**A block-chain-based authentication mechanism for medical systems in the Internet of Things**

|  |
| --- |
| **Gholam Reza Zargar†** , **Hamid Barati**††,  Gr.zargar@iaud.ac.ir barati@iaud.ac.ir  Azad University of Dezful**†**  Azad University of Dezful **††** |

Abstract

The Internet of Things is a collection of sensors with limited resources in which every entity is provided with the ability to send data through communication networks. The Internet of Things is the make smart of things, and in order to achieve this goal, things are equipped with sensors, so the connection of billions of objects and tools in the Internet platform requires confidentiality, integrity, identity authentication and access control mechanisms. The issue of authentication and correctness of data during sending from sensors to servers is very important, especially in medical information. In this thesis, an authentication protocol has been tried to be proposed for Internet of Things environments in the field of medicine with a block-chain platform, which has a light and secure architecture, by reviewing the previous works. The proposed protocol using the fuzzy extractor along with official/unofficial security analysis using AVISPA tool and BAN logic shows that the proposed plan is more efficient in terms of communication and calculation costs, and more resistant to various attacks..

Key words:

Authentication, security, Internet of Things, network attacks, blockchain

Information in medical systems is very valuable and insecurity in them can be a big challenge for the life and health of patients. In order to provide a better and more reliable service to a patient in the hospital, through the wireless network around the patient's body and with the help of sensors with low capabilities, sensitive information such as vital signs is collected and sent to remote networks for Monitoring and processing are sent.

Over the past few years, other technologies, including cloud computing, have helped a lot in providing the Internet of Things with the necessary capabilities to analyze and process information and turn it into knowledge (Zhaofeng et al., 2020). The data must be available and processed only by the person who has authorized access. As an example of this scenario, we can refer to the sensitive information of a patient in the hospital. In the hospital, data is processed and stored for some purposes such as treatment. Nevertheless, there are some security problems caused by unauthorized access to information (Hami et al., 2022). In order to protect privacy, secure communications against attackers through firewalls, authentication, and advanced encryption operations (Chen et al., 2020). In order to create a security framework, the integration of the Internet of Things and block-chain has been used in various ways, all of which are in the development stage, but still its security architecture has not reached its maturity (Alzoubi et al., 2020). In this Article, considering the challenges in the Internet of Things, an authentication protocol has been proposed for medical Internet of Things environments with a block-chain platform, which has a light and secure architecture. The proposed protocol is a two-way authentication, where each user's information will be stored in a private block-chain using a smart card. The proposed protocol using the fuzzy extractor and official/informal security analysis using AVISPA tool and BAN logic shows that the proposed plan is more efficient in terms of communication and calculation costs and more resistant to various attacks.

# Internet of things

The Internet of Things is a new concept in the world of technology and communication, which combines a decentralized Internet model of independent physical and digital objects with the sensitivity and process of the network. In smart object tags, they carry the details of a program that provides sensitivity to the situations, locations and reactions of human users and logging into the system, interpreting events and the world, working between them, communicating with each and exchanging. They feel information with humans.

The Internet of Things was created with the aim of providing a large scale, heterogeneous, adaptable to the development of simple applications for end users. In the Internet of Things environment, the user may have many devices to use and connect them to each other and share data. Also, in this technology, devices do not have powerful computing and storage power. The Internet of Things is a set of resource-constrained sensors with low battery consumption, so they are unable to perform heavy computations. In an authentication protocol, there must be a mechanism to authenticate legitimate users and a robust mechanism to identify malicious users. Passive attackers eavesdrop on protocol messages and try to calculate secret keys, and active attackers try to insert or drop messages to steal user session keys. Therefore, an ideal authentication protocol should be lightweight and secure against various attacks. In some systems, the speed of message transfer is really critical. Therefore, a secure and lightweight authentication mechanism is needed for these systems.

# Security in the Internet of Things

Protecting the system against sabotage or theft of hardware, software and data is presented as the definition of computer security, and cyber security is the protection of data in the network, according to the traditional definition of security in the form of a security pyramid based on three elements of information confidentiality, information integration, and data availability are defined.

Confidentiality of information: In order to control access and maintain the confidentiality of information, this security mechanism is defined and unauthorized users cannot access the system. One of these mechanisms is encryption, which changes information in the form of codes and passwords.

Information integration: In order to be more secure and to prevent information theft, only authorized people are able to change information under a specified process, and the integrity of information outside and inside the system must be maintained.

Data availability: It is one of the most important factors defined in the security pyramid and it means that information is always available for users even in difficult situations (Mohanta et al., 2020).

An Internet of Things system needs to comply with the following security protocols to become a secure system:

1. Authentication
2. Determine permission or access level
3. Confidentiality
4. Integrity

Authentication actually verifies the identity of users or devices in the Internet of Things system. The authorization process checks what privileges the entity is authorized to run on the system. In terms of data confidentiality and integrity, it will be ensured that the data is encrypted, so none of the users can make unauthorized changes even in storage or during data transfer.

# Block-chain

Block-chain technology has been extensively researched over the past few years. Satoshi Nakamoto introduced the concept of block-chain as a support mechanism for the digital cryptocurrency called Bitcoin. The basic concept of block-chain technology provides a framework for cooperation between unknown and untrusted things, while verifying the published characteristics of mobile devices, without the need for a security and authentication center, such as cloud computing architecture. Currently this core technology relies on an immutable public ledger, which is a record of data shared between all participants. This public ledger contains blocks of data that are linked using a cryptographic hash key. The linking process is called proof of work. Both ledgers and consensus mechanisms are inherently impervious to data manipulation. Block data cannot be changed after the fact, as this would invalidate the hash of previous blocks in the block-chain and break the consensus between nodes. Using block-chain technology allows Bitcoin public distributed ledgers to conduct digital currency transactions cheaply and securely without a third party, which verifies the transaction and avoids the multi-year double fee issue. Whenever a transaction is initiated, the smart contract is executed as a stored process. Key features of block-chain technology include decentralized control, data transparency and controllability, distributed information, and security from malicious actors (Lao et al., 2020).

# Block-chain architecture

Block-chain is an information technology that allows transactions to be verified by a group of untrusted actors. It is a distributed, immutable, transparent, secure and controllable ledger. It is basically a distributed database of all digital transactions or events that have been executed and shared among participating parties. Once entered into the block-chain, information can never be modified or deleted. Block-chain contains a unique and real record of every transaction ever made. Figure 1 shows the block-chain structure (Berdik et al., 2021).

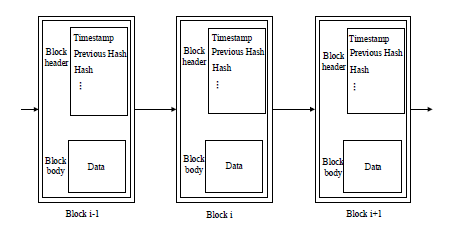


Figure 1 : The block-chain structure

Figure 2

Each block-chain consists of many blocks and each block consists of a block header and a block body. The block header contains a lot of Meta information about the current block. For example, a timestamp is a hash value for the block-chain body and a hash value for the previous block, which block body is usually used to record the actual data of current transactions (Fu et al., 2020).

# Relation Work

Nita and Marius (2023) in a research titled Elliptic Curve-based Authentication Protocol for IoT with the help of blockchain, an authentication mechanism for IoT devices based on elliptic curves is proposed, which has a low computational cost compared to other techniques. They are known to be used in cryptography, which provides a high level of security. The proposed system includes a blockchain network that verifies the identity of the device that tries to connect to the system to send data to it. When the valid identity is declared, the blockchain records the transaction and the storage server starts the data transfer. In addition to a lightweight authentication mechanism, the proposed method has several important features due to the use of the blockchain network compared to related works, which analysis shows that the proposed authentication mechanism is secure against common attacks. Al-Ahmad et al. (2023) have presented a chain authentication protocol that has a lightweight decentralized mechanism for the Internet of Things based on blockchain patterns. The proposed protocol arranges the nodes in clusters and creates an authentication blockchain for each cluster. These cluster chains are connected by another blockchain. The security performance of the proposed protocol is analyzed and tested by using the verification software of cryptographic protocols. Saruti and Safkhani (2023) have presented an authentication protocol based on elliptic curve encryption for health-care systems in the Internet of Things. Elliptic curve encryption has been used in Internet of Things due to the security and high speed of operations and limited resources. The proposed protocol is resistant to many attacks, which have been shown by formal and informal methods. Also, this system is optimal in terms of communication costs. Simoniak and Kesar (2023) presented a research on authentication protocol and session key in Internet of Things. In this article, the latest communication protocols designed to secure authentication processes and agreement on session keys in IoT environments are reviewed. The level of security, vulnerability and computational and communication costs for the proposed protocol have been analyzed. The results show that the desired protocol is more secure than other similar algorithms. Ng et al. (2023) have proposed an improved two-step authentication scheme for health-care systems. In this design, an authentication technique based on two factors is presented to increase security and privacy, while solving the problems of previous designs. The proposed scheme has been simulated using the Automatic Validation Tool, Protocols and Internet Security Programs (AVISPA), and the results show that this scheme is secure against active and passive attacks. The proposed protocol provides high security and better complexity based on communication, computational cost and execution time. Tai et al. (2022) in a research titled as a new three-factor authentication protocol for service providers in smart health care systems with the help of 6G presented a solution named (CL-UCSSO) to achieve a convenient communication and Low cost in a system with multi-server architecture has been introduced. In this method, due to the decentralization of service providers, the authentication system validates users in health care systems, and the results show that this system is resistant to some attacks and has an optimal calculation cost. Mirsarai et al. (2022) proposed a three-factor authentication protocol for IoT environments. This protocol uses blockchain technology, hash and XOR functions, as well as the concept of fuzzy mining and encryption techniques to ensure a suitable level of security. BAN logic, ROR model and Avispa tool have been used to protect data against information manipulation and attacks. With the help of formal analysis, the security capability of mutual authentication implemented in the proposed protocol is demonstrated. Also, the authors concluded that the proposed protocol is optimal and more secure in terms of calculation cost, communication cost, security requirements and resistance to attacks compared to other related protocols. Hu et al. (2022) proposed a two-factor authentication protocol for wireless sensor networks in IoT environments. It is a proposed two-factor authentication scheme based on the elliptic curve cryptosystem and its security has been proven by the official verification tool ProVerif. Compared to related schemes, the proposed protocol has a higher level of security, and it has also achieved an acceptable efficiency in computing cost. They claim, this is the first design that fulfills two-factor security and user anonymity under the attack taken from the sensor node. Hathaqib et al. (2022) have presented a three-factor authentication framework suitable for important applications based on the Internet of Things. The proposed protocol is designed based on identity, password and digital signature scheme. This framework uses various security patterns such as elliptic curve encryption (ECC) and hash chains with low computing power. Official and unofficial security analysis shows that the framework is resistant to various types of cryptographic attacks. Furthermore, automated validation performed with the Scyther tool confirms that there are no cryptographic attacks on any of the claims made in the proposed framework. Finally, a comparison of the framework's security features, computational and communication costs with other existing protocols has been made. Sahu et al. (2021) presented a three-factor authentication protocol for healthcare system efficiently in IoT, which used elliptic curve encryption for security and high speed of operation, as well as using fuzzy extractor for encryption. The biometric parameter of the user has increased the security of the proposed authentication system. The results show that this system is resistant to some attacks, but it has a high cost of calculations and communication. Takare et al. (2021) have presented a secure authentication scheme with a lightweight architecture in the IoT environment. In the registration phase by means of user ID and encryption, new parameters are created for the user and stored in the device. In the next step, a mutual authentication is used to identify the user in the network and finally, a session key is created. In the phase of changing the user's password, this is done with the help of the IoT server. Vahid et al. (2020) in a research titled security and privacy in the Internet of Things using machine learning and blockchain, stated the threats and countermeasures that every object in the Internet of Things is a factor for hackers to infiltrate. As a result, machine learning algorithms are used to generate accurate outputs from large complex databases. The generated outputs can be used to predict and identify vulnerabilities in IoT systems. In addition, block technique is important in modern Internet applications to address security and privacy issues. Hence, data privacy is the most important factor, which can only be valid when it ends. The current system lacks the coherence of the data set used to train the model. Any intruder or hacker can manipulate this data set to get the desired results. Currently, the integration of machine learning algorithms with the blockchain technique to achieve Internet of Things security and privacy is a relatively new area that has been applied to guarantee the security of the Internet of Things environment. Yazdinejad et al. (2020) presented in a research entitled authentication of blockchain-based SDN controllers for Internet of Things networks with optimal energy consumption. In this article, researchers have discussed the potential of integrating blockchain and software defined networks (SDN) in reducing some challenges. In particular, a secure and efficient blockchain architecture using SDN controllers for IoT networks using a cluster structure with a new routing protocol is proposed. This architecture uses public and private blockchains for peer-to-peer communication between IoT devices and SDN controllers. Experimental results show that the proposed protocol based on cluster structure has higher capacity, lower delay and lower energy consumption than other proposed protocols EESCFD, SMSN, AODV, AOMDV and DSDV. In other words, the architecture proposed in this article is improved compared to the classic blockchain. Koi et al. (2020) presented an approach for the authentication of multiple wireless sensor networks based on blockchain in an article. In this article, IoT nodes are divided into base stations, cluster head nodes and normal nodes according to their energy level, which form a hierarchical network. A blockchain network is built among different types of nodes to form a hybrid blockchain model including local chain and public chain. In this hybrid model, mutual authentication of nodes is realized in different communication scenarios, normal node authentication operation is performed by local blockchain, and cluster head node authentication is realized in public blockchain. The security and performance analysis of this method shows that this design is acceptable in terms of security and performance. In public blockchain, nodes create transactions by connecting to a non-permissive blockchain and create a decentralized trusted network through consensus. If all the IoT nodes are added to the public blockchain, the repeated authentication operation will consume a lot of resources and time, which cannot meet the real-time needs of the IoT. To join the network, private blockchain nodes must be authenticated, while nodes in different wireless sensor networks belong to different managers (base stations), so they cannot authenticate through authentication. Unified identity join the private chain. A local blockchain is a private blockchain that consists of all cluster head nodes in a single wireless sensor network. When the cluster head node is registered with the identity information in the public blockchain, the cluster head node is allowed to join the corresponding local blockchain. Local blockchain is used to register normal nodes for authentication. Smart contracts are deployed on cluster head nodes to verify registration and authentication requests sent by normal nodes. The registered node information is uploaded to the public chain for storage. Since the cluster head node is directly connected to the base station, when authenticating the subscriber node, the entire node information list is directly obtained from the local blockchain node to complete the normal node authentication. According to the designed network pattern and authentication requirements, the relevant authentication scheme mainly includes four steps:

• First, basic security parameters are set for all network member nodes.

• In the registration phase, the identity information of each node is registered and stored in the public client.

• In the authentication phase, various types of authentication requests are verified and authorized by the hybrid blockchain model.

• The node should be removed from the system in case of damage, attack, energy exhaustion, etc.

Mohanty et al. (2020) presented in an article entitled the use of lightweight blockchain for the personal security of Internet of Things networks. In this article, an efficient lightweight integrated blockchain (ELIB) model is prepared to meet the needs of the Internet of Things. The presented model is deployed in a smart home environment.

The limited resources in the smart home use the advantages of centralized management that generates shared keys to transfer data and process each input and output request. A series of three optimizations have been done in the presented ELIB model, which includes lightweight consensus algorithm, certificate encryption (CC) and power distribution management scheme. Compared to other methods, ELIB saves a total of 50% in processing time with a minimum energy consumption of 0.07 mJ. Abbasinejad et al. (2020) presented a secure signature-based protocol for privacy protection. The proposed protocol is suitable for IoT environments and uses elliptic curve encryption to create public and private keys to create a secure framework. This protocol is resistant to various attacks and has used the ProVerif tool to prove compliance with security requirements. The results show that the protocol has a high calculation and communication cost and the access level of users in the network has not been determined.

# Proposed protocol architecture

In order to increase the performance and security in the proposed protocol, it has been tried to provide a simple architecture to reduce consumption costs and information exchange, and also to create a security framework in the Internet of Things.

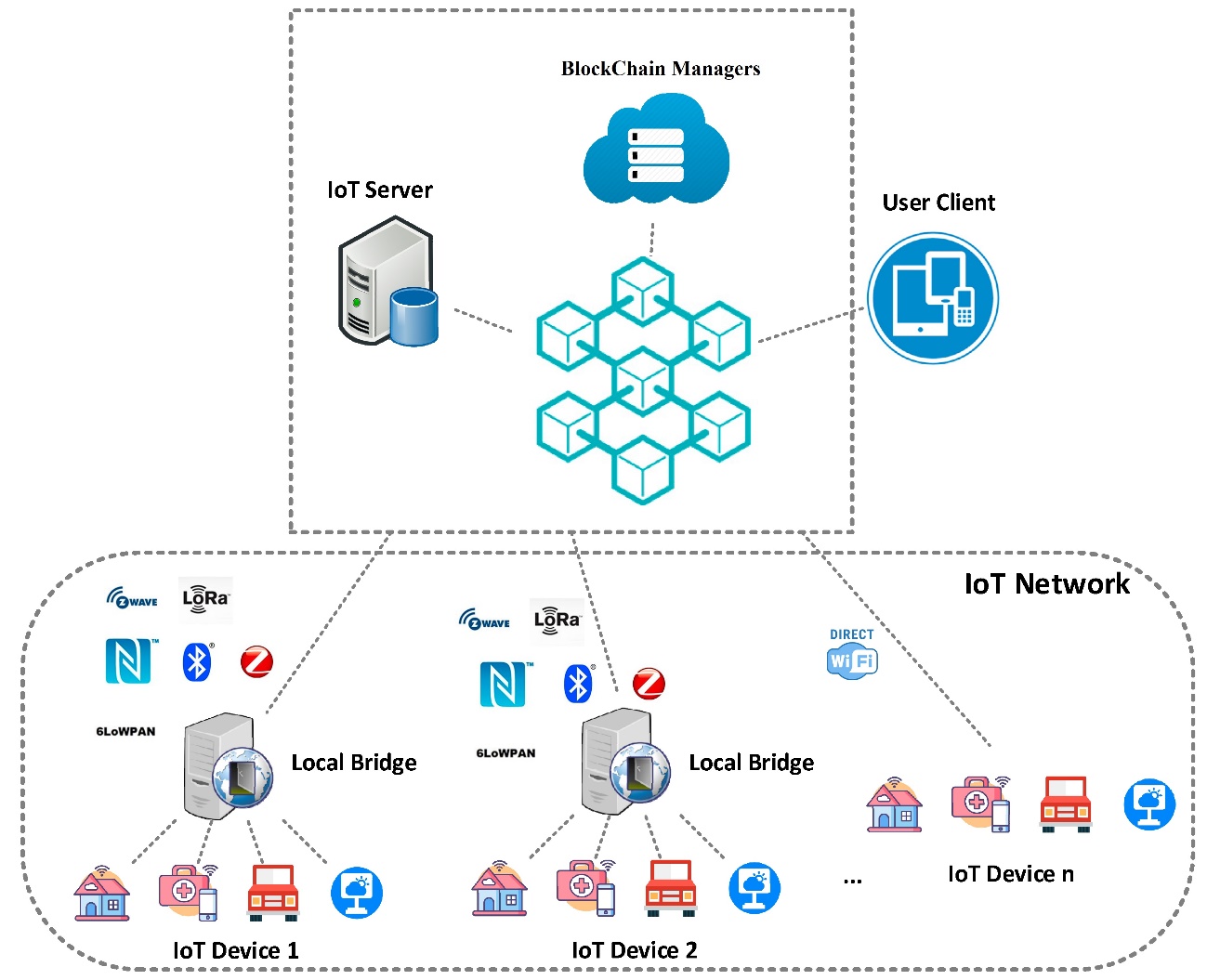


Figure 2 : Proposed protocol architecture

Figure 3: Block structure in blockchain

Entity layer: This layer includes the objects in the Internet of Things, which are connected with the Internet of Things server.

Operating layer: This layer includes the authentication operation between the user and the Internet of Things server, which after confirming the identity and specifying the access level, the user can exchange information with the network with his session key.

Blockchain layer: This layer includes the network infrastructure in the blockchain platform and the core of the memory structure of the proposed protocol. Most blockchains are distributed, transparent, and have secure ledgers that record a chain of changes in chronological order. Based on the requirement, blockchain is offered in public, private and consortium (combined) platforms. In the proposed protocol, the private model is used because private blockchains are fast and the number of participants is small compared to the public blockchain, as a result, less time is needed to reach an agreement in the network and transactions they are done faster. Private blockchains are more scalable. In a private blockchain, only a few nodes are allowed to confirm transactions, which means that it doesn't matter if the network grows, the private blockchain will work at its previous speed and efficiency. The user's smart card and the information required by the servers are stored in it. The existence of a Blockchain Managers interface on the user side in order to manage the communication between the user and the blockchain will lead to increased security. The user's device stores the smart card in the blockchain through the interface and stores the address of the encrypted block in itself, and through it, it has access to the smart card corresponding to the user, which is shown in Figure 2 and 3.

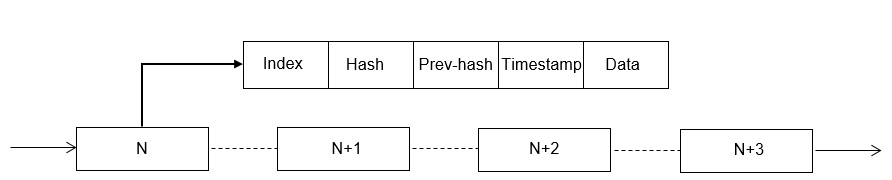


Figure 3 : Block structure in blockchain

# Block structure in blockchain

Considering the increasing use of Internet of Things in society and the challenges and limitations in it, the need for security and privacy is of great importance. Various authentication systems were presented, including one-factor and two-factor, which were associated with various problems, as a result, biometrics was added as a third security factor to authentication plans. Nevertheless, a number of three-factor authentication schemes still have security weaknesses.

In this research, a plan based on three-factor

Authentication has been proposed and finally, by presenting an improved and secure authentication plan in the context of blockchain block chains and using elliptic curve encryption, a new proposed protocol has been presented and referred to. And will be compared with other previous researches in order to evaluate the results. In this protocol, security has been tried in two layers: 1- authentication 2- encryption. Also, the information will be stored in the blockchain platform, which increases the security of data preservation and decentralized management. The parameters are implemented with the secure hashing function of SHA-3.

Abstract function: SHA-3 is the newest member of the secure abstract algorithm family provided by the National Institute of Technology and Standards. The internal structure of SHA-3 is different from the structure of SHA-1 and SHA-2, which are more similar to MD5. Yes, although it is considered a member of the same series of standards. Since the information related to the authentication process is carried out in the servers of the Internet of Things and there is a possibility of their change by a third party, therefore, the information is coded with a secure abstracting algorithm so that it cannot be discovered (Mahandram and Velosamy, 2020).

The abstract function is a function where is a constant number and is a string of arbitrary length and is a string of fixed length . Therefore, the abstract generator function receives the input with arbitrary length and calculates the output with fixed length. It is also necessary:

1. The calculation of the abstractor function should be simple, that is, having and , the calculation of should be done simply.
2. From a computational point of view, the reverse of its operation is impossible, that is, with and , it is difficult to calculate the input .
3. It is difficult to find two different inputs and such that .

# Proposed protocol

In this section, the registration and authentication protocol and the creation of a smart card for the privacy protection system of the Internet of Things on the blockchain platform will be described. This protocol is based on elliptic curve encryption and includes three phases: 1- registration phase, 2- login phase, authentication 3- password and biometric update phase. Each of the phases will be explained separately. The symbols used in the proposed protocol are shown in Table 1.

# Registration phase

Table 1: Symbols used

|  |  |
| --- | --- |
| explanation | symbol |
| 𝑈𝑖 | user |
| 𝑆𝑗 | server |
| 𝑆𝐶𝑖 | user smart card |
| 𝑃𝑊𝑖 | User password |
| 𝐼𝐷𝑖 | User ID |
| 𝐵𝑖 | User biometrics |
| 𝑆𝐼𝐷j | Server ID |
|  | The server's private key |
| K𝑝𝑢b | Public key |
| k𝑐/r | Randomly generated numbers |
| ℎ(.) | scrambler function |
| H(.) | Biohashing function |
| 𝑇𝑐/ 𝑇𝑠 | Current time in the server system/user system |
|  | Maximum acceptable transmission delay |
|  | Variable |
| ⨁ | Operator XOR |
| || | concatenation operator |
| 𝑃 | The fundamental point of the elliptic curve |
| (PX,PY) | Coordinates of the point |
| (.) | Point multiplication operator |
| BC/ 𝑆C | Smart card/Blockchain |

Whenever a new user wants to access the Internet of Things services on the blockchain platform, he must first register in the Internet of Things server, then the server will issue a smart card to the new user, and the user can use the service using this smart card. During the registration stage, the server selects an elliptic curve with the equation (mod p) on the field , and also determines the first number of in a large interval within the field. so that is a finite field and , also the point O is at infinity and the server's public and private key is Neha is created.

First step: the user firstly enters , password 〖 and his biometric , then the algorithm first generates the random number , then the value of which is hidden in With the help of , it calculates as follows.

(1)

Finally, the device sends the user message (𝑃𝑊𝐷𝑖, 𝐼𝐷𝑖) to the server through a secure channel.

Second step: As soon as the server receives the information sent from the user, it will first check and save the user ID, then calculate the parameter with the help of the sent information and the secret key of the server:

(2)

(3)

Finally, a smart card {, , } is issued and sent to the user through a secure channel.

Third step: After receiving the smart card, the user performs the following calculations:

(4)

Finally, the parameters {, , , , } are placed in the smart card and the smart card will be stored in the blockchain, and the encrypted address of the desired block will be returned and stored in the device, in Figure 4 phase.

# Login and authentication phase

After the successful execution of this phase (login, authentication), a registered user can access IoT services on the blockchain platform.

First step: First, the user enters  *,* password and biometricsthen, with the encrypted address of the desired block stored in the device and with the help of the blockchain management interface, the device obtains the information of the user's smart card and the following calculations are performed:

(5)

Then the device compares the value with the value stored in the card. If these two values are not equal, the connection ends. Otherwise, the device makes sure that the entered information is related to the real user, then the random number , and a time tag are selected and the following parameters are calculated:

(6)

(7)

(8)

(9)

(10)

(11)

(12)

Finally, the device sends the message {, , , , , } } to the server through an insecure channel.

Second step: As soon as the server receives the connection request message, the correctness of the following relationship is first checked.

(13)

The server checks the condition ( maximum acceptable transmission delay), to ensure that the message is new.

(14)

(15)

(16)

(17)

(18)

(19)

Considering that the server is aware of valid user IDs, if the user ID obtained from relation 14 is not valid, the connection will be disconnected. Next, if the condition in this part is fulfilled, the connection ends. Otherwise, if the value of is equal to the value of, then the server ensures that the message {, , , ,,} is sent from the user side and is on the way to manipulation it has not been done. Then the server selects the random number along with the time tag and calculates the following parameters and the session key as follows:

(20)

(21)

(22)

(23)

(24)

(25)

Then the server sends the message { , , , , } to the user through the insecure channel.

Third step: After receiving the message, the user first checks the correctness of the following condition, and if

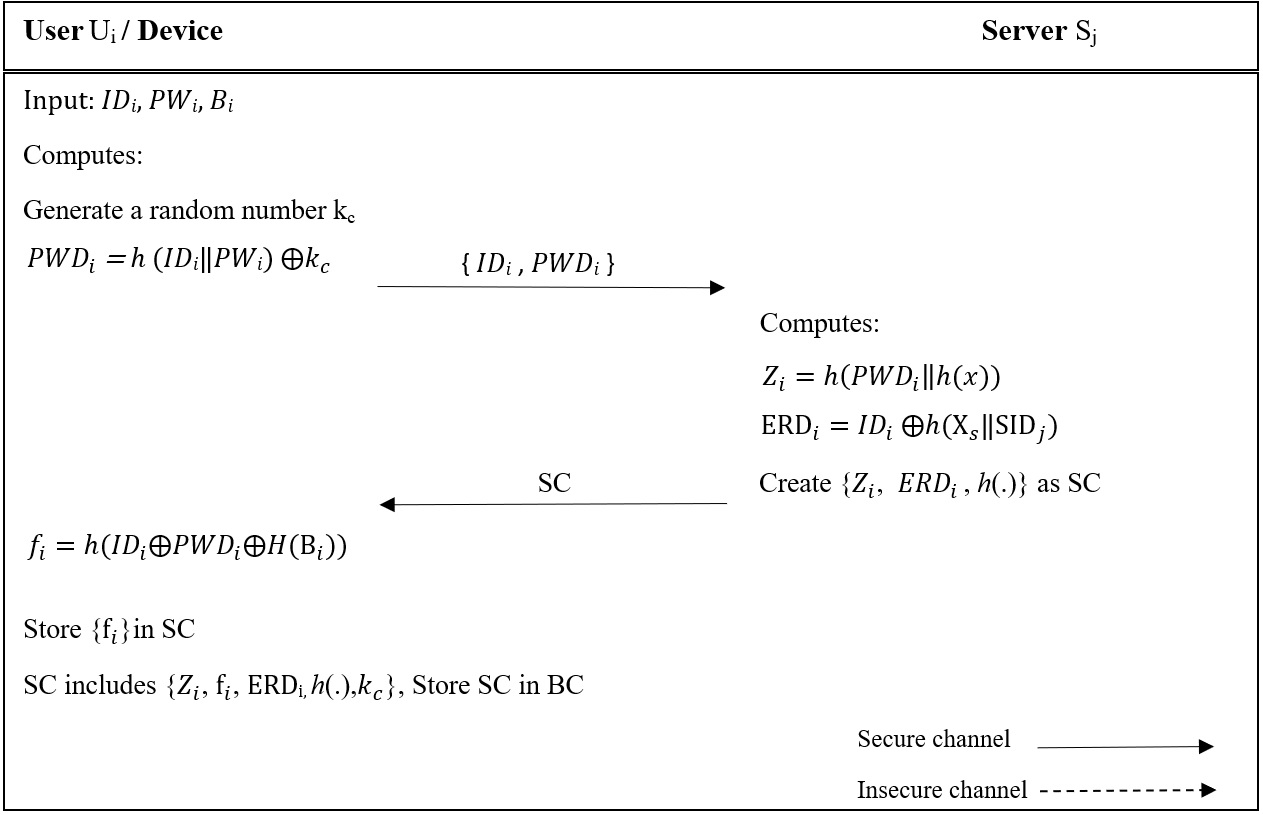


Figure 4: User registration in the Internet of Things server

The condition is met, performs the following calculations:

(26)

(27)

(28)

(29)

(30)

The user authenticates the server by checking the condition . If the condition is met, the connection is terminated, otherwise the user makes sure that the message { , , , , } has been sent from the server side. Therefore, the user and the server agree on the same key. As mentioned, in this protocol there is two-way authentication between the user and the server. Also, using a time tag prevents replay attacks. Figure 5 shows the stages of login, authentication and key agreement in the proposed protocol.

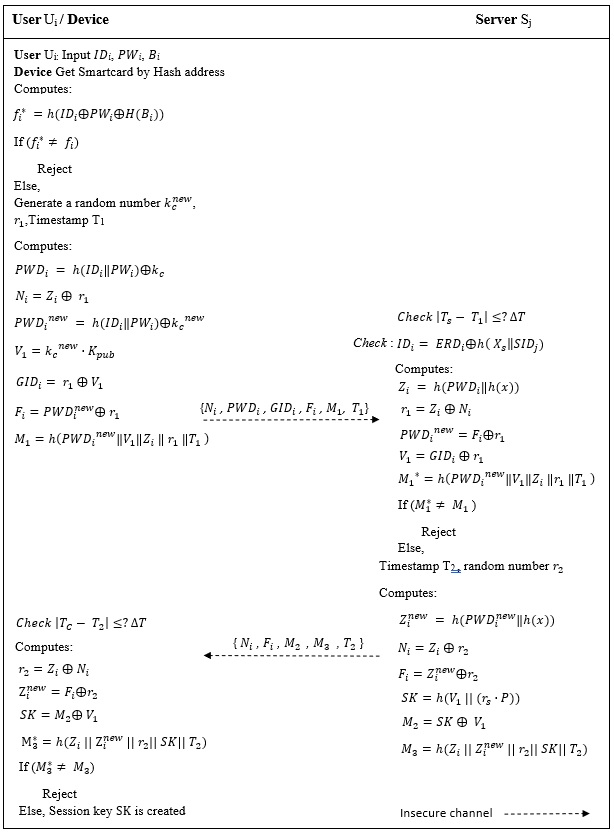


Figure 5: The steps of the second phase of authentication and shared key determination

# Password and biometric update phase

After a long period of time has passed or due to the disclosure of the password, the user must change his password. In a secure IoT system, to avoid wasting server time, the user must be able to update their password and biometrics without involving the server.

The first step: First, the user enters the identifier , the current password and the biometric , then the device with the encrypted address of the desired block and the help of the blockchain management interface, the card information Smart gets the user and performs the following calculation:

(31)

If the condition = is not met, the connection will end, otherwise, the device will ensure the correctness of the entered information. Second step: Now, the device asks the user to enter the new password and the new biometric Then, they calculate the new parameter "" and replace the old parameter "" in the smart card memory. The steps for updating password and biometrics are shown in Figure 6.

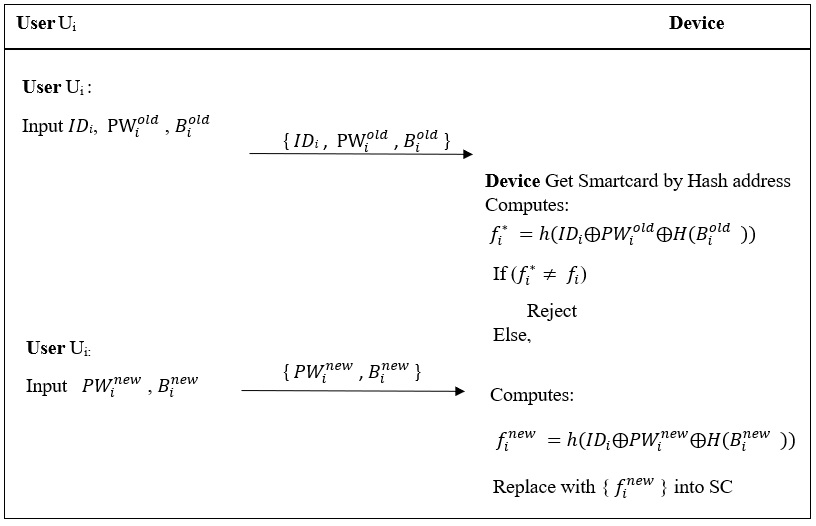


Figure 6 : The third phase of updating the user's password and biometrics

# Informal evaluation of the security performance of the proposed protocol

In this section, an attempt has been made to analyze the steps and messages used in the proposed protocol against attacks and security features, which have been evaluated and described in detail, and a number of logical assumptions for the protocol's security analysis have been presented.

**Assumption 1**: The attacker cannot obtain the server's private key from the relationship because of ECDLP security.

**Assumption** 2: The adversary cannot obtain all three security factors of the user at the same time.

**Assumption 3**: The adversary can obtain only one parameter in a relationship at the same time.

**Data confidentiality**: This feature will ensure that the messages exchanged between the user and the server cannot be detected by an attacker. All the parameters in {, , , , , , } and {, , , , } are encoded using the abstract generator function or changed by XOR operation. also because the random numbers and are randomly selected by the user and the server in each session, so the adversary will not be able to identify that the sessions are related by listening and collecting the messages of the entry phase, authentication and key agreement to different users or related to the same user.

**Two-way authentication**: based on the provided protocol, first the user Ui sends a login request to the server Sj in the form {, , , , , , }. The server checks the condition and if its validity is confirmed, then Ui is authenticated by the server Sj, then the server creates the session key and sends the message {, , , , } to the user Ui sends After receiving the message by the user, first the condition is checked and if its validity is confirmed, the server will be authenticated by the user. Therefore, the protocol achieves secure two-way authentication.

**Data Integrity**: This feature ensures that the parameters must be created and used correctly, if a parameter is changed, the protocol will not confirm the authentication operation. If an adversary changes the values {, , , , , , } sent from the user to the server in any way, then will be established and the connection will be interrupted. Similarly, if an adversary changes the values {, , , , } sent from the server to the user in any way, then the relation will be established and the connection will be interrupted.

**Progressive security**: In cryptography, progressive security is a property of key exchange methods. This property ensures that the previous and current session keys will still be secure if long-term confidential cryptographic information is exposed. If an adversary somehow obtains the server's private keys, according to the session key relation , it is not possible to obtain the session key because in each session random numbers with a large length are created, from Therefore, it is computationally impossible to find random numbers by trial and error and testing the entire state space.

**Three-factor confidentiality**: This feature refers to three factors: password, smart card, and user's biometrics. If the adversary obtains two factors, he still cannot enter the system non-virtually, and a third factor is needed.

**Update the password safely**: after a long period of time has passed or because the password has been leaked, the user must change his password. In a secure IoT system, to avoid wasting server time, the user must be able to update their password and biometrics without involving the server. This operation will be done using user ID, password and biometric parameters by the device, first the user's identity and information from relationship will be checked, and if approved, the user's password and biometric agent will be updated safely.

**Replay attack**: Replay attack occurs when the attacker obtains the authentication information, records it first, and sometimes after the connection ends, uses them to create a new connection with the name of the previous server/user. It makes the destination server or user unable to recognize that the received message is old and duplicate. In the proposed protocol, this attack has been prevented due to the use of time tags and and random numbers.

**Server spoofing attack**: If the adversary tries to spoof the server's identity, he must send a fake message {, , , , } but correct to be authenticated by the user. For this purpose, the adversary must choose a timestamp and a random number, and then calculate the valid and as follows:

To calculateand, the adversary must be aware of the random number chosen by the user, server and SK. To calculate the session key, it must calculate the random numbers of the user and the server, because the length of the random numbers is large, so finding random numbers by trial and error and testing the entire state space is computationally impossible.

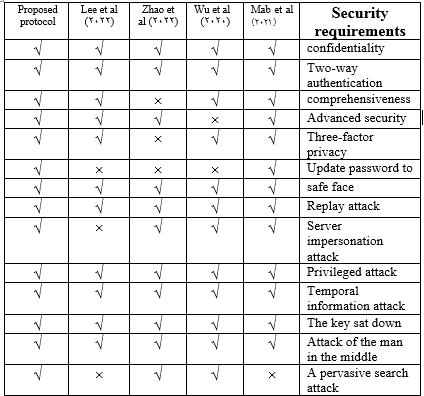
**Privileged person attack**: In this attack, a privileged person in the system can attack based on the information he has. Assuming that the hostile person obtains the basic information of a user's smart card that is created on the server side {, ,}, he still cannot introduce himself to the system as a legitimate user because he needs to calculate It has relation below which includes parameters that the enemy does not have access to and are not stored in the smart card.

**The attack of knowing the temporary information of the secret key**: In this attack, the hostile person has somehow obtained the temporary information of the secret key, which is the random number . After confirming the authentication of both parties, they will start creating the session key. To make the session key, the hostile person needs to know , point P and the abstract generator function , and only knowing random numbers is not enough, also before using the session key, the user must confirm the identity of the server, as a result It is not able to create a session key.

**Man-in-the-middle attack**: In this attack, the hostile person changes, eavesdrops or intercepts the information transferred between the user and the server. One of the most effective solutions to prevent this type of attack is the use of two-way authentication, which the proposed protocol uses. If the adversary somehow gets {, , , , , , } and {, , , , } messages, he still can't get the values inside it. Because all the information sent is encrypted. If the adversary makes a change in the messages due to the use of a two-way authentication mechanism, the opposite party will not confirm the identity of the sender of the messages. As a result, this protocol is resistant to this attack.

**Comprehensive search attack**: In this attack, the adversary tries to obtain the user's password, but considering that the user's password will be encrypted with the hashing function, user ID and random number k\_c, as a result, this protocol is resistant to this attack. Be A comparison of the type of resistance against attacks and security requirements between the proposed protocol and other protocols is made in Table 2. The result of the comparison shows that the proposed protocol is resistant to more attacks and meets the security requirements.

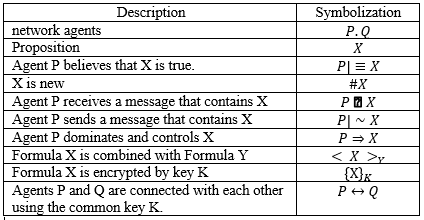
Table 2: Comparison of protocols from the point of view of security requirements and attacks



# Research tools

The proposed protocol should be investigated and analyzed in terms of security, and there are different methods to analyze the security of authentication and key distribution protocols. One of the most reliable and widely used methods used in most research works is the BAN method. In order to use the logic of BAN, the rules, notations specified in Table 3, assumptions and goals should be defined correctly and then it should be proved.

Table 3: BAN logic symbols



1. The semantic code of the message
2. Nance approval rule
3. Rule of government territory
4. Being a new rule
5. Confidence rule

The proposed protocol should follow the following goals in order to prove two-way authentication:

1. The first goal:
2. The second goal:
3. The third goal:
4. The fourth goal

The proposed protocol forms are idealized as follows:

M1:

M2 :

With the help of BAN logic, the following assumptions are presented:

A1:

A2:

A3:

A4:

A5:

A6:

Proving the theorem using BAN logic :

Step 1: Based on M1, we have:

Step 2: Based on the semantic rule of the message with S1 and A3, we have:

Step 3: based on the rule of newness together with A1 we have:

Step 4: Based on Nance's rule, we have:

Step 5: Based on the rule, we are sure:

Objective 2 was confirmed.

Step 6: Based on the rules of the territory of the government, we have:

Objective 1 was confirmed.

Step 7: Based on M2, we have:

Step 8: Based on the semantic rule of the message with S7 and A4, we have:

Step 9: Based on the new rule with A2, we have:

Step 10: Based on Nance's rule A2, we have:

Step 11: Based on the rule, we are sure:

Objective 4 was confirmed.

Step 12: Based on the rules of the territory of the government, we have:

Objective 3 was confirmed.

According to the set objectives and steps 1 to 12, the proposed protocol has obtained the security feature of two-way authentication.

# Security analysis using AVISPA simulation tool

In this part, the security analysis of the proposed protocol is discussed using the AVISPA tool. AVISPA tool is a push-button tool for automatic validation of Internet security protocols written with HLPSL as a role-based model. Each role defines the main parameters and a communication channel with other roles that four tools OFMC, CL-AtSe, SATMC and TA4SP are used in AVISPA (Vigano, 2006). We implemented the proposed protocol on SPAN Ubuntu 10.10 virtual machine with 6144 MB RAM, installed on Windows 10 operating system, Intel Core i5-6400 processor. Two-phase registration and authentication have been implemented along with the main roles of user and server. Session and Environment roles are defined using HLPSL. The analysis results in Figure 7 show that the proposed protocol is safe against active and passive attacks, including replay attacks and crowd attacks.

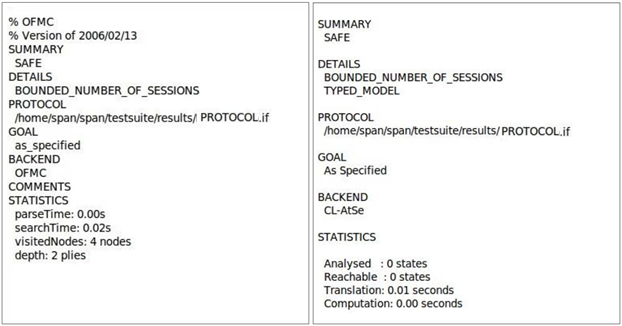
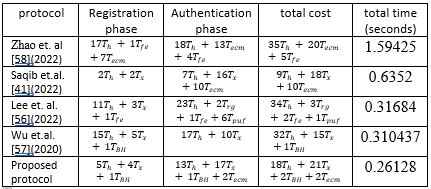


Figure7 : Implementation results of CL-AtSe back-end and OFMC back-end

**Calculation cost:** The evaluation of performance analysis results in terms of calculation cost is specified in Table 4. In this comparison between the proposed protocol and other related protocols, different parameters have been used.represents the one-way abstractor function with approximate time (≈ 0.0005 seconds), represents operations and system functions with approximate time (≈ 0.0120 seconds), represents the scalar multiplication operation with approximate time (≈ 0.294437 seconds), represents the elliptic curve encryption operation with Approximate time (≈0.06307 seconds), denotes the operation of generating non-random numbers with approximate time (≈0.05390 seconds), denotes the biohashing operation with approximate time (≈0.06307 seconds), denotes the approximate time of XOR operation. Because the approximate time of XOR operation is negligible compared to other operations, also represents fuzzy extraction operation. Measuring the execution time of cryptographic operations in the processor environment: Intel(R) Core(TM) 3.2 GHz, 8 GB memory, 64-bit Win7 system and SHA-3 has been used as the abstract generator function (Ravanbakhsh et al., 2018, Park et al., 2017). The results in table 4 and diagram figure 8 show the optimality of the proposed protocol.

Table 4: Comparison of the calculation cost of related protocols



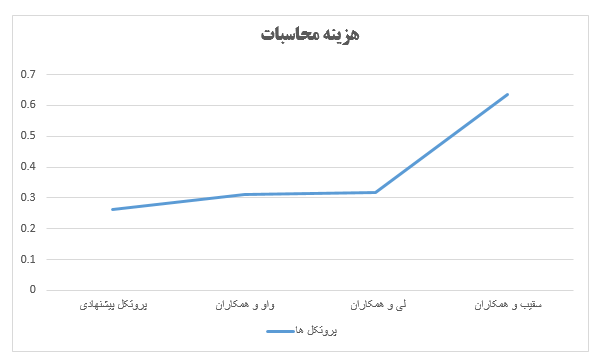
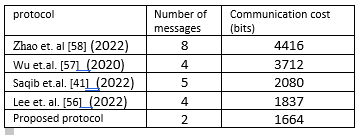


Figure 8: Comparison of the calculation cost of related protocols

**Communication cost:** The proposed protocol is compared with other related protocols in terms of communication cost in Table 5. The cost of the used parameters include 160-bit digest function, 160-bit ECC, 32-bit time stamp and user ID, 160-bit random numbers, 128-bit symmetric encryption and decryption, and 64-bit access level token (Ravanbakhsh et al., 2018). , Park et al., 2017). In the proposed protocol, the messages transmitted between the server and the user in the authentication phase in the insecure channel in two stages {, , , , , , } and {, , , , } are The communication cost of the proposed protocol is (bit992=32+160+160+160+160+160+160) and (bit672=160+160+160+160) respectively.

Table 5: Comparison of communication cost of related protocols



# Conclusion

In this work, an attempt was made to present a three-factor authentication protocol by studying the previous works and identifying the security vulnerabilities in the authentication system of Internet of Things networks. Privacy protection using ECC lightweight encryption scheme despite limited resources will make the IoT network more resistant to attacks and security threats. The proposed protocol is an efficient three-factor authentication protocol using ECC encryption on the blockchain platform. This protocol has three main phases: registration phase, login and authentication phase, and password and biometric update phase.

# Future work

References

[1] Shafique, K., Khawaja, B.A., Sabir, F., Qazi, S. and Mustaqim, M. ,2020, Internet of things (IoT) for next-

generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. Ieee Access, 8, pp.23022-23040.

[2] Tahir, M., Sardaraz, M., Muhammad, S. and Saud Khan, M., 2020. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. Sustainability, 12(17), p.6960.

[3] Mudhar, J.K., Kalra, S. and Malhotra, J., 2020. An efficient blockchain based authentication scheme to secure fog enabled IoT devices. In 2020 Indo–Taiwan 2nd International Conference on Computing, Analytics and Networks (Indo-Taiwan ICAN) (pp. 75-80). IEEE.

[4] Shin, S. and Kwon, T. ,2020, A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things. IEEE access, 8, pp.67555-67571.

[5] Goyat, R., Kumar, G., Alazab, M., Conti, M., Rai, M.K., Thomas, R., Saha, R. and Kim, T.H., 2020. Blockchain-Based Data Storage With Privacy and Authentication in Internet of Things. IEEE Internet of Things Journal, 9(16), pp.14203-14215.

[6] Zhaofeng, M., Jialin, M., Jihui, W. and Zhiguang, S., 2020. Blockchain-based decentralized authentication modeling scheme in edge and IoT environment. IEEE Internet of Things Journal, 8(4), pp.2116-2123

[7] Hammi B, Zeadally S, Khatoun R, Nebhen J. Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures. Computers & Security. 4:102677. vol. 117, Mar. ,2022, doi: 10.1016/j.cose.2022.102677

[8] Chen, F., Tang, Y., Cheng, X., Xie, D., Wang, T. and Zhao, C., 2021. Blockchain-based efficient device authentication protocol for medical cyber-physical systems. Security and Communication Networks, 2021, pp.1-13

[9] Alzubi, J.A., 2021. Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare. Computer Communications, 170, pp.200-208.

[10] Mwitende, G., Ye, Y., Ali, I. and Li, F., 2020. Certificateless authenticated key agreement for blockchain-based WBANs. Journal of Systems Architecture, 110, p.101777.

[11] Nabil, A.A., Ammar, M. and Hefny, H.A., 2020. Proposed authentication protocol for IoT using blockchain and fog nodes. International Journal of Advanced Computer Science and Applications, 11(4).

[12] Yao X, Farha F, Li R, Psychoula I, Chen L, Ning H. Security and privacy issues of physical objects in the IoT: Challenges and opportunities. Digital Communications and Networks. ,2021, Aug. [doi: 10.1016/j.dcan.2020.09.001](https://doi.org/10.1016/j.dcan.2020.09.001)

[13] Hussien, H.M., Yasin, S.M., Udzir, N.I., Ninggal, M.I.H. and Salman, S., 2021. Blockchain technology in the healthcare industry: Trends and opportunities. Journal of Industrial Information Integration, 22, p.100217.

[14] Chen, C.L., Deng, Y.Y., Weng, W., Sun, H. and Zhou, M., 2020. A blockchain-based secure inter-hospital EMR sharing system. Applied Sciences, 10(14), p.4958.

[15] J. Zhang, C. Shen, H. Su, M. T. Arafin and G. Qu, "Voltage Over-Scaling-Based Lightweight Authentication for IoT Security," in IEEE Transactions on Computers, vol. 71, no. 2, pp. 323-336, 1 Feb. ,2022, doi: 10.1109/TC.2021.3049543.

[16] Salimitari, M., Chatterjee, M. and Fallah, Y.P., 2020. A survey on consensus methods in blockchain for resource-constrained IoT networks. Internet of Things, 11, p.100212.

[17] Rachit, Bhatt, S. & Ragiri, P.R. Security trends in Internet of Things: a survey. SN Appl. Sci. 3, 121 ,2021, doi:10.1007/s42452-021-04156-9

[18] Sungjin, Y. and Park, Y., 2022. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions. IEEE Internet of Things Journal, 9(20), pp.20214-20228.

[19] Soni, M., Singh, D.K. LAKA: "Lightweight Authentication and Key Agreement Protocol for Internet of Things Based Wireless Body Area Network." Wireless PersCommun ,2021, doi:10.1007/s11277-021-08565-2

[20] Tariq, N., Qamar, A., Asim, M. and Khan, F.A., 2020. Blockchain and smart healthcare security: a survey. Procedia Computer Science, 175, pp.615-620.

[21] Mohanta, B.K., Jena, D., Satapathy, U. and Patnaik, S. ,2020, Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, p.100227

[22] Thilakarathne, N.N. ,2020, Security and privacy issues in iot environment. International Journal of Engineering and Management Research, 10.

[23] McGhin, T., Choo, K.K.R., Liu, C.Z. and He, D., 2019. Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, pp.62-75.

[24] Gan, C., Saini, A., Zhu, Q., Xiang, Y. and Zhang, Z., 2021. Blockchain-based access control scheme with incentive mechanism for eHealth systems: patient as supervisor. Multimedia Tools and Applications, 80, pp.30605-30621.

[25] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S. and Yang, Y. ,2020, A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR), 53(1), pp.1-32.

[26] Berdik, D., Otoum, S., Schmidt, N., Porter, D. and Jararweh, Y. ,2021, A survey on blockchain for information systems management and security. Information Processing & Management, 58(1), p.102397.

[27] Fu, J., Wang, N. and Cai, Y., 2020. Privacy-preserving in healthcare blockchain systems based on lightweight message sharing. Sensors, 20(7), p.1898.

[28] Nita, S.L. and Mihailescu, M.I., 2023. Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain. Sensors, 23(3), p.1371.

[29] Al Ahmed, M.T., Hashim, F., Hashim, S.J. and Abdullah, A., 2023. Authentication-Chains: Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks. Electronics, 12(4), p.867.

[30] Servati, M.R. and Safkhani, M., 2023. ECCbAS: An ECC based authentication scheme for healthcare IoT systems. Pervasive and Mobile Computing, p.101753.

[31] Taei, V. L., Guyon, L. Hasu, T. and Wouli, W. ,2022, A novel three-factor authentication protocol for multiple service providers in 6g-aided intelligent healthcare systems, IEEE Access, vol. 10, pp. 28975–2890, doi:10.1109/ACCESS.2022.3158756.

[32] Szymoniak, S. and Kesar, S., 2023. Key Agreement and Authentication Protocols in the Internet of Things: A Survey. Applied Sciences, 13(1), p.404.

[33] Mirsaraei, A.G., Barati, A. and Barati, H., 2022. A secure three-factor authentication scheme for IoT environments. *Journal of Parallel and Distributed Computing*, *169*, pp.87-105.

[34] Sahoo, S.S., Mohanty, S. and Majhi, B. ,2021, A secure three factor-based authentication scheme for health care systems using IoT enabled devices. Journal of Ambient Intelligence and Humanized Computing, 12(1), pp.1419-1434.

[35] Thakare, A., Fox, M. and Kim, Y.G. ,2021, Secure and Efficient Authentication Scheme in IoT Environments. Applied Sciences, 11(3), p.1260.

[36] Hu, B., Tang, W. and Xie, Q., 2022. A two-factor security authentication scheme for wireless sensor networks in IoT environments. *Neurocomputing*, *500*, pp.741-749.

[37] Nag, P., Chandrakar, P. and Chandrakar, K., 2023. An Improved Two-Factor Authentication Scheme for Healthcare System. *Procedia Computer Science*, *218*, pp.1079-1090.

[38] Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S.S. and Usman, M. ,2020, Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM Computing Surveys (CSUR), 53(6), pp.1-37.

[39] Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Zhang, Q. and Choo, K.K.R. ,2020, An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Transactions on Services Computing, 13(4), pp.625-638.

[40] Cui, Z., Fei, X.U.E., Zhang, S., Cai, X., Cao, Y., Zhang, W. and Chen, J. ,2020, A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 13(2), pp.241-251.

[41] Saqib, M., Jasra, B. and Moon, A.H., 2022. A lightweight three factor authentication framework for IoT based critical applications. Journal of King Saud University-Computer and Information Sciences, 34(9), pp.6925-6937.

[42] Mohanty, S.N., Ramya, K.C., Rani, S.S., Gupta, D., Shankar, K., Lakshmanaprabu, S.K. and Khanna, A. ,2020, An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. Future Generation Computer Systems, 102, pp.1027-1037.

[43] Satapathy, U., Mohanta, B.K., Panda, S.S., Sobhanayak, S. and Jena, D. ,2019, July. A secure framework for communication in internet of things application using hyperledger based blockchain. In 2019 10th international conference on computing, communication and networking technologies (ICCCNT) (pp. 1-7). IEEE.

[44] Abbasinezhad, D., Ostad-Sharif, A. and Nikooghadam, M. ,2020, Efficient provably-secure privacy-preserving signature-based key establishment protocol. Ad Hoc Networks, 100, p.102062.

Gholam Reza Zargar received his B.Sc. in Computer Hardware Engineering from Iran’s University of Science and Technology in 1991 and his M.Sc. in GIS (Geographic Information Systems) from Shahid Chamran University in 2008. He is received M.Sc. in ICT (Information Communication Technology in Communication Security) from the Iran’s University of Science and Technology. He has 15 years of work experience in Khozestan water & power autority Co. IT department (a subsidiary of Iranian ministry of energy). His main research area is in computer and network security.