International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 17 (2025) pp. 690-703

https://doi.org/10.70917/ijcisim-2025-0042
Article

Building Strong Single Sign-On Solutions in IoHT Environments Based on Blockchain Technology

Muwafaq Jawad [1], Ali A. Yassin [1,*], Mushtaq Hasson [1], Nada Ali [1], Abdulla J. Y. Aldarwish [1], Hamid Ali Abed AL-Asadi [1], Feda Hamdan Hamad [2] and Zahraa Sh. Alzaidi [1]

[1] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
[2] School Al Sarhan Secondary Mixed, Almafraq 25110, Jordan
* Correspondence author: ali.yassin@uobasrah.edu.iq

Received date: 30 November 2024; Accepted date: 12 November 2025; Published online: 31 December 2025

Abstract: The Internet of Health Things (IoHT) refers to an interconnected network of healthcare devices, software, and systems that facilitate remote healthcare services. While beneficial, IoHT devices often have insufficient processing power and security, creating significant vulnerabilities. Blockchain has been proposed as a solution, but its resource-intensive nature can hinder the scalability and time efficiency required for large-scale IoHT systems. To address these challenges, this study introduces a novel authentication framework specifically for IoHT environments. Our proposed scheme integrates a 3D chaotic-based public key cryptosystem with blockchain-enabled fog computing to enhance both security and performance. Therefore, these issues pose obstacles to achieving optimal scalability and time efficiency, which are essential factors for the effective operation of vast, time-sensitive IoHT systems. To achieve this objective, the present study introduces an authentication technique that is specifically designed for IoHT systems. Our authentication scheme consists of three phases: setup, registration, single sign-on (SSO), and login and authentication. To enhance efficiency and scalability, the proposed scheme employs a combination of 3D chaotic-based public key cryptosystems and blockchain-based fog computing technologies. Formal security verification using the Scyther tool confirms that the protocol is robust and finds no attack vulnerabilities within the specified bounds. Furthermore, our analysis demonstrates that the scheme is secure against a range of critical threats, including Man-in-the-Middle (MITM), replay, Sybil, and 51% attacks. Crucially, the performance results show that our approach achieves superior scalability and security. These findings establish our framework as a practical and secure solution for deploying strong, efficient single sign-on systems in time-sensitive IoHT environments.

Keywords: Internet of Health Things (IoHT); blockchain technology; single sign-on (SSO); fog computing;chaotic cryptography; healthcare cybersecurity; decentralized authentication

1. Introduction

As the digital world grows and more companies and healthcare facilities use online services, the use of effective and secure identification procedures has increasingly become a necessity. Managing usernames and passwords can be difficult for users, as this can cause weariness and loss. In turn, such a behavior results in decreased productivity and increased security threats because users frequently use weak or repeated passwords [1]. The sharp increase in cybercrimes, which are predicted to result in losses and material damage over the next few years, emphasizes the significance of creating robust authentication procedures [2]. With the single sign-on (SSO) option, users may now access various

applications with just one set of login credentials, making it a workable alternative. Consequently, the user experience is improved, and authentication procedures are made simpler. However, traditional SSO solutions may have built-in drawbacks, such as dependency on centralized identity providers and certain security vulnerabilities [3]. The primary advantage of SSO lies in its ability to improve customer satisfaction. In particular, SSO effectively eliminates the need for multiple logins, thus reducing user frustration and minimizing the time spent on authentication processes by allowing users to log in once and access various applications. Research suggests that SSO's capability to facilitate cross-platform access can boost productivity by up to 30% [4]. Additionally, SSO contributes to enhanced security by alleviating password fatigue, which often leads to poor password practices. With fewer credentials to remember, users are less likely to create weak passwords [5]. Another advantage of using SSO is that it simplifies the user access control procedure for IT departments. Organizations may better manage user permissions, track access, and enforce security regulations by offering a single point of authentication. This centralized approach helps firms maintain a clearer audit trail of user access, which enhances operational efficiency and helps them comply with rules and regulations [6,7].

Yet, even with their benefits, classic SSO solutions also have multiple drawbacks. One major concern are the security hazards connected to a central identity provider. An attacker could cause significant data breaches by gaining access to all related applications if their SSO credentials are compromised. For instance, the Okta hack of 2020 highlights the need for stronger security measures by underscoring the inherent vulnerabilities of centralized authentication systems [8,9]. Furthermore, adding SSO to already complicated IT infrastructures may make them more complex. Considerable work and experience are also required to integrate SSO with various apps and systems, especially in businesses that still use outdated technologies. Concerns regarding control over their credentials and privacy may also cause users to avoid adopting new authentication techniques; nonetheless, these issues need to be resolved for successful adoption [10–12].

Blockchain technology, first created as an underpinning structure for cryptocurrencies, has developed into a potent instrument for boosting security in a variety of applications, including digital identity management. Fundamentally, blockchain functions as a decentralized ledger that logs transactions across several computers and prevents data from being altered after the fact [13]. Owing to its immutability, blockchain is a desirable option for authentication systems, where maintaining data integrity is crucial [14]. The hazards associated with single points of failure that are characteristic of conventional authentication techniques are eliminated by the decentralized structure of blockchain [15]. User credentials can also be maintained in a blockchain-based SSO system, enabling users to authenticate independently of a central authority. With the help of this paradigm change, users can now regulate who has access to their credentials and exercise more control over their online identities [14,16].

Integrating blockchain into SSO frameworks has numerous noteworthy benefits.

- First, decentralization leads to increased security. Blockchain reduces the dangers of data breaches connected to centralized identity providers by dispersing user credentials among a network of nodes [17, 18].
- The bulk of nodes will continue to maintain accurate data, so even if one node is compromised, the system's overall integrity is preserved. Users can also maintain control over who they are because of blockchain technology.
- Users can also maintain the security of their own credentials with self-sovereign identity models, allowing access to only the applications that they select.
- By granting consumers ownership of their identity data, this method improves privacy and gives them more power against potential attacks [19].
- Furthermore, blockchain-based solutions can simplify identity verification on many platforms, which in turn lowers friction in user communications. Third, a safe audit trail for authentication events is offered by the incommensurability of blockchain data [20].

In this way, companies can quickly monitor and confirm user access, which enhances regulatory compliance and speeds up incident response. Given that users are assured that their data are maintained properly and are not tampered with, transparency can increase user trust [21].

Indeed, SSO and blockchain technology integration have provided new opportunities for improving security and user experience. By using blockchain technology and addressing the shortcomings of conventional SSO systems, enterprises can develop more adaptable and user-centered authentication solutions. Furthermore, recognizing the advantages and difficulties of this integration is essential for businesses hoping to prosper amid more complicated digital environments. Finally, our approach combines immutable blockchain technology and fog computing with an SSO authentication scheme to ensure the security of participants communicating through public channels in a decentralized environment. Blockchain technology also supports the identification of decentralized nodes.

Based on the information presented above, our work makes the following contributions:

- Use of multifactor authentication that includes several factors.
- Introduction of an SSO authentication scheme based on blockchain and fog computing.
- Use of a 3D map chaotic key cryptosystem to ensure scalability and efficiency while minimizing communication overhead during authentication; and
- Confirmation of the robustness of the proposed approach against well-known threats and modern cybersecurity attacks, such as 51%, hijacking, and Sybil, by conducting a thorough security analysis using the Scythe tool.

The remainder of the paper is organized as follows: a summary of related works is presented in Section 2; Section 3 discusses primitive tools; Section 4 describes the system model; Section 5 provides an explanation of the proposed scheme and its phases; Section 6 thoroughly discusses the performance analysis, simulation, and assessment metrics; Section 7 presents the formal security analyses; and Section 8 presents the conclusion.

2. Related Works

In 2018, Almadhoun et al. [22] proposed an authentication system using blockchain-enabled fog nodes and Ethereum smart contracts to mitigate the capacity limitations of the IoT, facilitate access to IoT devices, and authenticate users. This approach allows the system to augment its capability by using fog nodes for computing tasks. However, the system exhibited low time efficiency in authenticating IoT devices. Furthermore, despite providing robust security, the scheme failed to meet the demands of the majority of IoT connection situations. This approach also has drawbacks, including computational expense, because the integration of blockchain with a smart contract may not be appropriate for all IoT devices, particularly those with constrained processing capabilities. Furthermore, regarding scalability and security flaws, it is not completely impervious to assaults; possible weaknesses still exist inside smart contracts [23].

In 2020, Yang et al. [24] proposed a blockchain-based access control architecture named AuthPrivacyChain, focusing on privacy protection in cloud environments. In this system, all transaction-related authorizations are recorded on the blockchain by users. Furthermore, the framework was developed using an enterprise operating system (EOS) blockchain to provide access to permissions and information, serving as an additional elucidation of blockchain transactions. AuthPrivacyChain also provides access control, authorization revocation, and authorization management. However, the experimental findings indicate that only authorized users may access resources and that AuthPrivacyChain is ineffective in thwarting assaults from external users [25].

In 2022, Umoren et al. [26] used blockchain smart contracts to resolve challenges associated with user authentication and other limitations in fog and IoT technology. The decentralized fog computing architecture incorporated secure authentication, immutability, and scalability, as well as addressed issues of scalability and immutability associated with fog computing. Despite providing robust security, the proposal failed to meet the demands of typical IoT networking situations. The paper not only inadequately addressed the implementation of the suggested system but also provided ambiguous explanations for the data format and code, thus hindering other researchers' ability to replicate and enhance the study. Moreover, the information addressing the trial design and performance indicators is insufficient. Comprehensive elucidations of the simulation model and its results are necessary to adequately validate the findings.

In 2022, Manoj et al. [27] used the Hyperledger Indy public permissioned blockchain architecture to handle patients' self-sovereign identification by storing their decentralized IDs and schemas for each form of credential. The credentials were maintained "off-ledger" in digital wallets owned by patients. Hyperledger Aries functioned as a middleware layer (API) that facilitated the connection between Hyperledger Indy and digital wallets. Hyperledger Indy and Aries, both created by the Hyperledger Foundation, have been used in prior studies to incorporate blockchain technology with electronic health records.

In 2023, Fugkeaw et al. [28] suggested a blockchain-based system for identity verification and access management tailored for SSO data access. In this system, smart contracts govern access control for cloud resources by data users, thus ensuring traceability throughout the access process. Furthermore, the SSO authentication uses a hash-based token management system to accurately validate identities. Notwithstanding these developments, the storage of access control rules in cloud storage continues to pose a danger of data leakage.

In 2024, Asaeed et al. [29] introduced a group authentication method using the SSS algorithm, ECC, fog computing, and multilevel blockchain to provide a lightweight and scalable solution for group authentication in the Internet of Medical Things (IoMT), thus addressing challenges such as scalability and time efficiency. The assessment exam exhibited commendable scalability and temporal efficiency.

However, the ECC algorithm had difficulties in managing the substantial number of devices and sensors due to its restricted key size. Therefore, in the current study, we used the chaotic method of 3D maps to solve this problem. Table 1 shows a comparison of the related works.

Table 1. Comparison feature summary of the related work.

Author name	Chaiotic	SSO	Fog	Block chain	51% Attack	Sybil attack	Hijacking
Almadhoun et al 2018 [22]	N	N	N	Y	Y	N	N
Yang et al [24] 2020	N	N	N	Y	Y	N	N
Umoren et al [26] 2022	N	-	N	Y	Y	N	-
Manoj et al [27] 2022	N	N	N	N	Y	Y	Y
Fugkeaw et al [28] 2023	N	Y	Y	N	Y	-	Y
Asaeed et al [29] 2024	N	Y	N	Y	Y	N	Y
Our work	Y	Y	Y	Y	Y	Y	Y

Some of the concerns mentioned above have been solved in our previous studies [30], and this paper came as an extension to address the remaining ones by focusing on merging SSO technology with blockchain.

3. Preliminaries

3.1.Blockchain Technology

In 2008, Satoshi Nakamoto introduced blockchain technology [31], a decentralized network that manages chronologically recorded documents. The system, which is based on transparency, decentralization, and immutability, ensures secure data sharing in the IoT [14]. It is also widely used in mutual authentication and secure storage. Meanwhile, the healthcare industry places high importance on patient data protection due to technological advancements. Thus, many experts believe that integrating blockchain technology into the healthcare sector is a viable option to improve data protection. In the current study, the Ethereum blockchain was chosen for its superior performance in managing large transactions [32].

3.2. SSO Technology

The SSO system allows users to access numerous apps, services, or websites using a single set of credentials. This is advantageous because it eliminates the need for several passwords and mitigates the risk of intrusions. SSO solutions enhance user control by enabling IT managers to efficiently monitor and manage user permissions, thus mitigating the risk of unauthorized access. Streamlined login procedures are implemented, particularly in sectors such as healthcare and law enforcement, where rapid access is essential. SSO also improves security by enabling users to select more intricate passwords, safeguarding them against cyber threats through a unified access point. Organizations may also use supplementary security protocols, such as multifactor authentication, to augment their system security [33,34].

3.3. Chaotic Cryptography

This study employed chaos-based key management and a public key cryptosystem developed by Mohammed [1]. The cryptosystem has been used to provide features of a public-key cryptosystem, including key exchange, administration, and encryption/decryption of the designated information. Moreover, the cryptographic protocol of the system adeptly mitigates the threat of man-in-the-middle (MITM) assaults by employing chaotic management systems as its underpinning element. The provided key management system is founded on the beta-transformation mapping. In this study, an evaluation was performed to contrast the novel chaotic key exchange protocol with the Diffie-Hellman elliptic curve cryptosystem (DHECC). Figure 1 illustrates the key generation duration for the ECC and chaotic-based systems.

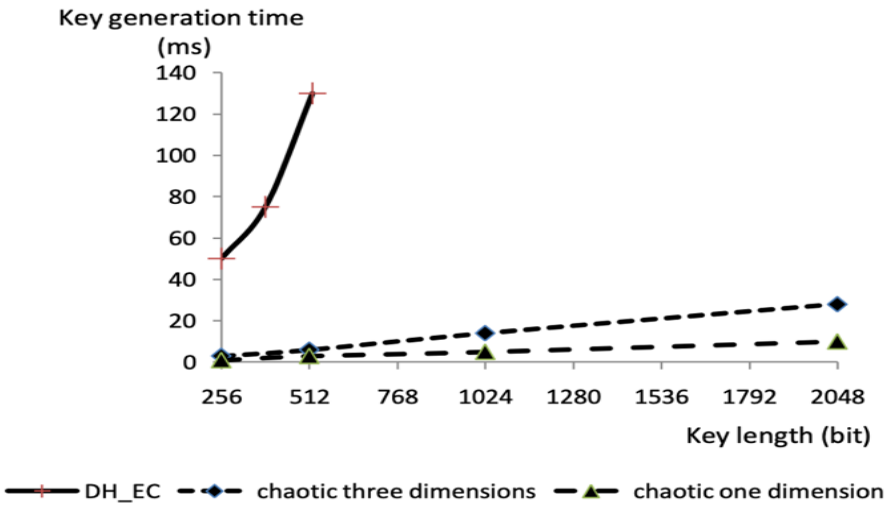


Figure 1. Key generation time in each ECC and chaotic-based system [1].

3.4. Fog Computing

Cisco launched fog computing in 2012 to mitigate network congestion and latency problems associated with traditional cloud services. Fog computing extends computational functions to the periphery, including terminal nodes within its scope. The implementation of intermediary infrastructure, referred to as *fog nodes*, occurs between the cloud's virtualized environment and end-users at terminal nodes. These nodes function as immediate centers for data processing and storage prior to transmission to the cloud. Two principal fog computing topologies can be found in IoT systems: a tri-tiered architecture that includes a cloud tier and a fog layer [35]. The cloud layer offers extensive computational and storage capabilities, while the fog tier provides near-real-time storage and computing services for IoT devices. The fog tier directly supports IoT devices by using localized tiny cloud infrastructures, thus eliminating the need for external cloud hosting [36]. The rest of the section describes the proposed scheme's network and security models.

4. Network Model

It is crucial to understand the fundamental ideas that enable our proposed scheme before diving into its deep specifics. These fundamental principles are of great importance in blockchain-based authentication systems as they serve as crucial points of reference [26,37]:

- Fog computing - The ecosystem encompasses a diverse array of mobile and stationary devices, including smartphones, sensors, embedded systems, and stationary edge servers. These devices are closely linked through numerous communication networks.
- The device employed by registered users effectively integrates and uses blockchain technology, hence improving the functionality of the system.
- To efficiently carry out its designated tasks, a fog server must satisfy certain specific requirements, such as the ability to serve as a host for the blockchain and operate as a server or node within the network structure.

The network model comprises four layers, which are illustrated in Figure 2 and explained below.

A) ***User Layer (U):*** A system user is an individual who possesses the knowledge and skills to efficiently utilize system resources. Users possess unique roles and characteristics within the system, which enable their identification. The system is interacted with by *patients, doctors, nurses, administrators, and other individuals*, whose main duty is to engage with the system to carry out vital tasks, such as producing, reading, updating, deleting, accessing, and managing medical records.

B) ***Fog Computing Layer (FCS)***: This layer comprises several fog servers that function as blockchain nodes, along with dedicated servers to uphold the decentralized blockchain system. These devices guarantee the secure and efficient transfer of data from IoHT devices and provide various services, while also maintaining synchronized copies of the blockchain, ledger, and smart contracts. Furthermore, fog servers are responsible for registering and authenticating the users.

C) ***Healthcare Server Provider Layer (HCS):*** This server is in charge of initiating the blockchain network and registering all fog servers. It is also responsible for generating all required parameters such as private, public, and shared keys for fog services, users, and the HCS itself.

D) ***Blockchain Layer (BC):*** This serves as a decentralized entity responsible for the identification and registration of all FCS, users, and IoHT devices. Smart contracts embedded into the blockchain architecture handle the management of authentication and identity operations. Every fog server verifies the identity of IoHT devices and users within its designated region using blockchain technology. Importantly, the blockchain is accessible at all levels of the system architecture.

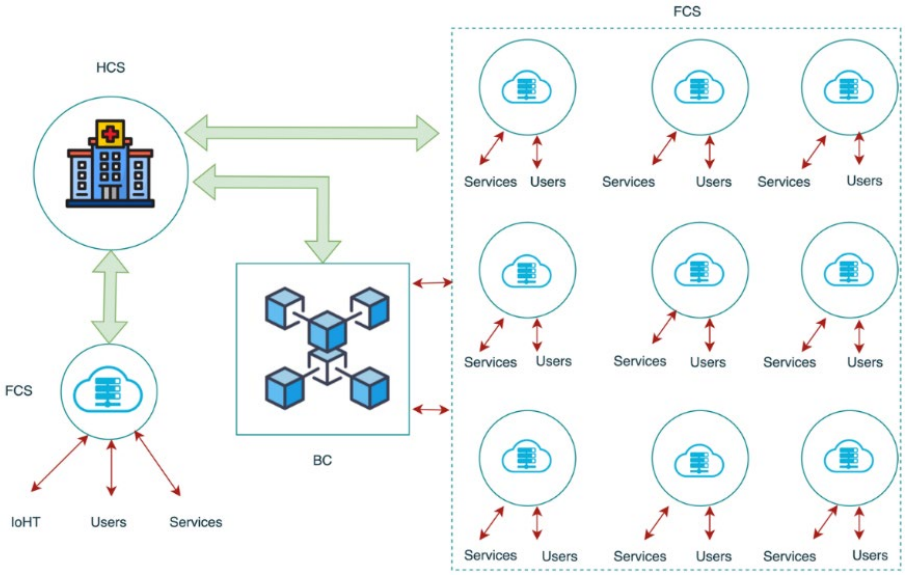


Figure 2. Proposed System Model.

5. Threat Model

Security is the primary concern in the healthcare sector, greatly impacting the dependability and privacy of devices and services. Therefore, it is crucial to proactively design comprehensive solutions to strengthen these systems against various potential threats [38]. Thus, our next focus is on analyzing common attacks that target IoHT systems. Doing so will help us gain better knowledge of the security concerns that exist in the healthcare systems.

A) **Mutual Authentication**: To protect sensitive information from potential interception by malicious individuals, all parties involved must verify their identities before any data transfer takes place [39].

B) **User's Identity Anomaly and Untraceability**: Anonymity is achieved by securely combining a legitimate user's personal information in a way that precludes unauthorized individuals from discovering or identifying the user. Several variables are used to retrieve user information from the database, including encryption, cryptographic hash functions applied to decryption keys, passwords, and extra factors intended to distinguish a user's identity [40].

C) **Forward Secrecy**: This ensures that the cryptographic key used for the current session is unique and cannot be compromised by unauthorized individuals. Furthermore, it forbids the use of a primary session key to start a new session [21].

D) **Unlikability**: This is a characteristic of privacy that occurs when an attacker is unable to distinguish between two or more components of a system. As a result, the attacker is unable to penetrate the system or exploit it incorrectly. This feature is essential for identifying systems. For instance, a perpetrator might find it difficult to demonstrate a correlation between the content of several communications, multiple sets of login passwords, or many bank withdrawal activities [24].

E) **Scalability**: This refers to the ability of the components of an authentication system to adjust and develop in response to changes in the surrounding environments [29].

6. Proposed Scheme

Our work focuses on three main phases: setup, registration, SSO/login, and authentication. Furthermore, the environment of the proposed scheme consists of four main components: health server provider (HCS), fog service provider (FCP), blockchain (BC), and users (U), including admin (Adm_i), patient (P_i), and doctor (Dr_i). Our goal is to establish a secure environment for data exchange between its components based on blockchain. Moreover, we employ fog computing to reduce the load on healthcare server providers and to bring the services provided by the system to the end user. This study uses SSO technology to enable users to access all services provided by the system with one login. Our

work also provides other benefits, such as mutual authentication, streamlined key management, password anonymity, and robust protection against a range of malicious attacks, including insider threats, MITM attacks, replay attacks, 51%, Sybil, and hijacking attacks.

6.1. Setup Phase

In this phase, HCS is in charge of handling the initialization of system components, including the BC network, fog node, and IoHT device registration, as well as the generation of essential parameters, such as private, public, and shared keys (Pr, Pu, and Sk) for the server itself and the fog servers.

6.2. Registration Phase

Here, a user (U_i) who wishes to register in the system must perform the following steps of the patient registration (Figure 3):

Step 1: U_i registers their information, such as username (Un_{U_i}), address (Ad_{U_i}), phone number (Pn_{Ui}), password (Pw_{Ui}), wallet address (Wa_{U_i}), and computed HP_{Ui} anomaly by calculating HP_{Ui} = h (Un_{U_i} || Pw_{Ui}|| Wa_{U_i}) and then sends it to FCS.

Step 2: FCS checks if the user is present or not in the system. If a user is already registered, then the phase is terminated; otherwise, it proceeds to Step 3.

Step 3: FCS generates the private key ($U_{i_{pr}}$) and public key ($U_{i_{pu}}$).

Step 4: FCS computes a shared key (SK_{U_i}), ensuring that the encryption (Enc(.)) and decryption (Dec(.)) processes for safeguarding S_i sensitive health information data are carried out with a robust key.

Step 5: $FSPcreate$ encrypts an electronic health record (HER_{Pi}) with all of the aforementioned medical information and lists of doctors associated with a new patient. The information is then saved.

Step 6: $FSP\ sends$ the (Pr, Pu, and SK) to the user via a secure path.

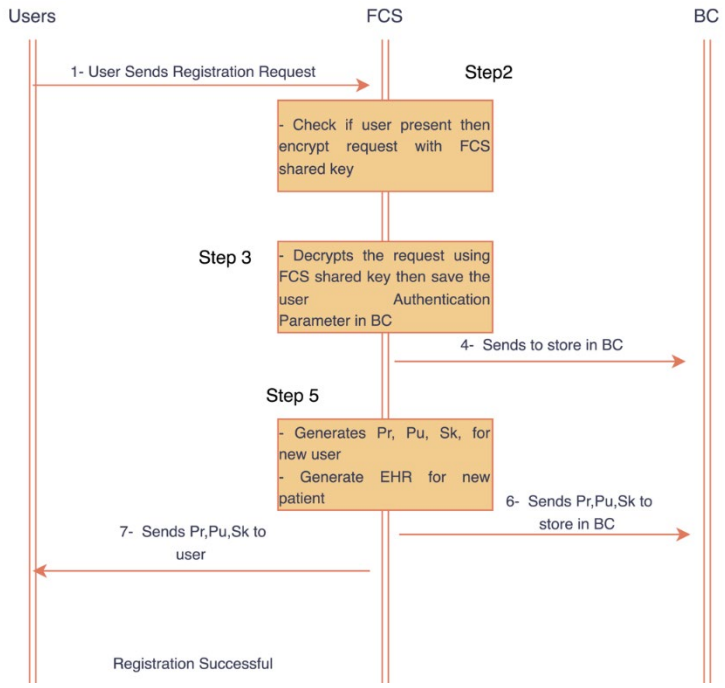


Figure 3. User Registration.

6.3. SSO Login and Authentication Phase

In this scenario, a user (U_i) wants to gain access to the system's services, and resources must provide valid parameters to the system. The following process steps, also shown in Figures 4(a) and (b), are described below:

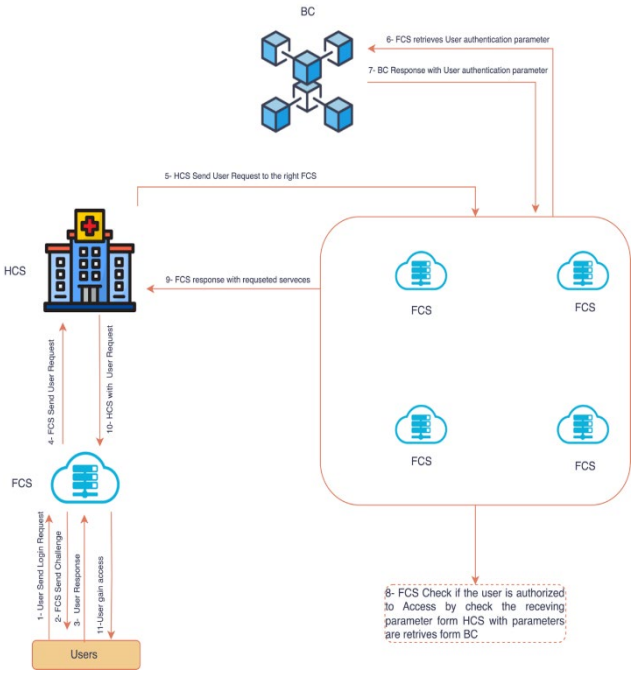
Step 1: U_i enters their Un_{U_i} and Pw_{U_i} and then chooses a random number $r_i \in Z_n^*$. Furthermore, U_i calculates A = h(Un_{U_i}) and HU_{U_i} = H (Pw_{U_i} || Un_{U_i}|| h(r_i)).

Step 2: U_i encrypts (r_i) with the shared keySK_{U_i}, E =$Enc_{SK_{U_i}}$ (r_i).

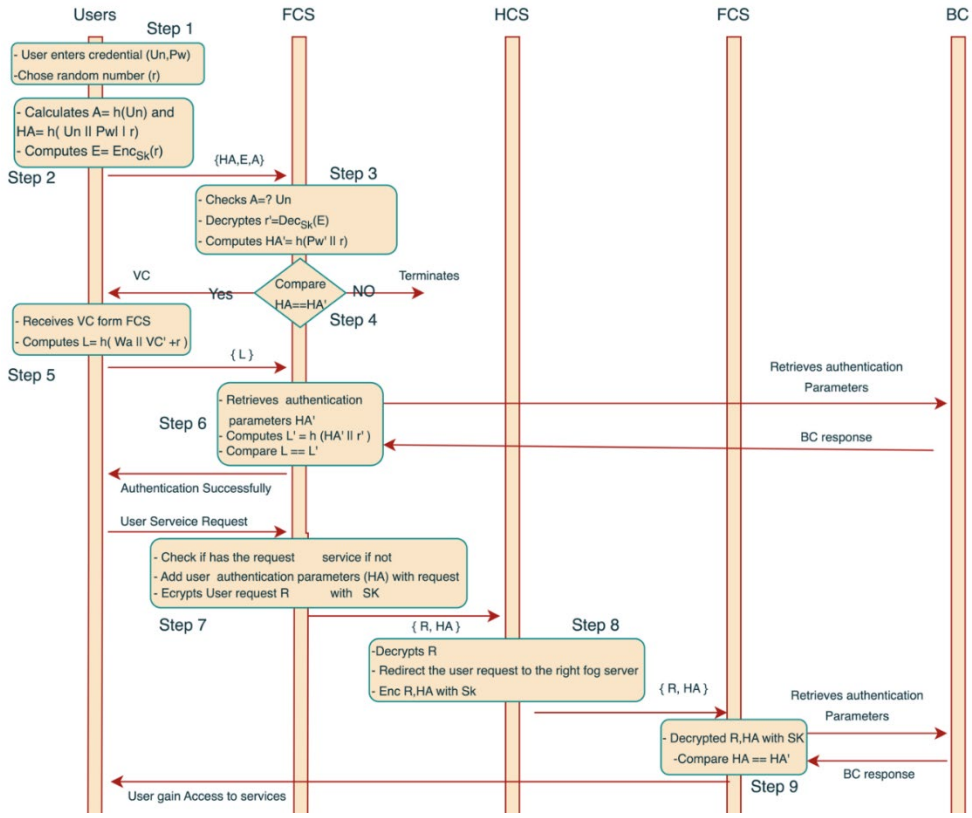
Step 3: U_i sends the login request {HA_{U_i} , E, A} to the FCS as a first authentication factor.

Step 4: When FCS receives the login request from U_i , FCS verifies it as follows:
a. FCS checks A $\stackrel{?}{=} Un'_{U_i}$; if there is a match, FCS restores the random number by decryption $r'_i = Dec_{SK_{U_i}}$ (E).
b. FCP retrieves Pw'_{U_i} and computes HA'_{Ui} = h (Pw'_{U_i} || H (r'_i)) and then compares $HA_{U_i} \stackrel{?}{=} HA'_{Ui}$ .If true, then the user is accepted; FCS sends the challenge verification code (VC) to U_i.
Step 5: When U_i receives VC' from the FCS, L = h ($Wa_{U_i} \oplus VC' \oplus$ h(r_i)) is computed, after which L is sent to the FCS.
Step 6: When FCS receives the L form U_i, FCS retrieves Wa_{U_i} from BC and calculates L' = h ($Wa_{U_i} \oplus$ VC $\oplus$ h(r'_i)). Then, it compares $L \stackrel{?}{=} L'$. In this case, the $U_i$is allowed to login and is authenticated successfully. Otherwise, the login process is terminated.

In case the user wants to access a service provided by the system but this service is provided by other fog servers, then the following steps are implemented:
Step 7: The user sends a request asking for services to FCS.
Step 8: FCS receives the request from the user and checks whether it has the requested service. If not, FCS encrypts the user credential and makes a request using the FCS shared key (Sk) and sends it to HCS.
Step 9: HCS decrypts the message using FCS (Sk), and then redirects the request to the right FCS server after encrypting the message with the destination FCS shared key (Sk).
Step 10: FCS decrypts the message with (Sk), retrieves the user authentication parameter from BC, and checks if true. If it is true, then the user is given access to the requested services.



(a)



(b)

Figure 4. Overview of SSO login and authentication shown in **(a)**, Sequence diagram of SSO login and authentication shown in **(b)**.

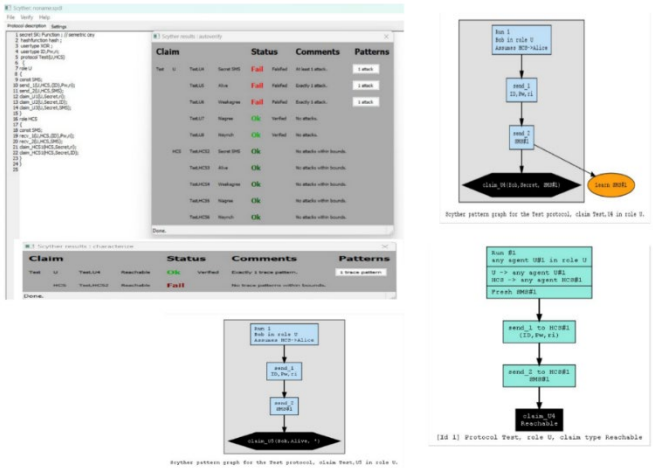
7. Security Analysis

This section explains the security analysis and presents the experimental results. The security analysis is presented in two ways: the initial approach involves a rigorous examination utilizing Scyther, while the subsequent approach involves a less structured evaluation employing the CK threat model [41]. Subsequently, we ascertained that the suggested protocol attains superior levels of privacy and security in comparison to the other options.

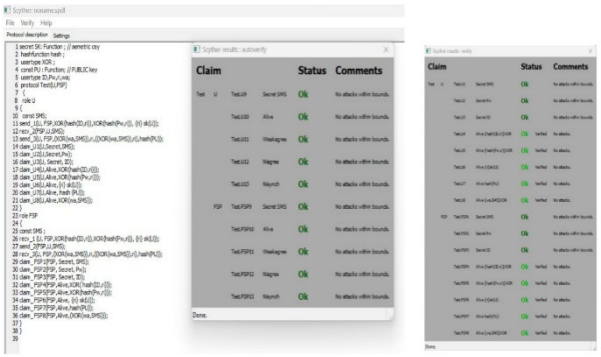
The graphical user interface (GUI) is designed for individuals seeking to validate or understand a protocol. In this study, we implemented the proposed system without employing security features used in conventional systems. The diagram pertains to the conventional system and elucidates its limitations.

7.1. Formal Analysis

In this part, we discuss the thorough examination of the proposed system and present evidence of its ability to protect data against different types of assaults. To provide security, our proposed solution uses symmetric key encryption, a crypto-hash function, and encryption and decryption functions based on a chaotic system. As shown by the results, this approach effectively addresses the limitations of conventional approaches. In addition, as presented in Figures 5(a) and (b), the outcomes of the suggested system exhibit resilience against widely recognized malicious attacks.



(a)



(b)

Figure 5. Weaknesses of the traditional system of the users shown in (a), User Verify Protocol, and Automatic Climes are shown in (b).

7.2. Informal Analysis

This section assesses the security needs of the proposed architecture to illustrate its resilience against prevalent network threats in the IoHT system.

Decentralization: A unique identity, including its ID, is associated with every $Node_i$ together with its public and private keys (Pr and Pu). This identification signifies the public address of the $Node_i$. The amalgamated architecture of chaotic and blockchain alleviates the necessity for key distribution, enabling instantaneous key assignment to any i-node with little collision risk.

Integrity: Given that all registration and building transactions are hashed and recorded on local and global blockchains, data alteration is impossible. The suggested architecture maintains all actions as unchangeable transaction records, as it makes use of tamper-proof blockchain technology.

Mutual Authentication: 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 perform the authentication:

Step 1: U_i enters their Un_{U_i}, Pw_{U_i}, then chooses a random number $r_i \in Z_n^*$. Furthermore, U_i calculates A = H (Un_{U_i}) and HU_{U_i} = H ($Pw_{U_i} \parallel Un_{U_i} \parallel$ H(r_i).

Step 2: U_i encrypts **(**r_i) with the shared key SK_{U_i} , $E = Enc_{SK_{U_i}}(r_i)$ using the symmetric key.

Step 3: U_i sends the login request < HA_{U_i}, E, A> to the FCS as a first authentication factor.

Step 4: When FCS receives the login request from U_i, FCS verifies it as follows:

a. FCS checks A $\stackrel{?}{=} Un'_{U_i}$ if there is a match, then FCS restores the random number by decrypting r'_i = $Dec_{SK_{U_i}}$(E).

b. FCS retrieves Pw'_{U_i} from BC, computes HA'_{Ui} = H (Pw'_{U_i} || H (r'_i)), and compares $HA_{U_i} \stackrel{?}{=} HA'_{Ui}$. If true, it then accepts; FCS sends the challenge as a VC to U_i in the form of an SMS message.

Step 5: When U_i receives VC' from the FCS, it computes L = H ($Wa_{U_i} \oplus VC' \oplus$ H(r_i)) and then sends L to the FCS.

Step 6: At the time FCS receives L from U_i, FCS retrieves Wa_{U_i} from BC, calculates L' = H ($Wa_{U_i} \oplus$ VC $\oplus$ H(r'_i)), and compares $L \stackrel{?}{=} L'$. In this case, FCS confirms the U_i login and authenticates it successfully. As a result, our proposed scheme accomplishes mutual authentication between the two entities (U_i and FCS). Otherwise, the current phase is rejected.

Anonymity: Using the adversary's perspective, an adversary has difficulty revealing the user's identity/password. To reflect anonymity, the identity of login information transmitted among system components must be verified. As the crypto hash function is integrated with r_i , which the attacker cannot identify, he cannot decipher the user's identity if he 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 {HA_{U_i}, E, A} to FCS as a first authentication factor. Thus, it has been encrypted using a shared key that is known only by U_i and *FCS*.

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.

Unlikability: This feature confirms that an individual can make many logins attempts to the *FCS* to access resources and services without anybody else being able to link the logins together and identify the individual. Under the suggested plan, whenever a user wants to access the system, they send {HA_{U_i}, E, A} to *FCS*. Thus, the basic elements of {HA_{U_i} , E, A} are constructed once using the following set of points:

A) FCS checks A $\stackrel{?}{=} Un'_{U_i}$ if match; FCP restores the random number by decrypting $r'_i = Dec_{SK_{U_i}}$ (E).

B) FCS retrieves Pw'_{U_i} from BC, computes HA'_{Ui} = H (Pw'_{U_i} || H (r'_i)), and compares $HA_{U_i} \stackrel{?}{=} HA'_{Ui}$. If true, it then accepts; FCS sends the challenge as VC to U_i in the form of an SMS message

C) U_i receives VC' from the FCS , computes L = H ($Wa_{U_i} \oplus VC' \oplus$ H(r_i)), then sends L to the FCS.

D) FCS receives L from U_i; FCS retrieves Wa_{U_i} from BC, calculates L' = H ($Wa_{U_i} \oplus$ VC $\oplus$ H(r'_i)), and compares $L \stackrel{?}{=} L'$. In this case, FCS confirms the U_i login and authenticates successfully. Otherwise, it refuses the login process.

Consequently, the primitive parameters {HA_{U_i}, E, A} are only generated once, making it impossible to connect many logins with the same U_i. Therefore, our proposed scheme can support unlikability.

Forward Secrecy: During the login and authentication phase, the widely used session key relies on SK_{U_i}. Even if the shared key is revealed or leaked, our proposed system protects the password. Furthermore, the shared key SK_{U_i} is only generated once based on VC; thus, 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_{U_i} = H (Pw_{U_i} || Un_{U_i} || H(r_i)). Furthermore, if a malicious party intercepts all messages that are sent { HA_{U_i} , E, A}, that attacker won't be able to use them again to log into the system because these parameters are created just once for each user login request. Consequently, absolute forward secrecy is guaranteed by our suggested scheme.

Confidentiality: Strong authentication and encryption/decryption techniques allow for authorized access to medical data. The recipient's public key is used to encrypt all communications, preventing unauthorized i-nodes from decrypting or representing the data.

MITM Attack: An MITM attacker intercepts, alters, and resends all information during a conversation without the knowledge of the participants. We presume that the attacker has obtained { HA_{U_i}, E, A} and changed it to {$HA^*_{U_i}$, E^*, A^*}. The modified settings, however, are rendered ineffective because the FSP verifies A and finds (A ≠ A^*), where A represents user identity. Additionally, the request {HA_{U_i}, E, A} is generated just once for each login. Thus, our proposed system does not allow MITM attacks.

Replay Attacks: As per our recommended plan, any new login attempt must precisely match the FSP parameters {HA_{U_i}, E, A}. However, these parameters are generated only once for every user login request r_i and cannot be obtained by the user again. Therefore, it 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 attack.

Insider Attack: Here, instead of sending these parameters (Pw_{U_i}, Un_{U_i}), users provide {HA_{U_i}, E, A}

when they register with FSP, where HU_{U_i} = H ($Pw_{U_i} \parallel Un_{U_i}$), $E = Enc_{SK_{U_i}}$ (r_i), A = H (Un_{U_i}). It is difficult for an attacker to use a one-way hash function to obtain the user's password from the hashed result. Furthermore, 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_{U_i}) or forge such a parameter; thus, the attempt will not succeed.

Hijacking Attack: Blockchain technology protects data and transactions with strong cryptographic techniques. Digital signatures and encryption are two techniques used to verify the authenticity of the user and the data. It employs multifactor authentication to resist any attempts at hijacking. This adds another layer of protection by requiring users to provide several means of verification, including passwords, biometrics, and one-time passwords (OTPs), to access the system, making it more difficult for attackers attempting to take over user accounts.

51% Attack: A 51% assault occurs when attackers gain control over more than half of a network's mining power, giving them the ability to change transactions on a blockchain network. A distributed network, in which no single authority controls the network's computing capacity, is maintained to fend off such attacks. The computation of the resistance attack is as follows: Let N be the network's total hashing capacity and H be the attacker's hashing power required to successfully carry out a 51% assault. An attacker has to control over 50% of the total hashing power; that is, H must be more than or equal to 0.5 times N to execute such an assault. As a result, the degree of decentralization in the network (i.e., the absence of a single organization holding the bulk of the hashing power) determines the capacity to prevent a 51% assault.

Sybil Attack: To carry out a Sybil attack, attackers try to imitate identities that send false signals to i-nodes. Each i-node in the suggested architecture has a unique identity, and each identity has a unique pair of public and private keys. The private key associated with such an identity $Node_i$ is used to sign all communications. Furthermore, the identities are saved on the global blockchain and authorized only by the cloud server. As a result, a hacker cannot mimic authorized identities.

Spoofing attack: The person who attacks strives to create several virtual identities. To perpetrate identity spoofing, the attacker must obtain an $Node_i$ ID associated with its public key. However, this cannot be done via blockchain. Furthermore, the private key of the $Node_i$ is challenging for an attacker to determine due to the 3D map chaotic cryptography.

8. Conclusion

This paper focuses on significant concerns about privacy and security within healthcare systems. Our approach integrates fog computing to offer reliable computational support for IoHT devices. Then, we use a key cryptosystem that incorporates chaotic keys to reduce the amount of communication required for authentication. As these keys are tiny, they help minimize communication overhead, and their size is suitable for the restricted processing capabilities of IoHT devices and users. Furthermore, our research integrates an authentication mechanism that uses unchangeable blockchain technology to ensure the security of individuals engaging in communication across public channels within a decentralized setting. The use of blockchain technology also provides support for decentralized node identification.

The evaluation result demonstrates that our suggested work has excellent scalability and dependability, as well as strong security and resistance against well-known threats. Additionally, our proposed system exhibits decreased latency compared to contemporary blockchain-based authentication techniques. Apart from using SSO technology to enable users to access all services provided by the system with one login, our work also provides other benefits, such as mutual authentication, streamlined key management, password anonymity, and robust protection against a range of malicious attacks, including insider threats, MITM attacks, replay attacks, 51%, and impersonation.

Finally, the security analysis of the proposed scheme was conducted using the Scyther tool. The formal and informal security analysis results show that the proposed scheme is secure and resistant to potential attacks. Overall, our work supports the scalability of the IoHT system.

Author Contributions
All authors contributed equally, and all authors read and approved the final version of the paper.

Funding
This research received no external funding.

Conflict of Interest Statement
The authors declare no conflict of interest

Data Availability Statement
Not applicable.

References

1. M. T. Mohammed, A. E. Rohiem, A. El-moghazy, and A. Ghalwash, "Chaotic based key management and public-key cryptosystem," *International Journal of Computer Science and Telecommunications,* vol. 3, no. 11, pp. 35-42, 2012.
2. M. Carr and S. F. Shahandashti, "Revisiting security vulnerabilities in commercial password managers," in *ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21–23, 2020, Proceedings 35*, 2020: Springer, pp. 265-279.
3. S. G. Morkonda, S. Chiasson, and P. C. van Oorschot, "Empirical analysis and privacy implications in OAuth-based single sign-on systems," in *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, 2021, pp. 195-208.
4. A. K. R. Sadhu, "Enhancing Healthcare Data Security and User Convenience: An Exploration of Integrated Single Sign-On (SSO) and OAuth for Secure Patient Data Access within AWS GovCloud Environments," *Hong Kong Journal of AI and Medicine,* vol. 3, no. 1, pp. 100-116, 2023.
5. M. Yusuf, M. Yusup, R. D. Pramudya, A. Y. Fauzi, and A. Rizky, "Enhancing user login efficiency via single sign-on integration in internal quality assurance system (espmi)," *International Transactions on Artificial Intelligence,* vol. 2, no. 2, pp. 164-172, 2024.
6. Š. Čučko and M. Turkanović, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access,* vol. 9, pp. 139009-139027, 2021.
7. J. Liu, A. Hodges, L. Clay, and J. Monarch, "An analysis of digital identity management systems-a two-mapping view," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 2020: IEEE, pp. 92-96.
8. V. Paulsen, "Implementation of a component to manage authorization for a web application."
9. K. Daga, K. C. Viswanath, and K. Shankar, "Single Sign-On and application integration using cloud Okta," in *AIP Conference Proceedings*, 2024, vol. 3075, no. 1: AIP Publishing.
10. A. Rashed and N. Alajarmeh, "Towards understanding user perceptions of biometrics authentication technologies," *International Journal of Computer Science and Information Security,* vol. 13, no. 6, p. 25, 2015.
11. L. A. Jones, A. I. Antón, and J. B. Earp, "Towards understanding user perceptions of authentication technologies," in *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, 2007, pp. 91-98.
12. A. Nanda, J. J. Jeong, S. W. A. Shah, M. Nosouhi, and R. Doss, "Examining usable security features and user perceptions of Physical Authentication Devices," *Computers & Security,* vol. 139, p. 103664, 2024.
13. S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf,* vol. 4, no. 2, p. 15, 2008.
14. S. M. Umran, S. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi, "Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry," *Internet of Things,* vol. 24, p. 100969, 2023.
15. S. Roy, S. Matloob, and D. Mukhopadhyay, "On Application of Blockchain to Enhance Single Sign-On (SSO) Systems," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021: IEEE, pp. 1191-1195.
16. S. Matloob, *Exploring applicability of blockchain to enhance Single Sign-On (SSO) systems*. University of North Florida, 2019.
17. A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in *2018 15th Learning and Technology Conference (L&T)*, 2018: IEEE, pp. 112-119.
18. G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Future Internet,* vol. 14, no. 11, p. 341, 2022.
19. I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *International Journal of Medical Informatics,* vol. 142, p. 104246, 2020.
20. M. A. Rashid and H. H. Pajooh, "A security framework for IoT authentication and authorization based on blockchain technology," in *2019 18th IEEE international conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, 2019: IEEE, pp. 264-271.
21. M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and IoT environment," *IEEE Internet of Things Journal,* vol. 8, no. 4, pp. 2116-2123, 2020.
22. R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA)*, 2018: IEEE, pp. 1-8.
23. U. Khalil, O. A. Malik, M. Uddin, and C.-L. Chen, "A Comparative Analysis on Blockchain versus Centralized Authentication Architectures for IoT-Enabled Smart Devices in Smart Cities: A Comprehensive Review, Recent Advances, and Future Research Directions," *Sensors,* vol. 22, no. 14, p. 5168, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/14/5168.
24. C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access,* vol. 8, pp. 70604-70615, 2020.

25. Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-rimy, "Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges," *Applied Sciences,* vol. 11, no. 19, p. 9005, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/19/9005.
26. O. Umoren, R. Singh, Z. Pervez, and K. Dahal, "Securing fog computing with a decentralised user authentication approach based on blockchain," *Sensors,* vol. 22, no. 10, p. 3956, 2022.
27. T. Manoj, K. Makkithaya, and V. Narendra, "A blockchain based decentralized identifiers for entity authentication in electronic health records," *Cogent Eng,* vol. 9, no. 1, p. 2035134, 2022.
28. S. Fugkeaw, "Achieving decentralized and dynamic sso-identity access management system for multi-application outsourced in cloud," *IEEE Access,* vol. 11, pp. 25480-25491, 2023.
29. 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.
30. M. Jawad *et al.*, "Towards Secure IoT Authentication System Based on Fog Computing and Blockchain Technologies to Resist 51% and Hijacking Cyber-Attacks," *Jordanian Journal of Computers and Information Technology,* p. 1, 01/01 2025, doi: 10.5455/jjcit.71-1736013097.
31. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
32. 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.
33. V. Balatska, V. Poberezhnyk, P. Petriv, and I. Opirskyy, "Blockchain Application Concept in SSO Technology Context," 2024.
34. S. Benefits, "Sso login: Key benefits and implementation," ed, 2016.
35. O. Mounnan, A. El Mouatasim, O. Manad, T. Hidar, A. Abou El Kalam, and N. Idboufker, "Privacy-aware and authentication based on blockchain with fault tolerance for IoT enabled fog computing," in *2020 fifth international conference on fog and mobile edge computing (FMEC)*, 2020: IEEE, pp. 347-352.
36. N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing IoT-enabled applications at the fog layer," *Journal of Sensor and Actuator Networks,* vol. 8, no. 1, p. 16, 2019.
37. A. A.-N. Patwary, A. Fu, S. K. Battula, R. K. Naha, S. Garg, and A. Mahanti, "FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain," *Computer Communications,* vol. 162, pp. 212-224, 2020.
38. B. Bai, S. Nazir, Y. Bai, and A. Anees, "Security and provenance for Internet of Health Things: A systematic literature review," *Journal of Software: Evolution and Process,* vol. 33, no. 5, p. e2335, 2021.
39. Adoption of Bloom Filter and Firebase Framework to Enhance Authentication Time for Healthcare Systems Based on Blockchain Technology", *J. Basrah Res. (Sci.)*, vol. 50, no. 1, p. 16, Jun. 2024, doi: 10.56714/bjrs.50.1.23
40. Abdulla J. Y. Aldarwish, Dr. Kalyani Patel, Ali A. Yassin, and Aqeel A. Yaseen, "Virtual SmartCards-based Authentication in Healthcare Systems and Applications", *IJCISIM*, vol. 15, p. 9, Sep. 2023
41. T. Wu, Q. Meng, S. Kumari, and P. Zhang, "Rotating behind security: A lightweight authentication protocol based on IoT-enabled cloud computing environments," Sensors, vol. 22, no. 10, p. 3858, 2022.