Received: 19 April 2024 | *Revised:* 1 August 2024 | *Accepted:* 10 August 2024
DOI: 10.37917/ijeee.22.1.33 *Vol. 22 | Issue 1 | June 2026*

Iraqi Journal for Electrical and Electronic Engineering
Original Article

Open Access
IJEEE University of Basrah College of Engineering

Securing Healthcare Data Exchange Based on Fog Computing and Blockchain Technologies

Muwafaq Jawad*, Ali A. Yassin, Hamid Ali Abed AL-Asadi
Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq

Correspondance
*Muwafaq Jawad
Department of Computer Science,
College of Education for Pure Sciences, University of Basrah
Email: pgs.muwafaq.abbas@uobasrah.edu.iq

Abstract
IoHT has several benefits for real-time smart healthcare, but because of its limited processing power, storage capacity, and self-defense capabilities, security issues are growing. Although newer blockchain-based authentication solutions have strong security features due to their tamper-resistant decentralized architecture, they come with a high resource cost, requiring a lot of processing power, more storage, and time-consuming authentication procedures. As such, these difficulties provide barriers to reaching the ideal levels of scalability and temporal efficiency, which are essential for the efficient functioning of large-scale, time-sensitive IoHT systems. To solve these challenges, this paper presents an authentication approach designed especially for IoHT systems. Our work consists four-phase process, which includes setting, registration, login and authentication, and HERs Exchange data. To enhance both efficiency and scalability, the proposed scheme employs a combination of 3-D map dimensions chaotic-based public key cryptosystems, and blockchain-based, fog computing technologies and IPFS. We simulate the proposed work to implement health electronic record (HER) by the Ethereum platform and solidity language, the simulation experiments were tested using the JMeter tool. Showed that the key generation time for chaotic-based is faster than (ECC)—furthermore, the average latency ≈ 3.7 ms. A security analysis of the proposed scheme was implemented by the Scyther tool. The formal security analysis demonstrated that the proposed scheme is secured against potential attacks and supports the scalability of the IoHT system.

Keywords
Blockchain, Chaotic Cryptography, Fog Computing, IPFS, IoHT.

I. Introduction

An idea called the Internet of Healthcare Things (IoHT) combines Internet of Things (IoT) technology with medical equipment. In addition, it is anticipated that IoHT will form the basis of future healthcare systems, where all medical devices will be Internet-connected and supervised by healthcare professionals. As it expands, the IoHT offers quick and reasonably priced healthcare [1]. Currently, IoT is used in several sectors, including healthcare [2, 3]. Especially, when considering IoHT, this quick growth gives rise to important doubts regarding user privacy and security, needing thorough consideration and focus. Healthcare systems are vulnerable to many vulnerabilities that may lead to security and privacy breaches [4]. These probabilities include the potential for unapproved entry into extensive numbers of subtle patient information, including personal and health records that are crucial for determining lifesaving [5]. Consequently, safeguarding privacy and security in IoHT systems has drawn focus in recent years. Critical security needs include data integrity, confidentiality, non-repudiation, and the authentication and identification of IoHT devices and users. Authentication stands out as a fundamental concern because it is necessary to sustain the fulfillment of other security standards [6]. There

is a chance that authorization and authentication procedures will be compromised because healthcare equipment is monitored, operated, and managed by several apps and users. The majority of the authentication methods discussed in IoHT literature fall into one of two architecture types: decentralized or centralized [7, 8]. In centralized using a single server or a trustworthy third party to distribute and manage login credentials is one way to centralize authentication. In addition, it consists of three steps. One type of authentication is one-way, which happens when two parties wish to communicate but only one of them authenticates to the other, leaving the other party unauthenticated. The second type of authentication is two-way authentication, or mutual authentication, in which the two entities authenticate one another. The final type of authentication is called three-way authentication, in which a central authority verifies each party's identity and helps them verify each other's identities [9]. As the number of users increases, scalability issues with central authentication systems may cause performance bottlenecks. They are also vulnerable to single points of failure, which have the potential to undermine the authentication procedure as a whole. Furthermore, privacy risks may arise from the concentration of sensitive user credentials [10, 11]. Due to their compatibility with the dispersed and diverse character of IoHT systems, decentralized authentication solutions utilizing blockchain technology are becoming more and more recommended [8, 12]. The fundamental characteristics of blockchains, such as consensus, immutability, decentralization, and security, have been emphasized by researchers. The advantages of employing blockchain technology for big data management and authentication were emphasized [13, 14]. These benefits included boosting security and privacy protocols, facilitating seamless data exchange, boosting data integrity, and generally improving the quality of large data. Consequently, other blockchain platforms have surfaced, including Multichain, Ethereum, Bitcoin, and others, with unique benefits over the others. These systems use several consensus techniques to provide variable degrees of security and scalability [3, 15]. Because of this, some blockchain platforms—including Multi-chain, Ethereum, Bitcoin, and others—have evolved throughout time, each with unique benefits over the others. These systems use various consensus techniques to provide variable degrees of security and scalability [16]. Thus, by scattering several fog nodes across different regions, the fog concept establishes a decentralized computing platform. By residing between the physical layer and cloud layers, it efficiently manages data processing and resolves computational restrictions in cloud and IoHT devices [17]. Our proposed work uses fog computing bringing cloud services to network edges and offering suitable computational support for IoHT devices to achieve this goal. In our work, we also use a three-dimensional (3-D) map chaotic Key Cryptosystem to reduce communication overhead during authentication. This system uses a 3-D map of chaotic keys, is small, minimizes communication overhead, and is sized to fit the restricted processing power of IoHT devices [18]. Lastly, our approach combines immutable blockchain technology, fog computing, and Interplanetary File System (IPFS) with an 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. As a result, this work makes the following contributions:

- We proposed a multi-factor authentication scheme.
- Our work utilized a chaotic Key Cryptosystem to reduce communication overhead during authentication and guarantee scalability and efficiency.
- Also, in our work, we do a formal security analysis using the Scyther tool to validate the strength of the proposed scheme against will-known attacks.
- We employ IPFS files to reduce the load on blockchain and that led to making our work faster than many modern schemas.
- Finally, our work was simulated by utilizing Ethereum blockchain, Ganache, Solidity, and node JS to evaluate it for two main metrics latency and throughput this metric was tested by using apache-JMeter.

The structure of the paper is as follows: Related Work Section II. Primitive Tools is covered in Section III. The System model is explained in Section IV. The planned scheme and its phases are explained in Section V. Performance analysis, simulation, and evaluation metrics are all covered in depth in Section VI. The formal security analyses are presented in Section VII. The research is finally concluded in Section VIII.

II. Related Work

In 2008 Satoshi Nakamoto et al [19], proposed blockchain technology, a distributed decentralized network that serves as a network of independent networks in charge of overseeing an assortment of time-stamped records, which was first presented in 2008. The structure of the blockchain is made up of linked blocks that are protected by basic cryptography. Three fundamental ideas underpin this technology's operation: immutability, decentralization, and transparency.
In 2018, Liu et al [20], supported the use of both local and remote authentication methods. The local authentication method combines a hash-based limited disclosure approach and a map

of chaos to provide mutual authentication among a smartwatch and a mobile phone. After the device has been verified on a local level, the cloud conducts remote authentication via a mechanism known as yoking-proof. 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. The system had a low time efficiency, to authenticate IoT devices. 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 2019, Liang et al, [22] 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 2021 Javed et al, [23] introduced blockchain-based decentralized identity control utilizing smart contracts for electronic health records. This technology has been the subject of numerous research studies, including Health-ID for EHRs and Health-ID for remote healthcare. Furthermore, a blockchain-based authentication technique was developed to lessen the need for re-authentication between several hospitals, improving productivity and cutting down on time spent on devices with limited memory and processing power. This document has limitations, such as issues with a system's or process's capacity to effectively manage growing volumes of work or data. While the proposed blockchain-based method enhances decentralization and security, there are still concerns about blockchain networks' capacity to manage massive volumes of data and transactions. The system may encounter delays and incur higher operating costs as the number of users and transactions increases, according to performance metrics like transaction gas cost and transactions per second. The research also notes that while the blockchain has the ability to increase transparency and trust, it is difficult to guarantee that all participants will abide by privacy laws and healthcare regulations. This is particularly important when dealing with diverse regulatory environments that span several states and regions. Chen et al. [24] suggested a way to reduce the time needed for authentication in 2022. Complete authentication and lightweight authentication are the two components of the approach. They employed CP-ABE for full authentication in order to maintain confidentiality. The XOR gate and hash function were employed for the purpose of lightweight authentication. This technique made it possible to create a physiological sensing device that can calculate parameters even though it has less processing power. They created a random number generator with the patient data as seeds. Lastly, this approach does not leverage the blockchain to strengthen the security mechanism; instead, it makes use of a third party.

Umoren et al. [25] deployed blockchain smart contracts in 2022 to address issues related to user identification and other constraints in fog and IoT technologies. Secure authentication, immutability, and scalability were all included in the decentralized fog computing framework. It also covered the scalability and immutability concerns with fog computing. Although the plan offers strong security, it is unable to satisfy the requirements of common IoT connectivity scenarios. The study's coverage of the proposed system's implementation is insufficient. More specifically, there are unclear explanations in the provided data structure and code, which could make it difficult for other researchers to duplicate and improve the work. Furthermore, there is not enough information provided regarding the experimental design and performance metrics. More thorough explanations of the simulation model and the outcomes are required in order to appropriately validate the findings. There isn't a detailed comparison of the proposed approach and current solutions in the discussion. A comprehensive assessment that takes into account variables like assault resistance, computing expense, computation duration, and communication overhead would provide a deeper comprehension and validation of the recommended methodology. Asaeed et al. in 2024 [26], presented a group authentication using the SSS algorithm, ECC, fog-based computing, and multi-level blockchain to build lightweight and scalable group authentication in IoMT, introducing a way to handle challenges like scalability and time. The evaluation test demonstrates good scalability and time efficiency. Additionally, the ECC algorithm faces challenges managing the massive quantity of devices and sensors, because it has limited key size. Consequently, we employed the 3-D maps chaotic algorithm to address this issue.

III. Primitive Tools

A. Blockchain Technology

In 2008, Satoshi Nakamoto introduced blockchain technology, a distributed decentralized network that oversees a collection of chronologically recorded documents. The blockchain is comprised of interconnected blocks that are safeguarded by fundamental cryptography. This system functions based on

three fundamental principles: transparency, decentralization, and immutability [19]. The decentralized nature of blockchain enables secure and dependable data sharing in the Internet of Things (IoT) [18]. It is widely used in mutual authentication and functions as a reliable framework for authentication systems and safe storage [14, 27]. The benefits of utilizing blockchain technology in healthcare are significant. It is a prudent choice, especially because the healthcare industry has given high importance to safeguarding patient data in light of technological progress [1]. Furthermore, numerous specialists have determined that integrating blockchain technology into the healthcare sector would be a viable remedy [21]. Consequently, we opted to utilize the Ethereum blockchain in our proposed work, due to Ethereum's superior performance in various areas, including efficient management of a substantial volume of transactions, in addition to the following rationales [28–30].

1) Architecture

Ethereum employs a public blockchain structure, enabling universal participation in the network and the deployment of decentralized applications (Dapps) through the use of smart contracts.

2) Mechanism

Ethereum is now using a Proof of Work (PoW) consensus mechanism, however, it is in the process of converting to a Proof of Stake (PoS) consensus model through the Ethereum 2.0 upgrade.

3) Smart Contract

Ethereum is widely recognized for its groundbreaking smart contract capability, which empowers programmers to design programmable contracts that autonomously execute upon meeting specified requirements.

4) Scalability

Ethereum has seen scalability issues as a result of its Proof of Work (PoW) consensus process, leading to network congestion and elevated transaction costs during times of increased demand. Finally, Table I shows some comparisons of Ethereum platforms.

B. Fog Computing

Implementing "sensor-to-cloud" connectivity is not feasible for several healthcare applications. Some apps prohibit the storage of health information beyond the healthcare facility's premises, and ensuring patient safety is a significant concern in the event of network and data center malfunction [31]. Fog computing is a solution to the aforementioned concerns. Fog computing is an outgrowth of cloud computing. It is positioned or placed in the middle of the cloud and IoHT devices.

TABLE I.
COMPARISONS OF ETHEREUM

Characteristic	Ethereum
Architecture	Public blockchain
Smart Contract	Introducing innovative capabilities for smart contracts
Scalability	Encountering difficulties in achieving scalability
Mechanism	PoW and PoS

Instead of sending data to the cloud for retrieval and processing, fog computing offers services that are located close to the end units [32]. Healthcare apps are highly responsive to latency and demand quick feedback. This allows fog computing to efficiently analyze real-time data generated by IoT devices with minimal additional processing. The fog design alleviates the computational load on the cloud. Fog and cloud computing provide users with the ability to access and utilize capacity, processing power, and network resources. Nevertheless, fog nodes distinguish themselves from clouds by their proximity to the network edge, which allows for the minimization of time delay [33]. Fog nodes are designed to carry out basic computational tasks, hence reducing the need for more advanced devices such as routers, set-top boxes, access points, and mobile phones. Fog computing enables real-time analysis by conducting storage and computation near the end devices [34], it can meet the requirements of healthcare systems.

C. Chaotic Cryptography

In this work, we utilized chaotic-based key management and a public key cryptosystem provided by Mohammed [18]. The cryptosystem has been used to offer aspects of a public-key cryptosystem, including "key exchange, management system, and encryption/decryption" of the intended content. Furthermore, the system cryptography protocol effectively addresses the issue of man-in-the-middle attacks by utilizing chaotic management systems as its foundation. The key management system supplied is based on the beta-transformation mapping. An assessment is conducted to compare the new chaotic key exchange protocol with the Diffie-Hellman elliptic curve cryptosystem (DHECC). Fig. 1 shows key generation time in each ECC and Chaotic-based.

D. Hash Function

The SHA-256 algorithm, developed by the NSA, is widely utilized in encryption protocols such as SSL, TLS, and SSH. Hashing is a very secure encryption process that is challenging to decrypt and extremely unlikely to generate identical data items. The US government utilizes this technology to safe-

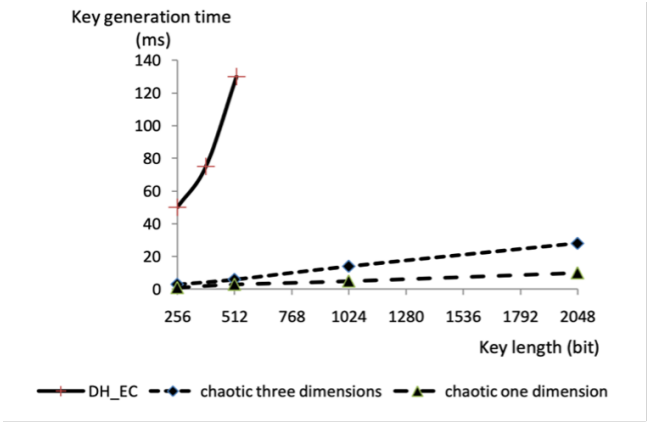

Fig. 1. Key generation time in each ECC and Chaotic-based [18].

guard confidential data and authenticate passwords [35, 36]. In our work utilizing the hash function was a very important tool to guarantee the integrity of data and the anomaly.

E. Interplanetary File System (IPFS)

The Interplanetary File System, or IPFS, is a decentralized file storage system that stores and retrieves data via a distributed network. In such a scenario, files, documents, and other application-related data can be stored on IPFS. IPFS is used to store the encrypted files that the administrator uploaded. Every file on IPFS has a distinct content identifier (CID), making it simple to retrieve and validate. By using content addressing, which refers to a file's content rather than its location, IPFS ensures redundancy, fault tolerance, and simple file retrieval [37, 38]. IPFS is utilized to store patients' encrypted healthcare data on off-chain storage (IPFS) or retrieve and receive the stored data. The patient is responsible for storing and retrieving the information, while the healthcare provider is only able to obtain the data.

IV. System Model

A. Network Model

The proposed framework in our study comprises three primary layers. These layers, along with their components, are illustrated in Fig. 2.

1) User layer:

As we deal with healthcare institutions, it means we engage with a diverse group of individuals, including (Administrators, patients, doctors, nurses, and the staff) within those institutions.

- Administrators:The administrator (Adm_i) plays a pivotal role in supervising and managing access to the various components of the system.

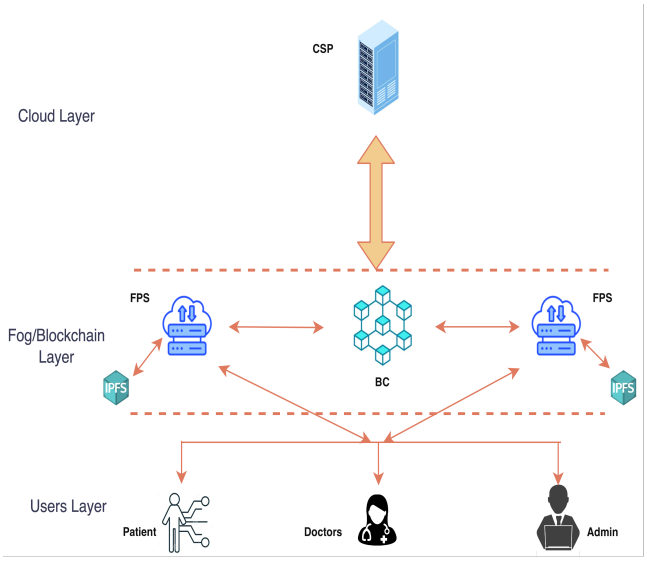

Fig. 2. Proposed System Model.

- Patients: Patients (P_i), who are the main benefiting of healthcare services, are getting more involved in their care using digital health tools. This helps them take a more active role in making decisions about their healthcare.

- Doctors: Doctors (Dr_i), play a vital role in the healthcare system. They diagnose illnesses, provide treatments, and offer guidance to patients.

- Nurses: Nurses are the backbone of the healthcare system, providing essential care and support to patients.

2) Fog layer:

This layer consists of many fog servers, with each fog server responsible for delivering sufficient computation and storage capacity to its allocated users and IoHT devices. The fog server contains significant storage and computational capacities and is tasked with managing the blockchain and verifying user credentials. Furthermore, it stores and secures the healthcare data of patients on off-chain storage (IPFS) and retrieves and receives the stored data [38].

3) Cloud Layer:

The fog servers are linked to the cloud layer, which consists of cloud servers with high-level computing and storage capabilities. The main duty of the cloud server is to register nodes "fog servers, users, and IoHT devices" [39].

4) Blockchain:

The blockchain serves as a decentralized authority for the verification and authentication of every entity in the IoHT system

such as users and devices. Each fog server is connected to the blockchain to authenticate and validate the identification of both the user and the IoHT nodes. The verification step is conducted by the fog server in the corresponding location utilizing a smart contract [40].

B. Ck Threat Model

By employing the Canetti-Krawczyk model (CK), we may methodically create and assess the proposed strategy. The inclusion of multiple essential security features [41]. is vital for the implementation of the proposed system. This study encompasses the following aspects:

- Scalability.
- Mutual authentication
- Protection of personal privacy.
- Defense against assaults.
- Ensuring the accuracy and reliability of communication.

V. Proposed Schema

This part shows a resilient healthcare authentication system that is organized across four distinct phases: Setting, Registration, Login and Authentication, and (HER) data Exchange. Our work introduces a healthcare system that includes six main components: Cloud Healthcare server provider (CSP), Users (U_i) such as (Patients (P_i), Administrators (Adm_i), and Doctors (Dr_i)), Fog server provider (FPS) and blockchain (BC). The goal is to establish a secure environment for the exchange of data between its components based on blockchain. Furthermore, it employs the (FPS) to reduce the latency and bring the cloud service near to the end user. In addition, This work provides other benefits, such as mutual authentication, streamlined key management, password anonymity, and robust protection against a range of malicious attacks, including insider threats, Man-in-the-Middle (MITM) assaults, replay attacks, and impersonation. The symbols employed in our investigation are specified in Table II.

TABLE II. Symbol Used in Our Scheme

Symbol	Description
CSP	Cloud Healthcare server provider
BC	Blockchain
Adm_i	Administrator
U_i	Patient
T_s	Difference between sent and receive time
Pr_{Adm}	Admin private key
Pr_U	Doctor private key
Pu_U	Doctor public key
SK	Shared Key
HER_P	Patient Health Electronic Record
SK_U	Admin shared key
O_{HER}	HER owner
U_{HER}	HER request

A. Setting Phase

In this phase, the (CSP) is considered the main responsible for managing and registering the users, Fog Service Provider (FPS), and IoHT devices. Each user and $IoHT$ device obtain the shared key (SK) locally by implementing a key exchange protocol based on a chaotic logistic system to guarantee security. The CSP employ 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 chaotic-base cryptography for the Encryption function ($Enc()$), and the Decryption function ($Dec()$).

1) $Node_i$ registration

At first, each $node_i$ such as (FPS, Pd_i, $IoHT$ sensor S_i .... $etc.$) generates own private key ($node_{i_{pr}}$) and public key ($node_{i_{pu}}$) using the chaotic system (as described in section 3.3). the following step explains $node_i$ registration process.

Step 1: $node_i$ selects an identification $node_{i_{ID}}$ and time (T_s) and send registration request to the CSP $\{node_{i_{ID}}, T_s, node_{i_{pu}}\}$.

Step 2: CSP checks the freshness of the received request by calculating $T'_s - T_s \leq T_s$ where T'_s denotes request receiving time and represents the acceptable difference between T' and T.

Step 3: CSP classifies the $node_{i_{ID}}$ to add to related list such as (FPS list, pd_i list, S_i list) then Save ($node_{i_{ID}}$, $node_{i_{pu}}$, CSP_{pu}) in the BC.

Step 4: CSP check if registered $node_{i_{ID}}$ its IoHT device (pd_i) then need to assign to the FSP then sends $\{CSP_{pu}, Pd_{i_{pu}}, FPS_{pu}\}$ to BC.

Step 5: After assigning pd_i to the FSP, finally the registration of $node_i$ successful.

B. User Registration Phase

At this point, will outline the registration process with a specific focus on the registration of the Fog Service Provider, IoHT devices, and users such as (Administrators, Patients, and doctors). Every user is required to enter accurate and complete information, including their username, password, Ethereum wallet address, and other relevant details, only once. Here is a description of the registration process. In this part, the Users (U_i) who wishes to register in the system must do

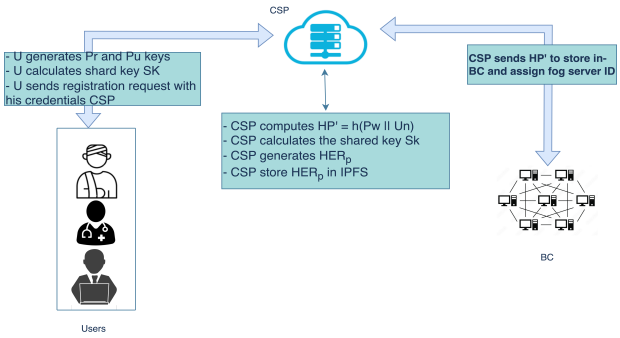

Fig. 3. User Registration.

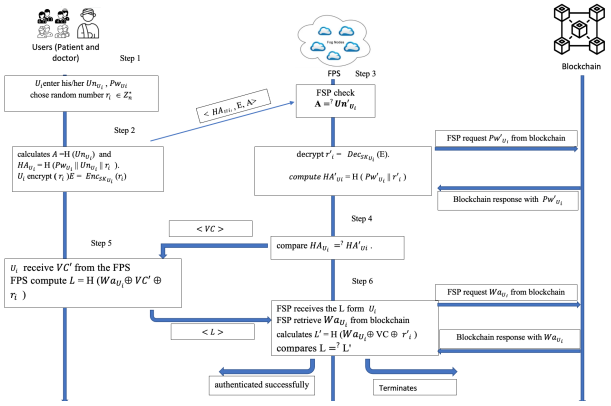

Fig. 4. User Login and authentication.

the following steps, and the patient registration is shown in Fig. 3.

Step 1: U_i should register his information such as (Username (Un_{U_i}), address (Ad_{U_i}), phone number (Pn_{Ui}), password (Pw_{Ui}), Ethereum wallet address (Wa_{U_i}), Type of disease Td_{Ui})) in the CSP computed HP_{Ui} anomaly by calculating HP_{Ui} = h (Un_{U_i} || Pw_{Pi}) then store it in the BC through a smart contract.

Step 2: U_i generates the private key (U_{ipr}) and public key (U_{ipu}) based on the chaotic system as described in section 3.3.

Step 3: The U_i 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 based on the chaotic logistic system.

Step 4: CSP creates and encrypts Electronic Health Record (HER_{Pi}) with all of the aforementioned medical information and lists of doctors associated with a new patient and saves it on IPFS.

Step 5: CSP assigns Patient (U_i) information to the fog server FPS_{ID} that connects within the same area.

Step 6: CSP sends the patient (U_i) information (HP_{Ui})to the BC by calling the smart contract.

C. Login and Authentication Phase

At this time, the User (U_i) wants to gain access to the system's services, and resources must provide valid parameters to the system. Fig. 4 describes the process steps.

Step 1: U_i enters his/her Un_{U_i} , Pw_{U_i} , then chose 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 key SK_{U_i} , $E = Enc_{SK_{U_i}}$ (r_i)

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

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

a. FPS check A ? Un'_{U_i} if match FPS restore the random number by decrypt $r'_i = Dec_{SK_{U_i}}$ (E).

b. FPS retrieves Pw'_{U_i} from BC and computes HA'_{Ui} = h (Pw'_{U_i} || H (r'_i)) and compare HA_{U_i} ? HA'_{Ui} . If true, accept; FPS sends the challenge a verification code (VC) to U_i.

Step 5: Upon the U_i receive VC' from the FPS compute L = h ($Wa_{U_i} \oplus VC' \oplus$ h(r_i)) then sends L to the FPS.

Step 6: At the time FPS receives the L form U_i , FPS retrieves Wa_{U_i} from BC and calculates L' = h ($Wa_{U_i} \oplus$ VC $\oplus$ h(r'_i)) and compares L? L'. In this case, the FPS confirms the U_i login and authenticated successfully. Otherwise, refuses the login process. The Doctors login and authentication are the same process as the patients. doctors must provide valid parameters to gain access to the system to check the HER_{Pi} and make an update based on the role and privileges given to them by the administrator.

D. HER Data Exchange Phase

During this time, after users complete the registration and authentication phases, a HER related to the patient is created, these HERs consist of personal health data that are generated after patient examination inside the hospital. Furthermore. HER can be reached by each HER owner and the user. in addition, HER owner predefines access privileges such as (read, write, and edit). This phase includes four components: HER owner (O_{HER}), Users (U_{HER}) such as (Doctor, Nurse, and Admin), FPS, and BC. Furthermore, we establish Secure HER data exchange for Patients and Users. In addition, we employ fog computing to guarantee the security of exchanging HER data. Smart contracts are designed to automatically execute their functions once certain access requirements are fulfilled. The following steps and Fig. 5 explain the process:

Patient side

Step 1: O_{HER} sends a query request to FPS to ask for HER with these parameters $<ID_{P_i}>$.

Step 2: At the moment FPS receives the request from the O_{HER} , FPS retrieves the SK_P and Wa_P from BC.

Step 3: FPS retriever HER_P from IPFS.

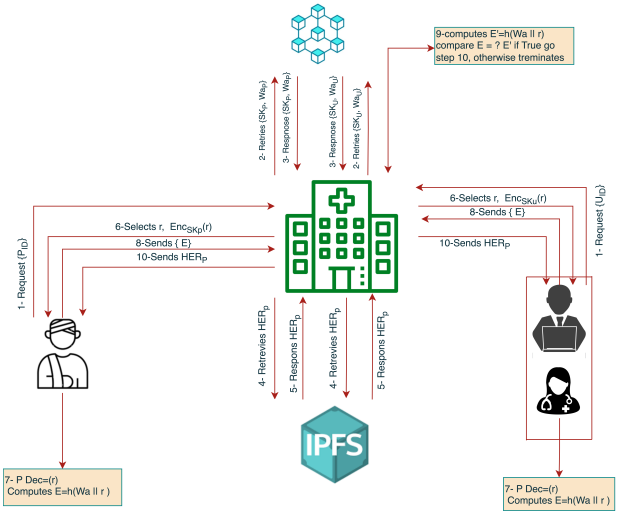

Fig. 5. HER Data Exchange.

Step 4: FPS selects a random number (r) and calculates E= Enc_{SK} (r). and sends E to O_{HER}.

Step 5: O_{HER} restore (r) by computes Dec_{SK}(E) then calculates E = h (wa_P || r) and send E to FPS.

Step 6: FPS computes E = h (wa_P || r) and compares if E ==E' then O_{HER} gain access to HER, otherwise Terminates the phase

User side

Step 1: U_{HER} sends a query request to FPS to ask for HER with these parameters $<ID_{U_i}>$.

Step 2: At the moment FPS receives the request form the U_{HER} , FPS retrieves the SK_U and Wa_U from BC.

Step 3: FPS retriever HER_P from IPFS.

Step 4: FPS selects a random number (r) and calculates E= Enc_{SK} (r). and sends E to U_{HER}.

Step 5: U_{HER} restore (r) by computes Dec_{SK}(E) then calculates E = h (wa_U || r) and send E to FPS. **Step 6**: FPS computes E = h (wa_U || r) and compares if E ==E' then U_{HER} gain access to HER, otherwise Terminates the phase.

VI. PERFORMANCE ANALYSIS

A. Simulation Environment

Table III provides a comprehensive overview of the equipment employed in the conducted test, which leveraged the widely used simulator tool, Ganache. Ganache serves as a valuable resource, enabling developers to establish a local Ethereum blockchain environment for supervised experimentation and analysis. The testing and deployment of smart contracts on the blockchain were facilitated through the Truffle tool. Additionally, Node.js played a pivotal role in constructing the proposed framework. The simulation was carried out on a

TABLE III. INSTRUMENTS EMPLOYED DURING THE SIMULATION OF OUR WORK

Component	Description
MacOS	Operating System
Solidity	Smart contract programming language
Truffle	Testing smart contract
Ganache	Local Ethereum blockchain Simulator tool
Node.js	Developing tool for clients

Mac OS 476.0.0.0.0 LTS 64-bit system, equipped with 8 GB of RAM, and powered by a Dual-Core Intel Core i5 CPU operating at 2.7 GHz. Figure visually depicts the interplay of various tools involved in executing and simulating our project.

B. Metric

The latency and throughput are among the criteria utilized for evaluation. The following is a brief explanation of these:

1) Throughput:

$$Throughput = Total number of transactions / Total time in seconds. \quad (1)$$

2) Latency:

$$Latency = CommitTime - Submittime \quad (2)$$

C. Analytics and Finding

To evaluated the practical utility of our findings for various user roles and responsibilities through a thorough performance assessment using Apache JMeter version 5.6.3 [42]. The system's ability to function in real-world scenarios was fully examined using Apache JMeter, a renowned tool for measuring load performance. In this work employed JMeter to conduct simulations including a range of 100 users. The users engaged with the system, performing different tasks. JMeter measures throughput in kilobytes per second, representing the data transferred within a specific time frame. Fig. (6), (7), and (8), display a graphical depiction of the achieved throughput in the proposed scheme. The experiment revealed a direct linear relationship between the system's throughput and the quantity of users and requests. The consistent increase in throughput illustrates the efficiency of our job. Furthermore, Latency is the time differential between sending a request and receiving a response within a system. We utilized JMeter to analyze the average latency of the proposed design in this study.The average latency of the system, compared to the throughput of the specified job. The experiment's highest recorded latency was approximately $\approx$ 3.7 ms.

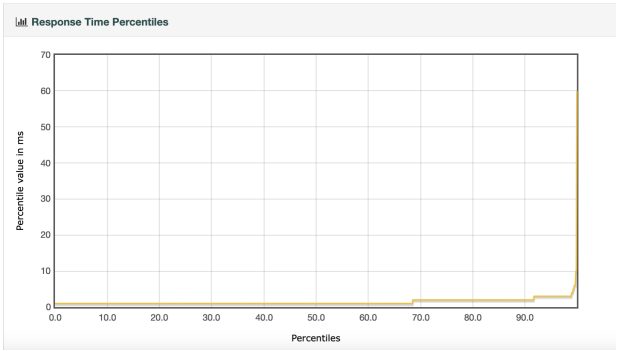

Fig. 6. Response Time Percentiles.

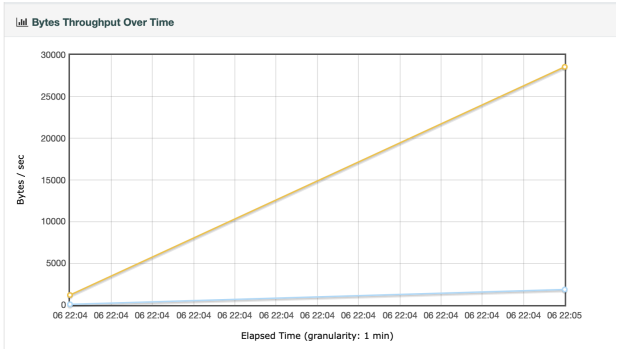

Fig. 7. Throughput Over Time.

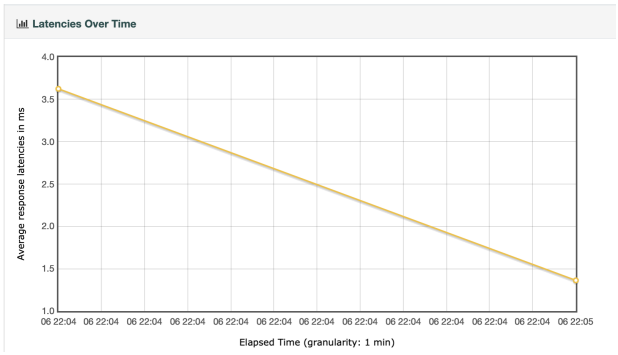

Fig. 8. Latencies Over Time.

```
secret SK: Function; // symmetric key
 hashfunction hash;
 usertype XOR;
 const PU: Function; // PUBLIC key
 usertype ID, Pw, ri, wa;
 protocol Test (U, FPS)
  {
  role U
{
  const SMS;
send_1(U, FPS, XOR (hash (ID,ri)),XOR(hash(Pw,ri)), {ri} sk(W));
recv_2(wa, U, SMS);
send_3(U, FPS, (XOR (wa, SMS)), ri, ((XOR (wa, SMS)), ri), hash (PU));
claim_U1(U, Secret, SMS);
claim_U2 (U, Secret, Pw);
claim_U3(U, Secret, ID);
claim_U4(U, Alive, XOR (hash (ID, ri)));
claim_U5(U,Alive,XOR(hash(Pw,ri)));
claim_U6(U, Alive, {ri} sk(U));
claim_U7(U, Alive, hash (PU));
claim_U8(U, Alive, XOR (wa, SMS));
}
 role FPS
{
const SMS;
recv_1 (U, FPS, XOR (hash (ID, ri)), XOR (hash (Pw, ri)), {ri} sk(U));
send_2(FPS, U, SMS);
recv_3(U, FPS, (XOR (wa, SMS)), ri, (XOR (wa, SMS)), ri), hash (PU));
claim_ FPS 1(FPS, Secret, SMS);
claim_ FPS 2(FPS, Secret, Pw);
claim_ FPS 3(FPS, Secret, ID);
claim_ FPS 4(FPS, Alive, XOR (hash (ID, ri)));
claim_ FPS 5(FPS, Alive, XOR (hash (Pw, ri)));
claim_ FPS 6(FPS, Alive, {ri} sk(U));
claim_ FPS 7(FPS, Alive, hash (PU));
claim_ FPS 8(FPS, Alive, (XOR (wa, SMS)));
}
}
```

Fig. 9. Scyther formal analysis.

VII. Security Analysis

In order to verify the effectiveness of the suggested secure mechanism, formal security evaluations were carried out using the Scyther tool for formal analysis, as shown in Fig. 9. Furthermore, examined the effectiveness of the suggested method in relation to security and privacy. When creating security protocols for any system, it is crucial to take into account three fundamental security principles: Confidentiality, Integrity, and Availability, commonly known as CIA [43]. Confidentiality ensures that only authorized users can access the system's communications. Data integrity ensures that only authorized individuals can modify stored data, while data availability guarantees that users can access the data as needed. Moreover, our method provides benefits such as mutual authentication, efficient key management, and password anonymity. The system is engineered to endure common harmful at-tempts including insider threats, Man-in-the-Middle (MITM), and Reply. We will now summarize the aforementioned primary security requirements assessment in Table VI. As shown in Table V, we thoroughly examined some attacks and evaluated the robustness of the system against each one. To protect privacy, our plan places a high priority on data ownership, making sure that only users are in control of their data. The use of blockchain technology for transaction authentication strengthens the system's defenses against hostile incursions, increasing the likelihood that an adversary won't be able to take over 51% of the network's resources or alter the data. The method also guarantees other privacy-enhancing features like auditability and transparency of data. By keeping the control policy on a blockchain ledger, which the patient alone can amend or revoke, fine-grained access control is made possible. Furthermore, A comparison study of suggested model against several current systems is shown in Table IV.

TABLE IV.
COMPARISONS OF DIFFERENT EXISTING SCHEMES

Scheme	Blockchain	Distributed Model	Mutual Authentication	Multifactor Authentication	Scalability	Chaotic Based	Robust Against Attacks
Chen **[24]**	N	NA	Y	N	NA	N	Y
Meisami **[44]**	Y	N	Y	N	Y	N	N
Almadhoun **[21]**	Y	Y	Y	N	Y	N	Y
Shao **[45]**	Y	Y	NA	N	NA	N	Y
Esposito **[46]**	Y	Y	N	N	NA	N	NA
Imine **[47]**	Y	Y	Y	NA	NA	N	NA
Alsaeed **[26]**	Y	Y	Y	N	Y	N	Y
Umoren **[25]**	Y	Y	Y	Y	Y	N	Y
Our work	Y	Y	Y	Y	Y	Y	Y

TABLE V. SECURITY ANALYSIS

Resist	Defense	Definition	Attack
√	Employ strong security features including data encryption, the use of nonce parameters, distinct token identities in their apps, appropriate session administration, and reliance on protocols with the integrity of message checks.	This kind of attack leverages a valid authenticated transaction and thus is not a true-time attack.	Replay
√	A legitimate node has a restricted capacity to transmit transactions within the network. Once the blockchain network gets a transaction, miners verify that the transaction was generated by a legitimate node before approving it.	This is a distributed form of the DOS attack.	DDOS
√	Employing strong encryption and decryption techniques.	Personal information from a particular session can be modified or read with this approach.	MITM
√	Blockchain uses an immutable ledger.	The hacker alters or deletes the patient's data contained on the ledger of the blockchain, such as access policies and hash.	Modification
√	To guard against eavesdropping assaults, encrypt data while it's being transmitted and during private discussions. Attackers cannot read data sent between two parties thanks to encryption.	Makes it possible for a hacker to obtain the message and monitor the network's communications.	Eavesdropping
√	A hash of the encrypted data is saved on the blockchain ledger, enabling easy detection of any modifications in the data.	The attacker wants to remove, alter, or add data in the storage.	Storage
√	The attack's likelihood is minimal due to the implementation of a private blockchain and the PBFT consensus technique.	The intruder has gained control of over 51% of the miners and is attempting to manipulate the consensus process to create a fraudulent block.	51% Attack

TABLE VI.
SECURITY REQUIREMENTS

Requirement	Scheme Solution
Confidentiality	Done by utilization of symmetric key cryptography.
Integrity	Hashing of data blocks in blockchain is achieve integrity.
Availability	Achieved by restricting reactions that are considered valid within the network.

VIII. CONCLUSION

This paper explores important privacy and security concerns related to electronic health records (EHRs) and the Internet of Healthcare Things IoHT. To give IoHT devices enough computational assistance, our approach incorporates fog computing, which expands cloud services to network edges. Using a 3D Chaotic Key Cryptosystem during authentication to reduce communication overhead. These chaotic keys are especially useful for IoHT devices with constrained processing power because they are small and effective in lowering communication overhead. Furthermore, combine immutable blockchain technology with an authentication system to provide secure interactions over public channels in a decentralized setting. Blockchain technology also makes decentralized node identification possible. The evaluation results show that suggested strategy has lower latency when compared to current blockchain-based authentication techniques and exhibits strong scalability, dependability, and resilience against known attacks. The methodology used for implementing and evaluating smart contracts involves utilizing Ganache, an Ethereum platform, and the Solidity programming language. In addition, evaluate latency and throughput via the Apache JMeter tool. Finally, the Scyther tool is utilized to do a comprehensive security analysis of our method, demonstrating its robustness and resilience against potential threats. For future work, attend to use biometrics such as fingerprints to authenticate the admin to add extra security level.

CONFLICT OF INTEREST

The authors have no conflict of relevant interest to this article.

REFERENCES

[1] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for iot-based healthcare: background, consensus, platforms, and use cases," 2020.

[2] M. R. Naqvi, M. Aslam, M. W. Iqbal, S. K. Shahzad, M. Malik, and M. U. Tahir, "Study of block chain and its impact on internet of health things (ioht): challenges and opportunities," 2020.

[3] 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," 2023.

[4] M. A. Haque, D. Sonal, S. Ahmad, and K. Kumar, "Enhancing security for internet of things based system," 2023.

[5] Z. A. Hussien, H. Jin, Z. A. Abduljabbar, M. A. Hussain, A. A. Yassin, S. H. Abbdal, M. A. Al Sibahee, and D. Zou, "Secure and efficient e-health scheme based on the internet of things," 2016.

[6] V. O. Nyangaresi, Z. A. Abduljabbar, J. Ma, and M. A. Al Sibahee, "Verifiable security and privacy provisioning protocol for high reliability in smart healthcare communication environment," 2022.

[7] M. T. Hammi, P. Bellot, and A. Serhrouchni, "Bctrust: A decentralized authentication blockchain-based mechanism," 2018.

[8] M. Jmaiel, M. Mokhtari, B. Abdulrazak, H. Aloulou, and S. Kallel, "The impact of digital technologies on public health in developed and developing countries: 18th international conference, icost 2020, hammamet, tunisia, june 24–26, 2020, proceedings," 2020.

[9] G. Apruzzese, P. Laskov, E. Montes de Oca, W. Mallouli, L. Brdalo Rapa, A. V. Grammatopoulos, and F. Di Franco, "The role of machine learning in cybersecurity," 2023.

[10] S. Matsumoto, R. M. Reischuk, P. Szalachowski, T. H.-J. Kim, and A. Perrig, "Authentication challenges in a global environment," 2017.

[11] S. C. Seak, N. K. Siong, W. H. Loon, and G. R. Haron, "A centralized multimodal unified authentication platform for web-based application," 2014.

[12] D. Nkomo and R. Brown, "Hybrid cyber security framework for the internet of medical things," 2019.

[13] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," 2022.

[14] S. M. Umran, S. Lu, Z. A. Abduljabbar, Z. Lu, B. Feng, and L. Zheng, "Secure and privacy-preserving data-sharing framework based on blockchain technology for al-najaf/iraq oil refinery," 2022.

[15] H. Sheth and J. Dattani, "Overview of blockchain technology," 2019.

[16] P. Paul, P. Aithal, R. Saavedra, and S. Ghosh, "Blockchain technology and its types—a short review," 2021.

[17] K. Pareek, P. K. Tiwari, and V. Bhatnagar, "Fog computing in healthcare: A review," 2021.

[18] M. T. Mohammed, A. E. Rohiem, A. El-Moghazy, and A. Ghalwash, "Chaotic based key management and public-key cryptosystem," 2012.

[19] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," 2008.

[20] H. Liu, H. Ning, Y. Yue, Y. Wan, and L. T. Yang, "Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices," 2018.

[21] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of iot devices using blockchain-enabled fog nodes," 2018.

[22] Y. Liang, "Identity verification and management of electronic health records with blockchain technology," 2019.

[23] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-id: A blockchain-based decentralized identity management for remote healthcare," 2021.

[24] I.-T. Chen, J.-M. Tsai, Y.-T. Chen, and C.-H. Lee, "Lightweight mutual authentication for healthcare iot," 2022.

[25] O. Umoren, R. Singh, Z. Pervez, and K. Dahal, "Securing fog computing with a decentralised user authentication approach based on blockchain," 2022.

[26] 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," 2024.

[27] S. M. Umran, S. Lu, Z. A. Abduljabbar, J. Zhu, and J. Wu, "Secure data of industrial internet of things in a cement factory based on a blockchain technology," 2021.

[28] C. Kim, "Ethereum 2.0: How it works and why it matters," *Coindesk: https://www. coindesk. com/wp-content/uploads/2020/07/ETH-2.0-072120. pdf*, 2020.

[29] I. M. Coelho, V. N. Coelho, R. P. Araujo, W. Yong Qiang, and B. D. Rhodes, "Challenges of pbft-inspired consensus for blockchain and enhancements over neo dbft," *Future Internet*, vol. 12, no. 8, p. 129, 2020.

[30] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[31] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog computing in healthcare–a review and discussion," 2017.

[32] P. Verma and S. K. Sood, "Fog assisted-iot enabled patient health monitoring in smart homes," 2018.

[33] Y. Shi, G. Ding, H. Wang, H. E. Roman, and S. Lu, "The fog computing service for healthcare," 2015.

[34] Q. Qi and F. Tao, "A smart manufacturing service system based on edge computing, fog computing, and cloud computing," 2019.

[35] M. Lamberger and F. Mendel, "Higher-order differential attack on reduced sha-256," 2011.

[36] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain for healthcare," 2019.

[37] N. Sangeeta and S. Y. Nam, "Blockchain and interplanetary file system (ipfs)-based data storage system for vehicular networks with keyword search capability," 2023.

[38] L. N. Kodavali and S. Kuppuswamy, "Adaptation of blockchain using ethereum and ipfs for fog based e-healthcare activity recognition system," 2022.

[39] F. Firouzi, S. Jiang, K. Chakrabarty, B. Farahani, M. Daneshmand, J. Song, and K. Mankodiya, "Fusion of iot, ai, edge–fog–cloud, and blockchain: Challenges, solutions, and a case study in healthcare and medicine," 2022.

[40] A. Khatoon, "A blockchain-based smart contract system for healthcare management," 2020.

[41] X. Li, J. Ma, and S. Moon, "On the security of the canetti-krawczyk model," 2005.

[42] R. K. Lenka, M. R. Dey, P. Bhanse, and R. K. Barik, "Performance and load testing: Tools and challenges," 2018.

[43] L. Kim, "Cybersecurity: Ensuring confidentiality, integrity, and availability of information," 2022.

[44] S. Meisami, M. Beheshti-Atashgah, and M. R. Aref, "Using blockchain to achieve decentralized privacy in iot healthcare," 2021.

[45] W. Shao, C. Jia, Y. Xu, K. Qiu, Y. Gao, and Y. He, "Attrichain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain," 2020.

[46] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," 2021.

[47] Y. Imine, D. E. Kouicem, A. Bouabdallah, and A. Lounis, "Masfog: An efficient mutual authentication scheme for fog computing architecture," 2018.