Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 11, No. 02, June 2025.

TOWARDS SECURE IOT AUTHENTICATION SYSTEM BASED ON FOG COMPUTING AND BLOCKCHAIN TECHNOLOGIES TO RESIST 51% AND HIJACKING CYBER-ATTACKS

Muwafaq Jawad[1], Ali A. Yassin[1], Hamid Ali Abed AL-Asadi[1], Zaid Ameen Abduljabbar[1,2], Vincent Omollo Nyangaresi[3], Zaid Alaa Hussien[4] and Husam A. Neamah[5]

(Received: 7-Jan.-2025, Revised: 14-Mar.-2025, Accepted: 1-Apr.-2025)

ABSTRACT

The Internet of Health Things (IoHT) is a network of healthcare devices, software and systems that enable remote monitoring and healthcare services by gathering real-time health data through sensors. Despite its significant benefits for modern smart healthcare, IoHT faces growing security challenges due to the limited processing power, storage capacity and self-defense capabilities of its devices. While blockchain-based authentication solutions have been developed to leverage tamper-resistant decentralized designs for enhanced security, they often require substantial computational resources, increased storage and longer authentication times, hindering scalability and time efficiency in large-scale, time-critical IoHT systems. To address these challenges, we propose a novel four-phase authentication scheme comprising setup, registration, authentication and secret-construction phases. Our scheme integrates chaotic-based public-key cryptosystems, a Light Encryption Device (LED) with a 3-D Lorenz chaotic map algorithm and blockchain-based fog computing technologies to enhance both efficiency and scalability. Simulated on the Ethereum platform using Solidity and evaluated with the JMeter tool, the proposed scheme demonstrates superior performance, with a computational-cost reduction of 40% compared to traditional methods like Elliptic Curve Cryptography (ECC). The average latency for registration is 1.25 ms, while the authentication phase completes in just 1.50 ms, making it highly suitable for time-critical IoHT applications. Security analysis using the Scyther tool confirms that the scheme is resistant to modern cyberattacks, including 51% attacks and hijacking, while ensuring data integrity and confidentiality. Additionally, the scheme minimizes communication costs and supports the scalability of large-scale IoHT systems. These results highlight the proposed scheme's potential to revolutionize secure and efficient healthcare monitoring, enabling real-time, tamper-proof data management in IoHT environments.

KEYWORDS

Blockchain, Fog computing, IoHT, Authentication, Chaotic cryptography, Healthcare.

1. INTRODUCTION

The Internet of Healthcare Things (IoHT) is a concept that integrates Internet of Things (IoT) technology with healthcare devices. Furthermore, the IoHT is predicted to be the cornerstone of future healthcare systems; every piece of healthcare equipment will be internet-connected and under the supervision of healthcare providers. As the IoHT grows, it can provide speedy and affordable healthcare [1]. Technological development over recent years has enabled the diagnosis of a multitude of illnesses and the monitoring of health through the utilization of compact devices, such as smartwatches, electrocardiography (ECG) machines and shoes.

Furthermore, the paradigm for healthcare has changed due to technology, moving from hospital-focused to patient-centred. For example, many clinical evaluations, such as blood pressure, blood glucose and pO2 readings, can now be performed at home without the need for direct medical

1. M. Jawad, A. Yassin, H. AL-Asadi and Z. Abduljabbar are with the Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq. Emails: pgs.muwafaq.abbas, ali.yassin, hamid.abed, zaid.ameen@uobasrah.edu.iq
2. Z. Abduljabbar is with the Department of Business Management, A-Imam University College, 34011 Balad, Iraq and with Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 518000, China. Email: zaid.ameen@uobasrah.edu.iq
3. V. Omollo is with the Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya; and with the Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tamil Nadu, 602105, India. Email: vnyangaresi@jooust.ac.ke
4. Z. Alaa is with Management Technical College, Southern Technical University, Basrah 61004, Iraq. Email: zaid.alaa@stu.edu.iq
5. H. A. Neamah is with the Department of Electrical Engineering and Mechatronics, Faculty of Engineering, University of Debrecen, Ótemető u.4-5, Debrecen 4028, Hungary. Email: husam@eng.unideb.hu

assistance. Furthermore, advanced telecommunication technologies enable the transmission of clinical data from remote places to healthcare facilities [2]; the explosive growth highlights serious issues with user privacy and security, especially in the context of the IoHT and needs careful consideration and attention. Various vulnerabilities exist within healthcare systems that could lead to security and privacy breaches, including unauthorized access to vast amounts of sensitive patient data, encompassing personal and health records critical for making life-saving decisions [3]. As a result, in recent years, the protection of security and privacy in IoHT applications has gained attention. Confidentiality, non-repudiation, data integrity and the authentication and identification of IoHT devices and users are all critical security requirements. Since authentication is essential to maintaining the fulfilment of other security requirements, it stands out as a primary concern [4]-[5]. Authentication is the process of verifying and authenticating an entity's identification. Every entity should be able to recognize and verify every other entity in the system or the particular part of the system that it communicates with [6]. Due to the involvement of multiple applications and users in the monitoring, operation and management of healthcare devices, the potential for breaches in authentication and authorization schemes exists.

The authentication techniques described in the literature for the IoHT mostly belong to two architecture categories: centralized and decentralized. The centralization of authentication can be performed by distributing and managing login credentials through a single server or a reliable outside source. Moreover, it comprises three procedures. First, there is one-way authentication, which occurs when two parties want to communicate and only one party authenticates itself to the other, while the other party remains unauthenticated. Second, there is two-way authentication, also known as mutual authentication, where both entities authenticate each other. Lastly, there is three-way authentication, where a central authority authenticates each of the parties and assists them in mutually authenticating themselves [7]. Scalability problems with central-authentication systems could result in performance bottlenecks as user numbers increase. In addition, they are exposed to single points of failure, which can compromise the entire authentication process. Furthermore, the concentration of sensitive user credentials may give rise to privacy concerns [8].

Decentralized authentication solutions that employ blockchain technology are recommended more and more for IoHT systems because they are compatible with the scattered and heterogeneous nature of these systems [9]-[10]. Researchers have highlighted the basic properties of blockchains, which include consensus, immutability, decentralization and security [11]. They emphasised the benefits of using blockchain technology to improve big-data management and authentication in many areas, such as enhancing data integrity, promoting seamless data sharing, bolstering security and privacy measures and improving big-data overall quality [12]. As a result, several blockchain platforms, such as Multichain, Ethereum, Bitcoin and others, have emerged, each offering distinct advantages over the rest. These platforms operate on diverse consensus protocols, ensuring security and scalability at varying levels [13]. To strengthen the discussion and provide deeper insights into the computational complexity of cryptographic algorithms, consensus mechanisms and smart contracts, this study positions itself within the broader context of blockchain research. Blockchain-assisted systems are particularly relevant for IoHT due to their ability to address the limitations of centralized systems, such as scalability and single points of failure. By leveraging blockchain's inherent properties, such as decentralization and immutability, the proposed system ensures secure and efficient authentication while minimizing computational overhead and communication costs [14]-[15].

Smart and edge devices generate large amounts of data that are quickly transferred to the cloud via IoT devices. This can sometimes lead to network congestion [16]. Therefore, the fog-computing concept creates a decentralized computing environment by dispersing several fog nodes over various areas. It effectively handles data processing, solving computing constraints in cloud and IoT devices, by occupying the space between the edge and cloud layers [17]. This method improves cloud-based services by enabling quick data processing and data transfer from edge devices to the cloud. As a result, it lessens network congestion and the reliance of edge and IoT devices on direct cloud connection [18]. For this purpose, our devised work incorporates fog computing, extending cloud services to network edges and providing acceptable computational support for IoHT devices. To mitigate communication overhead during authentication, a chaotic-key cryptosystem is employed within our work that utilizes chaotic keys, is compact, minimises communication overhead and

considers the limited computational capabilities inherent in IoHT devices [19]-[20]. In recent years, many authentication techniques have been suggested to enhance the security of the Internet of Human Things (IoHT) system. The present study proposes a decentralized authentication system that leverages fog computing and blockchain technology to contribute to these efforts. Multiple factors of authentication, including wallet address, password, OTP and fingerprint, are utilized. By leveraging the features of blockchain technology, such as peer-to-peer communication, cryptography, consensus mechanisms and smart contracts, it facilitates authentication through decentralized peer-to-peer communication among fog nodes. The suggested approach resists common attacks and modern threats like 51% attacks and hijacking. Furthermore, this work accomplishes authentication without relying on a central authority. Finally, to guarantee the security of parties interacting through public channels in a decentralized environment, our work combines an authentication mechanism with immutable blockchain technology. Additionally, decentralized node identification is supported by blockchain technology. Consequently, the following contributions are provided by this paper:

- We provide a lightweight authentication scheme over fog computing for a blockchain-based IoHT system. The proposed work employs blockchain in the fog-computing layer to allocate the IoHT into fog areas.
- The proposed scheme utilizes a chaotic-based cryptosystem to provide a higher level of scalability and efficiency. Furthermore, the chaotic cryptosystem offers remarkable efficiency and rapidity in encryption and decryption, particularly in the domain of image encryption.
- A comprehensive security evaluation is conducted using the well-regarded Scyther tool to showcase the robustness of the suggested design against common threats, such as replay attacks, man-in-the-middle attacks, 51% attacks and Hijacking. Moreover, it has been proven that our proposed approach is resistant to these malicious attacks. Preliminary security assessment is conducted to verify adherence to security requirements, including decentralization, identification, secrecy, non-repudiation and integrity.
- The proposed work is simulated and designed by the Ethereum blockchain platform to evaluate it for two main metrics, latency and throughput. We utilize Apache JMeter, which is a strong tool used for measuring evaluation metrics, like latency and throughput. Furthermore, the assessment results indicate that the suggested strategy is time-efficient (0.3201 ms), with latencies of 1.25 ms for registration and 1.50 ms for authentication.

The paper is ordered as follows: the related authentication schemes in the IoHT environment are presented in Section 2. Backgrounds are in Section 3. The network model is explained in Section 4. Moreover, the security model is shwon in Section 5. The proposed scheme and its phases are described in Section 6. The performance analysis, simulation, evaluation metrics, key-generation time, LED with 3-D Lorenz chaotic encryption and decryption time, computational cost and smart contract costs are detailed in Section 7. The formal and informal security analyses are presented in Section 8. Finally, the conclusion is presented in Section 9.

2. RELATED WORKS

In 2018, Almadhoun et al. [21] introduced an authentication system that utilizes blockchain-enabled fog nodes and Ethereum smart contracts to address the capacity constraints of the IoT, grant access to IoT devices and verify users. This method enables the system to expand its capacity by using fog nodes for computational operations. Although the scheme offers strong security, it does not align with the requirements of most IoT connectivity scenarios. This work has limitations, such as computational overhead, because the integration of the blockchain with a smart contract may not be suitable for all IoT devices, especially those with limited processing power. Moreover, in terms of scalability and security vulnerabilities, it is not entirely immune to attacks; there are potential vulnerabilities in smart contracts.

In 2018, Mehmood et al. [22] proposed a mutual-authentication method and key-agreement methodology utilizing chaotic maps and Diffie-Hellman key exchange. The suggested solution guarantees that only authorized healthcare professionals can retrieve patients' health data collected through body sensors in the medical system. This paper has major limitations, particularly in terms of computational complexity. The technique used in this paper involves complex cryptographic operations, which can result in a longer processing time and increased energy consumption.

Furthermore, it experiences scalability challenges when it comes to managing a substantial number of users and devices.

Moreover, the scheme's objective of safeguarding user anonymity is compromised by the privacy hazards associated with relying on a centralized cloud. This includes the potential for data breaches and unauthorized access to critical health information. Additionally, there is vulnerability in having a single point of failure if the cloud server experiences a failure. In 2019, Liang et al. [23] developed a blockchain-powered system for managing and verifying identities. The system's goal is to enhance patient-data confidentiality while allowing more flexibility in accessing health records. This study has limitations in scalability due to the degradation of the blockchain performance as the number of transactions increases, resulting in significant implementation challenges in the healthcare sector. Furthermore, it poses data-privacy concerns. In 2020, Cheng et al. [24] created a blockchain-based multiple-identity authentication system for a safe medical-data exchange model that did not require a third party. This paper has limitations. The ability to scale large-scale blockchain applications faces a hurdle, as the performance of the technology can deteriorate with the growing volume of medical data. The complexity of integrating blockchain technology into current medical-data systems is an intricate process that necessitates substantial modifications to the existing-infrastructure issues with the protection of personal information. Despite the security aspects of the blockchain, ensuring complete data privacy remains a tough task.

In 2021, Wu et al. [25] examined the security of different authentication techniques. Their study showed that the examined schemes were susceptible to established attacks, such as session-specific temporary data, user impersonation and server impersonation. The examined scheme utilized formal and informal security studies, both of which verified its lack of security. However, as the numbers of servers and users increase, the scheme may face scalability issues, potentially affecting the overall efficiency and performance. In 2021, Guo et al. [26] provided FogHA, a lightweight cryptographic primitive for fog computing and an undetectable handover-authentication strategy. This system facilitates managing keys and mutual authentication among a mobile device and fog computing by removing redundant authentication messages. The method includes characteristics, like untraceability, anonymity and low latency, making it secure against attacks from insiders. Opponents can utilize the untraceability and anonymity characteristics to carry out attacks without being identified by the system. This paper has limitations. Scalability refers to the ability of a system or process to handle an increasing amount of work or data efficiently and effectively. The approach may face challenges when expanding to a significant number of devices due to the inherent computational and communication burdens associated with fog nodes. Furthermore, limitations on the available resources that fog nodes possess constrain the processing resources in comparison to cloud servers, potentially impacting the performance and efficiency of the authentication process. Moreover, in terms of security vulnerability, the scheme's objective is to offer reliable authentication; however, achieving a satisfactory equilibrium between security and performance can be difficult, especially in contexts with limited resources.

In 2021, Javed et al. [27] introduced blockchain-based decentralized identity control using smart contracts for electronic health records, having been the focus of various research investigations, such as Health-ID for remote healthcare and Health-ID for EHRs. Additionally, a blockchain-enabled authentication method was created to reduce the necessity of re-authentication across multiple hospitals, enhancing efficiency and reducing the time overhead for devices with constrained processing and memory capabilities. This paper has limitations, including challenges related to the ability of a system or process to handle increasing amounts of work or data efficiently. Although the suggested blockchain-based approach improves security and decentralization, the ability of blockchain networks to handle large amounts of data and transactions is still a matter of concern. The performance measures, such as the transaction gas cost and the transactions per second, suggest that as the numbers of users and transactions grow, the system may experience delays and incur larger operational expenses. In addition, the report acknowledges that although the blockchain has the potential to improve openness and trust, but it is challenging to ensure that all players comply with healthcare rules and privacy requirements. This is especially crucial in varied regulatory landscapes spanning multiple regions and nations.

In 2022, Chen et al. [28] proposed a method to shorten the time taken for authentication. The method

consists of two parts; complete authentication and lightweight authentication. For complete authentication, they used CP-ABE to ensure confidentiality. For lightweight authentication, they utilized the hash function and XOR gate. This method enabled the creation of a physiological sensing device with a lower computing ability that can handle parameter calculations. They used the patients' information as seeds for a random-number generator. Finally, this method uses a third party and does not take advantage of the blockchain to make the security mechanism robust. In 2022, Umoren et al. [29] implemented blockchain smart contracts to tackle user authentication and other limitations in IoT and fog technology. The decentralized fog-computing framework incorporated scalability, immutability and secure authentication for fog devices. Additionally, it addressed issues of immutability and scalability in fog computing. The scheme provides robust security, but does not meet the needs of typical IoT connectivity scenarios. The proposed system's implementation is not sufficiently covered in the study. More precisely, the data structure and code offered lack clear explanations, which may impede the ability of other researchers to replicate and advance the work.

Moreover, the description of the experimental setup and performance measures is insufficient. In order to properly validate the findings, it is necessary to provide more comprehensive explanations of the simulation model and the results. The discussion lacks a thorough comparison between the suggested method and existing solutions. An extensive evaluation considering factors, such as the resilience to attacks, computational cost, calculation time and communication overhead would offer a more thorough understanding and verification of the suggested approach.

In 2023, H. Miriam et al. [30] introduced the LGE-HES algorithm to improve blockchain-based healthcare cybersecurity, focusing on securing medical-image data. Simulations show that the method achieves high PSNR (63 dB) and minimal MSE (0.003) while optimizing encryption and decryption times. Compared to standard approaches, it effectively identifies 94.9% of malicious communications. The results demonstrate superior image secrecy, suggesting future exploration of hybrid optimization techniques for enhanced security scalability. In 2024, Alsaeed et al. [20] introduced a method to address issues, like scalability and time; they proposed group authentication utilizing Shamir's secret-sharing (SSS) algorithm, ECC, fog-based computing and a multi-level blockchain to implement lightweight and scalable group authentication in the IoMT. The evaluation test shows good scalability and time efficiency, but although there are many good aspects to this method, one of the foundations of healthcare systems is missing: a robust authentication mechanism for users, particularly administrators and patients. In addition, handling the enormous number of devices and sensors presents difficulties for the ECC algorithm. Thus, we used the chaotic algorithm to solve this problem.

The next section examines the current authentication schemes and systems used in IoT and fog environments and explores how blockchain technology might be used to improve security and decentralization. However, the majority of the centralized systems are constrained by limits in terms of scalability, security and privacy. Additionally, some of the schemes rely on a centralized fog and IoT authentication system, which also has its own limitations. We provide a lightweight authentication scheme over fog computing for a blockchain-based IoHT system. Furthermore, the proposed work employs the blockchain in the fog-computing layer to allocate the IoHT into fog areas. Additionally, we utilized a 3-D chaotic cryptosystem to provide a higher level of scalability and efficiency. Finally, Table 1 provides a comparison of some different related schemes.

3. BACKGROUNDS

3.1 Blockchain Technology

In 2008, Satoshi Nakamoto introduced blockchain technology, as well as its distributed decentralized network which functions as a network of independent networks responsible for managing a collection of time-stamped documents. The blockchain's structure comprises interconnected blocks secured through fundamental cryptography. This technology operates on three core principles: transparency, decentralization and immutability [31]. Blockchain's decentralized nature allows secure, reliable data sharing in IoT, popular in mutual authentication. It serves as a dependable platform for authentication systems and secure storage. These advantages make use of blockchain technology in healthcare with several benefits [32]. It is a sensible decision, particularly because the healthcare sector has prioritized patient-data security due to technological advancements. Moreover, various experts have concluded

that incorporating blockchain technology into the healthcare industry would be a feasible solution [33]. The blockchain is a secure method of exchanging information. It comprises a series of interconnected blocks that store encrypted data. Each block includes the data, its cryptographic hash and the hash of the preceding block [34], as illustrated in Figure 1.

Table 1. Comparison of different related schemes.

Authors	Year	Problem	Contribution	Technique	Platform
Almadhoun [21]	2018	IoT devices are vulnerable to security breaches; centralized authentication systems are prone to single points of failure. IoT devices lack the capacity to secure themselves; high latency and communication overhead in IoT-cloud interactions.	Proposed a decentralized and scalable authentication mechanism using blockchain-enabled fog nodes and Ethereum smart contracts for authenticating user access to IoT devices; introduced a system where fog nodes handle authentication tasks, relieving IoT devices from heavy computational loads.	Blockchain, Fog Computing, Ethereum Smart Contracts, Elliptic Curve Cryptography	Ethereum, Remix IDE
Cheng et al. [24]	2020	Difficulty in secure sharing of medical data due to reliance on trusted third parties in Medical Cyber Physical Systems (MCPS).	Proposed a blockchain-based secure medical data sharing scheme that ensures data integrity, untraceability and secure authentication without relying on trusted third parties. Utilized bilinear mapping and intractable problems for secure authentication.	Blockchain, Bilinear Mapping, Cloud Storage	Blockchain, Cloud Storage
Guo et al. [26]	2021	High latency and security issues in handover authentication for mobile devices in fog computing.	Proposed FogHA, an efficient handover authentication scheme for mobile devices in fog computing, ensuring mutual authentication, key agreement and resistance to known attacks.	Lightweight cryptography, Symmetric trivariate polynomials, hash functions	Fog Computing
Javed et al. [27]	2021	Centralized identity management in eHealth restricts interoperability and security.	Proposed a decentralized identity-management system for remote healthcare using blockchain.	Blockchain, Smart Contracts, JSON Web Tokens (JWT)	Ethereum Blockchain
H. Miriam et al. [30]	2023	Ensuring the cybersecurity of blockchain-based healthcare systems is challenging due to vulnerabilities in medical-image data and the need for robust encryption mechanisms.	The proposed LGEHES algorithm enhances the cybersecurity of blockchain in healthcare by optimizing encryption and decryption processes while preserving medical-image quality and resisting malicious attacks.	The LGE-HES algorithm integrates Lionized Golden Eagle optimization with homomorphic encryption	Blockchain -Healthcare
N. Alsaeed [20]	2024	IoMT faces security challenges due to limited computational and storage capacities, making traditional authentication methods unsuitable for large-scale, time-sensitive systems.	proposed a lightweight and scalable group-authentication framework for IoMT systems using blockchain technology, enhances efficiency and scalability, achieving 0.5-second latency and 400 transactions per second.	ECC for lightweight and (SSS) algorithm for secure secret construction and group authentication	IoMT-Blockchain

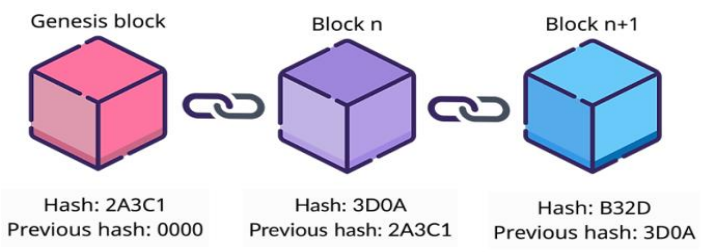


Figure 1. Blockchain.

3.1.1 Architecture

Let's use the following Figure 2, which illustrates the entire process of a transaction being sent from a user on the blockchain network, to better understand the blockchain architecture.

- Once a user initiates a transaction on a blockchain network, it is disseminated to all nodes within the network. Every node maintains a complete replica of the blockchain, which is instrumental in the verification process. All connected nodes collaborate to ensure that the block encompassing the user's transaction remains unaltered. If the validation process is successful, the nodes append that block to their version of the blockchain.
- To append a fresh block to the blockchain, consensus must be achieved amongst the network nodes regarding the validity of the blocks. This agreement is attained *via* a validation procedure that employs precise algorithms to authenticate the transaction and confirm the sender's membership in the network.
- Once the validation process is completed, the block is added to the blockchain.
- Subsequently, when the whole validation process has been completed, the transaction is considered finalized.

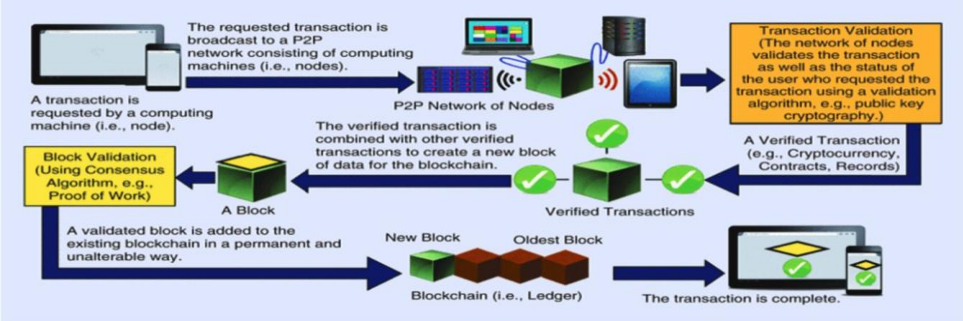


Figure 2. An overview of blockchain architecture.

3.1.2 Consensus Algorithm

For a block to become a part of the blockchain, it must follow specific consensus guidelines. To ensure this, blockchain technology employs consensus algorithms. In the Bitcoin network, Nakamoto [31] introduced the Proof of Work (PoW) algorithm, which is now the most commonly used consensus method. The fundamental idea behind this algorithm is that since multiple nodes or users are present on a blockchain network, any transaction request made by a participating node must be computed before it can be added to the network. The nodes responsible for performing these calculations are called miners and this process is known as mining [35].

3.1.3 Key Features of Blockchain

1) **Decentralization:** Blockchain distributes information throughout the network as opposed to concentrating it in one place. Additionally, this means that information control will be dispersed and managed by consensus determined by the collective input of all connected nodes on the network. Nowadays, several reliable organizations handle the data that was previously centralized at one location [36].
2) **Data Transparency:** To achieve data transparency in any technology, relationships based on trust must exist between entities. The relevant data or record needs to be safe from heat and secure. Any data stored on the blockchain is dispersed throughout the network rather than being concentrated in one location or under the control of a single node. Since data ownership is now shared, it is transparent and protected from outside interference.
3) **Security and Privacy:** Blockchain technology employs cryptographic functions to provide security to the nodes connected to its network. It uses the SHA-256 algorithm for the hashes stored on the blocks, known as the "secure hash algorithm" (SHA), which ensures data integrity and adds security to the blockchain. Digital data is assigned checksums through strong one-way functions called cryptographic hashes, rendering them unusable for data extraction. This makes blockchain a decentralized and secure platform, using cryptographic techniques to safeguard user privacy, thus making it a reliable option for applications that require privacy protection [37].

3.2 Fog Computing

Industry first used the term fog computing to refer to the fundamental architectural concept of the technology: fog is a region that lies between the ground, where user devices are located and the cloud or data centers. In general, fog is referred to as a decentralized distributed computing system in which various fog devices are owned by various entities and organizations can interact with the system from various locations, including smart hubs, hospitals, schools and airports. [38] Fog computing's topology is the geographically dispersed nodes that carry out computation and providing network and storage services is its primary feature. In addition to standard network features, fog-computing resources can be incorporated into network gateways, routers and access points. Additionally, there might be specific fog-computing nodes, such as edge computing [39]. The following is a description of the main characteristics of fog computing [40]-[41].

1) Adaptability: This consists of multiple fog devices and network sensors that provide storage and perform computing tasks.
2) Reduced latency: Fog computing's proximity to edge devices shortens the time taken for information to be computed with those devices and helps the host-fog devices respond to position queries at multiple sites.
3) Physical distribution: Fog computing presents distributed applications and services that are hosted in various locations.
4) Compatibility: Fog modules can be used across a variety of platforms and service providers.

3.3 Chaotic Cryptography

Within systems, security is of the utmost importance. It is critical to ensure security, confidentiality, data-origin authentication, message integrity and non-repudiation of origin. The use of symmetric and asymmetric cryptographic algorithms is the foundation for improving message security over unsecured networks [42]. There has been a noticeable increase in the exploration of chaos-based cryptography in recent years, driven by a renewed interest in leveraging chaotic systems for various applications. Our work will utilize chaotic systems, such as the use of the logistic map for key pair generation, the beta-transform for key exchange and the integration of the Lorenz system for encryption and decryption [42].

4. NETWORK MODEL

Before delving into the intricate details of our proposed IoHT system, understanding the fundamental assumptions that form the foundation of this initiative is critical. These fundamental premises hold significance in blockchain-based authentication systems, serving as pivotal reference points.

- In the context of fog computing, the ecosystem comprises a wide range of both mobile and stationary devices, such as smartphones, sensors, embedded systems and stationary edge servers. These devices are intricately interconnected across a multitude of communication networks.
- The device used by registered users is adept at integrating and utilizing blockchain technology, thereby enhancing the system's functionality.
- To fulfill its role effectively, a fog server must meet specific pre-requisites, including the capability to host the blockchain and function as a server or node within the network architecture.
- The smart contracts are expected to execute the critical functions of device and user registration and authentication, playing a pivotal role in the seamless operation of the system.

The network model consists of four layers. These layers are shown in Figure 3 and explained below.

4.1 User Layer

A system user is a person who realizes the way to use system resources effectively. Users have distinct roles and attributes within the system that allow them to be identified. Patients, doctors, nurses, administrators and others are among those who interact with the system. Their primary responsibility is to interact with the system in order to perform essential functions, such as creating, reading, updating, deleting, accessing and managing medical records.

4.2 Edge-device Layer

In this layer, the IoHT ecosystem serves as a crucial and essential component, fulfilling diverse roles, such as gathering, managing data computation, secure storage and initial processing of IoHT sensor information. Its primary function involves meticulously safeguarding and organizing data, ensuring its integrity and security before transmission to the fog-computing infrastructure.

4.3 Fog-computing Layer

This layer includes more than one fog servers that act as blockchain nodes and devoted servers to support the decentralized blockchain infrastructure. These devices ensure secure information transmission from IoHT gadgets even as additionally retaining synchronized copies of the blockchain, ledger and smart contracts. The elaborate interplay of fog computing and blockchain enhances the latency, reduces the time cost and adds another layer of security.

4.4 Cloud Layer

A large quantity of data is generated inside IoHT sensors and gadgets. The cloud computing proposes as a robust actor with its extremely good computational skills, substantial storge capacity and strong bandwidth. It serves as an infrastructure that is specifically designed to store, compute and examine significant amounts of data. The cloud layer is responsible for the registration and approval of all of the fog servers, users and IoHT devices. Additionally, our scheme allowed the authorized users to communicate with other nodes which include cloud servers, fog servers, users and IoHT gadgets. Furthermore, the scheme employs a blockchain structure and smart contracts that hold an essential position in enhancing security and privacy.

- **Blockchain:** Operates as a decentralized authority for identifying and registration of all entity and IoHT devices. Authentication and identity procedures are controlled through smart contracts included in the blockchain infrastructure. Utilizing blockchain technology, every fog server authenticates IoHT gadgets and customers within its location. Significantly, the blockchain remains on hand throughout all layers of the system architecture.
- **Smart Contract:** It's self-executing codes on blockchains, replacing centralized oversight in transactions. All contract executions are publicly documented, ensuring transparency across network nodes. Blockchain's allotted records storage, secure protocols and consensus mechanisms extensively boost protection and streamline system gadget performance, decreasing time and charges. To register and manage the identities of all IoHT devices and users, the proposed scheme incorporates blockchain technology. Each fog server takes on the responsibility of authenticating IoHT devices in its network. Furthermore, the architecture is intended to address the scalability concerns inherent in blockchain-based authentication schemes, ensuring support for the IoHT system's scalability requirements.

5. SECURITY MODEL

In the healthcare part, security is the predominant concern, exerting a profound influence on the reliability and confidentiality of devices and services. Consequently, there is a compelling necessity to initiate the proactive development of comprehensive solutions aimed at fortifying these systems against a wide array of potential threats, as substantiated by [43]. Subsequently, our discussion will pivot towards an examination of prevalent attacks directed at IoHT systems, thereby enhancing our understanding of the security challenges inherent in the healthcare sector.

Certain security requirements must be satisfied by authentication techniques used in wireless networks. These characteristics enhance the feasibility of implementing any proposed plan in the wireless body-area network (WBAN) environment. The Canetti-Krawczyk (CK) model allows the formal development and analysis of the suggested scheme. In addition, the proposed system must possess numerous crucial security attributes [44]-[45].

5.1 Security Requirements

Mutual Authentication: To safeguard sensitive information from potential interception by evil individuals, all parties must authenticate their identities before any data transfer [46].

- User Identity Anomaly and Untraceability: Anonymity is attained by the consolidation of a legitimate user's personal information in a manner that prevents an unauthorized individual from discovering or identifying the user.
- Forward Secrecy: It guarantees that the key used for the current session is distinct and will not be vulnerable to unauthorized access. Additionally, it prohibits the utilization of a primary session key for initiating a fresh session.
- Unlinkability: It is a private attribute that is effective when an attacker is unable to differentiate between two or more components of a system. Consequently, the attacker is unable to breach the system or improperly exploit it. This attribute is crucial in identifying systems. For example, an attacker may be unable to establish a connection between the contents of any communications, multiple sets of login credentials or multiple bank withdrawal transactions [47].
- Scalability: The constituents of an authentication system should possess the ability to adapt and evolve following alterations in the surrounding environment [48].

5.2 Threat Model

The attacker can execute the following threats:

- Distributed Denial-of-Service (DDoS) Attack: This attack represents a form of network manipulation characterised by the deliberate inundation of a targeted system with an overwhelming volume of network traffic, surpassing its operational capacity. As a consequence, these attacks cause a significant increase in the workload of the system [49].
- Man-in-the-Middle (MITM) Attack: This attack is a security threat that aims to compromise the privacy and integrity of data exchanged during a session. In this type of attack, an adversary strategically positions him/her self between two communicating hosts, intercepting and potentially modifying the data traffic, thereby breaching both confidentiality and integrity [50].
- Insider Attack: This attack occurs when an individual who possesses authorised access to an organization's systems, data or network deliberately compromises the privacy, accuracy or availability of sensitive information or resources for personal gain or malicious intent [51].
- Eavesdropping Attack: An attacker can access IoHT network traffic and read the contents of messages being transmitted across the network by using an eavesdropping attack. The payload and wireless session are passively observed by the attacker. If the communication is encrypted, the attacker may eventually be able to decrypt it [52].
- Impersonation Attack: To obtain the information that an attacker is not authorized to access, he/she assumes the identity of another person or impersonates a legitimate IoHT user (or group of users) or server [53].
- Replay Attack: This type of attack accesses the WLAN using phony authentication sessions and does not occur in real time. The attacker initially obtains a session's authentication. The attacker then replicates the initial session, changing or tampering with it [43].

6. PROPOSED SCHEME

Our work focuses on four main phases: Setup, Registration, Login and Authentication and Secure Construction. Furthermore, the environment of the proposed scheme consists of four main components: Health Cloud Server (HCS), Fog Service Provider (FSP), Blockchain (BC) and Wireless Body Area Network (WBAN) depending on three layers: IoHT sensors layer $(S_i = S_1, S_2, S_3, , S_n)$, Personal Devices Layer (Pd_i) (like mobile phone, Computer, tablet, …etc.) that use by (admin(ADM_i)), patient(P_i)) and doctor(Dr_i))), and Internet layer (such as gateway or FSP layer). Figure 3 explains the major components of our work.

6.1 Setup Phase

During this phase, *HCS* is regarded as the primary entity accountable for managing and enrolling users, *FSP* and *IoHT* devices. Each user and *IoHT* device obtains the shared key (*SK*) locally by implementing a key-exchange protocol based on a chaotic logistic system to guarantee security. The *HCS* employs a highly secure cryptographic hash function, known as the h(.) function, implemented through SHA-256 which is a member of the SHA-2 family and plays a main role in

verification and anomaly for major parameters. Additionally, our proposed scheme uses CTR_{mode} for the Encryption function ($Enc()$) and the Decryption function ($Dec()$).

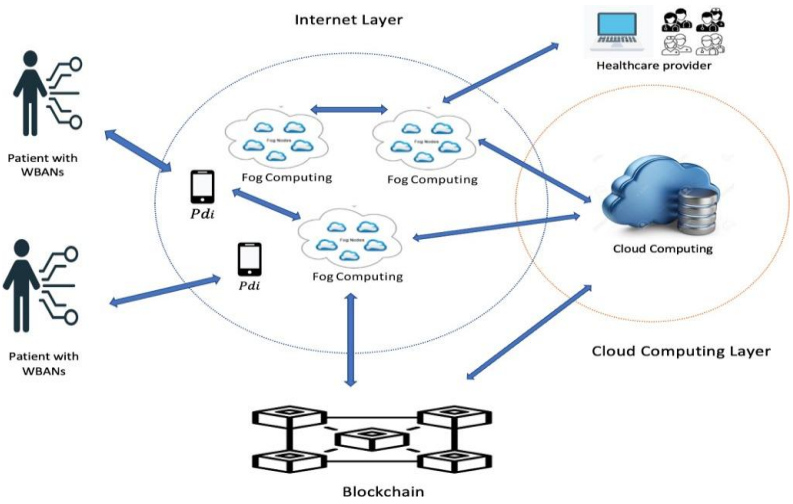


Figure 3. The proposed scheme's architecture.

6.2 Registration Phase

This sub-section describes the user-registration process of our proposed scheme; we focus on the FSP, IoHT devices and administrator, patient and doctor registration. Each user must provide valid information (username, password, wallet address, …etc.) one time. The user data is hashed and stored. Below is a description of the registration process.

6.2.1 Node$_i$ Registration

First, each $node_i$ (FSP, Pd_i, IoHT sensor S_i.....etc.) generates its own private key ($node_{i\_pr}$) and public key ($node_{i\_pu}$) using the chaotic system. The following step explains $node_i$ registration process.
Step 1: $node_i$ selects an identification $node_{iID}$ and time (T_s) and sends a registration request to the HCS{$node_{iID}$, T_s, $node_{ipu}$}.
Step 2: HCS checks the freshness of the received request by calculating T'_s - $T_s \leq T_s$, where T'_s denotes the request-receiving time and represents the acceptable difference between T' and T.
Step 3: HCS classifies the $node_{iID}$ to add to related list, such as (FSP list, pd_i list, S_i list) then, Save {$node_{iID}$, $node_{ipu}$, HCS_{pu}} in the BC.
Step 4: HCS checks if registered nodeiID its IoHT device (pdi), then need to assign to the FSP, then send {HCS_{pu}, Pd_{ipu}, FSP_{pu}} to BC.
Step 5: After assigning pd_i to the FSP, finally the registration of $node_i$ is successful.

6.2.2 Administrator Registration

The administrator (ADM_i) is in charge of controlling the system components in the healthcare domain. As a result, the administrator must register specific details, such as (username (Un_{ADMi}), address (Ad_{ADMi}), phone number (Pn_{ADMi}), password (Pw_{ADMi}), wallet address (Wa_{ADMi}) and fingerprint Fn_{ADMi})) in the HCS once and generates the private key (ADM_{ipr}) and public key (ADM_{ipu}) based on the chaotic system as described in sub-section 6.1. Furthermore, ADM_i computes the shard key (SK_{ADMi}). Then, HCS submits the following set of steps.

Step 1: The HCS computes the following anonymous parameters based on the following:
1) $Un'_{ADMi} = h(Un_{ADMi})$.
2) $Pw'_{ADMi} = h(Pw_{ADMi} \| Un_{ADMi})$
3) $F'n_{ADMi}$ = FEX-ADM (Fn_{ADMi}), where FEX-ADM is the function used for fingerprint pre-processing and feature extraction and then returns the feature-extraction vector; as a result, it refers to level 2 of the administrator's fingerprint-feature extraction.

Step 2: The HCS generates the shared key (SK_{ADMi}) to encrypt Enc (.) / decrypt Dec (.) data based on symmetric key encryption Counter (CTR) based on the chaotic system.

Step 3: The HCS assigns admin (ADM_i) information to the fog server FSP_{ID} that connects within the same area.
Step 4: The HCS sends ADMi information $\{Pw'_{ADMi}, Un'_{ADMi}\ Fn'_{ADMi}\}$ to the Blockchain by calling the smart-contract registration method.

6.2.3 Patient Registration

In this part, the patient (P_i) who wishes to register in the system must do the following steps.

Step 1: The patient should register his/her information such as (username (Un_{Pi}), address (Ad_{Pi}), phone number (Pn_{Pi}), password (Pw_{Pi}), wallet address (Wa_{Pi}), type of disease Td_{Pi})) in the *HCS* computed HP_{Pi} anomaly by calculating HP_{Pi} = H ($Un_{Pi} \parallel Pw_{Pi}$), then stores it in the *BC* through a smart contract.
Step 2: The patient generates the private key (Pi_{pr}) and public key (Pi_{pu}) based on the chaotic system.
Step 3: The patient computes a shared key (SK_{Pi}), ensuring that the encryption (Enc(.)) and decryption (Dec(.)) processes for safeguarding Si sensitive health information data are carried out with a robust key based on the chaotic logistic system.
Step 4: HCS creates an Electronic Health Record (EHR_{Pi}) with all of the aforementioned medical information associated with a new patient.
Step 5: HCS assigns Patient (P_i) information to the fog server FSP_{ID} that connects within the same area.
Step 6: HCS sends the patient (P_i) information (HP_{Pi}) to the BC by calling the smart contract.

6.2.4 Doctor Registration

At this time, the doctors (Dr_i) send a registration request to HCS with their personal information, such as (username (Un_{Dri}), address (Ad_{Dri}), phone number (Pn_{Dri}), password (Pw_{Dri}), wallet address (Wa_{Dri}) and specialization (Sp_{Dri})) in the HCS once, which then generates the private key (Dr_{ipr}) and public key (Dr_{ipu}) based on the chaotic system as described in sub-section 6.1. HCS impalement HD_{Dri} = h ($Un_{Dri} \parallel Pw_{Dri}$), after that, HCS sends the information (HD_{Dri}) above to the Blockchain to register the new doctor.

6.3 Login and Authentication Phase

In this phase, once all entities are registered, the login and authentication phase of user, like Administrator, Patient, Doctor, is describe below.

6.3.1 Administrator Login and Authentication

Here, the main interaction occurs between the two basic parts (*FSP*) and the system administrator (ADM_i). Through this structure, all system privileges are linked with ADM_i accessed and overseed critical processes and system components overseen; the phase is defined as follows:

1: ADMi inputs Un_{ADMi}, Pw_{ADMi} and selects a $r_i \in Z^*$. Then, ADM_i computes A = h (Un_{ADMi}) and HA_{ADMi}=h($Pw_{ADMi} \| Un_{ADMi} \| h(r_i)$).
2: ADM_i encrypts (r_i) using the SK_{ADMi}, $E = Enc_{SK_{ADMi}}(r_i)$.
3: ADM_i submits the login request HA_{ADMi}, E, A to the FSP as the first factor.
4: When the FSP obtains the login credentials from ADM_i, it performs the following verifications:
- **a.** FSP checks if A =? Un′ADMi. If true, the FSP retrieves r'_i, where $r'_i = Dec_{SK_{ADMi}}(E)$.
- **b.** The FSP fetches Pw'_{ADM_i} from the BC, calculates $HA'_{ADM_i} = h(Pw'_{ADM_i} \| h(r'_i))$, and verifies if $HA_{ADM_i} =? HA'_{ADM_i}$. If the verification passes, the FSP sends a challenge vc *via* email to Admin.

5: Upon receiving vc′ from FSP, ADM_i evaluates L= h(FEX-ADM (Fn'_{ADMi})⊕vc′⊕h(ri)) and transmits L to FSP.
6: When FSP obtains L from ADM_i, it retrieves Fn_{ADMi} from the BC and computes L′ = h($Fn'_{ADMi} \oplus vc' \oplus h(r'_i)$). The FSP then compares L and L′. If L == L′, the FSP confirms the successful authentication of ADMi, granting access to the system's resources and services. Otherwise, the login process is denied.

Remark 1: Even though our work used fingerprints, it can also deal with biometric-based authentication methods, such as facial recognition, iris scanning, keystrokes and voice authentication.

6.3.2 Users' (Patients' and Doctors') Login and Authentication

At this stage, the user (U_i) requests access to the system's resources and services by providing valid credentials, outlining the procedural steps as follows:

1: U_i inputs Un_{Ui}, Pw_{Ui} and selects a $r_i \in Z^*$. Additionally, it computes $A = h(Un_{U_i})$ and $HU_{U_i} = \mathrm{H}(Pw_{U_i} \| Un_{U_i} \| \mathrm{h}(r_i))$.

2: U_i encrypts r_i using SK_{Ui} , $E = Enc_{SK_i}(r_i)$ *via* symmetric encryption.

3: U_i submits the login parameters $\{HA_{U_i}, \mathrm{E}, A\}$ to FSP as the first factor for authentication.

4: Upon receiving login parameters from U_i, FSP validates:

a. The FSP checks if $A =? Un'_{U_i}$. If matched, the FSP retrieves r'_i, where $r'_i = Dec_{SK_{U_i}}(E)$.

b. FSP fetches Pw'_{U_i} from BC, computes $HA'_{U_i} = \mathrm{h}(Pw'_{U_i} \| \mathrm{h}(r'_i))$ and verifies whether $HA_{U_i} = ? HA'_{U_i}$.

If the confirmation is positive, the FSP sends a challenge vc *via* email to Admin.

5: Upon receiving vc′, U_i performs $L = \mathrm{h}(Wa_{U_i} \oplus vc' \oplus \mathrm{h}(r_i)$ and transmits L toward FSP.

6: When FSP obtains L from Ui, it retrieves Wa_{U_i} from the BC, evaluates $L' = \mathrm{h}(Wa_{U_i} \oplus vc \oplus h(r'_i))$, h (r′)), The FSP then compares L and L′. If L == L′, FSP verifies Ui authentication and grants access to system resources. Otherwise, the login request is denied.

Remark 2: The login and authentication process for doctors follows procedure for P_i. Dr_i, necessity inputs a valid credential to gain an access to system services, allowing to review EHR_{P_i} and making updates as permitted by roles and privileges assigned by the administrator.

6.4 Secure Construction Phase

The initiation of this phase includes the assignment of the responsibility for formulating a construction group secret (*GS*) to the *FSP*. The procedural steps are outlined as follows:

1: *HCS* picks T_s and calls the smart-contract method of the BC to assign *FSP* by creating the following transaction (TR):

$$TR\ \{HCS_{Pu}, FSP_{Pu}, T_s\}.$$

2: The smart-contract mechanism verifies HCSP u and assesses the transaction's freshness using the criterion $T'_s - T_s \leq T_s$. Subsequently, it validates whether FSP_{pu} corresponds to the designated fog server and, if affirmative, activates *FSP*.

3: $Node_{Fog}$ initiates a request to *FSP* for the creation of $Node_{Fog_{GS}}$ dedicated to its group members. Following this, $Node_{Fog}$ selects a time (T_s) and employs FSP_{pu} to encrypt a message. Subsequently, $Node_{Fog}$ transmits the encrypted message {E($Msg \| T_s$)} to *FSP*.

4: FSP decrypts the encrypted message {E(M sg || Ts)} through the utilization of FSPP r. Subsequently, FSP assesses the timeliness of the message by verifying $T'_s - T_s \leq T_s$.

5: Utilizing the smart contract, *FSP* employs a transaction to retrieve $Node_{D_{pu}}$, where ($Node_D$ represents a medical device), associated with the medical device owned by *FSP* from the *BC*.

$$TR\ \{FSP_{Pu}, Node_{Fog_{pu}}\}.$$

6: *BC* responds by sending the public key of the medical device $Node_{D_{pu}}$ to *FSP*.

7: *FSP* selects the present timestamp (T_s) and signs $\{S_i \| T_s\}$ using FSP_{Pr}. Consequently, *FSP* encrypts E $\{(Si \| Ts)\}$ utilizing the public key of $Node_{D_{pu}}$. Then E $\{(Si \| Ts)_{signed}\}$ signed distributed across the medical devices (D_1, D_2, ..., D_n) affiliated with $Node_{Fog}$.

8: $Node_D$ decrypts $(Si \| Ts)$ using $Node_{D_{pu}}$, subsequently validating $Si \| Ts$ through FSP_{Pu}. Following this, it performs calculating $T'_s - T_s \leq T_s$. $Node_D$ and saving S_i for future utilization.

9: FSP picks T_s and then uses the method in the SM of *BC* to calculate:

$$TR\ \{FSP_{Pu}, Node_{Fog}, Node_{GS}, T_s)\}$$

10: *BC* verifies the validity of FSP_{Pu} and evaluates the transaction's timeliness by applying the condition $T'_s - T_s \leq T_s$. Subsequently, it stores $H(Node_{Fog_{GS}})$. In conclusion, the construction of the secret is completed.

7. PERFORMANCE ANALYSIS

In this section, we examine the outcome of the simulation process and the evaluation metrics used in our work, with particular attention to the performance assessment of the generation time of private, public, encryption/decryption and shared keys. This analysis considers equivalent key sizes for several 3-D map chaotic public-key cryptosystems and elliptic-curve cryptography (DHECC). Furthermore, we explore the computational costs and smart-contract costs.

7.1 Simulation

Simulation was conducted using the widely recognized Ganache simulator tool. Ganache enables the local deployment of the Ethereum blockchain in a controlled environment, offering developers a practical platform for testing and evaluation. The Truffle framework was utilized to test and deploy the smart contracts on the blockchain. Node.js was also utilized in the development of the proposed framework implemented on a Mac OS 476.0.0.0.0 LTS 64-bit platform, equipped with 8 GB of RAM and powered by a Dual-core Intel Core i5 processor operating at 2.7 GHz.

7.2 Results and Analysis

To assess the practical effectiveness of the proposed framework across various user roles and functionalities, a comprehensive performance evaluation was conducted using Apache JMeter version 5.6.3. As a widely recognized and robust performance-testing tool, Apache JMeter facilitated an in-depth analysis of the framework's capabilities, simulating real-world scenarios to ensure its reliability and efficiency.

7.2.1 Key-generation Time

The proposed work followed the DHEC key-generator algorithm of Mohammed et al. [54]; the proposed chaotic cryptosystem involves a two-part initiation time, encompassing private-key and public-key generation times. The private key is derived from a logistic chaotic map and after private-key generation, the public key is created using a modified three-dimensional beta transform system. Figure 4 illustrates a comparative analysis of DHEC key-generation times alongside one-dimensional and three-dimensional chaotic key-generation methods. Notably, the DHEC key generator exhibits a significantly slower performance than the chaotic cryptosystem's key generator at equivalent key sizes.

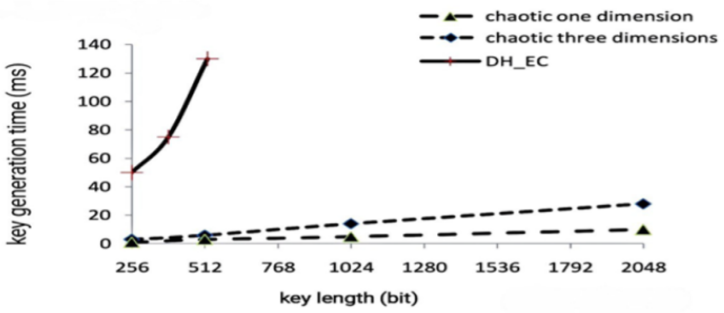
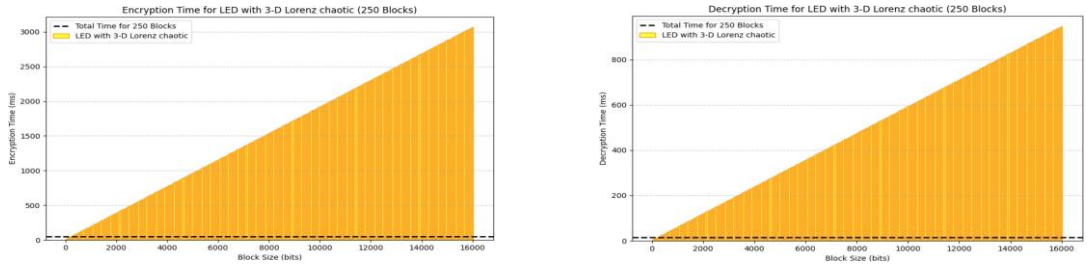


Figure 4. Comparison of DHEC key generation and one-dimensional and three-dimensional chaotic key generation [54].

7.2.2 LED with 3-D Lorenz Chaotic Encryption and Decryption Time

In the context of block-cipher encryption and decryption, the utilization of chaotic maps and the LED algorithm, as proposed by Hussain et al. [55], is explored. The shared key, generated through the chaotic Lorenz map, undergoes a double XOR operation with the state during the encryption process, contributing to the creation of ciphertext for a data block. The user-friendly nature of block ciphers is acknowledged, with an emphasis on the pivotal role of the key-generation process in determining their strength. The enhancement of the LED algorithm through integration with a 3-D Lorenz chaotic map amplifies both diffusion and randomization aspects. This augmentation results in the creation of an unexpectedly robust key, thwarting potential attacks, such as MITM and scan-based attacks. After

calculating the completion time for 250 blocks, each block with a size of 64 bits takes 19.1400 ms for the encryption process and 14.7750 ms for the decryption process. Figure 5 illustrates the amount of time taken by the process along the 250 blocks.



(a) Encryption time (b) Decryption time

Figure 5. (a) Encryption time. (b) Decryption time.

7.2.3 Computational Cost

The computational cost serves as a metric for measuring the temporal complexity of the proposed methodology within this research paper. Moreover, Table 2 and Figure 6 compare our technique with other relevant research endeavors to thoroughly evaluate its computational efficiency. Within the scope of our investigation, the proposed protocol delineates four distinct phases: setting, registration, login and authentication and secret-construction phases. Our focus will be directed towards analyzing the computational requisites specifically associated with the registration and authentication of the proposed system, as this is the most frequently accessed and utilized in the context of our research. To streamline computational analysis, we establish a clear framework by defining the computational pre-requisites associated with a verification T_v, one-way hash function T_h, symmetric key encryption and decryption T_{sym}, exclusive-or operations as T, the paring operation T_p , signature time T_{sign}, the exponential operation T_e, the one-point addition T_a , the concatenation operation T and one-point multiplication as T_m [56]-[57]. The performance evaluation of the proposed procedure includes a comprehensive comparison with contemporary state-of-the-art schemes, similar to those published in prominent publications, such as Arun et al. [58], Wu et al. [25], Jia et al. [59] and Nora et al. [20]. The proposed solution clearly outperforms them, except that there is a slight difference in the computational-time consumption between our proposed scheme and that of Wu et al. [25]. However, Wu et al. failed to meet security features, such as multi-factor authentication, and to provide a lightweight and distributed model. Moreover, their method does not use blockchain technology.

The time duration for various cryptographic operations is summarized as follows:

The time required for one-point multiplication (T_m) is 2.226 ms, while the pairing operation (T_p) takes 2.91 ms. The time to generate a signature (T_{sign}) is 0.085 ms and the exponential operation (T_e) takes 3.85 ms. The concatenation operation ($T||$) is highly efficient, requiring only 0.001 ms. Verification (T_v) is performed in 0.09 ms and a one-way hash function (T_h) takes 0.0023 ms. The time taken for encryption/decryption (T_{sym}) is 0.14 ms, whereas the exclusive OR operation (T) takes just 0.001 ms. Finally, one-point addition (T_a) is also completed in 0.001 ms.

7.2.4 Smart-contract Costs

Our approach leverages Remix as the tool for smart-contract development, formulating the contract through the Solidity language and deploying the compiled contract *via* the Ethereum Ganache tool. To determine the authentic gas costs for individual functions within the smart contract, we employed Meta- mask and Ether-scan. Within the Ethereum blockchain paradigm, fees are defined as the gas required, aligning with the payment or value essential for the successful completion of each transaction or contract execution. A user cannot execute any service and the transaction is deemed illegitimate if he/she does not have an active balance on his/her account. The deployment and expenditures of our proposed contract occur within the Remix IDE and the Meta-mask software cryptocurrency wallet, along with the corresponding blockchain block in Ganache Ethereum. The detailed outcomes of the smart contract costs are systematically documented in Figure 5 and Table 3. It is obvious from the findings presented in Table 3 that our suggested contract entails reduced costs

for both deployment and function requests.

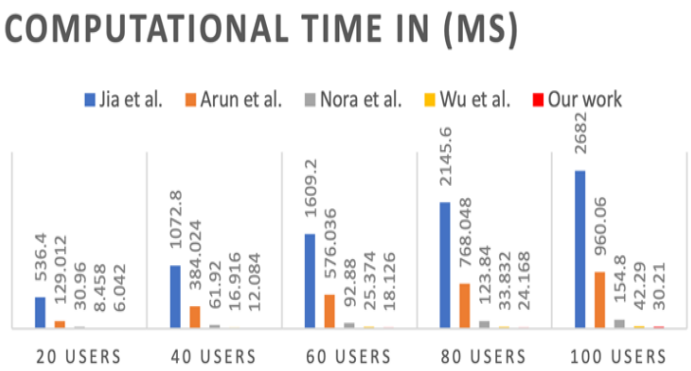


Figure 6. Computational time compared with those of other schemes.

Table 2. Relation for the calculation of computational time for registration and login and authentication phases.

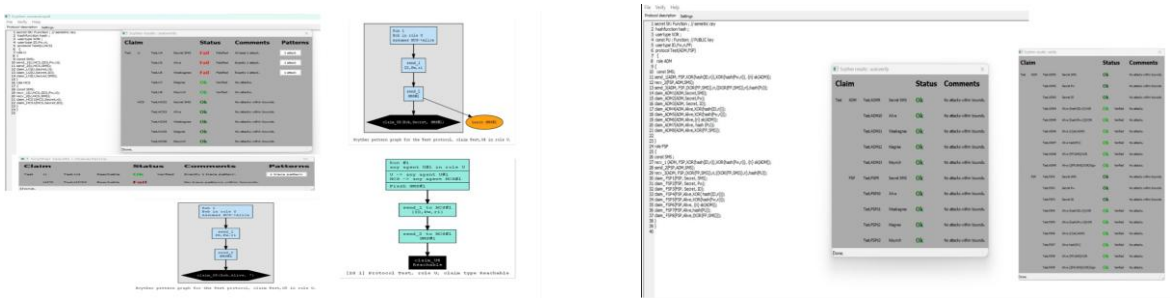
Schemes	Registration phase	Authentication phase	Total Time (ms)
Jia et al. [59]	$4T_m+T_e+5T_h$	$T_p+5T_m+(2n+1)T_a+5T_h$	**26.82**
Wu et al. [25]	$8T_h+3T+7T$ ||	$35T_h+11T+30T$ ||$+2T_{sym}$	**0.4229**
Arun et al. [58]	$2T_m+T_h+4T$	$T_m+3T+T_h+T_p+T_a$	**9.6006**
Nora et al. [20]	$4T_v+T$||	$5T_v+2T_{sign}+4T_{sym}+7T$ ||	**1.548**
Our work	$2T_h+T$ ||	$5z_h+2T+2T_{sym}+2T$ ||	**0.3021**

8. SECURITY ANALYSIS

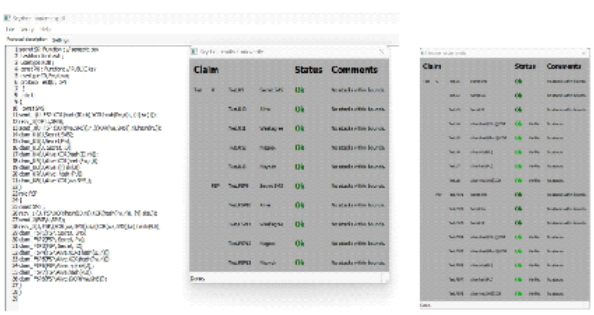
The security analysis and experimental results are explained in this section. Furthermore, the security analysis is shown in two ways: the first is a formal analysis using Scyther and the second is an informal analysis using the CK threat model [60]-[61]; after that, we determined that the proposed protocol achieves greater privacy and security than the alternatives. The GUI is intended for anyone who wants to verify or comprehend a protocol. We implemented the proposed system without utilizing security functions in the same traditional systems. Figure 7 refers to the traditional system and explains its shortcomings.

8.1 Formal Analysis

In this sub-section, we officially analyze the proposed system and demonstrate the system's data security against various attacks. By utilizing Symmetric Key Encryption, the crypto-hash function and the encryption and decryption function based on a chaotic system, we created a secure system that over-comes the disadvantages of traditional methods. Furthermore, as illustrated in Figure 7, the results of the proposed system are resistant to well-known harmful attacks.



(a) (b)



(c)

Figure 7. (a) Weakness of the traditional system of user, (b) Admin-verification protocol and automatic climes and (c) User-verification protocol and automatic climes.

Table 3. Smart-contract gas cost.

Gas Cost	**Contact Functions**
711699	Deploy contract
24765	Create_User
26621	Update_User
26621	Delete_User
175029	Add_Document

8.2 Informal Analysis

Therom1: The proposed work provides mutual authentication
Proof: This safety measure indicates that an attacker should be unable to impersonate components of the legal system, such as U_i (Admin, Patient and Doctor). The following six steps were used in this work to authenticate:
1: U_i inputs their Un_{Ui}, Pw_{Ui} and selects a $r_i \in Z_n^*$. Additionally, it computes A=h(Un_{Ui}) and HU_{Ui}=H($Pw_{Ui}\|Un_{Ui}\|$h (r_i)).
2: U_i encrypts r_i using SK_{Ui}, $E = Enc_{SK_{Ui}}(r_i)$ *via* symmetric encryption.
3: U_i submits the login parameters $\{H\ A_{Ui}, E, A\}$ to FSP as the first factor for authentication.
4: Upon receiving login parameters from U_i, FSP validates:

- **a.** The FSP checks if A =? Un'_{Ui} . If matched, the FSP retrieves r'_i, where $r_i' = Dec_{SK_{Ui}}E$.
- **b.** FSP fetches Pw'_{Ui} from BC, computes H A′Ui = h(Pw'_{Ui} ‖h(r_i')) and verifies whether $H\ A_{Ui}$ =? $H\ A'_{Ui}$. If the confirmation is positive, FSP issues a challenge VC to U_i *via* email.

5: Upon receiving VC′, U_i evaluates L = h(Wa_{Ui}⊕vc′⊕h(r_i)) and transmits L toward FSP.
6: When FSP obtains L from U_i, it retrieves Wa_{Ui} from the BC, evaluates L′ = h(Wa_{Ui}⊕vc⊕h (r_i')), the FSP then compares L and L′. If L == L′, FSP verifies U_i authentication and grants access to system resources. Otherwise, the login request is denied.

As a result, our proposed scheme accomplishes mutual authentication between the two entities (Ui, FSP). Otherwise, the current phase is rejected.

Therom2: Our proposed work aims to provide support for user anonymity.
Proof: Using C.K. adversary's perspective, an adversary has difficulty revealing the user's identity/password.
To reflect anonymity, checking the identity of login information transmitted among system components is currently required. Because the crypto hash function is integrated with r_i, which the attacker cannot identify, he/she cannot decipher the user's identity if he/she eavesdrops on the login request. Furthermore, the system generates a unique hash for every login request made by a user depending on the random number r_i. During the period of login and authentication phase, U_i sends the login request $\{H\ A_{Ui}, E, A\}$ to the *FSP* as a first authentication factor. Thus, it has been encrypted using a shared key that is known by Ui and FSP only.

An attacker finds it challenging to identify the user and is unable to recover the shared key, which is created just once for each login attempt. This suggests that our proposed scheme can support user

anonymity.

Therom 3: Our proposed work can provide unlikability.
Proof: This feature confirms that an individual can make many login attempts to the FSP to access resources and services without anybody else being able to link the logins together and identify the individual. Under the suggested plan, whenever he/she wants to access the system, he/she sends $\{H\ A_{Ui}, E, A\}$ to FSP. Thus, the basic elements of $\{H\ A_{Ui}, E, A\}$ are constructed once using the following set of points:

- **a.** The FSP verifies whether A =? Un_{Ui}. If they match, the FSP restores the r_i', where $r_i' = Dec_{SK_{Ui}}(E)$.
- **b.** The FSP obtains PwU′ from the BC, calculates HA'_{Ui} = h(Pw'_{Ui}‖h(r_i') and checks if HA_{Ui}= HA'_{Ui}. If the values match, the FSP sends a challenge, which is typically delivered *via* email.
- **c.** After receiving VC′, U_i evaluate L = h(Wa_{Ui}⊕VC′⊕h(r_i)) and transmits L back to the FSP.
- **d.** Upon receiving L from U_i, the FSP retrieves Wa_{Ui} from the BC, performs L′ = h($WaUi$⊕VC⊕h(r_i')), the FSP then compares L and L′. If L == L′, FSP performs U_i authentication and grants access. Otherwise, the login process is denied.

Therom 4: Our suggested work can guarantee forward secrecy.
Proof: During the login and authentication phase, the widely used session key relies on SK_{Ui}. Even if the shared key is revealed or leaked, our suggested system protects the password. The shared key SK_{Ui} is only generated once based on VC, so even if an attacker discloses it, the system's authentication remains secure during subsequent login attempts. It is very difficult for an opponent to determine the random number and password, as well as the characteristic of the crypto one-way hash function HU_{Ui} = h (Pw_{Ui} ‖ Un_{Ui} ‖ h(r_i)). Furthermore, this is the case if a malicious party can intercept all messages that are sent $\{H\ A_{Ui}, E, A\}$, since these parameters are created just once for each user's login request, so he/she won't be able to use them again to log into the system. Consequently, absolute forward secrecy is guaranteed by our suggested scheme.

Therom 5: Our suggested work can resist MITM attacks.
Proof: A Man-in-the-Middle attacker intercepts, alters and resends all information during a conversation, without the knowledge of the participants. We presume that the attacker has obtained $\{H\ A_{Ui}, E, A\}$and changed it as $\{HA^*_{Ui}, E^*, A^*\}$. The modified settings are ineffective and do not work because the FSP verifies A and finds (A≠A*), where A represents user identity. Additionally, the request $\{H\ A_{Ui}, E, A\}$ is generated once for each login. Thus, our suggested work does not allow MITM attacks.

Therom 6: Our proposed scheme is resistant to replay attacks.
Proof: As per our recommended plan, any new login attempt must precisely match the FSP parameters $\{H\ A_{Ui}, E, A\}$. These parameters are generated only once for every user's login request based on r_i and cannot be obtained by the user again. Therefore, this prevents any replayed message from being sent for verification, making it impossible for an attacker to launch such an attack. Hence, this technique ensures that the enemy cannot use this type of strike.

Therom 7: Our recommended scheme is resistant to eavesdropping.
Proof: This is the process for deciphering communications to find information. Each parameter shared between the user and the FSP is used only once $\{H\ A_{Ui}, E, A, VC, SK_{Ui}\}$. Consequently, if these variables are intercepted, the attacker will be unable to access the system. The user sends $\{H\ A_{Ui}, E, A\}$to FSP, then FSP decrypts r_i and sends VC to the user. Finally, the user sends L = h (Wa_{Ui} ⊕VC′⊕h(r_i)) to the FSP. As we notice, these parameters are generated once. Accordingly, the recommended scheme is resistant to eavesdropping.

Therom 8: Our proposed scheme affords key management.
Proof: For every login request, the principal parties have consented to generate a shared key using chaotic key management and public-key cryptography to ensure the security of the shared key (*SK*) between the user and the *FSP* based on (r_i, SK_{Ui}). Once the patient checks in successfully, the following actions are carried out by the primary parties (U_i, *FSP*) to carry out this phase:

- **a.** U_i calculates $SK_{Ui} = SK_{Ui} \oplus r_i$.
- **b.** *FSP* side computes $SK_{Ui} = SK_{Ui} \oplus r_i'$.

Therom 9: Our offered scheme withstands an insider attack.
Proof: Here, instead of sending these parameters (Pw_{Ui}, Un_{Ui}), users provide {HA_{Ui}, E, A} when they register with FSP, where HU_{Ui} = h ($Pw_{Ui} \parallel Un_{Ui}$), $E = Enc_{SK_{Ui}}(r_i)$, A = h (Un_{Ui}). It's difficult for an attacker to use a one-way hash function to get the user's password from the hashed result. Also, to pretend to be a real user, the attacker must create a genuine login-request parameter. However, the attacker will be unable to obtain the user's shared key (SK_{Ui}) or forge such parameters.

Theorem 10: Our scheme withstands a 51% attack.
Proof: A 51% attack in a blockchain network refers to the situation where an entity acquires more than a half of the network's mining power, enabling it to alter transactions. To resist such attacks, a distributed network is maintained where no single authority has control over the network's computer capacity. Resistance attack calculation: Let N represent the overall hashing power of the network. Let H denote the hashing power held by the attacker in order to execute a 51% attack effectively. To carry out such an attack, the attacker must have control over more than 51% of the total hashing power, where H is less than 0.5 times N and greater than 0.5 times N. Thus, the ability to prevent a 51% attack is determined by the level of decentralization in the network, where no single entity possesses the majority of the hashing power.

Theorem 11: Our scheme withstands a hijacking attack.
Proof: Blockchain technology utilizes robust cryptographic methods to safeguard data and transactions. By employing methods, such as digital signature and encryption, one may effectively check the legitimacy of both the user and the data. This, in turn, thwarts any efforts at hijacking by implementing multi-factor authentication. It enhances security by implementing an additional layer that necessitates users to submit several forms of verification, such as passwords, biometrics and OTP, before gaining access to the system. This enhances the level of complexity for potential attackers attempting to seize control of user accounts.

9. CONCLUSION

This research elucidates significant concerns about privacy and security within the IoHT industry. Our developed system integrates fog computing, extends cloud services to network peripheries and offers enough computational support for IoHT devices, so that there is less communication needed for authentication. Our work uses a chaotic key cryptosystem that works with random keys, is small, reduces communication needs and is the right size for IoHT devices' limited processing power. In addition, to protect people and organizations that use public channels in a decentralized setting, our research combines an authentication system with blockchain technology that can't be changed. Furthermore, blockchain technology facilitates decentralized node identification. According to the results of the evaluation, the proposed approach is very reliable and scalable, which means that it will provide strong security and be resistant to common attacks. In addition, it has less latency than current blockchain-based authentication systems, which shows how useful and efficient it is in the real world. We conducted a simulation of the proposed project using the Ethereum platform, Ganache and the Solidity programming language for the deployment and testing of smart contracts. Additionally, we used the Apache JMeter tool to assess both latency and throughput, with a time cost of 0.3021 ms, an average registration delay of 1.25 ms and an authentication time of 1.50 ms. A security study of the suggested method was conducted using the Scyther tool. The formal and informal security assessments demonstrated that the proposed method is secure and resilient against possible assaults. Furthermore, our research bolstered the scalability of the IoHT system. Future development plans also include the use of quantum cryptography as an alternative to existing technology and the utilization of 6G networks to enhance speed and efficiency.

REFERENCES

[1] A. H. Ameen, M. A. Mohammed and A. N. Rashid, "Dimensions of Artificial Intelligence Techniques, Blockchain and Cyber Security in the Internet of Medical Things: Opportunities, Challenges and Future Directions," Journal of Intelligent Systems, vol. 32, no. 1, p. 20220267, 2023.

[2] B. Pradhan, S. Bhattacharyya and K. Pal, "IoT-based Applications in Healthcare Devices," Journal of Healthcare Engineering, vol. 2021, no. 1, p. 6632599, 2021.

[3] N. Garg et al., "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," IEEE Access, vol. 8, pp. 95956–95977, 2020.

[4] Y. Aydin, G. K. Kurt, E. Ozdemir and H. Yanikomeroglu, "A Flexible and Lightweight Group Authentication Scheme," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10277–10287, 2020.

[5] S. M. Umran et al., "Secure Data of Industrial Internet of Things in a Cement Factory Based on a Blockchain Technology," Applied Sciences, vol. 11, no. 14, p. 6376, 2021.

[6] M. El-Hajj, A. Fadlallah, M. Chamoun and A. Serhrouchni, "A Survey of Internet of Things (IoT) Authentication Schemes," Sensors, vol. 19, no. 5, p. 1141, 2019.

[7] G. Apruzzese et al., "The Role of Machine Learning in Cyber-security," Digital Threats: Research and Practice, vol. 4, no. 1, pp. 1–38, 2023.

[8] S. Matsumoto et al., "Authentication Challenges in a Global Environment," ACM Transactions on Privacy and Security (TOPS), vol. 20, no. 1, pp. 1–34, 2017.

[9] S. C. Seak et al., "A Centralized Multi-modal Unified Authentication Platform for Web-based Application," Proc. of the World Congress on Engineering and Computer Science (WCECS 2014), vol. 1, San Francisco, USA, 2014.

[10] D. Nkomo and R. Brown, "Hybrid Cyber Security Framework for the Internet of Medical Things," Blockchain and Clinical Trial: Securing Patient Data, Part of the Book Series: Advanced Sciences and Technologies for Security Applications (ASTSA), pp. 211–229, 2019.

[11] M. Jmaiel et al., "The Impact of Digital Technologies on Public Health in Developed and Developing Countries," Proc. of the 18th Int. Conf. on Smart Homes and Health Telematics (ICOST 2020), vol. 12157, Hammamet, Tunisia, 2020.

[12] I. Purdon and E. Erturk, "Perspectives of Blockchain Technology, Its Relation to the Cloud and Its Potential Role in Computer Science Education," Engineering, Technology & Applied Science Research, vol. 7, no. 6, 2017.

[13] N. Deepa et al., "A Survey on Blockchain for Big Data: Approaches, Opportunities and Future Directions," Future Generation Computer Systems, vol. 131, pp. 209–226, 2022.

[14] S. M. Umran et al., "Secure and Privacy-preserving Data-sharing Framework Based on Blockchain Technology for Al-Najaf/Iraq Oil Refinery," Proc. of the 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (Smart-World/UIC/ScalCom/DigitalTwin/PriComp/Meta), pp. 2284–2292, 2022.

[15] H. Sheth and J. Dattani, "Overview of Blockchain Technology," Asian J. For Convergence in Technology (AJCT), vol. 5, no. 1, 2019.

[16] S. M. Umran et al., "Multi-chain Blockchain Based Secure Data-sharing Framework for Industrial IoTs Smart Devices in Petroleum Industry," Internet of Things, vol. 24, p. 100969, 2023.

[17] S. Tuli, R. Mahmud, S. Tuli and R. Buyya, "FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing," Journal of Systems and Software, vol. 154, pp. 22–36, 2019.

[18] H. Reffad, A. Alti and A. Almuhirat, "A Dynamic Adaptive Bio-inspired Multi-agent System for Healthcare Task Deployment," Engineering, Technology & Applied Science Research, vol. 13, no. 1, pp. 10192–10198, 2023.

[19] O. Umoren, R. Singh, S. Awan, Z. Pervez and K. Dahal, "Blockchain-based Secure Authentication with Improved Performance for Fog Computing," Sensors, vol. 22, no. 22, p. 8969, 2022.

[20] 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, pp. 162–181, 2024.

[21] R. Almadhoun et al., "A User Authentication Scheme of IoT Devices Using Blockchain-enabled Fog Nodes," Proc. of the 2018 IEEE/ACS 15th Int. Conf. on Computer Systems and Applications (AICCSA), pp. 1–8, Aqaba, Jordan, 2018.

[22] A. Mehmood et al., "Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications," IEEE Access, vol. 6, pp. 33552–33567, 2018.

[23] Y. Liang, "Identity Verification and Management of Electronic Health Records with Blockchain Technology," Proc. of the 2019 IEEE Int. Conf. on Healthcare Informatics (ICHI), pp. 1–3, Xi'an, China, 2019.

[24] X. Cheng, F. Chen, D. Xie, H. Sun and C. Huang, "Design of a Secure Medical Data Sharing Scheme Based on Blockchain," Journal of Medical Systems, vol. 44, no. 2, p. 52, 2020.

[25] T.-Y. Wu et al., "Improved ECC-based Three-factor Multiserver Authentication Scheme," Security and Communication Networks, vol. 2021, no. 1, p. 6627956, 2021.

[26] Y. Guo and Y. Guo, "FogHA: An Efficient Handover Authentication for Mobile Devices in Fog Computing," Computers & Security, vol. 108, p. 102358, 2021.

[27] I. T. Javed et al., "Health-ID: A Blockchain-based Decentralized Identity Management for Remote Healthcare," Healthcare, vol. 9, no. 6, p. 712, MDPI, 2021.

[28] I.-T. Chen, J.-M. Tsai, Y.-T. Chen and C.-H. Lee, "Lightweight Mutual Authentication for Healthcare IoT," Sustainability, vol. 14, no. 20, p. 13411, 2022.

[29] O. Umoren, R. Singh, Z. Pervez and K. Dahal, "Securing Fog Computing with a Decentralized User Authentication Approach Based on Blockchain," Sensors, vol. 22, no. 10, p. 3956, 2022.
[30] H. Miriam et al., "Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology," Intelligent Automation & Soft Computing, vol. 35, no. 2, 2023.
[31] S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," [Online], Available: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf, 2008.
[32] A. A.-N. Patwary et al., "FogAuthChain: A Secure Location-based Authentication Scheme in Fog Computing Environments Using Blockchain," Computer Communications, vol. 162, pp. 212–224, 2020.
[33] W. J. Gordon et al., "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-driven Interoperability," Computational and Structural Biotechnology J., vol. 16, pp. 224– 230, 2018.
[34] P. P. Ray, D. Dash, K. Salah and N. Kumar, "Blockchain for IoT-based Healthcare: Background, Consensus, Platforms and Use Cases," IEEE Systems Journal, vol. 15, no. 1, pp. 85–94, 2020.
[35] Z. Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus and Future Trends," Proc. of the 2017 IEEE Int. Congress on Big Data (BigData Congress), pp. 557–564, Honolulu, USA, 2017.
[36] N. Z. Benisi, M. Aminian and B. Javadi, "Blockchain-based Decentralized Storage Networks: A Survey," Journal of Network and Computer Applications, vol. 162, p. 102656, 2020.
[37] R. Zhang, R. Xue and L. Liu, "Security and Privacy on Blockchain," ACM Computing Surveys (CSUR), vol. 52, no. 3, pp. 1–34, 2019.
[38] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," Proc. of the 1st Edition of the MCC Workshop on Mobile Cloud Comp. (MCC'12), pp. 13–16, 2012.
[39] Y. C. Hu et al., "Mobile Edge Computing: A Key Technology Towards 5G," ETSI White Paper, vol. 11, no. 11, pp. 1–16, 2015.
[40] H. Sabireen and V. Neelanarayanan, "A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges," ICT Express, vol. 7, no. 2, pp. 162–176, 2021.
[41] M. Yannuzzi et al., "Key Ingredients in An IoT Recipe: Fog Computing, Cloud Computing and More Fog Computing," Proc. of the 2014 IEEE 19th Int. Workshop on Computer-aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 325–329, Athens, Greece, 2014.
[42] M. Mohammed et al., "Chaotic-based Public Key Cryptosystem for PGP Protocol," Proc. of the Int. Conf. on Aerospace Sciences and Aviation Technology, vol. 15, pp. 1–17, The Military Technical College, Cairo, Egypt, 2013.
[43] B. Bai, S. Nazir, Y. Bai and A. Anees, "Security and Provenance for Internet of Health Things: A Systematic Literature Review," J. of Software: Evolution and Process, vol. 33, no. 5, p. e2335, 2021.
[44] V. O. Nyangaresi, "Biometric-based Packet Validation Scheme for Body Area Network Smart Healthcare Devices," Proc. of the 2022 IEEE 21st Mediterranean Electrotechnical Conf. (MELECON), pp. 726–731, Palermo, Italy, 2022.
[45] X. Li, J. Ma and S. Moon, "On the Security of the Canetti-Krawczyk Model," Proc. of the Int. Conf. on Computational and Information Science, Part of the Book Series: Lecture Notes in Computer Science, vol. 3802 pp. 356–363, 2005.
[46] S. Shamshad et al., "An Enhanced Scheme for Mutual Authentication for Healthcare Services," Digital Communications and Networks, vol. 8, no. 2, pp. 150–161, 2022.
[47] Z. Bao et al., "A Group Signature Scheme with Selective Linkability and Traceability for Blockchain-based Data Sharing Systems in E-health Services," IEEE Internet of Things Journal, vol. 10, no. 23, pp. 21115–21128, 2023.
[48] A. A. Mazlan et al., "Scalability Challenges in Healthcare Blockchain System: A Systematic Review," IEEE Access, vol. 8, pp. 23663– 23673, 2020.
[49] G. Somani et al., "DDoS Attacks in Cloud Computing: Issues, Taxonomy and Future Directions," Computer Communications, vol. 107, pp. 30–48, 2017.
[50] N. Sivasankari and S. Kamalakkannan, "Detection and Prevention of Man-in-the-Middle Attack in IoT Network Using Regression Modeling," Advances in Engineering Software, vol. 169, p. 103126, 2022.
[51] C.-M. Chen, Z. Chen, S. Kumari and M.-C. Lin, "LAP-IoHT: A Lightweight Authentication Protocol for the Internet of Health Things," Sensors, vol. 22, no. 14, p. 5401, 2022.
[52] W. Yang et al., "Security Analysis of a Distributed Networked System under Eavesdropping Attacks," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 7, pp. 1254–1258, 2019.
[53] X. Xiang, M. Wang and W. Fan, "A Permissioned Blockchain-based Identity Management and User Authentication Scheme for E-health Systems," IEEE Access, vol. 8, pp. 171771–171783, 2020.
[54] M. T. Mohammed et al., "Chaotic Based Key Management and Public-key Cryptosystem," Int. J. of Computer Science and Telecommunications, vol. 3, no. 11, pp. 35–42, 2012.
[55] H. M. Al-Saadi and I. Alshawi, "Provably-secure Led Block Cipher Diffusion and Confusion Based on Chaotic Maps," Informatica, vol. 47, no. 6, pp. 105-114, 2023.

[56] S. Majumder et al., "Wearable Sensors for Remote Health Monitoring," Sensors, vol. 17, no. 1, p. 130, 2017.

[57] D. Formica and E. Schena, "Smart Sensors for Healthcare and Medical Applications," Sensors, vol. 21, no. 2, p. 543, 2021.

[58] A. S. Rajasekaran et al., "Blockchain Enabled Anonymous Privacy-preserving Authentication Scheme for Internet of Health Things," Sensors, vol. 23, no. 1, p. 240, 2022.

[59] X. Jia, D. He, N. Kumar and K.-K. R. Choo, "A Provably Secure and Efficient Identity-based Anonymous Authentication Scheme for Mobile Edge Computing," IEEE Systems Journal, vol. 14, no. 1, pp. 560–571, 2019.

[60] M. Burrows, M. Abadi and R. Needham, "A Logic of Authentication," DEC System Research Centre Report, ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, February 1990.

[61] M. N. Aman, K. C. Chua and B. Sikdar, "A Light-weight Mutual Authentication Protocol for IoT Systems," Proc. of GLOBECOM 2017-2017 IEEE Global Communications Conf., pp. 1–6, Singapore, 2017.

ملخص البحث:

إنّ إنترنت الأشياء الصّحّية عبارة عن شبكةٍ من أجهزة الرّعاية الصّحّية والبرمجيات والأنظمة الّتي تمكّن من الرّصد عن بُعد وتقديم خدمات الرّعاية الصّحّية عبر جمع بياناتٍ تتعلّق بالصّحّة في الزّمن الحقيقي من خلال المجسّات. وعلى الرّغم من فوائدها الجمّة للرّعاية الصّحّية الحديثة الذّكية، فإن إنترنت الأشياء الصّحّية تواجه تحدّياتٍ ترتبط بالأمان ترجع إلى القدرة المحدودة على المعالجة وسعة التّخزين وإمكانيات الدّفاع عن النّفس لأجهزتها. وبينما تمّ تطوير حلول مصادقة قائمة على سلاسل الكُتل ومستندة إلى تحسين أمن البيانات، فإنها تتطلّب مصادر حوسبة عديدة وزيادة في إمكانات التّخزين وتحتاج إلى أزمان طويلة من أجل إنجاز المصادقة، الأمر الّذي يعيق إمكانية توسيعها وزيادة فاعليتها في أنظمة إنترنت الأشياء الصّحّية الموسّعة والّتي يلعب الزّمن فيها دوراً حاسماً.

وللتعامل مع هذه التّحدّيات، نقترح في هذه الورقة نظام مصادقةٍ مكوّناً من أربع مراحل تشمل الإعداد، والتّسجيل، والمصادقة، وإنشاء السّرّية. ويدمج النّظام المقترح بين أنظمة ترميز المفاتيح العامّة بناءً على "الفوضى"، وجهاز ترميز مع خوارزمية خريطة لورنس الفوضوية ثلاثية الأبعاد، وتقنيات الحوسبة الضّبابية القائمة على سلاسل الكُتل؛ من أجل تحسين كلٍّ من الفاعلية وإمكانية التّوسيع.

وبتقييم النّظام المقترح عبر مقارنته بأنظمة مصادقةٍ تقليديةٍ وردت في أدبيات الموضوع، أبدى النّظام المقترح أداءً متفوّقاً مع تخفيض في تكلفة الحوسبة. وقد بلغ معدّل زمن التّأخير اللّازم للتّسجيل (1.25) ميلي ثانية، بينما تكتمل عملية المصادقة في (1.50) ميلي ثانية، الأمر الذي يجعل النّظام المقترح ملائماً لتطبيقات إنترنت الأشياء للرّعاية الصّحية الّتي يُعدّ فيها الزّمن عاملاً حاسماً. وأثبت تحليل الأمان أن النّظام المقترح مقاوم للهجمات الإلكترونية بما فيها هجمات 51% وهجمات الاختطاف، بينما يتمّ الحفاظ على تكامل البيانات وسرّيتها. علاوة على ذلك، فإنّ النّظام المقترح يخفض تكلفة الاتّصال ويدعم إمكانية توسيع أنظمة إنترنت الأشياء الصّحّية ذات الحجم الكبير.

والجدير بالذّكر أنّ هذه النّتائج تبين أنّ النّظام المقترح يمتلك الإمكانية لإحداث ثورةٍ في مجال الرّصد الآمن والفعّال لبيانات أنظمة إنترنت الأشياء الصّحّية، الأمر الّذي يمكّن من إدارة البيانات في الزّمن الحقيقي في بيئات إنترنت الأشياء الصّحّية بأمانٍ وفاعلية.