cloud server.

Yu et al. [41] identified vulnerabilities such as Man in the Middle (MITM) attack, impersonation, and secret key disclosure attacks, besides high computational overhead in the authentication method for Internet of Vehicles (IoV) proposed by Vasudev et al. [42], which relies on encryption and signatures by means of bilinear pairing. Therefore, Aman et al. [43] introduced IoT systems to lightweight mutual authentication methods that rely on physical characteristics that cannot be replicated. The first example involves a communication between an IoT device and a server, and the second involves the establishment of a session between two IoT devices. The protocols for these two cases are then provided. Similarly, to reduce the impact of road accidents and improve the comfort and safety of the drivers and passengers, Parmar et al. [44] suggested blockchain powered privacy-preserving authentication system for IoV, which utilizes certificates and smart contracts. This system secures exchanges among vehicles and Trusted Authorities (TAs) and protects vehicles against various security attacks.

Sabrina et al. [45] implemented a method called Lightweight Time-Based Identification Protocol (LiTBIP), designed to manage device identities in blockchain-IoT networks. The approach is designed to overcome security vulnerabilities and reduce technical and design related issues observed commonly in IoT systems. A central hub is employed to check and validate data, and blockchain technology is utilized blockchain to store device identities securely. The prototype is implemented on the Raspberry Pi platform to assess its effectiveness for handling a large quantity of hubs while maintaining low computational overhead.

Al Hwaitat et al. [46] proposed a reliable, secure, and efficient authentication mechanism to overcome storage and complexity issues in blockchain-based industrial IoT systems, utilizing homomorphic encryption to encrypt data at the user's site before uploading it to the cloud and a Support Vector Machine (SVM) for user classification. This approach enhances privacy and security while reducing processing and communication expenses by integrating a permissioned blockchain architecture.

Harbi et al. [47] proposed a lightweight authentication protocol called Lightchain by integrating blockchain technology with fog computing using exclusive-OR and hash functions to authenticate a remote user of a cloud. The computation and communications costs are low compared to the related works. But Kim et al. [48] identified several attacks in the study by Harbi et al. [47], such as insider, Denial of Service (DoS), and stolen verifier attacks. To overcome these attacks, Harbi et al. [47] implemented blockchain based authentication protocol on the NS3 platform.

Wang et al. [49] proposed a lightweight mutual authentication protocol by leveraging unmanned aerial vehicles (UAVs) with blockchain to maintain the security and privacy of drone data and communications between users and drones. The scheme significantly reduced computational and communicational costs by 98.9% and 58.7%, respectively. However, Ju et al. [50] later found that Wang et al. [49] are susceptible to session key exposure and drone impersonation attacks, and they further lack to ensure the validity of login and key agreement processes. To overcome these limitations and enable secure data exchange between UAVs and related nodes in the multi-server Internet of Drones (IoD) environments, they proposed a lightweight authentication protocol by integrating IoD with blockchain technology. This approach effectively balances security and efficiency, ensuring minimal communications costs. Later, Bera et al. [51] proposed a blockchain-based four-factor key agreement protocol for Air Smart Vehicular Networks (ASVN) to offer secure data sharing between users and drones. A concise summary of these studies, including their methodologies, advantages, and limitations, is provided in Table 1.

Table 1. Overview of authentication approaches proposed by researchers in existing literature

Paper	Methodology	Advantages	Limitations
		Centralized Non-Distributed Authentication	
Vernam and Bhardwaj [30]	Hash function, nonce, and digital certificates	+ Improves the ability to manage authentication for a large number of IoT devices	– Local and global databases require additional memory, incur higher maintenance costs, and may result in data inconsistencies – Not suitable for time sensitive applications
Lansky et al. [31]	Asymmetric encryption, hash functions, and digital certificates	+ Maximizes efficiency + Minimizes communication cost	– Incompatible with some wireless communication technologies
Höglund et al. [32]	Constrained Application Protocol (CoAP) for communication, Datagram Transport Layer Security (DTLS), TLS for encryption, and Concise Binary Object Representation (CBOR) for encoding X.509 certificate	+ Reduced memory and communication overhead	– Devices prone to being cloned and hacked – Servers should not employ basic protection measures to reduce the effect of the attack
Gupta and Varshney [33]	PUF, Exclusive OR (XOR), and a hash function	+ Secure secret key + Protection against replay attacks	– Communication cost is higher in this model
Alruwaili et al. [34]	Physically Unclonable Functions (PUF), Advanced Encryption Standard (AES), and a hash function	+ Protects against Man in the Middle (MITM) attack, reply, impersonation, Denial of Service (DoS), and insider attacks + Resistant to physical attacks	– Failure of single server operations
Ju and Park [37]	Hash function, AES	+ Secure against various attacks	– Server requires more computation, and high delay levels are observed
Rana et al. [38]	Hash functions, XOR, and symmetric encryption	+ Attacker can't spoof a legitimate user	– Does not preserve user untraceability and anonymity
Darman et al. [39]	Elliptic curve cryptography, hash function, and XOR	+ Protects from active and passive attacks	– Communication cost is higher
		Non-Centralized Distributed Authentication	
Tahir et al. [40]	Blockchain, Ethereum	+ Improved security with low overheads	– Lack of more efficient consensus mechanisms
Yu et al. [41]	Blockchain, Elliptic Curve Cryptography (ECC), hash functions, and XOR	+ Resistant to many attacks	– Susceptible to DoS attack – Key management issues not resolved
Vasudev et al. [42]	Hash functions and XOR	+ Prevents from potential attacks	– Communication cost is not analysed
Parmar et al. [44]	Blockchain, ECC, AES, Secure Hash Algorithm (SHA)-256	+ Transparent and secure against various attacks	– Lacks in exchanging messages among multiple vehicles
Sabrina et al. [45]	Blockchain, fuzzy extractor, Raspberry Pi	+ Handles transactions securely	– Data integration and configuration issues are not discussed
Al Hwaitat et al. [46]	Blockchain, Medium Access Control (MAC), hash function, Support Vector Machine (SVM), homomorphic encryption	+ Reduced latency and improved performance and security	– Unable to classify users based on trust
Kim et al. [48]	Blockchain, hash functions, XOR	+ Provides mutual authentication and secure key agreement	– Computational cost is higher in this model
Wang et al. [49]	Blockchain, hash function, bitwise-XOR	+ Reduced computational overhead	– Multi-chain synchronization and state consistency are not explored
Ju et al. [50]	PUF, hash functions, blockchain	+ Mitigating the risks of common security attacks	– The delay was introduced due to an increase in computation cost

A substantial amount of research in recent years has been directed towards the development of authentication mechanisms to avoid unauthorized access and ensure the security and privacy of sensed data, whether it is on a distributed or centralized IoT network. However, the rapid growth of smart network usage further increases cyber-attacks, challenging existing schemes. Presently, there is an urgent need for a more robust, lightweight authentication method with the potential to identify users and devices reliably while providing strong security assurance. Despite the current authentication schemes being used in the IoT setting, which can be seen as a positive move towards improving security and privacy, there are a number of underlying limitations that have not been addressed yet. Through this, overall performance and resilience to large-scale or adversarial IoT deployments are typically uncharted territory, as in the study by Verma and Bhardwaj [30], where performance is not evaluated on a performance-scale basis.

Authentication methods relying on biometrics are better at identity assurance, but they are often vulnerable to privacy violations because of on-board biometric template storage or inadequate security controls. Such constraints exist since biometric security is frequently discussed as an independent concept, along with trust management and decentralized control, resulting in systems that are reliable in solitude but brittle in integrated IoT systems. Likewise, the use of blockchain-based authentication schemes can effectively solve the challenges of decentralization and of trust, but present too much overhead in computations and communication because of their complicated consensus protocol and smart contract execution, and thus are not applicable to IoT devices with limited resources. Unlike in previous literature, the proposed protocol is fundamentally different as it combines biometric hashing and decentralized authentication using smart contracts in one lightweight protocol. The proposed solution avoids the raw biometric storage, considers the overhead of the blockchain interaction, and the absence of centralized authorities, which is why the proposed solution will target the underlying causes of the limitations found in the current literature, as opposed to addressing them as independent problems.

3. PROPOSED METHOD

In the design of a decentralized, secure, lightweight protocol for mutual authentication and key agreement for IoT enabled smart networks. The framework combines blockchain technology and biometric hashing within resource-constrained IoT networks to deliver robust security and privacy protection during data exchange by utilizing hash functions, XOR, and symmetric cryptography. To securely store credential records and effectively verify user identities before granting access to sensed data, blockchain technology is utilized for its intrinsic properties of tamper resistance, immutability, and distributed trust. Additionally, biometric hashing is applied to transform and securely store biometric characteristics and authentication components as a block in the blockchain, ensuring integrity and resistance against different types of assaults. Moreover, incorporating hash functions, XOR, and symmetric cryptography creates a lightweight authentication and key agreement system, rendering the scheme exceptionally well-suited for secure and reliable communication in smart IoT settings.

3.1 System architecture

In this work, the general idea of the system architecture is modelled in Figure 3. The system consists of five components: users with biometric scanners, gateways, blockchain, smart contracts, and IoT devices.

It is designed and optimized for secure authentication and lightweight decentralized credential verification through blockchain gateways. The simple way of integrating blockchain into IoT involves establishing gateways that function as a blockchain across different IoT networks, as it requires only a shared ledger for storing credential records of users and devices. This avoids the need for extra complex infrastructure to construct a blockchain. In the proposed architecture, users and IoT devices function as endpoints that perform registration and interact with the system via an adjacent gateway device in the IoT network. The gateways of different networks form a blockchain to maintain a copy of identity authentication, key generation, and distribution in blockchain consensus. The blockchain keeps and shares ledgers of trusted individuals' credentials, ensuring secure, immutable, tamper-resistant, and decentralized authentication. A block in blockchain stores credentials, secret keys, and authenticators along with the hash of these values, the current timestamp, and the hash of the previous block. Furthermore, smart contracts on top of the blockchain of gateway nodes automate and enforce the rules for user authentication and key distribution, enabling seamless and secure exchange among users and IoT nodes.

The design presented makes the gateways of various IoT networks a permissioned blockchain that is managed at the gateway level. Practical Byzantine Fault Tolerance (PBFT) fits more with consortium blockchain or permissioned blockchain setups, in which other gateways are authenticated and partially trusted entities. The PBFT consensus mechanism supports rapid block verification with finality determinism and has a much lower transaction latency than public blockchain mechanisms. The fact that consensus is reached when messages are exchanged amongst a small number of gateway nodes ensures that the computational and energy needs are within the reach of gateway devices, hence maintaining throughput and scalability to IoT deployments.

Implementation of the PBFT-based consensus mechanism has direct consequences on the performance of the system in reducing the authentication latency and communication overheads. Since PBFT does not use cryptographic puzzles and mining, it does not use a lot of energy and minimizes the time to confirm a block, which is crucial to real-time authentication of IoT. In addition, the ability to restrict blockchain involvement to gateways makes sure that resource-constrained IoT devices cannot take part in consensus mechanisms, so that end devices remain lightweight and yet enjoy the benefits of decentralized trust management. The chosen consensus mechanism offers a fair trade-off between security, latency, and throughput, which is why it should be used in scalable and time-sensitive IoT.

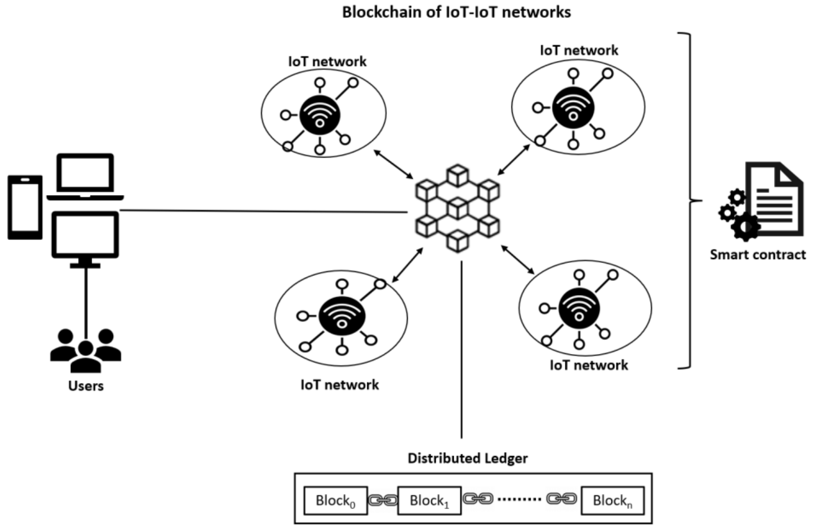


Figure 3. System architecture of blockchain-based IoT-IoT networks

3.2 Proposed authentication and key distribution protocol

The proposed protocol employs 5 phases. Initial setup, user registration, device registration, authentication and key agreement, and update phases. Table 2 provides the notation used in the proposed scheme along with descriptions.

Table 2. Notations and their descriptions

Notation(s)	Descriptions
U_x	User entity
D_x	IoT device
G_x	Gateway node
ID_u, ID_d	User ID and Device ID
PW_u, PW_d	User/Device password
N_1, N_2, U_1,U_2	Random nonces
K_{gu}, K_{gd}	Keys shared between the gateway-device and the gateway-user
ID_g, K_g	ID and master key of the gateway
Biou	Biometric user input
BH_u	Biometric hash of the user
T_i, TC, ΔT	Timestamp, current timestamp, and maximum delay
BC	Blockchain ledger entry
SK	Session key
H(.)	Secure hash function
$\oplus$	XOR operation
E_{Ki} / D_{Ki}	Symmetric encryption with secret key K_i
R_i	Random numbers

3.2.1 Initial setup

Assuming that gateways with identity, ID_g, and master keys, K_g, from different IoT networks form a blockchain network to serve as a distributed ledger for recording user and device registrations, storing and updating credentials. Furthermore, all the entities involved in the communication are assumed to be synchronized with their clocks. The extraction of unique characteristics from biometric traits involves different methodologies, each specific to the type of biometric data. Therefore, we assume that the IoT system uses specific methodologies for the feature extraction and biometric template generation. Figure 4 shows the general method to generate a hash value from biometric data.

3.2.2 User registration phase

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

1. The user, U_x records the system timestamp, T_1, chooses ID_u, PW_u, captures biometric input B_{iou}, generates nonce, N_1, and computes $BH_u = H(B_{iou})$, $M_u = H(ID_u \| PW_u \| BH_u)$, $M_b = BH_u \oplus H(M_u \| N_1 \| T_1))$, $RN_u = N_1 \oplus H(ID_u \| M_b \| T_1)$ and sends $\langle ID_u, M_b, M_b, RN_u, T_1 \rangle$ to the gateway node, G_x through the secure channel.
2. The Gateway, $G_{x,}$ receives the message and terminates if $|TC\text{-}T_1| > \Delta T$. Else, verifies uniqueness of ID_u. If valid, then computes $N_1{}^* = RN_u \oplus H(ID_u \| M_b \| T_1)$ and $BH_u{}^* = M_b \oplus H(M_u \| N_1{}^* \| M_u \| T_1)$. Then, selects RU, records timestamp, T_2, and generates key based on the biometric, $K_{gu} = H(BH_u{}^* \| M_u \| H(RU \| N_1{}^* \| K_g))$. Then computes $V_u = H(ID_u \| ID_g \| H(M_u \| K_g \| K_{gu}))$, $MV_u = V_u \oplus H(M_u \| N_1{}^* \| K_{gu} \| T_2)$, $MK_{gu} = H(K_{gu} \| M_u \| H(K_{gu} \| N_1{}^* \| MV_u) \| T_2)$, $RK_{gu} = K_{gu} \oplus H(MK_{gu} \| N_1{}^* \| T_2)$ and creates a blockchain entry, BC_user = $(ID_u,M_{u,}BH_u,K_{gu},V_u,T_2$, Prev_Hash).Now, appends BC_user to blockchain and sends the message $\langle MV_u, MK_{gu}, RK_{gu}, TS_2 \rangle$ to user.
3. After receiving, U_x rejects if $|TC\text{-}T_2| > \Delta T$. Else, computes $K_{gu}{}^* = RK_{gu} \oplus H(MK_{gu} \| N_1 \| MV_u \| T_2)$, $MK_{gu}{}^* = H(K_{gu}{}^* \| M_u \| H(K_{gu}{}^* \| N_1 \| MV_u) \| T_2)$ and checks$MK_{gu}{}^*$? = MK_{gu}.

If yes, computes $V_u{}^* = MV_u \oplus H(M_u \| N_1 \| K_{gu}{}^* \| T_2)$ then stores $\{M_u, BH_u, K_{gu}, V_u\}$securely in local memory.

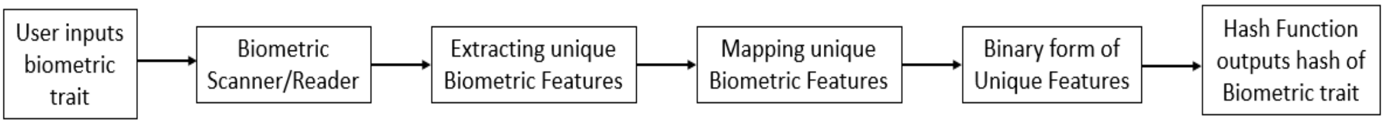

User inputs biometric trait
Biometric Scanner/Reader
Extracting unique Biometric Features
Mapping unique Biometric Features
Binary form of Unique Features
Hash Function outputs hash of Biometric trait

Figure 4. Process of generating a hash value from a biometric trait

3.2.3 Device registration phase

The device D_x registers with a gateway node in the nearby IoT network as follows:

1. The device, D_x, records timestamp, T_3, and chooses ID_d, PW_d, generates nonce, $N_{2,}$ and computes $M_d = H(ID_d \| PW_d)$, $RN_n = N_2 \oplus H(ID_d \| M_d \| T_3)$ and sends $\langle ID_d, M_d, RN_n, T_3 \rangle$ to the gateway G_x.
2. The gateway $G_{x,}$ receives the message and terminates if $|TC\text{-}T_3| > \Delta T$. Else, verifies ID_d. If doesn't exist, computes $N_2{}^* = RN_n \oplus H(M_d \| ID_d \| T_3)$, selects RD, generates key $K_{gd} = H(M_d \| H(RD \| N_2{}^* \| K_g))$,$V_d = H(ID_d \| ID_g \| H(M_d \| K_{gd} \| K_g))$, $MV_d = V_d \oplus H(M_d \| N_2{}^* \| K_{gd})$, $MK_{gd} = H(K_{gd} \| M_d \| H(K_{gd} \| N_2{}^* \| MV_d) \| T_4)$, $RK_{gd} = K_{gd} \oplus H(MK_{gd} \| N_2{}^* \| T_4)$ and create blockchain entry, BC_device = $(ID_d, M_d,V_d, K_{gd}, T_4$, Prev_Hash). Append BC_device to blockchain and send $\langle MV_d, MK_{gd}, RK_{gd}, T_4 \rangle$ to device.
3. After receiving the message, D_x rejects if $|TC\text{-}T_4| > \Delta T$. Else, recovers$K_{gd}{}^* = RK_{gd} \oplus H(MK_{gd} \| N_2 \| T4)$, $MK_{gd}{}^* = H(K_{gd} \| M_d \| H(K_{gd} \| N_2 \| MV_d) \| T_4)$, and verifies $MK_{gd}{}^*$? = MK_{gd}. If yes, computes $V_d{}^* = MV_d \oplus H(M_d \| N_2 \| K_{gd} \| T_4)$ then stores $\{M_d, V_d, K_{gd}\}$ in local memory.

The user and device register with the nearby gateway, and their blocks are stored in the distributed ledger of the blockchain. Figure 5 demonstrates the process of user and device registrations.

3.2.4 Authentication and key distribution phase

The mutual authentication and key distribution between the user and device are as follows:

1. The user U_x initiates the login process by providing ID_u, PW_u, B_{iou}, and computes $BH_u = H(B_{iou})$ and $M_u = H(ID_u \| PW_u \| BH_u)$. The computed M_u validated against stored M_u.If yes, then user generates U_1, computes AuthToken = $H(ID_u \| K_{gu} \| H(BH_u \| V_u \| U_1))$, Masked = AuthToken$\oplus H(U_1 \| T_1 \| H(V_u \| K_{gu} \| ID_u))$, Nonce_mask = $U_1 \oplus H(\text{Masked} \| T_1)$, UID_mask = $ID_u \oplus H(\text{Masked} \| H(\text{Nonce\_mask} \| U_1 \| T_1))$, DID_mask = $ID_d \oplus H(H(U_1 \| ID_u \| \text{AuthToken}) \| T_1)$ and sends $\langle T_1$, Nonce_mask, UID_mask, Masked, DID_mask$\rangle$ to gateway, G_x.
2. Upon receiving, G_x verifies T_1 and computes $U_1{}^*$ =

$Nonce\_mask \oplus H(Masked \| T_1)$ and$ID_u^* = UID_mask \oplus H(Masked \| H(Nonce_mask \| U_1^* \| T_1))$. Then, it searches ID_u^* in the blockchain and obtains the user's credential record. Now, computes AuthToken * = Masked $\oplus H(U_1 \| T_1 \| H(V_u \| K_{gu} \| ID_u))$ with received values and AuthToken = $H(ID_u^* \| K_{gu} \| H(BH_u \| V_u \| U_1^* \| T_1))$ with retrieved values from the user's block. Then, validates U_x by comparing AuthToken with AuthToken*. If both are the same, extracts ID_d from DID_mask by calculating $ID_d^* = DID\_mask \oplus H(H(U_1^* \| ID_u^* \| AuthToken^*) \| T_1)$. Now, verifies ID_d against the device's block in the blockchain. If yes, selects R_1 and U_2, and generates shared session key, $SK = H(K_{gu} \| K_{gd} \| K_g \| H(R_1 \| V_u \| V_d))$. It then computes $E_u = SK \oplus H(K_{gu} \| V_u \| U_2)$, $ME_u = H(SK \| ID_d \| U_2 \| T_2)$, $E_d = SK \oplus H(K_{gd} \| V_d \| U_2)$, $ME_d = H(SK \| ID_u \| U_2 \| T_2)$, and finally sends $E_{Kgu}(ME_u, E_u, U_2, T_2)$ and $E_{Kgd}(ID_u, ME_d, E_d, U_2, T_2)$ to the user and device, respectively.

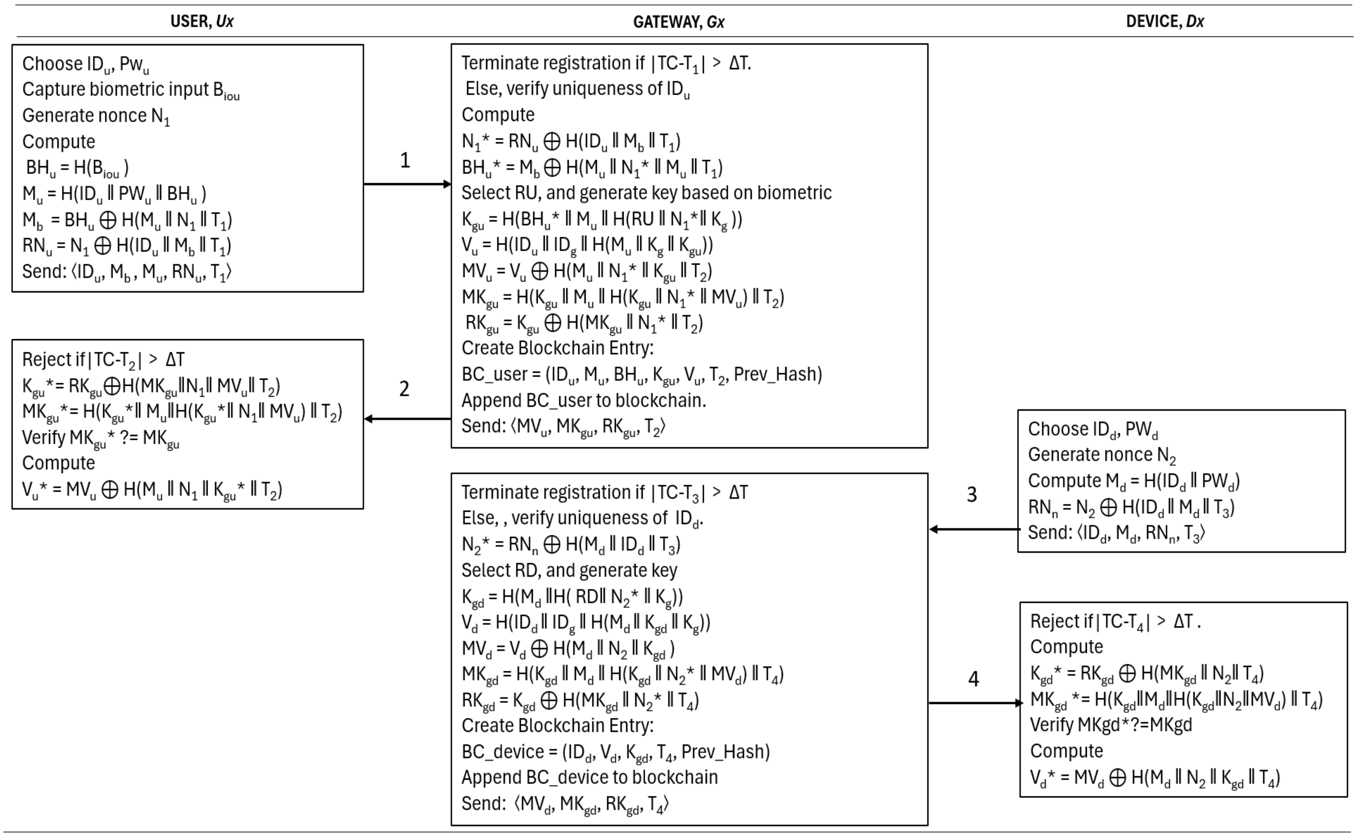

USER, *Ux*
GATEWAY, *Gx*
DEVICE, *Dx*
Choose ID_u, Pw_u
Capture biometric input B_{iou}
Generate nonce N_1
Compute
$BH_u = H(B_{iou})$
$M_u = H(ID_u \| PW_u \| BH_u)$
$M_b = BH_u \oplus H(M_u \| N_1 \| T_1)$
$RN_u = N_1 \oplus H(ID_u \| M_b \| T_1)$
Send: $\langle ID_u, M_b, M_u, RN_u, T_1 \rangle$
1
Terminate registration if $|TC-T_1| > \Delta T$.
Else, verify uniqueness of ID_u
Compute
$N_1^* = RN_u \oplus H(ID_u \| M_b \| T_1)$
$BH_u^* = M_b \oplus H(M_u \| N_1^* \| M_u \| T_1)$
Select RU, and generate key based on biometric
$K_{gu} = H(BH_u^* \| M_u \| H(RU \| N_1^* \| K_g))$
$V_u = H(ID_u \| ID_g \| H(M_u \| K_g \| K_{gu}))$
$MV_u = V_u \oplus H(M_u \| N_1^* \| K_{gu} \| T_2)$
$MK_{gu} = H(K_{gu} \| M_u \| H(K_{gu} \| N_1^* \| MV_u) \| T_2)$
$RK_{gu} = K_{gu} \oplus H(MK_{gu} \| N_1^* \| T_2)$
Create Blockchain Entry:
BC_user = $(ID_u, M_u, BH_u, K_{gu}, V_u, T_2, Prev\_Hash)$
Append BC_user to blockchain.
Send: $\langle MV_u, MK_{gu}, RK_{gu}, T_2 \rangle$
2
Reject if $|TC-T_2| > \Delta T$
$K_{gu}^* = RK_{gu} \oplus H(MK_{gu} \| N_1 \| MV_u \| T_2)$
$MK_{gu}^* = H(K_{gu}^* \| M_u \| H(K_{gu}^* \| N_1 \| MV_u) \| T_2)$
Verify $MK_{gu}^* ?= MK_{gu}$
Compute
$V_u^* = MV_u \oplus H(M_u \| N_1 \| K_{gu}^* \| T_2)$
Choose ID_d, PW_d
Generate nonce N_2
Compute $M_d = H(ID_d \| PW_d)$
$RN_n = N_2 \oplus H(ID_d \| M_d \| T_3)$
Send: $\langle ID_d, M_d, RN_n, T_3 \rangle$
3
Terminate registration if $|TC-T_3| > \Delta T$
Else, , verify uniqueness of ID_d.
$N_2^* = RN_n \oplus H(M_d \| ID_d \| T_3)$
Select RD, and generate key
$K_{gd} = H(M_d \| H(RD \| N_2^* \| K_g))$
$V_d = H(ID_d \| ID_g \| H(M_d \| K_{gd} \| K_g))$
$MV_d = V_d \oplus H(M_d \| N_2 \| K_{gd})$
$MK_{gd} = H(K_{gd} \| M_d \| H(K_{gd} \| N_2^* \| MV_d) \| T_4)$
$RK_{gd} = K_{gd} \oplus H(MK_{gd} \| N_2^* \| T_4)$
Create Blockchain Entry:
BC_device = $(ID_d, V_d, K_{gd}, T_4, Prev\_Hash)$
Append BC_device to blockchain
Send: $\langle MV_d, MK_{gd}, RK_{gd}, T_4 \rangle$
4
Reject if $|TC-T_4| > \Delta T$.
Compute
$K_{gd}^* = RK_{gd} \oplus H(MK_{gd} \| N_2 \| T_4)$
$MK_{gd}^* = H(K_{gd} \| M_d \| H(K_{gd} \| N_2 \| MV_d) \| T_4)$
Verify MKgd*?=MKgd
Compute
$V_d^* = MV_d \oplus H(M_d \| N_2 \| K_{gd} \| T_4)$

Figure 5. Registration phases of user and device in the blockchain-based IoT-IoT networks

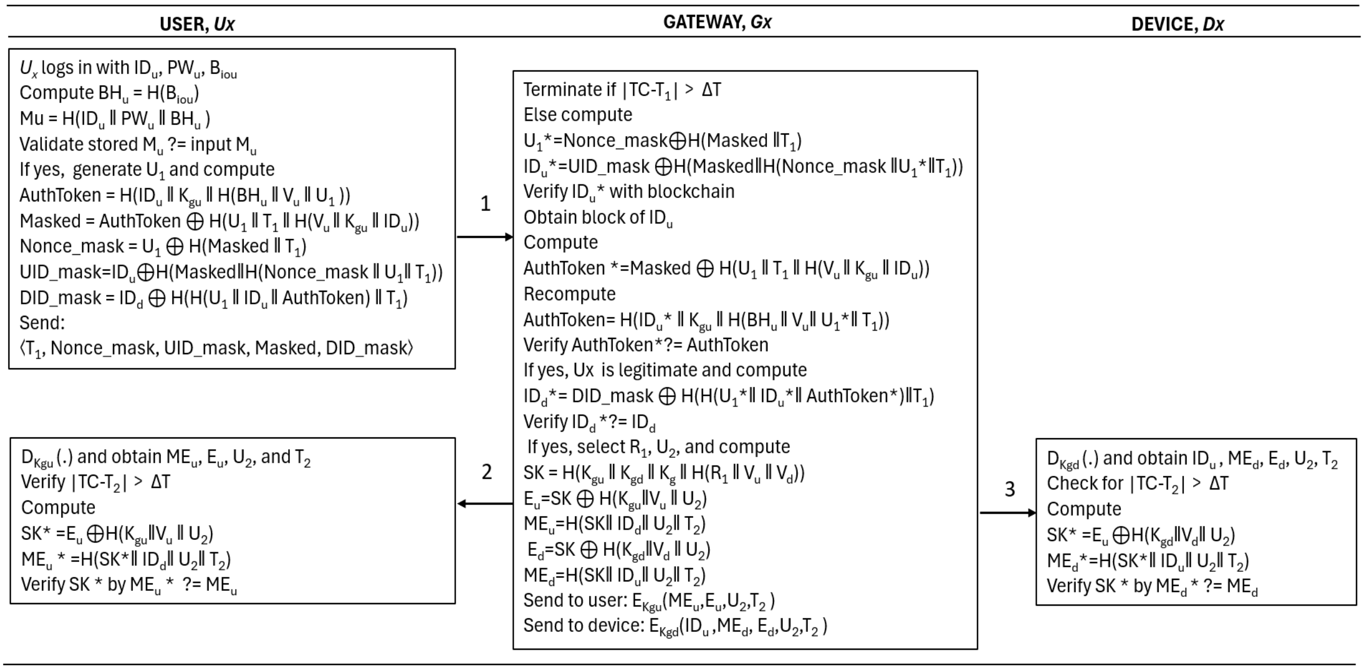

USER, *Ux*
GATEWAY, *Gx*
DEVICE, *Dx*
U_x logs in with ID_u, PW_u, B_{iou}
Compute $BH_u = H(B_{iou})$
$Mu = H(ID_u \| PW_u \| BH_u)$
Validate stored M_u ?= input M_u
If yes, generate U_1 and compute
$AuthToken = H(ID_u \| K_{gu} \| H(BH_u \| V_u \| U_1))$
$Masked = AuthToken \oplus H(U_1 \| T_1 \| H(V_u \| K_{gu} \| ID_u))$
$Nonce\_mask = U_1 \oplus H(Masked \| T_1)$
$UID\_mask = ID_u \oplus H(Masked \| H(Nonce\_mask \| U_1 \| T_1))$
$DID\_mask = ID_d \oplus H(H(U_1 \| ID_u \| AuthToken) \| T_1)$
Send:
$\langle T_1$, Nonce_mask, UID_mask, Masked, DID_mask$\rangle$
1
Terminate if $|TC-T_1| > \Delta T$
Else compute
$U_1^* = Nonce\_mask \oplus H(Masked \| T_1)$
$ID_u^* = UID\_mask \oplus H(Masked \| H(Nonce\_mask \| U_1^* \| T_1))$
Verify ID_u^* with blockchain
Obtain block of ID_u
Compute
$AuthToken^* = Masked \oplus H(U_1 \| T_1 \| H(V_u \| K_{gu} \| ID_u))$
Recompute
$AuthToken = H(ID_u^* \| K_{gu} \| H(BH_u \| V_u \| U_1^* \| T_1))$
Verify AuthToken*?= AuthToken
If yes, Ux is legitimate and compute
$ID_d^* = DID\_mask \oplus H(H(U_1^* \| ID_u^* \| AuthToken^*) \| T_1)$
Verify $ID_d^* ?= ID_d$
If yes, select R_1, U_2, and compute
$SK = H(K_{gu} \| K_{gd} \| K_g \| H(R_1 \| V_u \| V_d))$
$E_u = SK \oplus H(K_{gu} \| V_u \| U_2)$
$ME_u = H(SK \| ID_d \| U_2 \| T_2)$
$E_d = SK \oplus H(K_{gd} \| V_d \| U_2)$
$ME_d = H(SK \| ID_u \| U_2 \| T_2)$
Send to user: $E_{Kgu}(ME_u, E_u, U_2, T_2)$
Send to device: $E_{Kgd}(ID_u, ME_d, E_d, U_2, T_2)$
2
$D_{Kgu}(.)$ and obtain ME_u, E_u, U_2, and T_2
Verify $|TC-T_2| > \Delta T$
Compute
$SK^* = E_u \oplus H(K_{gu} \| V_u \| U_2)$
$ME_u^* = H(SK^* \| ID_d \| U_2 \| T_2)$
Verify SK * by $ME_u^* ?= ME_u$
3
$D_{Kgd}(.)$ and obtain ID_u, ME_d, E_d, U_2, T_2
Check for $|TC-T_2| > \Delta T$
Compute
$SK^* = E_u \oplus H(K_{gd} \| V_d \| U_2)$
$ME_d^* = H(SK^* \| ID_u \| U_2 \| T_2)$
Verify SK * by $ME_d^* ?= ME_d$

Figure 6. Authentication and key distribution phases of the protocol

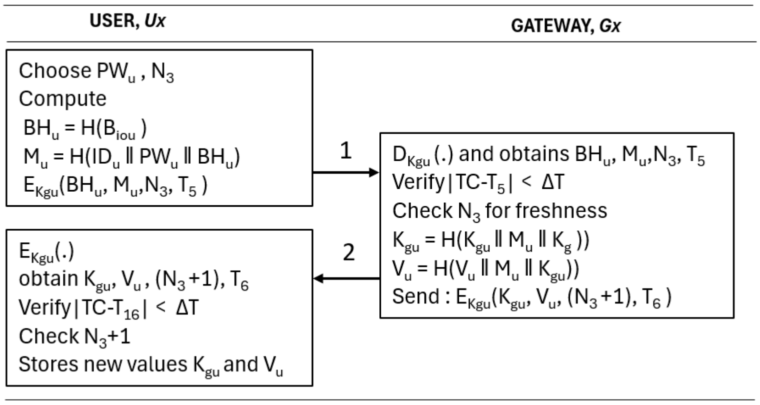

USER, Ux
GATEWAY, Gx
Choose PW_u , N_3
Compute
$BH_u = H(B_{iou})$
$M_u = H(ID_u \| PW_u \| BH_u)$
$E_{Kgu}(BH_u, M_u, N_3, T_5)$
1
$D_{Kgu}(.)$ and obtains BH_u, M_u, N_3, T_5
Verify $|TC-T_5| < \Delta T$
Check N_3 for freshness
$K_{gu} = H(K_{gu} \| M_u \| K_g))$
$V_u = H(V_u \| M_u \| K_{gu}))$
Send : $E_{Kgu}(K_{gu}, V_u, (N_3+1), T_6)$
2
$E_{Kgu}(.)$
obtain K_{gu}, V_u , (N_3+1), T_6
Verify $|TC-T_{16}| < \Delta T$
Check N_3+1
Stores new values K_{gu} and V_u

Figure 7. Update phases of the protocol

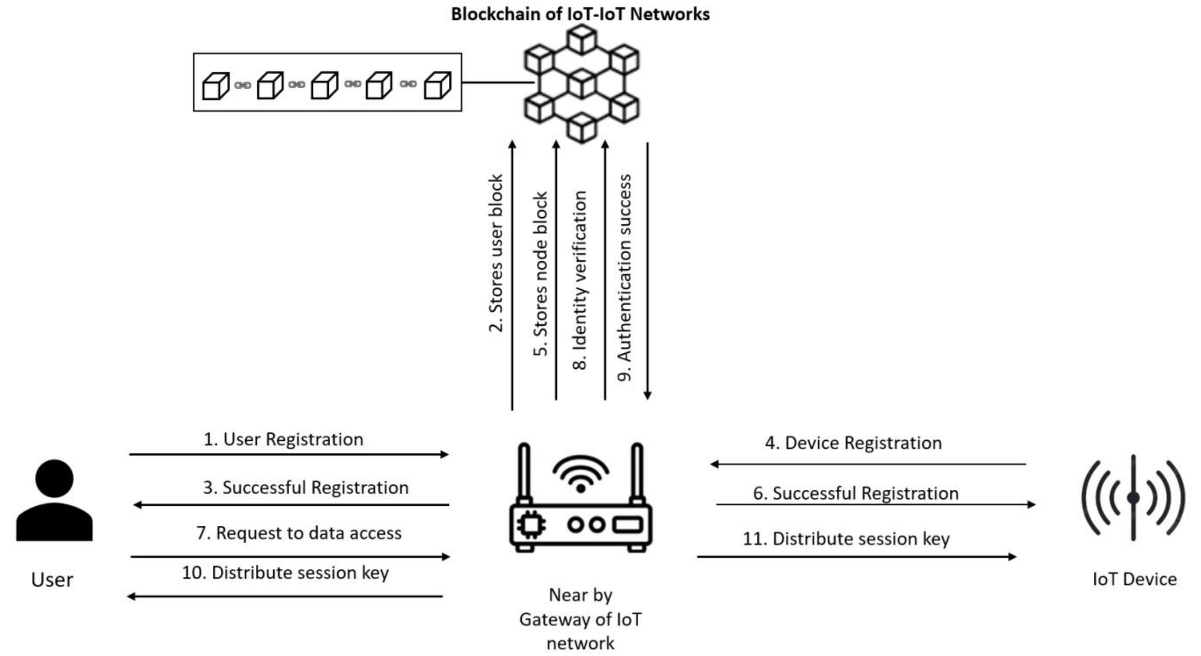

Blockchain of IoT-IoT Networks
2. Stores user block
5. Stores node block
8. Identity verification
9. Authentication success
1. User Registration
3. Successful Registration
7. Request to data access
10. Distribute session key
4. Device Registration
6. Successful Registration
11. Distribute session key
User
Near by Gateway of IoT network
IoT Device

Figure 8. Overview of the registration, authentication, and key distribution process using biometric hashing and blockchain

3. After receiving, the user decrypts the message $D_{Kgu}(.)$ and obtains ME_u, E_u, U_2, and T_2 elements. Now, the user computes $SK^* = E_u \oplus H(K_{gu} \| V_u \| U_2)$ and verifies SK * by $ME_u ? = H(SK^* \| ID_u \| U_2 \| T_2)$. If yes, meaning the user, U_x, successfully verified the device, D_x, legitimacy through the gateway, G_x.
4. Device also decrypts the message $D_{Kgd}(.)$ after receiving from the gateway, and obtains ID_u, ME_d, E_d, U_2, and T_2 elements. Now, the device reconstructs $SK^* = E_u \oplus H(K_{gd} \| V_d \| U_2)$ and verifies SK * by $ME_d? = H(SK^* \| ID_u \| U_2 \| T_2)$. If yes, meaning the device verified legitimacy of the user through the gateway, G_x.

The user and device are having a session key, which is distributed by the nearby blockchain gateway. Now, both the user and device can communicate securely with the secret session key, SK. Figure 6 demonstrates the process of authentication and key distribution.

3.2.5 Update phase

The user U_x, selects a new password, PW_u, then N_3, computes $BH_u = H(B_{iou})$, $M_u = H(ID_u \| PW_u \| BH_u)$ and sends $E_{Kgu}(BH_u, M_u, N_3, T_5)$ to the gateway, G_x. Upon receiving, the gateway decrypts it and verifies the timestamp $|TC-T_5| < \Delta T$ and the freshness of N_3. It then, computes $K_{gu} = H(K_{gu} \| M_u \| K_g))$ and $V_u = H(V_u \| M_u \| K_{gu}))$, and responds with $E_{Kgu}(K_{gu}, V_u, (N_3 + 1), T_6)$. Also, it updates user's block in the blockchain with the new K_{gu} and V_u values. After receiving the response, the user decrypts the message and verifies $|TC-T_6| < \Delta T$ and $N_3 + 1$, and updates its local values of K_{gu} and V_u accordingly. The entire process is shown in Figure 7.

The overview of registration, authentication, and key distribution using biometric hashing and Blockchain is depicted in Figure 8.

4. RESULTS AND DISCUSSIONS

Informal analysis of standard security parameters and formal analysis with the Automated Validation of Internet Security Protocols and Application (AVISPA) tools are discussed to evaluate the security of the proposed protocol.

4.1 Informal analysis

1. Replay attacks

A replay attack occurs when an adversary intercepts the message and retransmits previously stolen valid messages to gain unauthorized access. In our scheme, timestamps (T_i) and nonces (N_i, U_i) are used to ensure message freshness and prevent reuse of old messages. Moreover, nonces are masked with the XOR operation to enhance unpredictability. Each entity confirms the recency of the received message by checking the validity of the timestamp before proceeding with further computations. Consequently, any replayed or delayed message is immediately detected and discarded. Hence, the suggested protocol is immune to replay attacks.

2. User impersonation attack

An impersonation attack occurs when an adversary attempts to assume the identity of a legitimate user to gain unauthorized access. The proposed scheme mitigates such attacks effectively by integrating biometric hashing, session-dependent randoms, and mutual identification mechanisms. Moreover, during the registration and login phases, biometric input, B_{iou}, is transformed into biometric hash, $BH_u = H(B_{iou})$, which is combined with identity and password to compute $M_u = H(ID_u \| PW_u \| BH_u)$. This multi-factor hashing ensures that the authentication credentials are strongly user-specific and non-reproducible. Moreover, the raw biometric data are never stored or transmitted, making it infeasible for an attacker to spoof valid biometric features. Thus, the proposed biometric-based-scheme provides strong resistance to user impersonation attacks.

3. Man in the Middle attack

Mutual check elements, K_{gu} and V_u, along with nonce, U_1, and timestamp T_1, prove that the user is a trusted entity; later gateway returns masked SK with hash, which proves the ability of creating and distributing the session key. These are the anti-mechanisms to limit MIMT attacks. User/device specific values. V_u and V_d, are used to derive the session keys, SK. An attacker can manipulate the verification process to create uneven hashes or keys, which would result in rejection. Thus, the protocol effectively avoids an adversary to impersonate legitimate entity.

4. Anonymity

Anonymity ensures that the true identity of the entity remains concealed during authentication. The proposed scheme achieves anonymity by masking user and device identities by UID_mask = $ID_u \oplus H(Masked \| H(Nonce\_mask \| U_1 \| T_1)$ and DID_mask = $ID_d \oplus H(H(U_1 \| ID_u \| AuthToken) \| T_1)$ for transmission. Moreover, all transmitted parameters are strongly tied to time-variant values, such as T_i and U_i, ensuring that the same user generates different encrypted identities across sessions. Consequently, by observing traffic, an adversary can't trace user identities and activities. Hence, the protocol ensures anonymity.

5. User untraceability

Untraceability guarantees that an adversary cannot link multiple sessions to the same user. This is ensured by an element, UID_mask, a different mask of ID_u for each session, constructed based on session specific values AuthToken, Nonce_mask, U_1, and T_1. This process makes allows an eavesdropper cannot link across sessions. Thus, the proposed protocol achieves unlikability across sessions.

6. Biometric privacy

Biometric input, B_{iou}, is used during registration. Biometric input, B_{iou}, is converted into a unique biometric hash value, BH_u, which is combined with the ID_u and PW_d. This process ensures that the biometric template is never stored or transmitted in its raw form, thus preserving biometric privacy and preventing linkage across sessions.

The proposed protocol offers biometric privacy through a biometric hashing mechanism which avoids biometric data that has not been stored, sent, or rebuilt. This system uses a secure biometric hash, which is created by a one-way cryptograph hash algorithm in connection with randomness that is specific to the user. This is in line with the well-established biometric template protection systems, such as fuzzy extractors, as well as cancellable biometrics. Even though an adversary gets access to the stored hash values in the blockchain or at the gateway, the preimage resistance property of the hash-function ensures that one cannot reconstruct biometric properties.

As well, unlinkability of sessions between protocols is also provided by introducing new session-specific randomness through the creation of the biometric hash. The biometric hashes that have been calculated during a single authentication are computationally independent, and the adversaries cannot be capable of matching authentication of the same user by attempting to match the hash outputs with hash comparison attacks. Attacks are not resistant to the cross-matching and replay attacks because biometric hashes are fixed to dynamic session parameters, and challenges are confirmed using smart contracts. As such, no proper authentication is related to replaying the already intercepted authentication messages since the biometric hash cannot be reused or appended to subsequent sessions. Overall, the suggested scheme with no official principles of biometric protection and cryptographic security ensures high biometric privacy in both the active and passive adversarial models.

7. Mutual authentication

The protocol ensures mutual authentication by verifying both the user's and IoT device's identities through a gateway using encrypted exchanges, $E_{Kgu}(ME_u,E_u,U_2,T_2)$ and $E_{Kgd}(ME_d,ID_u, E_d,U_2,T_2)$. The elements, ME_u and ME_d, derived from session key SK and entity -specific parameters, are used to ensure mutual authentication between user and device.

8. Eavesdropping attack

Unauthorized interception of data in transit over an insecure network is difficult in the proposed protocol since authentication and data access request messages and key distribution messages are done by masking and encrypting elements. The messages {T_1, Nonce_mask, UID_mask, Masked, DID_mask} and $E_{Kgu}(ME_u,E_u,U_2,T_2)$ and $E_{Kgd}(ME_d,E_d,U_2,T_2)$ used are data request and session key distribution messages, respectively, contains masked, hashed, and encrypted values. If an adversary steals these messages, it cannot lead to leakage of credential records since most of the elements are session specific.

9. Key compromise impersonation attack

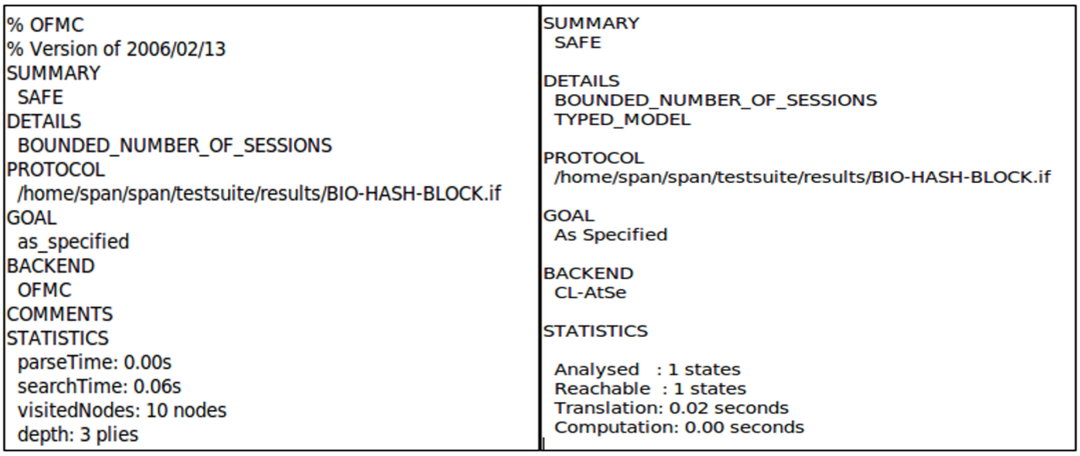
The new key values, K_{gu}, K_{gd}, and K_g are generated during the update phase after completion of the data exchange. Suppose an old key is compromised, the protocol invalidates it and won't allow the attacker to access the sensed data. Compromising keys alone should not be possible to impersonate the entities in the network. Knowledge of nonces and session key also required. Moreover, nonces ensure that keys cannot be reused maliciously.

10. Secure key exchange

Session key computed as $SK = H(K_{gu} \| K_{gd} \| K_g \| H(R_1 \| V_u \| V_d))$, which includes secret keys, Ki, authenticators, V_u, and V_d, and a random number, R_1. Later, it is masked and hashed with nonce, timestamps, and other entity specific elements, by computing $E_u = SK \oplus H(K_{gu} \| V_u \| U_2)$, $ME_u = H(SK \| ID_u \| U_2 \| T_2)$, $E_d = SK \oplus H(K_{gd} \| V_d \| U_2)$, and $ME_d = H(SK \| ID_d \| U_2 \| T_2)$. Then, securely exchanged by the symmetric encryption. Thus, we conclude that the session key for the user and device is exchanged securely.

4.2 Formal security analysis

AVISPA is a reliable tool for formally verifying any type of security protocol, which is coded as a role-based description and security goals in High-Level Protocol Specification Language (HLPSL), using Security Protocol ANalyzer (SPAN) to determine whether it is safe, unsafe, or inconclusive [52]. Registration, authentication, and key agreement are implemented with specific roles, sessions, and goals to defend against attacks, including impersonation, replay, and MITM. Figure 9 shows the results from AVISPA's formal analysis engines, On-the-Fly Model Checker (OFMC) and Constraint-Logic-based Attack Searcher (CL-AtSe), with the SPAN simulation.



```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/BIO-HASH-BLOCK.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.06s
 visitedNodes: 10 nodes
 depth: 3 plies
```

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/BIO-HASH-BLOCK.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 1 states
 Reachable  : 1 states
 Translation: 0.02 seconds
 Computation: 0.00 seconds
```

Figure 9. Automated Validation of Internet Security Protocols and Application (AVISPA) results of the proposed protocol

5. PERFORMANCE EVALUATION

Performance is demonstrated by comparing the proposed protocol with other related works that exist in the literature [34, 38, 39, 48, 50, 51] in the context of security features, computation cost, and communication cost. The scheme is proven to be suitable for smart environments with resource constraints.

5.1 Security features

Security features serve as fundamental criteria for evaluating the strength of the authentication protocol against a diverse array of cyber-attacks. The robustness of the proposed one is demonstrated in comparison with existing methods in the literature, based on key security features summarized in Table 3.

Table 3. Comparison of security parameters with related works in the literature

Attack	Alruwaili et al. [34]	Rana et al. [38]	Darman et al. [39]	Kim et al. [48]	Ju el al. [50]	Bera et al. [51]	Proposed
Replay Attack	√	√	√	√	√	√	√
Anonymity	√	√	√	√	√	√	√
User Untreceability	×	√	×	√	×	×	√
Biometric Privacy	×	NA	×	×	NA	×	√
Mutual Authentication	√	√	√	√	√	√	√
Secure Key Exchange	×	√	√	×	√	√	√
Blockchain Solution	×	×	×	√	√	√	√

Note: √: Secured; ×: Not Secured; NA: Not Applicable.

5.2 Computation cost

To prove the computational efficiency of the suggested protocol, we consider the authentication and key distribution phase. The process of computing cost includes feature extraction, hash function, and symmetric encryption/decryption, while XOR and concatenation have negligible overhead. According to the study by Huang [53], the execution times of extracting biometric features are 1.989 ms, one-way hash function T_H is 0.0026 ms, point multiplication T_{PM} is 1.989 ms, and symmetric encryption/decryption T_{EN} is 0.00325ms. The computation cost of the proposed protocol includes $20T_H$, $4T_{EN}$, and $1T_{FE}$operations. The estimated execution time of the proposed protocol is 2.05864 ms. Table 4 presents the comparison of the computational cost of the suggested protocol with similar contributions in the literature.

Table 4. Comparison of computational cost

Scheme	Total Cost	Estimated Execution Time (Milli Seconds)
Alruwaili et al. [34]	$25T_H + 40T_{EN} + 7T_{FE}$	14.118
Rana et al. [38]	$25\ T_H + 5\ T_{PM}$	10.0742
Darman et al. [39]	$40T_H + 16T_{PM} + 2T_{EN}$	31.9345
Kim et al. [48]	$38T_H + 1T_{FE}$	2.0878
Ju et al. [50]	$32T_H + 1T_{FE}$	2.06452
Bera et al. [51]	$21T_H + 5\ T_{PM}$	10.05359
Proposed	$20\ T_H + 4T_{SE} + 1T_{FE}$	2.05864

5.3 Communication cost

The metrics used to estimate the communication cost during the login, authentication, and key distribution phase length of the messages and the number of messages exchanged. According to the study by Huang [53], the lengths of identity, hash value, nonce, random number, XOR, timestamp, point on elliptic curve, and symmetric encryption/decryption are 32 bits, 160 bits, 128 bits, 128 bits, 160 bits, 32 bits, 160 bits, and 128 bits, respectively. Table 5 presents a comparison of the communication cost of the suggested protocol with related works.

Table 5. Comparison of communicational cost

Scheme	Messages Exchanged	Cost in Bits
Alruwaili et al. [34]	6	4606
Rana et al. [38]	6	3296
Darman et al. [39]	4	3072
Kim et al. [48]	4	2176
Ju et al. [50]	3	1376
Bera et al. [51]	4	2304
Proposed	3	928

The high frugality in communication of the suggested protocol is obtained by the joint actions of small message development, less authentication phase, and the application of lightweight cryptography primitives. In contrast to the available schemes, which use multiple challenge-response communication or send giant certificates and signatures, the suggested protocol uses short hash-based authentication tokens, biometric hash, and limited blockchain communication, which is only performed at the level of gateway verification.

Particularly, the protocol undertakes mutual authentication within a handful of message interactions, and every message relayed includes paramount parameters needed to complete a verification. The communication between IoT devices does not include public key certificates, raw biometric data, and large blockchain transaction payloads, and thus allows for vastly decreasing the number of bits sent without compromising security properties such as mutual authentication, anonymity, and resistance to replay.

5.4 Discussion and limitations

Though the suggested blockchain-biometric lightweight mutual authentication protocol shows high security assurance and efficiency rates with the help of formal analysis and simulation-based evaluation, the lack of real-world implementation is also considered to be one of the significant restrictions of the current paper. Real-world IoT applications can also add further limitations like heterogeneous hardware capacity, network unreliability, latency variation, and energy usage, which are hard to capture in models and deterministic simulation environments.

Specifically, the acquisition of real-time biometrics, the synchronization of the gateway, and the execution of smart contracts can present deviations in performance depending on the specifics of the hardware and the circumstances of the work. Although the suggested architecture reduces the contact of blockchain with the resources of resource-constrained IoT devices and is not connected to consensus directly, the suggested architecture needs empirical validation on physical devices to comprehensively evaluate scalability, fault tolerance, and long-term operation.

However, the methods of simulation-based analysis are a popular and well-received practice in the preliminary design of research on the security protocols of the IoT, since it allows conducting a systematic comparison with the existing schemes under equal conditions. The findings in this piece of work are thus a good indicator of evidence as to the protocol's feasibility and effectiveness. The next task will involve the implementation of the proposed protocol in the real-life IoT testbeds with the usage of real-time data to check the performance, energy consumption, and resilience of the protocol in practical operating conditions.

6. CONCLUSION AND FUTURE WORK

Unrestricted access to sensitive data has become increasingly probable with the surge in the adoption of smart environments. Traditional and modern methods used for authentication are extremely vulnerable to different attacks. This proposed protocol utilizes blockchain technology, biometric hashing, and smart contracts to enhance IoT environments in terms of security and privacy. The protocol has been verified using a formal security analysis tool, AVISPA, and is lightweight, efficient, and robust since hash functions, XOR operations, and symmetric encryption are employed. With an execution time of 2.05864 ms, it becomes ideal for resource-constrained devices. The next phase of research will be the application and testing of the proposed protocol in actual IoT settings to further determine how well it performs in the conditions of real deployment.

REFERENCES

[1] Yalli, J.S., Hasan, M.H., Badawi, A.A. (2024). Internet of Things (IoT): Origins, embedded technologies, smart applications, and its growth in the last decade. IEEE Access, 12: 91357-91382. https://doi.org/10.1109/ACCESS.2024.3418995

[2] Mouha, R.A. (2021) Internet of Things (IoT). Journal of Data Analysis and Information Processing, 9(2): 77-101. https://doi.org/10.4236/jdaip.2021.92006

[3] Mustafa, M.A.S. (2025). Predictive reliability-driven optimization of spare parts management in aircraft fleets using AI, IoT, and digital twin technologies. Journal of Engineering Management and Systems Engineering, 4(3): 218-236. https://doi.org/10.56578/jemse040305

[4] Chataut, R., Phoummalayvane, A., Akl, R. (2023). Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. Sensors, 23(16): 7194. https://doi.org/10.3390/s23167194

[5] Saikia, P., Sahu, B., Prasad, G., Kumar, S., Suman, S., Kumar, K. (2025). Smart infrastructure systems: A review of IoT-enabled monitoring and automation in civil and agricultural engineering. Asian Journal of Research in Computer Science, 18(4): 24-44. https://doi.org/10.9734/ajrcos/2025/v18i4606

[6] Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things, 15: 100420. https://doi.org/10.1016/j.iot.2021.100420

[7] Bagga, P., Das, A.K., Wazid, M., Rodrigues, J.J., Park,

Y. (2020). Authentication protocols in Internet of Vehicles: Taxonomy, analysis, and challenges. IEEE Access, 8: 54314-54344. https://doi.org/10.1109/ACCESS.2020.2981397

[8] Ahvanooey, M.T., Zhu, M.X., Li, Q., Mazurczyk, W., Choo, K.K.R., Gupta, B.B., Conti, M. (2021). Modern authentication schemes in smartphones and IoT devices: An empirical survey. IEEE Internet of Things Journal, 9(10): 7639-7663. https://doi.org/10.1109/JIOT.2021.3138073

[9] Ramachandraiah, K.R.D., Bommagani, N.J., Jayapal, P.K. (2023). Enhancing healthcare data security in IoT environments using blockchain and DCGRU with twofish encryption. Information Dynamics and Applications, 2(4): 173-185. https://doi.org/10.56578/ida020402

[10] Rao, P.M., Deebak, B.D. (2023). A comprehensive survey on authentication and secure key management in Internet of Things: Challenges, countermeasures, and future directions. Ad Hoc Networks, 146: 103159. https://doi.org/10.1016/j.adhoc.2023.103159

[11] Khan, A., Ahmad, A., Ahmed, M., Sessa, J., Anisetti, M. (2022). Authorization schemes for Internet of Things: Requirements, weaknesses, future challenges and trends. Complex & Intelligent Systems, 8(5): 3919-3941. https://doi.org/10.1007/s40747-022-00765-y

[12] Alsheavi, A.N., Hawbani, A., Othman, W., Wang, X., Qaid, G., Zhao, L., Al-Qaness, M.A. (2025). IoT authentication protocols: Challenges, and comparative analysis. ACM Computing Surveys, 57(5): 116. https://doi.org/10.1145/3703444

[13] Trnka, M., Abdelfattah, A.S., Shrestha, A., Coffey, M., Cerny, T. (2022). Systematic review of authentication and authorization advancements for the Internet of Things. Sensors, 22(4): 1361. https://doi.org/10.3390/s22041361

[14] Dargaoui, S., Azrour, M., El Allaoui, A., Amounas, F., Guezzaz, A., Attou, H., Bouazza, S.H. (2023). An overview of the security challenges in IoT environment. Advanced Technology for Smart Environment and Energy, 151-160. https://doi.org/10.1007/978-3-031-25662-2_13

[15] Yusop, M.I.M., Kamarudin, N.H., Suhaimi, N.H.S., Hasan, M.K. (2025). Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity. IEEE Access, 13: 13919-13943. https://doi.org/10.1109/ACCESS.2025.3528960

[16] Yang, X., Shu, L., Liu, Y., Hancke, G.P., Ferrag, M.A., Huang, K. (2022). Physical security and safety of IoT equipment: A survey of recent advances and opportunities. IEEE Transactions on Industrial Informatics, 18(7): 4319-4330. https://doi.org/10.1109/TII.2022.3141408

[17] El-Hajj, M. (2024). Cybersecurity and privacy challenges in extended reality: Threats, solutions, and risk mitigation strategies. Virtual Worlds, 4(1): 1. https://doi.org/10.3390/virtualworlds4010001

[18] Patibandla, R.L., Vejendla, L.N. (2021). Significance of blockchain technologies in industry. In Blockchain Security in Cloud Computing, pp. 19-31. https://doi.org/10.1007/978-3-030-70501-5_2

[19] Yang, W., Wang, S., Sahri, N.M., Karie, N.M., Ahmed, M., Valli, C. (2021). Biometrics for internet-of-things security: A review. Sensors, 21(18): 6163. https://doi.org/10.3390/s21186163

[20] Obaidat, M.S., Rana, S.P., Maitra, T., Giri, D., Dutta, S. (2018). Biometric security and Internet of Things (IoT). In Biometric-Based Physical and Cybersecurity Systems, pp. 477-509. https://doi.org/10.1007/978-3-319-98734-7_19

[21] Narayana, V.L., Gopi, A.P., Patibandla, R.S.M. (2021). An efficient methodology for avoiding threats in smart homes with low power consumption in IoT environment using blockchain technology. In Blockchain Applications in IoT Ecosystem. https://doi.org/10.1007/978-3-030-65691-1_16

[22] Gudala, L., Reddy, A.K., Sadhu, A.K.R., Venkataramanan, S. (2022). Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems. Journal of Artificial Intelligence Research, 2(2): 21-50. https://thesciencebrigade.com/JAIR/article/view/250.

[23] Ali, V., Norman, A.A., Azzuhri, S.R.B. (2023). Characteristics of blockchain and its relationship with trust. IEEE Access, 11: 15364-15374. https://doi.org/10.1109/ACCESS.2023.3243700

[24] Malik, G., Parasrampuria, K., Reddy, S.P., Shah, S. (2019). Blockchain based identity verification model. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, pp. 1-6. https://doi.org/10.1109/ViTECoN.2019.8899569

[25] Ferrag, M.A., Maglaras, L., Derhab, A., Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. Telecommunication Systems, 73(2): 317-348. https://doi.org/10.1007/s11235-019-00612-5

[26] Fereidouni, H., Fadeitcheva, O., Zalai, M. (2025). IoT and man-in-the-middle attacks. Security and Privacy, 8(2): e70016. https://doi.org/10.1002/spy2.70016

[27] Sharma, G., Vidalis, S., Anand, N., Menon, C., Kumar, S. (2021). A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues. Electronics, 10(19): 2365. https://doi.org/10.3390/electronics10192365

[28] Patel, N.D., Singh, A. (2023). Security issues, attacks and countermeasures in layered IoT ecosystem. International Journal of Next-Generation Computing, 14(2): 400. https://doi.org/10.47164/ijngc.v14i2.892

[29] Kumar, T., Bhushan, S., Sharma, P., Garg, V. (2024). Examining the vulnerabilities of biometric systems: Privacy and security perspectives. In Leveraging Computer Vision to Biometric Applications, pp. 34-67. https://doi.org/10.1201/9781032614663-3

[30] Verma, U., Bhardwaj, D. (2020). Design of lightweight authentication protocol for fog enabled Internet of Things—A centralized authentication framework. International Journal of Communication Networks and Information Security, 12(2): 162-167. https://doi.org/10.17762/ijcnis.v12i2.4464

[31] Lansky, J., Sadrishojaei, M., Rahmani, A.M., Malik, M.H., Kazemian, F., Hosseinzadeh, M. (2022). Development of a lightweight centralized authentication mechanism for the Internet of Things driven by fog. Mathematics, 10(22): 4166. https://doi.org/10.3390/math10224166

[32] Höglund, J., Lindemer, S., Furuhed, M., Raza, S. (2020).

PKI4IoT: Towards public key infrastructure for the Internet of Things. Computers & Security, 89: 101658. https://doi.org/10.1016/j.cose.2019.101658

[33] Gupta, C., Varshney, G. (2023). A lightweight and secure PUF-based authentication and key-exchange protocol for IoT devices. arXiv preprint arXiv:2311.04078. https://doi.org/10.48550/arXiv.2311.04078

[34] Alruwaili, O., Tanveer, M., Alotaibi, F.M., Abdelfattah, W., Armghan, A., Alserhani, F.M. (2024). Securing the IoT-enabled smart healthcare system: A PUF-based resource-efficient authentication mechanism. Heliyon, 10(18): e37577. https://doi.org/10.1016/j.heliyon.2024.e37577

[35] Das, S., Namasudra, S., Deb, S., Ger, P.M., Crespo, R.G. (2023). Securing IoT-based smart healthcare systems by using advanced lightweight privacy-preserving authentication scheme. IEEE Internet of Things Journal, 10(21): 18486-18494. https://doi.org/10.1109/JIOT.2023.3283347

[36] Wu, T.Y., Meng, Q., Kumari, S., Zhang, P. (2022). Rotating behind security: A lightweight authentication protocol based on IoT-enabled cloud computing environments. Sensors, 22(10): 3858. https://doi.org/10.3390/s22103858

[37] Ju, S., Park, Y. (2023). Provably secure lightweight mutual authentication and key agreement scheme for cloud-based IoT environments. Sensors, 23(24): 9766. https://doi.org/10.3390/s23249766

[38] Rana, M., Shafiq, A., Altaf, I., Alazab, M., Mahmood, K., Chaudhry, S.A., Zikria, Y.B. (2021). A secure and lightweight authentication scheme for next generation IoT infrastructure. Computer Communications, 165: 85-96. https://doi.org/10.1016/j.comcom.2020.11.002

[39] Darman, I., Mahmood, M.K., Chaudhry, S.A., Khan, S.A., Lim, H. (2022). Designing an enhanced user authenticated key management scheme for 6G-based industrial applications. IEEE Access, 10: 92774-92787. https://doi.org/10.1109/ACCESS.2022.3198642

[40] Tahir, M., Sardaraz, M., Muhammad, S., Saud Khan, M. (2020). A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. Sustainability, 12(17): 6960. https://doi.org/10.3390/su12176960

[41] Yu, S., Lee, J., Park, K., Das, A.K., Park, Y. (2020). IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment. IEEE Access, 8: 167875-167886. https://doi.org/10.1109/ACCESS.2020.3022778

[42] Vasudev, H., Das, D., Vasilakos, A.V. (2020). Secure message propagation protocols for IoVs communication components. Computers & Electrical Engineering, 82: 106555. https://doi.org/10.1016/j.compeleceng.2020.106555

[43] Aman, M.N., Chua, K.C., Sikdar, B. (2017). Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet of Things Journal, 4(5): 1327-1340. https://doi.org/10.1109/JIOT.2017.2703088

[44] Parmar, K., Patil, S., Patel, D., Patel, V., Parikh, B., Padaria, P. (2023). Privacy-preserving authentication scheme for VANETS using blockchain technology. Procedia Computer Science, 220: 40-47. https://doi.org/10.1016/j.procs.2023.03.008

[45] Sabrina, F., Li, N., Sohail, S. (2022). A blockchain based secure IoT system using device identity management. Sensors, 22(19): 7535. https://doi.org/10.3390/s22197535

[46] Al Hwaitat, A.K., Almaiah, M.A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17): 3618. https://doi.org/10.3390/electronics12173618

[47] Harbi, Y., Aliouat, Z., Harous, S., Gueroui, A.M. (2024). Lightweight blockchain-based remote user authentication for fog-enabled IoT deployment. Computer Communications, 221: 90-105. https://doi.org/10.1016/j.comcom.2024.04.019

[48] Kim, T., Kwon, D., Park, Y., Park, Y. (2025). Blockchain-based secure authentication protocol for fog-enabled IoT environments. Mathematics, 13(13): 2142. https://doi.org/10.3390/math13132142

[49] Wang, W., Han, Z., Gadekallu, T.R., Raza, S., Tanveer, J., Su, C. (2023). Lightweight blockchain-enhanced mutual authentication protocol for UAVs. IEEE Internet of Things Journal, 11(6): 9547-9557. https://doi.org/10.1109/JIOT.2023.3324543

[50] Ju, S., Park, H., Son, S., Kim, H., Park, Y., Park, Y. (2024). Blockchain-assisted secure and lightweight authentication scheme for multi-server internet of drones environments. Mathematics, 12(24): 3965. https://doi.org/10.3390/math12243965

[51] Bera, B., Bisht, A., Das, A.K., Bhargava, B., Yau, D.K., Lorenz, P., Sikdar, B. (2024). Bioka-ASVN: Biometric-based key agreement scheme for air smart vehicular networks using blockchain service. IEEE Transactions on Vehicular Technology, 73(7): 9478-9494. https://doi.org/10.1109/TVT.2024.3380392

[52] Genet, T. (2015). A short SPAN+AVISPA tutorial. Doctoral dissertation. IRISA. https://inria.hal.science/hal-01213074.

[53] Huang, W. (2024). ECC-based three-factor authentication and key agreement scheme for wireless sensor networks. Scientific Reports, 14(1): 1787. https://doi.org/10.1038/s41598-024-52134-z