NATURENGS
E-ISSN 2717-8013
https://dergipark.org.tr/en/pub/naturengs

BJWT-EHR: A novel JWT based Blockchain System for Electronic Health Records

Hamit Mızrak [a], Serpil Aslan [b] *, Muhammed Yıldırım [c]

[a] Malatya Turgut Ozal University, Department of Informatics, Malatya Türkiye – 44210
[b] Malatya Turgut Ozal University, Department of Software Engineering, Malatya Türkiye – 44210
[c] Malatya Turgut Ozal University, Department of Computer Engineering, Malatya Türkiye - 44210

*Corresponding author

ARTICLE INFO

Received	01.12.2023
Accepted	24.12.2023

Doi: 10.46572/naturengs.1398733

ABSTRACT

Since most transactions in the world now take place digitally, it is crucial to maintain data integrity, share data securely, and provide quick access to it. Our reliance on computers in our daily lives is growing, and new data will inevitably be generated to meet this need. Providing for safe data exchange is becoming increasingly crucial every day. Maintaining and safeguarding the security of this data is crucial. Recently, the term "block chain" has been used extensively for data security. A decentralized digital ledger called block chain is in charge of preserving data integrity and facilitating safe data sharing. Block chain transfers data by the principle of transparency, records data one way, and prevents reverse engineering. According to reports, block chain is the general term for the technology that promotes common data sharing of these recorded data and reduces access times, essential for preserving data security. There are several risks to patients' privacy when information from medical records is stolen or altered. The damage caused by malicious people with this information causes serious harm to both the patient and the financing institution. Therefore, cloud-based EHR (electronic health records) is becoming a focal point in many areas. Storing patient data, ensuring data accuracy, protecting data confidentiality, and ensuring fast data transmission in the cloud system is a significant concern in the healthcare industry. In this study, the layered architecture structure is also addressed in addition to the block chain for sharing health data with the help of cloud service providers while providing data access control and auditing for EHR records. To enter this layered architectural system, new solutions are proposed by applying JWT (JSON web token) and hashing function of patient information. This proposed method manages and controls the patient's health records electronically. Therefore, these technologies used in the block chain platform open new doors to more secure and sustainable solutions.

Keywords: Block chain, Electronic Health Record, Summary Function, Cloud Technology, Smart Contract, Database

1. Introduction

Recording and archiving data in paper form requires an extra workforce and may also cause data entry errors. Such errors lead to medical errors and can be costly as they cause repeat patient tests [1,2]. Patients may have to visit different hospitals during their treatment process. While patients distribute their health records to different hospitals throughout their lives, they may need help accessing their previous health records. It can also lead to poor management of fragmented health data records. Medical data must be digitalized and stored electronically [3]. Storing patients' medical information and obtaining it from unauthorized persons can cause serious harm to the patient and the hospital. Since the EHR is the environment where all information about the patient is kept, it must be stored securely. Nowadays, the health sector is stored in the computer environment compared to previous years. For example, electronic medical documents from magnetic resonance imaging (MRI) and X-rays to computed tomography (CT) and ultrasound scans can be carried on the cloud. With the increasing popularity of cloud services here, moving health records to cloud-based platforms makes sharing information between health and research institutions easier, allowing for faster and more efficient information exchange [4]. Cloud service providers are responsible for the control and flexible sharing of health records in their warehouses. While cloud-based systems that facilitate interactive collaboration have advantages such as researching and analyzing new information about treatments and better management of population health, it is noticed that they also bring various challenges. For example, storing high-dimensional data poses significant challenges for data management in the healthcare industry. Securing, remote access, and verifying health

* Corresponding author. e-mail address: serpil.aslan@ozal.edu.tr
ORCID : 0000-0001-8009-063X

records are significant challenges in the healthcare industry [5]. While overcoming these challenges, ensuring health records' integrity, reliability, and confidentiality is one of the main tasks [6]. For data owners and custodians, there is a risk that collected data may be vulnerable in the hands of malicious users. Such risks create an environment of distrust toward service providers. To overcome all obstacles, new recording systems are created that target efficient storage and fast data retrieval, secure data sharing, and the security of EHR records [7,8].

In modern societies, the creation of medical data, the emergence of new health techniques for treating diseases, and the application of these techniques to patients are a process of healing. Here, the importance of storing medical data in digital environments is increasing daily. Data sharing of big data, data security, ensuring that data is used only by relevant people, and preventing adverse risks become the duty of states. Serious investments are being made to reduce these risks. Block chain, a new technology field, is mentioned for storing this data, transporting the data securely, and entering and exiting the data into the system used to access classical data. Block chain is a digital ledger created with a distributed modeling system that is compatible with different technologies and is decentralized. To explain the block chain more comprehensively, they are public digital ledgers that record transactions on many computers designed to ensure secure data sharing and protect the integrity of decentralized data transactions, and which cannot be changed retroactively in any way later. The word block chain is named after the chain of transactions made in a network, block after block. The newly added chain is connected to the previous block, becoming a long chain. As a result, block chain is now spoken of as the name of record. When performing transactions on data in the block chain, each transaction is publicly recorded and controlled, thus providing higher accountability compared to other methods. No one can change all previously added information for each piece of data entered into the block chain. In other words, a new technology is mentioned that shows that the data is accurate and unchanged [9]. In block chain, data is stored in networks instead of a central database. In this way, the system's stability increases, and the damage it will suffer when attacked is minimized. Block chains are data with strategies that can solve serious data privacy, security, and integrity problems in healthcare. For example, in the healthcare sector, the confidentiality of patient records is recorded thanks to block chain technologies. Block chain technology offers a tremendous foundational network, decentralization, immutability, and interoperability for the healthcare industry. It works with many technologies and algorithms on the block chain. Cloud technology and hash function algorithms can be given as examples. Among these technologies, cloud technology provides fast, dynamic data sharing and data transmission. The hash function of the shares can be used to send data without allowing any changes to the raw data without the people's permission by using algorithms [10].

This study proposes JWT for sharing health data among cloud service providers while providing data access control and auditing for EHR records. In this proposed method, JWT, a new solution to the block chain, is aimed at transitioning to a more secure and centered application for system entry to ensure control of patient data.

2. Related Works

The block chain is a distributed architecture technology that does not have a central system and enables data sharing by becoming dynamic between end-to-end dependent users. Block chain ensures data sharing by adopting the principle of data security and transparency. Block chain is defined as a distributed database system. In his study, Begoyan [10] investigated the answer to the question of how classical data storage and data security can be made more secure on the cloud system of patient information [10]. For this purpose, the data is decentralized; each block chain lives on the server where it is located. Emphasis is placed on the safe transmission of data by carrying patient information on the cloud system and the speed and security of data in accessing this data.

Ying et al., [11] proposed the CP-ABE encryption technique for ciphertext policy attribute-based encryption using cryptographic techniques for EHR. The authors claim the proposed method protects EHR records against income and expense costs. Azarm et al. In their work, [12] proposed a cloud-based application and web service API to control the data shared in EHR systems to increase collaboration. The proposed framework has been tested using a comparative use case from the community perspective. The Ministry of Health controls the system to manage the hospitals or health centers with the EHR system. Yue et al. In their work, [13] proposed a single-center access control model for access control management for healthcare data sharing systems. The study divides data users into two types: (1) users trying to read raw data and (2) users trying to read data and get the results. The proposed model defines a limited time for data in a specific category for each data request, depending on the processing purposes. Samarin et al. In their study, [14] discussed health records that are privately stored in the cloud and can only be accessed by the patient. The study highlights the need to share health data with multiple organizations, such as healthcare providers. Xia et al. [15] proposed a block chain-based data-sharing model that addresses the access control challenges of EHR data stored in the cloud using the immutability feature of block chain. The proposed model aims to provide efficient access control and sharing of data pools with a permitted block chain using secure encryption techniques. Wang et al. In their study, [16] proposed a new scheme, which they called a secure BBDS, using attribute-based cryptography and block chain technology for EHR systems. The proposed model is a hybrid model. In the proposed model, while attribute-based encryption is used to encrypt medical data, a new cryptographic method called combined attribute-based/identity-based encryption and signature (C-AB/IB-ES) is introduced to apply digital signatures. In addition, block chain techniques were used in the study to ensure the integrity and accessibility of medical data. Ferdous et al. In their study, [17] proposed a new block chain-based system called DRAMs to ensure medical data integrity, reliability, and sharing. The proposed method is a decentralized architecture that enables distributed access control based on the assumption of a well-defined threat model. Ramani et al. [18] proposed a block chain-based collaboration scheme for EHR systems in their work. The proposed model is a secure and effective information access model based on doctor-patient block chain in a healthcare environment. The authors supported the proposed model with experimental results. Experimental results prove that the proposed model maintains integrity and can resist attacks known in the literature. Azaria et al. [19] proposed a decentralized MedRec model for large-scale EHR systems. In the study, confidentiality, authentication, and audits of medical data were kept through a comprehensive log using the MedRec model using the block chain technique.

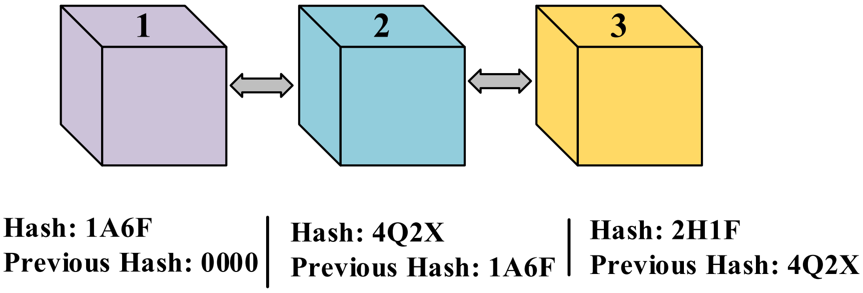

Figure 1. An example of a block chain structure

3. Backgrounds

3.1. Block chain

Block chain is called block chain because each data is added successively in blocks. The block chain function is a distributed architecture technology that does not have a central system and enables data sharing by becoming dynamic between end-to-end dependent users. Block chain ensures data sharing by adopting the principle of data security and transparency. The word block chain started to be used in 2008. The word Bitcoin, virtual currency, was used in 2009 [20]. It works by adding a new method block to the end of a chain, where the list of verified methods in the network continues. The figure shows the sequential ordering of data in blocks by chaining and encrypting them. A block chain visual is explained in Figure 1.

Block chain technology is of three types. These are public, private and consortium. Only authorized users can access the secret block chain system. Only authorized users can log in to the system in a private block chain. In this architecture, users can log in to the system with the user information given to them on the simple login screen. Each piece of information here is added to the block chain with the help of the API, and each added block is included in the block chain cycle. There are no entry restrictions in the public block chain. That is why it is called a private block chain. This type of chain works according to the principle of transparency and openness [21].

The architecture of block chain uses a variety of technologies. These are characteristics of hybrid keying, public, and private cryptography. There are benefits and drawbacks to each of these varieties. All cryptography does is conceal information from those who should not be. The data is encrypted when we use cryptography on data sent over a network. Only the sender and recipient's keys allow this encrypted data to communicate with one another. This data cannot be listened to by a third listener. For the transmitter and receiver to read this data, synchronous communication between the public and private keys is required.

3.2. Hashing Functions

Mathematical functions, known as hash functions, are designed to guarantee data integrity, consistency, and unique outputs. When using hash functions, the same value always yields the same result. For every set of data, it always generates a different set of values. In cryptography, hash functions play a crucial role. Data integrity and security in distributed systems and block chain are made possible by hash functions. One-way algorithms are what hash functions are (One Way Algorithms). Since it is one-way, the initial input cannot be accessed. Because hash functions are deterministic, every input yields the same result. One-way functions are used in hashing functions security applications, particularly in cryptocurrencies, to ensure data security by preventing reverse operations and guaranteeing security. Attacks using brute force cannot defeat hashing. Figure 2 displays the diagram of the hash algorithm. Bidirectional use is made of encryption algorithms.

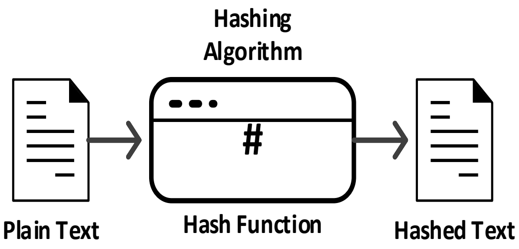

Figure 2. Diagram of hash algorithm

Hashing functions have different bit sizes, but each algorithm always gives the same output with the same input [22]. There are MD5, SHA, and RIPED-D types of hash function algorithms, and SHA is much more used due to the insecurity of the MD5 algorithm. MD5 is 128 bits long, and MD6 is 256 bits long. The SHA-256 hashing algorithm is used in the block chain. The hashing function enables the output data of different sizes in fixed size. It ensures data security in the block chain and always gets the same output. The hashing function ensures data integrity and reliability with the help of mathematical formulas. Figure 3 shows the hashing function algorithm usage in the block chain.

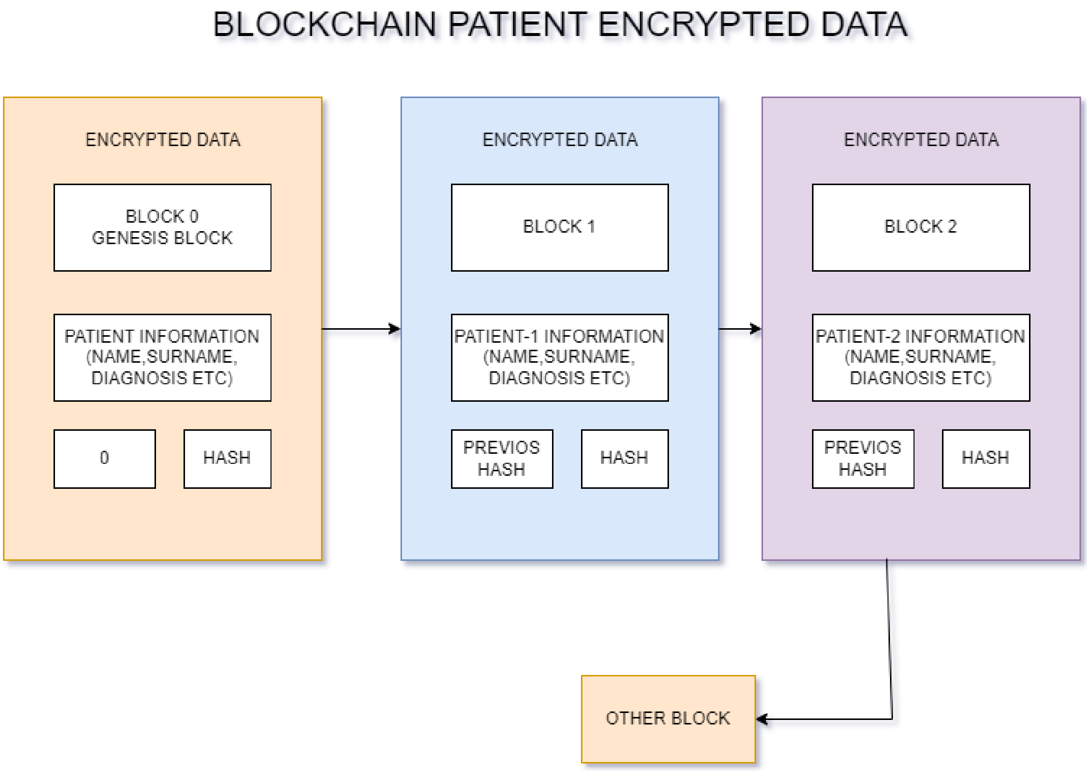

Figure 3. Use of hash function algorithm in block chain

3.3. Json Web Token (JWT)

JWT was prepared according to the RFC7519 industry standard [23]. It is used for authorization and identification in applications. The client makes a request. The server checks this incoming request, and if it returns a token it recognizes, it will log in to the system and return 200 as HTTP Status. If no such information exists in the system, it returns UnAuthorized, an unauthorized login warning, and 401 as HTTP status. In the JWT creation process, if there is no user in the system, he/she must be a member; if he/she is a member, the user logs into the system with the token given by the system. If the user's token expires, the system produces tokens again. Thus, the user can log in to the system. Figure 4 shows the JWT working mechanism. The JWT-generated token structure is encoded in base64 format and consists of 3 parts. It consists of header, data, and signature parts. The title is created in JSON format.

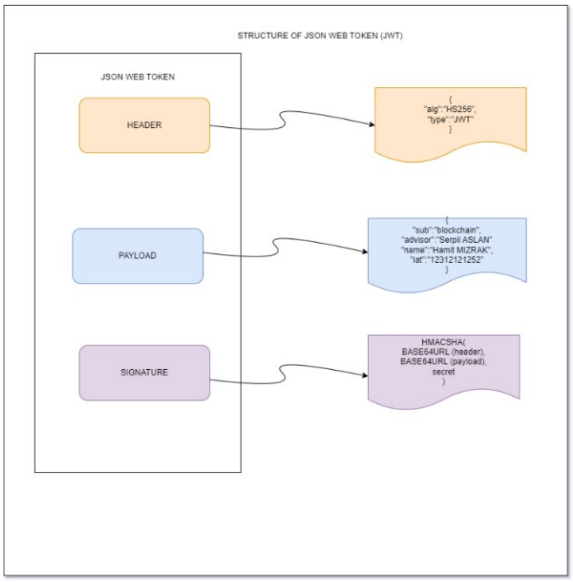

Figure 4. Structure of JWT

3.4. JavaEE and Spring Boot

Java is a high-level programming language. Java consists of three parts. The first part, JavaSE (Java Standard Edition), constitutes the essential components of JAVA. The second part, JavaME (Java Micro Edition), is used for embedded system coding of JAVA. The third part is JavaEE (Java et al.), the name of the technology used in corporate projects. In this article, Spring Boot technology, the latest technology in JavaEE, is used. Spring Boot technology is a configuration technology built on Spring Framework, and unlike Spring Framework, it provides coding convenience. The method proposed in the article used JavaSE for data structure systems. Spring Boot API (Application et al.) system was used to share data on different devices. API is a short application interface. It is the general name of the technology that enables data exchange between different devices. H2DB, an embedded database, was used as the database to record patient information. H2DB is an embedded database system that can run on the system. Spring Security was used for data security in Java. It filters malicious requests when they come to the system and blocks users who are not in the system.

It is a Spring-based application development platform that provides automatic configurations for corporate projects developed with the Spring Framework. It has components with a modular structure. Spring Data, Spring API, and Spring Security modules were used in the method proposed in this study. Lombok, Model Mapper, Gson, Swagger, Validation, and Actuator were used in third-party applications.

4. The Proposed Model

With the advancement of technology, progress has also been made in the field of health. Technologies are used for data security, data sharing and data transfer in healthcare services. Although using a cloud environment to transport data provides ease of data transfer, it also creates data security problems. Sharing data may cause the patient's personal information to be obtained by the wrong people. This situation may cause the patient's private information to be obtained by other people and have bad consequences. To avoid these risks, authorizing data access, sending data by encrypting it, and maintaining and storing the database are of vital importance [6].

Figure 5 shows the access and authorization status of data by authorized persons through the electronic system. Accessing system information without block chain is not said to be very secure. The proposed model in this study was coded using the Java programming language, which is a high-level and secure language. Spring framework, which is a Java framework, was preferred. Spring boot technologies, which are the file management of the Spring framework, spring data, spring API (Application Programming Interface), spring security, JWT, and H2 database, were preferred for the database. In this thesis, although block chain does not solve all the problems in the health field, solutions are proposed by focusing on the problems in areas such as data sharing speed, data access, and data security, which are essential problems.

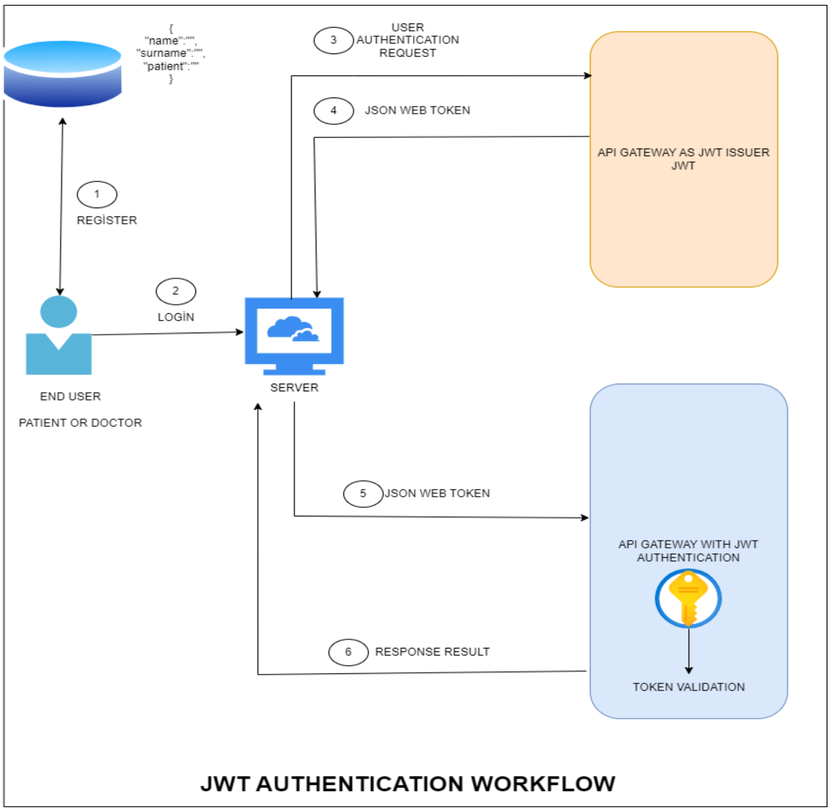

Figure 5. JWT Authentication Workflow for Health System

Before logging into the block chain automation system, some system registration and login procedures are carried out. For the doctor or patient to log in to the system, they must first register. After registering, they can log in to the system after approval is given by the hospital or system founder. A doctor logged into the hospital or the system founder can add patient information. Once the data is sent to the block chain, there is no change. Therefore, the data is added to the block chain after it is finalized. Patient information is added to the block chain in blocks within the hash function. There is a separate block chain for each patient. The block chain is broken if even one of these patients' information changes. After the patient logs into the system, his information is stored encrypted, and he can see his diagnostic information but cannot change the information. The block chain healthcare system visual is shown in Figure 6. The admin sees patient information added daily and can track it in the database or log file when changed. After adding the patient's diagnostic information, the doctor can send it to the block chain.

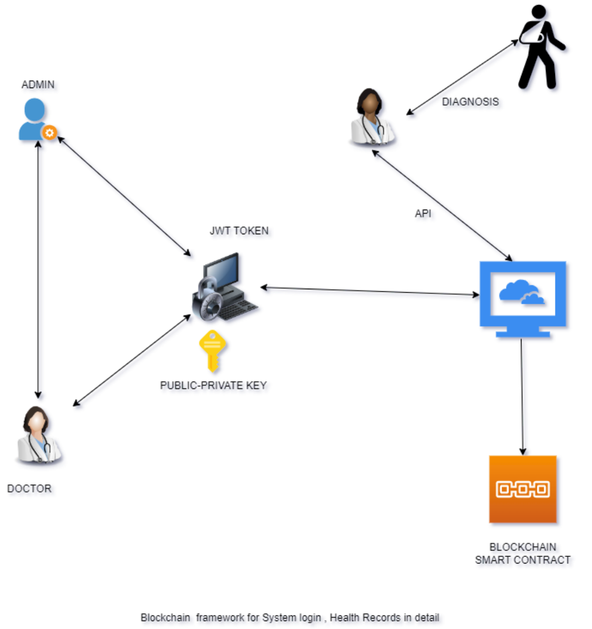

Figure 6. The proposed JWT based block chain system for EHR

Features and modules of the proposed BJWT-EHR Model:

- Using JWT HTTP to log in to the system rather than log in is more secure. Consequently, rather than querying the database for the information, it is preferable to enter the data into the system via JWT without requiring a login once the database has been logged in.
- Patient information is encrypted (masked) and stored in the database. The system is logged in using the application to access this data, which is integrated into the database system and application.properties structure.
- The Maven framework is used to eliminate library dependency. All errors that may occur in the system are stored in the log file. Lombok library is preferred to enable us to write less code in Java classes. Swagger library is used for API documents. Model mapper library is preferred for exchanging between Entity and dto classes.
- In the hospital module, individuals log in to the system via JWT with the previously given username and password information. It is the module where healthcare personnel working in the hospital are added to the system, and patient information is managed. The doctor or patient is responsible for activating the login rights granted to him/her when they enter incorrectly. It can access and print out doctor and patient information. It is responsible for adding the information of the healthcare worker who will leave the hospital to the system. It is possible to see all the information healthcare professionals add to the system.
- In the doctor module, individuals log in to the system via JWT with the previously given username and password. The module is responsible for recording patient information and diagnosis into the system. It can access patient information in the hospital. It can make changes before sending it to the block chain. Once it is recorded in the block chain, no changes can be made. Doctors' fast and secure access to patients' information plays a vital role in patient diagnosis.
- In the patient module, individuals log in to the system via JWT with the previously given username and password. This module is the module that will answer the information asked by the doctor. The patient can read his information but cannot change it.

5. Conclusions

With the proposed model, data transfer speed, data security, data transparency, and classical database storage in the health field, system user login database, instead of session method, JWT is more secure and less tiring on the database and the system. In addition to a data sharing model between cloud service providers using the block chain, providing secure login to the system and using access control mechanisms of smart contracts is an example of a better structure for data control. To provide a performance analysis of the system, its layered architecture with coding is compared with existing state-of-the-art solutions for data sharing between cloud service providers. It creates a model that will enable cloud service providers to exchange information faster, demonstrating a more stable and risk-free structure in data privacy. With the authorization in the system, importance is given to patient information privacy.

Acknowledgements

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

[1] **Raghupathi, W.,** and Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health information science and systems, 2, 1-10.

[2] **Krumholz, H. M.,** and Waldstreicher, J. (2016). The Yale Open Data Access (YODA) project--a mechanism for data sharing. The New England journal of medicine, 375(5), 403-405.

[3] **Taichman, D. B.,** Backus, J., Baethge, C., Bauchner, H., De Leeuw, P. W., Drazen, J. M., and Wu, S. (2016). Sharing clinical trial data: a proposal from the International Committee of Medical Journal Editors. Annals of internal medicine, 164(7), 505-506.

[4] **Longo, D. L.,** and Drazen, J. M. (2016). Data sharing. New England Journal of Medicine, 374(3), 276-277.

[5] **Fernandes, L. M.,** O'Connor, M., and Weaver, V. (2012). Big data, bigger outcomes. Journal of AHIMA, 83(10), 38-43.

[6] **Grozev, N.,** and Buyya, R. (2014). Inter-Cloud architectures and application brokering: taxonomy and survey. Software: Practice and Experience, 44(3), 369-390.

[7] **UNC** (2013) Healthcare relies on “Analytics to better manage medical data and improve patient care” IBM.

[8] **Burghard, C.** (2012). Big data and analytics key to accountable care success. IDC health insights, 1, 1-9.

[9] **Khezr, S.,** Moniruzzaman, M., Yassine, A., and Benlamri, R. (2019). Block chain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), 1736.

[10] **Begoyan, A.** (2007). An overview of interoperability standards for electronic health records. USA: society for design and process science.

[11] **Ying, Z.,** Wei, L., Li, Q., Liu, X., and Cui, J. (2018). A lightweight policy preserving EHR sharing scheme in the cloud. IEEE Access, 6, 53698-53708.

[12] **Azarm, M.,** Backman, C., Kuziemsky, C., & Peyton, L. (2017). Breaking the healthcare interoperability barrier by empowering and engaging actors in the healthcare system. Procedia computer science, 113, 326-333.

[13] **Yue, X.,** Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on block chain with novel privacy risk control. Journal of medical systems, 40, 1-8.

[14] **Fatokun, T.,** Nag, A., & Sharma, S. (2021). Towards a block chain assisted patient owned system for electronic health records. Electronics, 10(5), 580.

[15] **Xia, Q.,** Sifah, E. B., Smahi, A., Amofa, S., and Zhang, X. (2017). BBDS: Block chain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.

[16] **Wang, H.,** and Song, Y. (2018). Secure cloud-based EHR system using attribute-based cryptosystem and block chain. Journal of medical systems, 42(8), 152..

[17] **Ferdous, M. S.,** Margheri, A., Paci, F., Yang, M., and Sassone, V. (2017, June). Decentralised runtime monitoring for access control systems in cloud federations. In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (pp. 2632-2633). IEEE.

[18] **Ramani, V.,** Kumar, T., Bracken, A., Liyanage, M., and Ylianttila, M. (2018, December). Secure and efficient data accessibility in block chain based healthcare systems. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 206-212). IEEE.

[19] **Azaria, A.,** Ekblaw, A., Vieira, T., and Lippman, A. (2016, August). Medrec: Using block chain for medical data access and permission management. In 2016 2nd international conference on open and big data (OBD) (pp. 25-30). IEEE.

[20] **Kakavand**, H., Kost De Sevres, N., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. Available at SSRN 2849251.

[21] **Kasım, Ö.** (2020). Blok Zinciri Mimarisi ile Elektronik Tıp Kayıtlarının Modellenmesi Üzerine Bir Araştırma. Gumushane University Journal of Science, 10(1), 35-42.

[22] **Mizrak, H.,** and Aslan, S. (2023). Hastaların Elektronik Sağlık Kayıt (ESK) Sistemleri için Güvenli Blok Zincir Destekli Bulut Sistemi. Fırat University Journal of Engineering Sciences, 35(2), 517-526.

[23] **Jones, M.,** Bradley, J., and Sakimura, N. (2015). Json web token (jwt) (No. rfc7519).