Journal of Basrah Researches (Sciences) **50**(1), 288 (2024)
DOI: https://doi.org/10.56714/bjrs.50.1.23

Adoption of Bloom Filter and Firebase Framework to Enhance Authentication Time for Healthcare Systems Based on Blockchain Technology

Muwafaq Jawad Abba[1], **Ali A.Yassin** [1,*], **Hamid Ali Abed AL-Asadi** [1,*]

[1] Department of Computer Sciences, Education College for Pure Sciences, University of Basrah, 6100, Iraq.

A R T I C L E I N F O

Received 02 May 2024
Accepted 13 June 2024
Published 30 June 2024

K e y w o r d s :

Blockchain, Healthcare, Bloom Filter, Firebase Framework.

Citation: Muwafaq J. A. et al., J. Basrah Res. (Sci.) 50(1), 288 (2024).
DOI:https://doi.org/10.56714/bjrs.50.1.23

A B S T R A C T

Healthcare offers several advantages for actual-time smart healthcare. security concerns are growing due to its constrained computing power, storage capacity, and self-defense capabilities. The tamper-resistant decentralized architecture of more recent blockchain-based authentication solutions gives them significant security features, but they come with a high resource cost because they need a lot of processing power, additional storage, and lengthy authentication processes. Therefore, these challenges offer impediments to achieving the optimal degrees of temporal efficiency and scalability, which are critical for the effective operation of large-scale, time-sensitive IoHT systems. Our work provides an authentication solution specifically created for healthcare systems to address these issues. We work in three phases: initializing, registering, logging in, and authenticating. The suggested system combines blockchain technology, Firebase Framework, Bloom Filter, Multi-Factor authentication, and other elements to improve security and efficiency at the same time. We use the Python programming language to simulate the work, and our findings indicate that the Bloom filter decreases the amount of time it takes to determine whether a person is in the system compared to the previous way. Moreover, using Firebase may reduce transaction numbers by up to 73%. Using the Scyther tool, a security analysis of the proposed scheme proved that the suggested plan is safe from possible threats and maintains the IoHT system's scalability.

1. Introduction

Currently, the most common security challenges frequently involve data breaches, leakage of information, unauthorized access or modifications or modifications, and stealing of accounts about the Internet of Healthcare Things (IoHT) system. Therefore, it is crucial to create and strengthen systems that can withstand different detrimental attacks and malicious programs designed to weaken the security of multiple systems [1]. Consequently, there has been an increased focus on safeguarding

*Corresponding author email : ali.yassin@uobasrah.edu.iq

N: 1817-2695 (Print); 2411-524X (Online)
line at: https://jou.jobrs.edu.iq

the security and privacy of IoHT applications in recent years. Ensuring confidentiality, non-repudiation, data integrity, and the authentication and identification of IoHT devices and users are all essential security needs. Authentication is crucial for ensuring the achievement of other security criteria, making it a top priority [2]. The term authentication defines the steps used to confirm the identity of a given entity. Recognizing and authenticating each other and the system components with which it interacts is essential [3]. Healthcare tackle monitoring, operation, and management involve various apps and users, which increases the potential for authentication and authorization schemes to be breached. Centralized and decentralized architectures make up the bulk of the authentication methods discussed in IoHT literature. Due to their compatibility with the dispersed and heterogeneous character of IoHT systems, decentralized authentication methods that utilize blockchain technology are gaining increasing recommendations for these systems [4, 5]. Consensus, immutability, decentralization, and security are some of the fundamental features of blockchains that the researchers stressed. They highlighted the several ways in which blockchain technology may improve big data authentication and management, including making data more trustworthy, making data sharing easier, increasing privacy and security, and boosting the quality of big data overall [6]. The previous instances highlight the necessity of developing a robust authentication scheme that can withstand different well-known attacks. Furthermore, it discusses the attributes that Blockchain contributes to enhancing the level of security for various systems, specifically in IoHT systems. However, these characteristics may present specific challenges such as the considerable amount of time required for processing and implementation. Thus, many tools have appeared that can assist us in developing robust systems and in the seamless integration of authentication methods with revolutionary blockchain technology, such as Bloom Filter and Firebase Framework. Our work presents a multi-factor authentication method that utilizes blockchain technology to enhance system security by successfully resisting well-known attacks. Furthermore, the implementation of Bloom Filter in our suggested methodology has led to an impressive decrease in both the time and quantity of communications and transactions between the user, the server, and the blockchain. This is especially apparent while validating the authenticity of the user within the system. Similarly, using the Firebase framework led to a significant 73% decrease in the number of transactions, thus leading to areduction in the total amount of ether needed to execute the modification procedure for adding the block to the blockchain. The next parts will outline the contributions provided by this paper.

- Our work employs the multi-factor authentication scheme.
- Also, our work adopted blockchain technology to guarantee security and privacy.
- Adoption of Bloom filter to reduce the time and increase the system accuracy.
- Ultizing scyther tool to verify that our work resistance well-known attack.
- Adoption of Firebase framework to decrease the number of transactions and ether (Gas) cost used to create the transactions on blockchain network.

The paper is organized as follows: Related Work, Section 2. Section 3 discusses Primitive Tools. Section 4 explains the Proposed Scheme and its phases. The analysis of the results in Section 5. In Section 6, the formal security analyses are displayed. Section 8 covers the Conclusion last section of the Work.

2. Related Work

In 2005 Sahai et al [7], introduced Attribute-Based Encryption (ABE) as a beneficial method that provides both confidentiality and precise authorization for users who want to securely communicate data stored on a cloud-based server managed by a third-party. In their 2017 study, I. Chiuchisan et al [8], examined security strategies that specifically addressed the protection of electronic health record (EHR) storage, prevention of malicious code, administration of secure privileges, and other components that ensure the safety of the healthcare data system. They did not provide an option for a patient to migrate existing (EHR) to a health information system. Healthcare facility has the choice to develop their medical data system via rudimentary methods, without incorporating any security protocols. Furthermore, it is impractical for each patient to autonomously manage the transfer of their individual (EHR) through this method. In 2018 Almadhoun et al [9],

introduced an authentication system that tackles the limitations of IoT capacity, provides access to IoT devices, and verifies users through the use of blockchain-enabled fog nodes and Ethereum smart contracts. This technology enables the augmentation of the system's capacity by utilizing fog nodes for computational operations. The system exhibited low time efficiency, as it had an average latency of 2.30 seconds for authenticating IoT devices. Despite its strong security features, the scheme fails to comply with the majority of IoT security standards. In 2018, Mehmood et al [10], proposed a mutual authentication method and key agreement methodology utilizing chaotic maps and Diffie-Hellman key exchange. The suggested solution guarantees that only authorized healthcare professionals can retrieve patients' health data collected through body sensors in the medical system. This paper has major limitations, particularly in terms of computational complexity. The technique used in this paper involves complex cryptographic operations, which can result in longer processing time and increased energy consumption. Furthermore, it experiences scalability challenges when it comes to managing a substantial number of users and devices. Moreover, the scheme's objective of safeguarding user anonymity is compromised by the privacy hazards associated with relying on a centralized cloud. This includes the potential for data breaches and unauthorized access to critical health information. Additionally, there is vulnerability in having a single point of failure if the cloud server experiences a failure. In 2019, Liang et al [11], developed a blockchain-powered system for managing and verifying identities. The system's goal is to enhance patient data confidentiality while allowing for more flexibility in accessing health records. This study has limitations in scalability due to the degradation of blockchain performance as the number of transactions increases, resulting in significant implementation challenges in the healthcare sector. Furthermore, it poses a data privacy concern. In 2019 Dorri et al [12], introduced the concept of blockchain, which serves as an immutable and sequential ledger distributed across all participants in the network. This eliminates the need for a centralized governing authority. In 2020, Cheng et al [13], developed a blockchain-based authentication system that allows for the secure sharing of medical data without the need for a third party. In 2021, Javed et al [14], presented a method for decentralized identity control utilizing blockchain and smart contracts for electronic health records. This approach has attracted attention in research studies, including Health-ID for remote healthcare and Health-ID for EHRs. at addition, a blockchain-based authentication mechanism was developed to reduce the need for repeated authentication at many hospitals. This improves efficiency and reduces the time required for devices with limited processing power and memory. In 2022 Umoren et al [15], utilized blockchain smart contracts to address issues related to user authentication and other constraints in IoT and fog technology. The fog computing framework implemented decentralization, scalability, immutability, and secure authentication for fog devices. Furthermore, it tackled concerns with immutability and scalability in fog computing. The scheme offers strong security measures but does not fulfill the requirements of common Internet of Things (IoT) connectivity scenarios.

In 2024 Asaeed et al [16] proposed a method for group authentication in the Internet of Medical Things (IoMT) that addresses difficulties like scalability and time. Their approach utilizes the SSS algorithm, ECC, fog-based computing, and multi-level blockchain to create a lightweight and scalable group authentication system. The evaluation test exhibits commendable scalability and temporal efficiency. In addition, the ECC algorithm encounters difficulties in handling the vast number of devices and sensors due to its restricted key size.

3. Primitive Tools

3.1. Blockchain Technology

Nakamoto first introduced Bitcoin in 2008, it is a peer-to-peer electronic currency. The term blockchain technology which refers to the distributed ledger that records Bitcoin transactions. Three key tenets underpin the operation of this system: immutability, decentralization, and transparency [17]. Because blockchain is decentralized, it can share data securely and reliably over the Internet of Things (IoT), which is appealing for mutual authentication. It functions as a reliable platform for authentication systems and safe storage [18]. The utilization of blockchain technology in healthcare offers numerous advantages. The decision is prudent, especially considering the healthcare industry's emphasis on safeguarding patient data in light of technological progress. Furthermore, multiple

experts have determined that integrating blockchain technology into the healthcare sector would be a viable resolution [19-21].

The blockchain is a highly secure and reliable system for transferring information. The system consists of a sequence of interconnected blocks that store data in an encrypted format. Every block contains the data, its cryptographic hash, and the hash of the previous block [22], as shown in Figure 1.

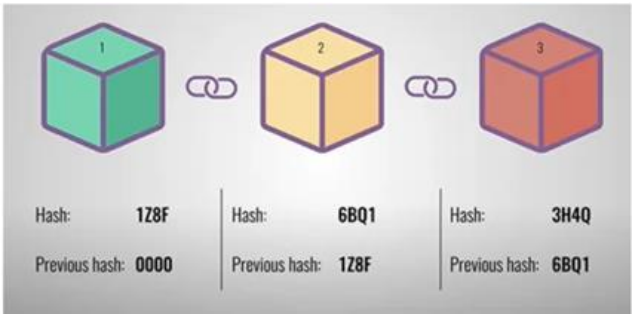


Fig. 1. Overview Blockchain Technology [23].

A. Blockchain Architecture

Let's utilize the following Figure 2 depicts the complete process of a transaction being transmitted from a user within the blockchain network, providing a clearer comprehension of the blockchain architecture[24].

- When a user starts a transaction on a blockchain network, it is distributed to all nodes in the network. Each node retains a comprehensive copy of the blockchain, which is crucial for the verification process. Every interconnected node works together to guarantee the integrity of the block containing the user's transaction. Upon successful validation, the nodes add the block to their respective versions of the blockchain.
- To add a new block to the blockchain, the network nodes must reach a consensus on the legitimacy of the blocks. This agreement is achieved through a validation process that utilizes accurate algorithms to verify the transaction and validate the sender's membership in the network.
- After the validation procedure is finished, the block is appended to the blockchain. Once the entire validation procedure has been finished, the transaction is regarded as finalized.

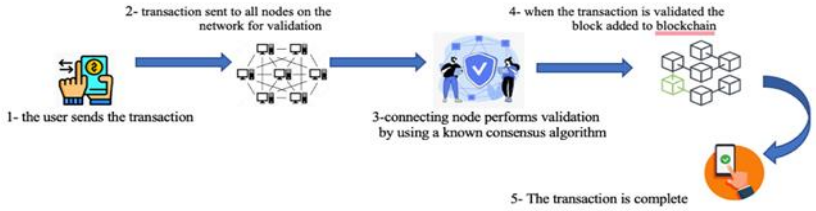


Fig. 2. An Overview of Blockchain Architecture.

B. Consensus Algorithm

For a block to be included in the blockchain, it must adhere to specified consensus protocols. To guarantee this, blockchain technology utilizes consensus algorithms. Nakamoto devised the Proof of Work (PoW) and Byzantine Fault Tolerance (BFT) algorithm in the Bitcoin network, which has become the prevailing consensus technique[25]. The underlying concept of this algorithm is that, due to the presence of numerous nodes or users in a blockchain network, any transaction request initiated by a participating node must undergo computation before it can be incorporated into the network.

The computational units responsible for executing these calculations are referred to as miners, and this procedure is commonly referred to as mining. Table 1 shows a comparison between Pow and BFT [26].

TABLE 1. Comparison between POW and BTF.

Feature	Proof of Stake (PoS)	Byzantine Fault Tolerance (BFT)
Security	More resistant to 51% attacks.	Capable of withstanding Byzantine failures and attacks.
Decentralization	Centralization can occur when there is a concentration of resources.	Facilitates distributed agreement among individual network nodes
Consensus Mechanism	Validators are selected based on the amount of stake they hold.	Consensus across nodes
Scalability	Typically, capable of adapting to accommodate massive networks	The scalability of a system is contingent upon the specific Byzantine Fault Tolerance (BFT) variation being used and the size of the network.
Speed	Transaction speed can be enhanced by expediting block validation.	Transactions may experience delays as a result of the consensus process.

3.2. Bloom Filter

A lightweight probabilistic data structure called the BLOOM filter [27] can be used to describe a set of parameters by allowing membership queries that have a manageable false positive rate. Right now, there are many uses for BF and its variations. BF has been used in networking to facilitate content delivery [28], network monitoring [29], routing and forwarding [30, 31], web caching [32], security enhancement [33] , and more. In terms of databases, BF is a suitable choice for supporting various functions such as query and search, duplicate detection, privacy preservation, key-value storage, content synchronization, and so forth. In addition to their usual applications in databases and networking, BFs have lately been applied to biometric problems, as well as navigational challenges in mobile computing settings [34-37]. Several surveys have further in-depth applications [38].

3.3. Firebase Framework

It is utilized as a means of storing data, while the Ethereum blockchain serves as both a monetary payment mechanism and an authentication method. Furthermore, this demonstrates the implementation of two-factor and multi-factor authentication through the use of an Ethereum account using Firebase Authentication as the authentication channel. The findings indicate that the integration of Firebase with blockchain technology leads to a significant reduction of around 73% in the transaction cost of each transaction conducted on the Ethereum platform [39].

4. Proposed Scheme

This part shows a healthcare authentication system as shown in Figure 3 organized across three phases: Initializing Phase, Registration, Login and Authentication. Our work introduces a healthcare system that includes six main components: Healthcare server provider (HCS), Users (U_i) such as (Patients (P_i), Administrators (Adm_i), and Doctors (Dr_i)), Bloom Filter (BF), Firebase

Framework (FF) and blockchain (BC). Our goal is to establish a secure environment for data exchange between its components based on blockchain. Furthermore, it employs the (BF) to reduce the time taken when checking if the user is present or not in the system and reduce the Ether cost. In addition, employ (FF) to reduce the number of transactions between the HCS and BC and that makes the system more time-efficient. our 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) attacks, replay attacks, 51%, and impersonation. The symbols employed in our investigation are specified in Table 2.

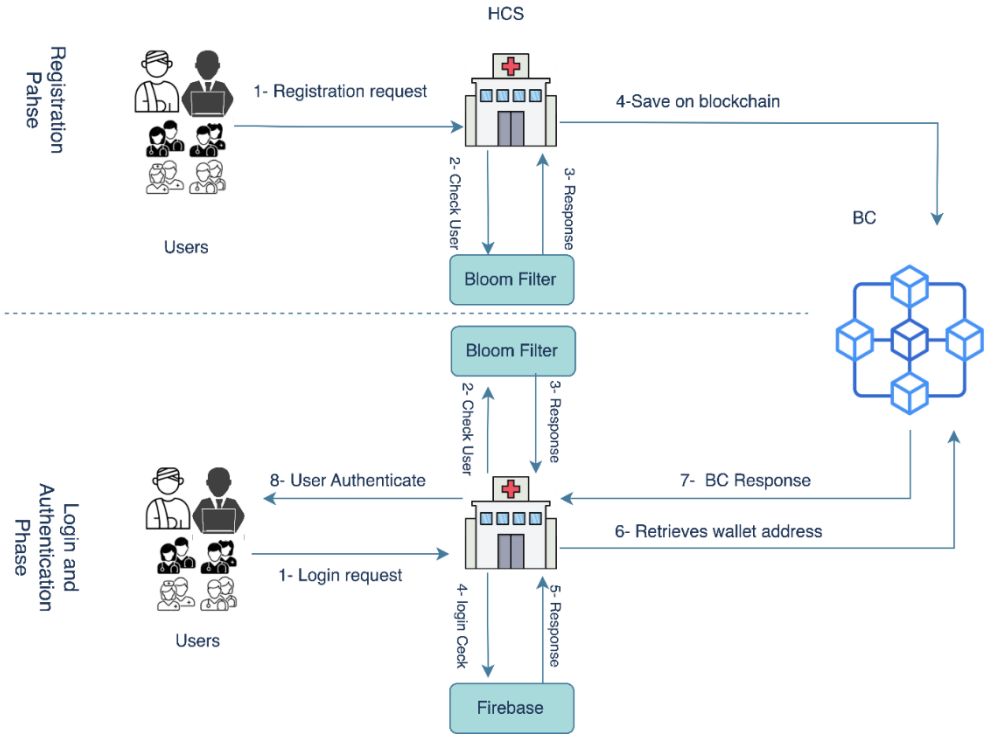


Fig. 3. Overview of Proposed Scheme.

TABEL 2. Symbol used in our scheme

Symbol	Description
HCS	Health Server Provide
BC	Blockchain
ADM_i	Administrator
P_i	Patient
Dr_i	Doctor
Pr_U	User private key
Pu_U	User public key
SK	Shared Key
BF	Bloom Filter
HER_P	Patient electronic record
FF	Firebase Framework

4.1 Initializing Phase

In this phase, HCS is responsible for initializing the system components such as the BC network, creating the (BF) for the user, setting up the (FF), and generating all necessary parameters such as Private, Public, and Shared keys (Pr, Pu, SK) for the server itself and the users and devices.

4.2 Registration Phase

At this point, the User (U_i) who wishes to register in the system must do the following steps, and the patient registration is shown in Figure 4.

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})) and computed HP_{Ui} anomaly by calculating HP_{Ui} = h (Un_{U_i} || Pw_{Pi}) then sends it to HCS.

Step 2: HCS checks if the user is present or not in the system using the BF. If a user already registers then terminate the phase, Otherwise go to step 3.

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

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

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

Step 7: HCS sends the (Pr, Pu, SK) to the user via a secure manner.

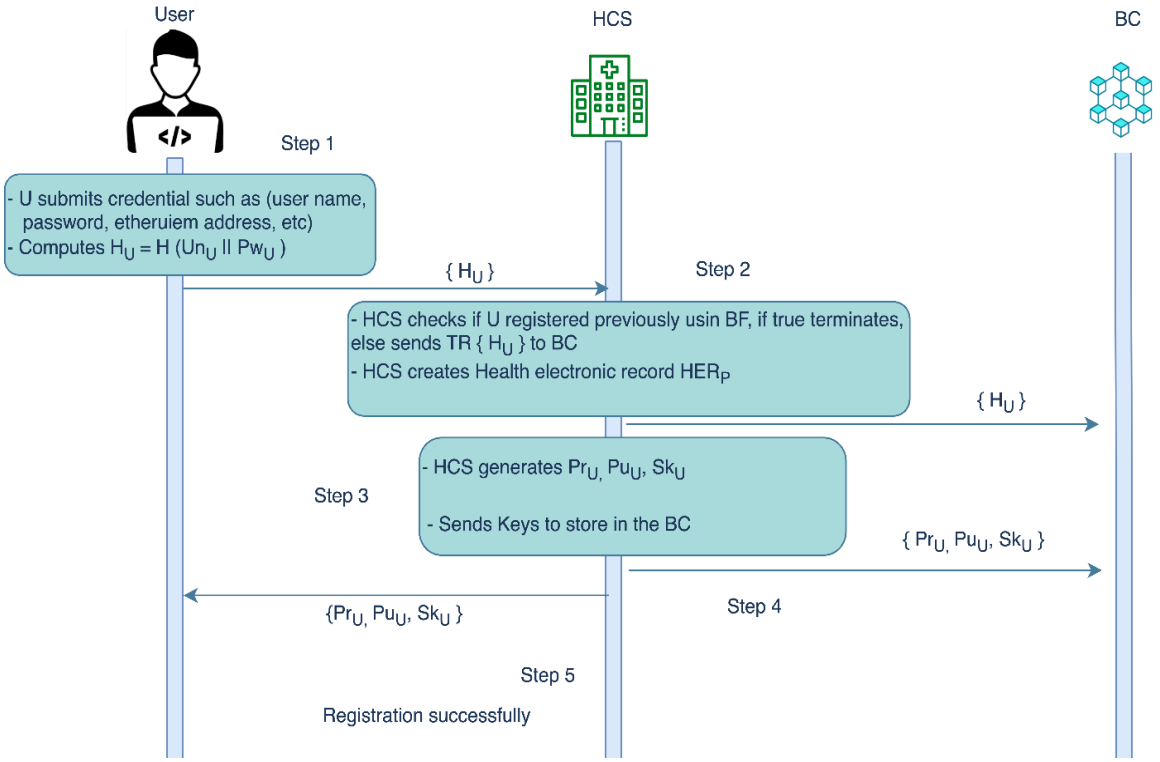


Fig. 4. Sequence diagram of registration phase.

4.3 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. Figure 5 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 HCS as a first authentication factor.

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

a. HCS check A $\stackrel{?}{=} Un'_{U_i}$ using BF, if match HCS restore the random number by decrypt

$r'_i = Dec_{SK_{U_i}}$ (E).

b. HCS retrieves Pw'_{U_i} from FF database and computes HA'_{Ui} = h (Pw'_{U_i} ‖ H (r'_i)) and compare $HA_{U_i} \stackrel{?}{=} HA'_{Ui}$. If true, accept; HCS sends the challenge a verification code (VC) to U_i.

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

Step 6: At the time HCS receives the L form U_i , HCS retrieves Wa_{U_i} from BC and calculates L' = h ($Wa_{U_i} \oplus$ VC $\oplus$ h(r'_i)) and compares $L \stackrel{?}{=} L'$. In this case, the HCS confirm the U_i login and authenticated successfully. Otherwise, refuses the login process.

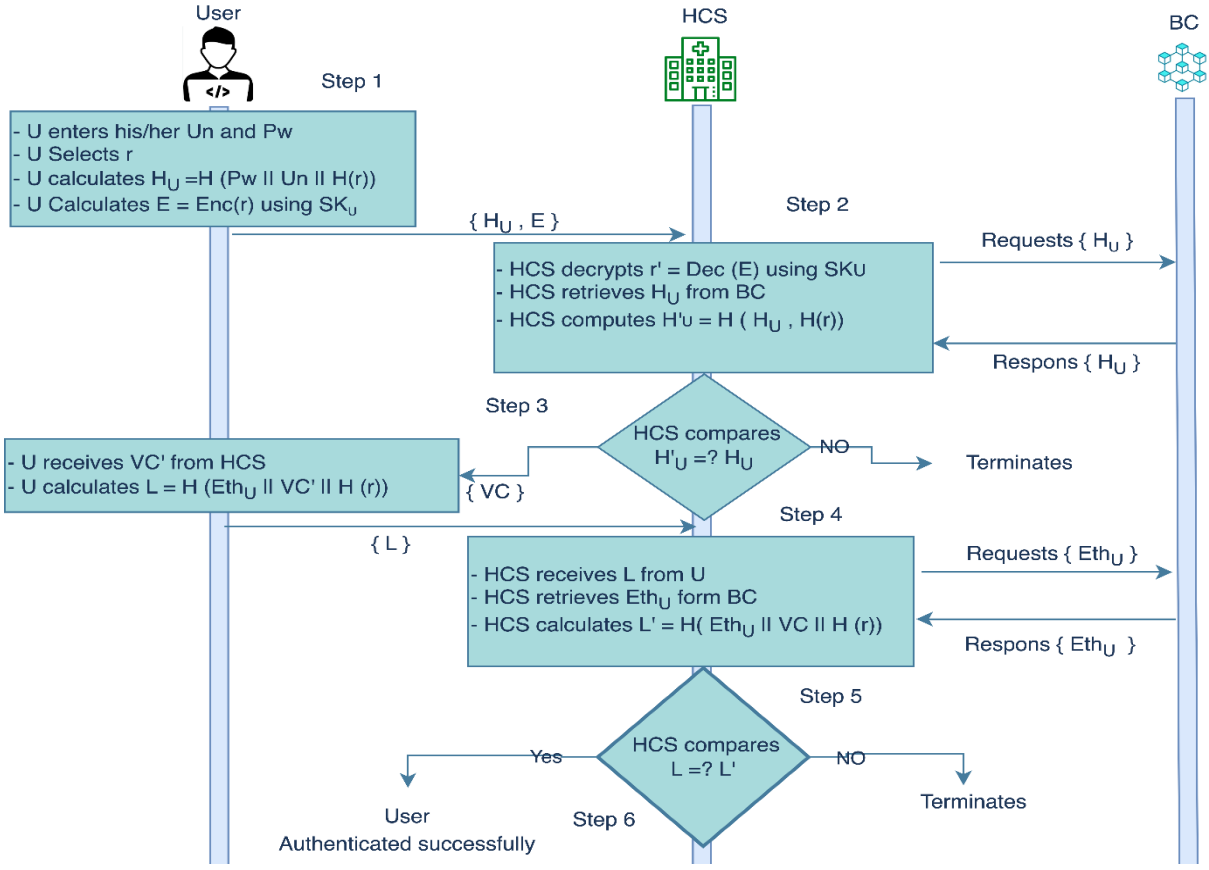


Fig. 5. Sequence diagram of authentication phase.

5. Result Analysis

In this section, will discuss the results obtained by using Firebase and Bloom Filter together in this section. The major objective of this paper is to develop a lightweight, multi-factor authentication scheme that can resist a variety of attacks against systems used in the healthcare sector. Time was reduced and the quantity of transactions between the blockchain and the server was lowered by using Bloom Filter and the Firebase workspace. A 10,000-record of healthcare database [40], of healthcare information was employed, to prove that Bloom Filter better than traditional methods in time-saving. The result clearly shows Bloom Filter's advantage in terms of time reductions and storage,

particularly when dealing with huge data sets. Furthermore, employing the Firebase framework leads to enhanced security and reduces the number of transactions as mentioned in section 3.3.

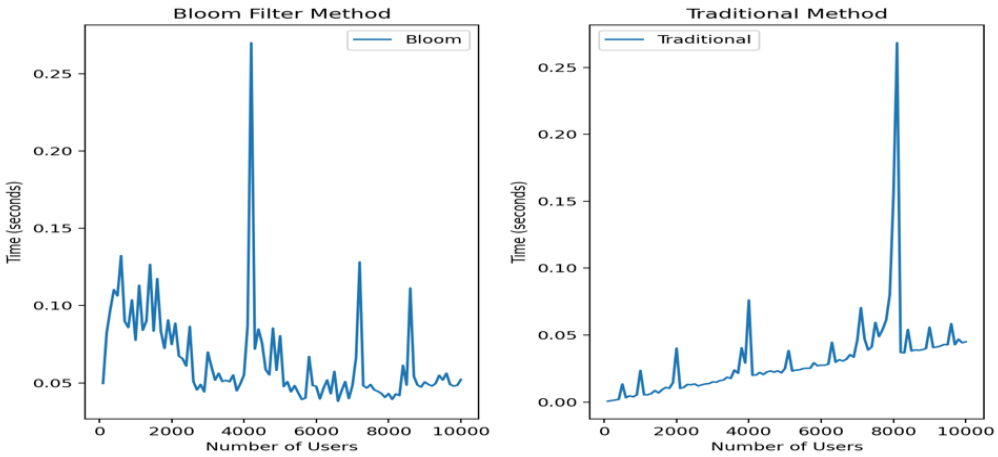


Fig. 6. Comparison between bloom filter and traditional way.

Figure 6, clearly shows Bloom Filter's advantage in terms of time reductions and storage, particularly when dealing with huge data sets. That proof using the bloom filter in our work leads to enhancing the time. The simulation was carried out on a 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. Furthermore, employing Firebase in our work leads to reducing the number of transactions. our work makes use of Remix as the smart contract development tool. the contract is written in Solidity and is deployed using the Ethereum Ganache tool and Metamask and Ether-scan to get the real gas prices for each of the smart contract's operations. In the Ethereum blockchain, fees are defined as the necessary gas, which corresponds to the amount of value that must be paid for every transaction to be completed or contract to be executed. If there is no current balance on the user's account, they are unable to perform any services, and the transaction is considered fraudulent. The deployment and expenses of our suggested contract are shown in Figure 7, together with the appropriate blockchain block in Ganache Ethereum, using the Remix IDE and the Metamask software cryptocurrency wallet. The comprehensive results of the smart contract expenses are methodically recorded in Table 3 .

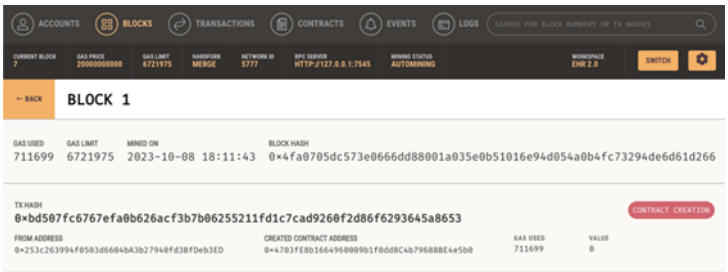


Fig. 7. Ethereum smart contract block.

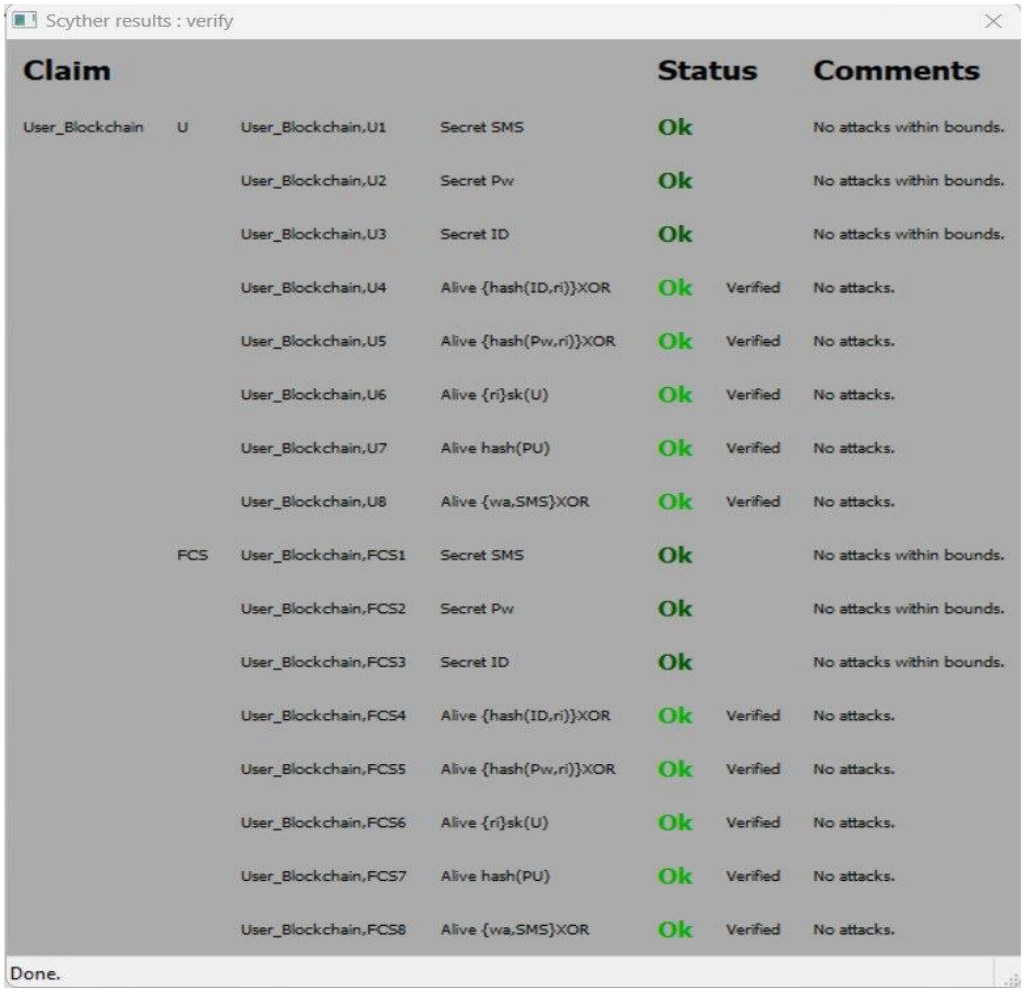
TABEL 3. Smart contract gas cost.

	Experimental result	
CRUD operations	Contact Functions	Gas Cost
	Deploy contract	711699
CRUD Users	Create_User	24765
	Update_User	26621
	Delete_user	26621
	Add_Document	175029

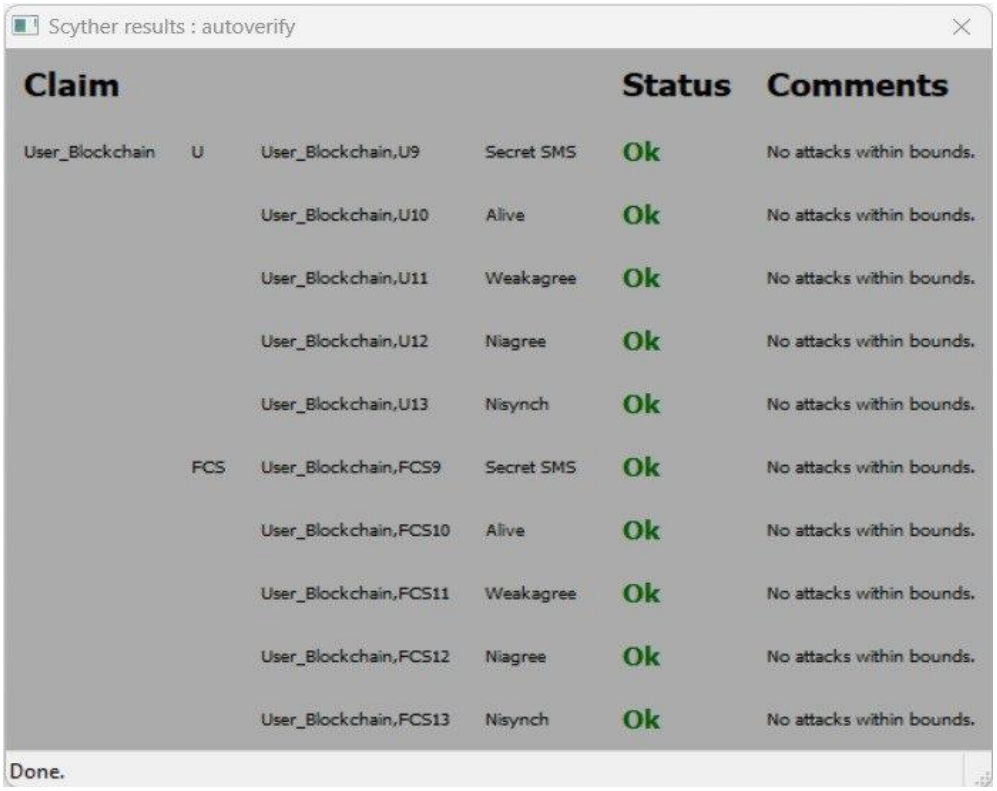
6. Security Analysis

This section, performed intensive safety evaluations to verify the efficacy of our secure technique. Furthermore, utilized the Scyther tool for formal analysis, as illustrated in Figure 8 (a) and (b). In addition, examined the effectiveness of our work method on security and privacy. When creating security measures for any system, it is crucial to take into account three main security criteria: Confidentiality, Integrity, and Availability, also referred to as CIA. Confidentiality guarantees that only individuals with proper authorization can gain access to the system's communications. Data integrity refers to the assurance that only personnel with proper authorization can make changes to stored data. Moreover, The system is designed to withstand common malicious attempts, such as insider threats, Man-in-the-Middle (MITM) attacks, and Reply attacks. Will now provide a summary of the key security requirements evaluation described earlier.

- **Confidentiality**: Done by utilization of symmetric key cryptography.
- **Integrity**: Hashing of data blocks in blockchain achieves integrity.
- **Availability:** Achieved by restricting reactions that are considered valid within the network.



(a)



(b)

Fig. 8. (a) and (b) shows Formal Analysis using the Scyther tool

Table 4 presents a comparative analysis of our proposed model with other existing systems. A comprehensive analysis of several assaults, where assessed the resilience of our system against each attack. To safeguard privacy, our strategy places significant emphasis on data ownership, ensuring that consumers have exclusive control over their data. Implementing blockchain technology for transaction authentication enhances the system's security measures against hostile intrusions, hence reducing the probability of an attacker gaining control over 51% of the network's resources or manipulating the data. In addition, our technology ensures other privacy-enhancing attributes such as the capacity to conduct audits and the transparency of data. By maintaining the control policy on a blockchain ledger, which can only be modified or canceled by the patient, it becomes feasible to provide precise access control. Finally, will discuss some of the common attacks and how can our work resist them.

Replay Attack: This kind of attack leverages a valid authenticated transaction and thus is not a true time attack. Our defense employs strong security features including data encryption, the use of nonce parameters and distinct token identities in their apps, appropriate session administration, and reliance on protocols with the integrity of message checks. Our work can resist this type of attack.

DDOS Attack: This is a distributed form of the DOS Attack. Our defense by utilizing legitimate nodes 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. Our work is capable of resisting this type of attack.

MITM Attack: Personal information from a particular session can be modified or read with this approach. Our defense is done by employing strong encryption and decryption techniques. Our work is efficient in resisting this type of attack.

Modification Attack: The hacker alters or deletes the patient's data contained on the ledger of the blockchain, such as access policies and hash. Our defense by the most blockchain advantage is that Blockchain uses an immutable ledger. Our work is capable of resisting this type of attack.

Eavesdropping Attack: makes it possible for a hacker to obtain the message and monitor the network's communications. Our defense to guard against eavesdropping assaults is to encrypt data while it's being transmitted and during private discussions. Attackers cannot read data that is sent between two parties thanks to encryption. Our work can resist this type of attack

51% Attack: The intruder has gained control of over 51% of the miners and is attempting to manipulate the process of consensus to create a fraudulent block. Our defense is done by implementing this scenario, the attack's likelihood is minimal because of the implementation of a private blockchain and PBFT consensus technique. Our work is capable of resisting this modern type of attack.

TABEL 4 Presents a comparative analysis of our proposed model with other existing schemes.

Scheme	***Blockchain***	***Mutual Authentication***	***Multifactor Authentication***	***Scalability***	***Bloom Filter***	***Robust Against Attacks***	***Firebase***
*Meisami **[41]***	*Y*	*Y*	*N*	*Y*	*N*	*N*	*N*
*Almadhoun **[9]***	*Y*	*Y*	*N*	*Y*	*N*	*Y*	*N*
*Esposito**[42]***	*Y*	*N*	*N*	*NA*	*N*	*NA*	*N*
*Imine **[43]***	*Y*	*Y*	*NA*	*NA*	*N*	*NA*	*Y*
*Alsaeed **[16]***	*Y*	*Y*	*N*	*Y*	*N*	*Y*	*Y*
*Umoren**[15]***	*Y*	*Y*	*Y*	*Y*	*N*	*Y*	*Y*
Our work	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*

(Y=yes, N=no, NA= not mentioned)

7. Conclusion and Future Work

Time and security issues associated with healthcare systems are examined in this work. To improve the time efficiency and security of the IoHT system. Our method uses a multi-factor authentication system based on blockchain technology. Also, use a Bloom Filter during the authentication process to reduce the time when the system checks if the user is present in the system or not. Additionally, utilize Firebase to reduce the number of transactions up to 73% which leads to reducing the gas cost. The goal of integrating an authentication system with immutable blockchain technology is to enable safe public channel communications inside a decentralized environment. Additionally, decentralized node identification is made possible by blockchain technology. The evaluation findings show the great scalability, reliability, and resilience against known attacks of our proposed strategy, along with a shorter execution time compared to existing blockchain-based authentication methods. Furthermore, a security analysis of our scheme is conducted using the Scyther tool, demonstrating its resilience to potential threats. In conclusion, fog computing will be utilized in future work to improve throughput and latency. Additionally, building and construction phase to handle the massive increase in IoHT.

8. References

[1] 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," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020: IEEE, pp. 1-6. doi: 10.1109/hora49412.2020.9152846.

[2] R. Priyadarshi and M. Gheisari, "Security and Privacy in Machine Learning for IoHT and IoMT: A Review," 2024. doi: 10.20944/preprints202403.0329.v1.

[3] M. Tahir, M. Sardaraz, S. Muhammad, and M. Saud Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," *Sustainability*, vol. 12, no. 17, p. 6960, 2020. doi:10.3390/su12176960.
[4] B. Alamri, K. Crowley, and I. Richardson, "Blockchain-based identity management systems in health IoT: A systematic review," *IEEE Access*, vol. 10, pp. 59612-59629, 2022. doi: 10.1109/ACCESS.2022.3180367.
[5] 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. https://doi.org/10.1016/j.iot.2023.100969.
[6] M. Arquam, A. Patel, and P. Nand, "The security strength of Blockchain technology: A Survey Report," *arXiv preprint arXiv:2205.09097*, 2022. doi.org/10.48550/arXiv.2205.09097.
[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24*, 2005: Springer, pp. 457-473. doi:10.1007/11426639_27.
[8] I. Chiuchisan, D.-G. Balan, O. Geman, I. Chiuchisan, and I. Gordin, "A security approach for health care information systems," in *2017 E-health and bioengineering conference (EHB)*, 2017: IEEE, pp. 721-724.
[9] 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. doi: 10.1109/aiccsa.2018.8612856.
[10] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, "Anonymous authentication scheme for smart cloud based healthcare applications," *IEEE access*, vol. 6, pp. 33552-33567, 2018.
[11] Y. Liang, "Identity verification and management of electronic health records with blockchain technology," in *2019 ieee international conference on healthcare informatics (ichi)*, 2019: IEEE, pp. 1-3.
[12] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180-197, 2019. doi:10.1016/j.jpdc.2019.08.005.
[13] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *Journal of medical systems*, vol. 44, no. 2, p. 52, 2020. doi:10.1007/s10916-019-1468-1.
[14] 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," in *Healthcare*, 2021, vol. 9, no. 6: MDPI, p. 712. doi.org/10.3390/healthcare9060712.
[15] 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. doi.org/10.3390/s22103956.
[16] 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. doi.org/10.1016/j.future.2023.09.032.
[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. doi.org/10.2139/ssrn.3440802.
[18] 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," *Applied Sciences*, vol. 11, no. 14, p. 6376, 2021. https://doi.org/10.3390/app11146376.
[19] 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. doi.org/10.1016/j.comcom.2020.08.021.
[20] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability," *Computational and structural biotechnology journal*, vol. 16, pp. 224-230, 2018. doi.org/10.1016/j.csbj.2018.06.003.

[21] 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. doi:10.1109/jsyst.2020.2963840.

[22] 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," in *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, 2022: IEEE, pp. 2284-2292.doi:10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp Metaverse56740.2022.00325

[23] S. M. Umran, S. Lu, Z. A. Abduljabbar, and X. Tang, "A Blockchain-Based Architecture for Securing Industrial IoTs Data in Electric Smart Grid," *Computers, Materials & Continua*, vol. 74, no. 3, 2023. https://doi.org/10.32604/cmc.2023.034331.

[24] X. Xu, I. Weber, and M. Staples, *Architecture for blockchain applications*. Springer, 2019. doi.org/10.1007/978-3-030-03035-3.

[25] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, 2017: Ieee, pp. 557-564. doi: 10.1109/BigDataCongress.2017.85.

[26] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, 2017: IEEE, pp. 2567-2572. doi : 10.1109/smc.2017.8123011.

[27] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422-426, 1970. doi :10.1145/362686.362692.

[28] B. M. Maggs and R. K. Sitaraman, "Algorithmic nuggets in content delivery," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 3, pp. 52-66, 2015. doi : 10.1145/2805789.2805800.

[29] Y. Li, R. Miao, C. Kim, and M. Yu, "{FlowRadar}: A better {NetFlow} for data centers," in *13th USENIX symposium on networked systems design and implementation (NSDI 16)*, 2016, pp. 311-324. doi/10.5555/2930611.2930632.

[30] F. Angius, M. Gerla, and G. Pau, "Bloogo: Bloom filter based gossip algorithm for wireless ndn," in *Proceedings of the 1st ACM workshop on Emerging Name-Oriented Mobile Networking Design-Architecture, Algorithms, and Applications*, 2012, pp. 25-30. doi/abs/10.1145/2248361.2248369.

[31] X. Tian and Y. Cheng, "Loop mitigation in bloom filter based multicast: A destination-oriented approach," in *2012 Proceedings IEEE INFOCOM*, 2012: IEEE, pp. 2131-2139. doi : 0.1109/infcom.2012.6195596.

[32] O. Rottenstreich and I. Keslassy, "The bloom paradox: When not to use a bloom filter," *IEEE/ACM Transactions on Networking*, vol. 23, no. 3, pp. 703-716, 2014. doi : 10.1109/infcom.2012.6195533.

[33] E. A. Durham, M. Kantarcioglu, Y. Xue, C. Toth, M. Kuzu, and B. Malin, "Composite bloom filters for secure record linkage," *IEEE transactions on knowledge and data engineering*, vol. 26, no. 12, pp. 2956-2968, 2013. doi:10.1109/tkde.2013.91.

[34] A. Margara and G. Cugola, "High-performance publish-subscribe matching using parallel hardware," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 126-135, 2013. doi:10.1109/tpds.2013.39.

[35] P. Jiang, Y. Ji, X. Wang, J. Zhu, and Y. Cheng, "Design of a multiple bloom filter for distributed navigation routing," *IEEE Transactions On Systems, Man, And Cybernetics: Systems*, vol. 44, no. 2, pp. 254-260, 2013. doi:10.1109/tsmc.2013.2242884.

[36] S. Xiong, Y. Yao, Q. Cao, and T. He, "kbf: A bloom filter for key-value storage with an application on approximate state machines," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 2014: IEEE, pp. 1150-1158. doi : 10.1109/infocom.2014.6848046.

[37] D. Guo and M. Li, "Set reconciliation via counting bloom filters," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2367-2380, 2012. doi : 10.1109/tkde.2012.215.

[38] S. Geravand and M. Ahmadi, "Bloom filter applications in network security: A state-of-the-art survey," *Computer Networks*, vol. 57, no. 18, pp. 4047-4064, 2013. doi : 10.1016/j.comnet.2013.09.003.

[39] K. M. Hlaing and D. E. Nyaung, "Electricity billing system using ethereum and firebase," in *2019 International Conference on Advanced Information Technologies (ICAIT)*, 2019: IEEE, pp. 217-221. doi:10.1109/aitc.2019.8920931.

[40] Kaggle. "Healthcare Dataset." kaggle. https://www.kaggle.com/datasets/prasad22/healthcare-dataset/data (accessed.

[41] S. Meisami, M. Beheshti-Atashgah, and M. Aref, "Using Blockchain to Achieve Decentralized Privacy In IoT Healthcare. arXiv 2021," *arXiv preprint arXiv:2109.14812*. doi.org/10.5121/ijci.2023.120208.

[42] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing & Management*, vol. 58, no. 2, p. 102468, 2021. doi:10.1016/j.ipm.2020.102468.

[43] Y. Imine, D. E. Kouicem, A. Bouabdallah, and L. Ahmed, "MASFOG: An efficient mutual authentication scheme for fog computing architecture," in *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, 2018: IEEE, pp. 608-613. doi 10.1109/TrustCom/BigDataSE.2018.00091.

Journal of Basrah Researches (Sciences) **50**(1), 288 (2024)
DOI: https://doi.org/10.56714/bjrs.50.1.23

اعتماد مرشحات بلوم و تقنية Firebase Framework لتعزيز وقت المصادقة لأنظمة الرعاية الصحية المعتمدة على تقنية Blockchain

موفق جواد عباس[1] ، علي عادل ياسين[1]، حامد عبد علي الاسدي [2]

[1] جامعة البصرة ، كلية التربية للعلوم الصرفة، قسم علوم الحاسبات

معلومات البحث

الاستلام 02 ايار 2024
القبول 13 حزيران 2024
النشر 30 حزيران 2024

الكلمات المفتاحية

البلوك تشين ، الرعاية الصحية ، مرشحات بلوم , Firebase

الملخص

تقدم الرعاية الصحية مزايا متعددة للمراقبة في الوقت الفعلي، ولكن تزداد المخاوف الأمنية بسبب محدودية قوة الحوسبة وسعات التخزين وقدرات الدفاع الذاتي. توفر الهندسة المعمارية اللامركزية، المقاومة للهجمات والتلاعب في البيانات، أمانًا كبيرًا من خلال المصادقة القائمة على تقنية البلوك تشين. ومع ذلك، فإنها تتطلب موارد عالية نظرًا لحاجتها إلى قوة معالجة إضافية وسعة تخزين وعمليات مصادقة مطولة. لذلك، تشكل هذه التحديات عوائق أمام تحقيق كفاءة زمنية فعالة وقدرة على التوسع، وهي أمور حاسمة لتشغيل الأنظمة الضخمة لإنترنت الأشياء في مجال الرعاية الصحية (IoHT) التي تتطلب استجابة سريعة.

نقدم في عملنا حلاً للمصادقة مصممًا خصيصًا لأنظمة الرعاية الصحية لمعالجة هذه المشكلات. يتكون النظام من ثلاث مراحل: التهيئة، التسجيل، تسجيل الدخول، والمصادقة. يجمع النظام المقترح بين تقنية البلوك تشين وإطار عمل Firebase ومرشحات بلوم والمصادقة متعددة العوامل، بالإضافة إلى عناصر أخرى لتحسين الأمان والكفاءة معًا. نستخدم لغة البرمجة بايثون لمحاكاة العمل، وتشير النتائج إلى أن مرشحات بلوم تقلل من الوقت المستغرق لتحديد وجود الشخص في النظام مقارنة بالطرق التقليدية. بالإضافة إلى ذلك، يمكن لتقنية Firebase أن تقلل عدد المعاملات بنسبة تصل إلى 73.%

أجرينا تحليل أمان للخطة المقترحة باستخدام أداة Scyther ، وأثبتت الدراسة الأمنية الرسمية أن الخطة المقترحة آمنة من التهديدات المحتملة وتحافظ على قابلية توسع النظام

Citation: Muwafaq J. A. et al., J. Basrah Res. (Sci.) 50(1), 288 (2024).
DOI:https://doi.org/10.56714/bjrs.50.1.23

***Corresponding author email :** ali.yassin@uobasrah.edu.iq

N: 1817-2695 (Print); 2411-524X (Online)
line at: https://jou.jobrs.edu.iq