UDC 004.056.53
DOI: 10.15587/1729-4061.2023.289325

ENHANCING HEALTHCARE DATA SECURITY: A TWO-STEP AUTHENTICATION SCHEME WITH CLOUD TECHNOLOGY AND BLOCKCHAIN

Olga Ussatova
PhD*
E-mail: olgaussatova@gmail.com
Shakirt Makilenov
Corresponding author
Master of Science in Engineering
Department of Information systems**
Arshidinova Mukaddas
Doctoral Candidate
Departament of IT**
Saule Amanzholova
Candidate of Technical Degree
Department of Cybersecurity
International Information Technology University
Manas str., 34/1, Almaty, Republic of Kazakhstan, 050040
Yenlik Begimbayeva
PhD
Department of Cybersecurity, Information Processing and Storage
Satbayev University
Satpaev str., 22a, Almaty, Republic of Kazakhstan, 050013
Nikita Ussatov
Student*
*Department of Information Security
Institute of Information and Computational Technologies
Shevchenko str., 28, Almaty, Republic of Kazakhstan, 050010
**Al-Farabi Kazakh National University
al-Farabi ave., 71, Almaty, Republic of Kazakhstan, 050040

In the modern world, medical data leakage has many external and internal threats. Information systems of medical organizations are constantly subject to various types of cyber-attacks and unauthorized penetration attempts, which leads to the publication of patient medical data online. Existing authentication schemes using blockchain technologies in medical organization systems ensure the integrity of medical data and secure access to patient data. However, one of the serious reasons for unauthorized access to the healthcare system is the human factor, which manifests itself in a negligent attitude towards account security, non-compliance with the rules and policies of information security, and transferring to third parties personal login details to the information system of a medical organization. This paper proposes a solution to this problem through an improved two-step authentication scheme using cloud technology and blockchain. The combined use of cloud technologies and blockchain is a distinctive feature of the proposed authentication scheme since it provides two levels of protection:

1) two-step authentication, the second stage of which includes biometrics through a mobile application. It prevents unauthorized access to the system by third parties;

2) cloud encryption keys for decrypting medical data, which are also accessed through the user's biometrics. The practical part of the paper includes the implementation of biometric login in Python using the OpenCV library. As a result of the practical part, unique fingerprint samples were obtained. The biometric user verification algorithm is designed for a mobile application, which we plan to implement in the future

Keywords: blockchain technology, two-step authentication, medical data security, fingerprint

Received date 20.09.2023
Accepted date 30.11.2023
Published date 28.12.2023

***How to Cite**: Ussatova, O., Makilenov, S., Mukaddas, A., Amanzholova, S., Begimbayeva, Y., Ussatov, N. (2023). Enhancing healthcare data security: a two-step authentication scheme with cloud technology and blockchain. Eastern-European Journal of Enterprise Technologies, 6 (2 (126)), 6–16. doi: https://doi.org/10.15587/1729-4061.2023.289325*

1. Introduction

One of the important tasks in the world community is to ensure information security in the field of information and communication technologies, and this is due to the increasing influence of global information technologies and data flows on most areas of activity of modern society, as well as the high pace of development of unified global information spaces. With the development of the Internet, a significant problem is the protection of transmitted data over communication channels. Many online threats require effective detection and data protection methods. Ensuring information security, tools, and methods for protecting against threats is a big problem worldwide.

The healthcare system is faced with insufficient organizational measures to protect information. Cybersecurity in healthcare has become a unique challenge because healthcare institutions use multiple networks and digital complexes with geographically distributed networks and heterogeneous infrastructure. The content of personal data and medical indications of the patient in information systems explains the attractiveness of medical institutions for cybercriminals. Attacks on medical data pose a significant risk to the security of the healthcare system, and there is a need for effective measures to protect data and prevent potential breaches.

Medical data leakage is both an external and internal threat. Most often, the causes of such incidents are imperfect work processes and information security policies of medical organizations, a weak layer of user identification in information systems, and the human factor, which manifests itself in negligent treatment of accounts and transfer of one 's login details to the healthcare system to third parties. As a result, unauthorized access to medical data by the patient and leakage of confidential information occur.

This paper uses blockchain technology to discuss a two-step authentication scheme for a medical information system. The solution proposed in this work can eliminate the human factor in the global problem of medical data leakage since the first and most important step in preventing this threat is the user authentication process, which serves as the primary means of protection [1].

Authentication is the process of confirming the identity of a user, device, or object in a computing environment. Identity verification is required to gain access to system resources very often. Positive verification is performed by comparing a certain identity attribute, such as a pre-established shared secret created when the person was allowed to use the system [2].

Multi-factor authentication (MFA) has become an important part of improving the security of sensitive information and implementing stronger access controls. MFA is a combination of at least two different components, each unique, that enhances the security of end users and enterprises by adding an extra layer of protection against many different forms of attacks that can be launched. An individual can be authenticated in three ways: through knowledge, possession, or inheritance. The knowledge factor refers to what a person must have in order to gain access. Password-based authentication is an extremely common method in which account holders are authenticated using a pre-shared value (password). The possession factor refers to a user's credentials for authentication based on items the user owns, typically hardware devices such as the user's phone or security token. In terms of inherent factors, the most common is the biometrics-based authentication method, which uses fingerprints, voice, or facial recognition to authenticate users. Because password-based authentication is still the dominant standard for online authentication and identity verification, it is more vulnerable to attacks using methods such as phishing. The secondary verification methods, such as fingerprints, iris scans, or other identifiers, used in conjunction with a password for verifying the user's identity, ensure that the user's critical credentials are protected and cannot be accessed by unauthorized parties [3].

However, despite the advanced authentication methods proposed in the current literature, existing authentication mechanisms based on centralized infrastructures are incompatible with distributed and decentralized structures and cannot protect against multiple attack vectors [4]. Distributed networks have changed how people and organizations interact with devices and things. Strong security measures and authentication mechanisms are required as different types of distributed applications are rapidly integrated into everyday activities. Thus, authentication mechanisms must secure hybrid and distributed networks to ensure that only authorized users can access the system and that sensitive credentials are stored in immutable and distributed ledgers [5].

Blockchain is a decentralized and distributed computing technology used to create traceable and static data records [6]. This technology was first used in Bitcoin and is now used in various fields. It is a network of nodes that maintain and update data records and link them using cryptography to form an immutable distributed ledger that guarantees the integrity and reliability of the data. Each block contains a unique hash value calculated from the data stored in the block. Every time a new block is added to the chain, the new block also contains the hash value of the previous block. Therefore, changing the contents of any previous block is impossible. Since the root hash value in this scheme is stored using tamper-proof blockchain technology, the root hash of each group can be stored on the blockchain and cannot be tampered with [7].

Blockchain-based authentication differs from centralized authentication, where a decentralized ledger can authenticate peers using a unique consensus algorithm. Sensitive user credentials are securely stored in registries and can be controlled by users after registration. Therefore, blockchain authentication must be carried out in several stages. First, organizations must register with the blockchain network to receive their cryptographic keys (public and private key pairs). Then, they create their authentication configuration (two-step) and credentials (passwords or biometrics), which will be mined and stored on the blockchain ledger. Second, if an entity wants to access a certain system, its credentials must be verified by the blockchain nodes before access can be granted to that entity by the system. Third, once the blockchain nodes have agreed on the provided credentials, the entity is granted access [3].

As the whole authentication scheme is complex and contains several crucial elements, it is essential to explore all of them, which is done in this research work.

2. Literature review and problem statement

In [8], the authors consider blockchain technology for creating a reliable decentralized authentication system. It is proposed to use a bioacoustic signal instead of traditional biometric characteristics used for the authentication procedure. However, the authentication scheme proposed by the authors has been tested in limited conditions and does not have industrial experience. In this study, there is no information about protection against the falsification of voice recordings and interchangeable methods in the event of voice distortion due to illness.

The paper [9] presents a blockchain-based Internet of Medical Things system and an anonymous authentication scheme integrated into it, called the group blind signature scheme. This authentication scheme is well suited for a distributed workflow, where users of the information system may be located in different medical institutions. But the anonymity of users, which can protect against quantum attacks and tracking of attackers, can interfere with the activities of internal control and audit services.

The paper [10] presents a simplified blockchain-based authentication scheme for sensor/actuator devices, users, and gateway nodes in medical cyber-physical systems. The proposed model ensures fast interaction between patients and the medical system. However, there are still unresolved issues regarding protection from unauthorized access due to the human factor. The reason for this may be the emphasis on sensory/actuator devices.

The paper [11] presents a data aggregation scheme based on blockchain technology for the medical environment. To implement remote medical monitoring, the authors developed a group authentication mechanism that allows multiple authorized users (such as the patient, physicians, caregivers, family, and friends) to have free access to the patient's personal medical records. Authorized group members agree on a group session key and use it to protect confidential patient information. But in case a new member joins the medical group or an old member leaves the medical group, the group session key needs to be updated. This scheme complicates the investigation process in the event of a data leak by one of the group's users.

The paper [12] presents medical implant consent, a non-embedded blockchain-based solution that provides authentication and authorization based on patient consent. The protocols developed by the authors allow doctors to obtain digital medical licenses, and patients to obtain and verify digital consent from patients. The results of the study are applicable in narrow medical areas and are not suitable for mass use due to the complex interaction pattern. This can lead to a significant decrease in the productivity of medical personnel.

The paper [13] presents a blockchain-based user authentication scheme that integrates with access control and physical non-cloning functionality. This design proposes the use of a trusted third party, which may not be provided in many healthcare infrastructures. In addition, the absence of a second stage of authentication cannot protect against unauthorized access due to human error.

The paper [14] presents a three-layer fog computing-based architecture, analytical model, mathematical framework, and advanced signature encryption (ASE) algorithm for identifying, verifying, and authenticating IoT medical devices. Similar to [13], this scheme also requires a trusted third party. And also, the proposed architecture does not provide protection against unauthorized access due to the human factor.

The paper [15] proposes a highly secure blockchain-enabled system for IoT medical devices using Lamport Merkle digital signature. This scheme provides a set of measures to protect medical data, and the authentication procedure of interest to us is performed during the generation of a digital signature. To generate keys, a certification authority is required, similar to [13, 14]. Using only digital signature keys cannot serve as protection against the human factor since, in this model, as in the previous two schemes, there is no biometric authentication method.

Despite the valuable contributions made by various studies in the field of blockchain-based authentication for medical data security, a general unresolved problem persists. The existing literature reveals local issues in each source, such as the untested nature of proposed authentication schemes, potential anonymity conflicts hindering internal control, and unresolved challenges related to unauthorized access due to the human factor. The identified local problems collectively contribute to a broader, overarching issue such as the absence of a comprehensive and industrially proven authentication mechanism that simultaneously addresses security concerns, human error, and scalability in the context of medical data. The aim of this study, therefore, is to bridge these gaps by developing and implementing advanced authentication mechanisms that integrate blockchain technology, a two-step authentication model, and a robust biometric authentication module based on fingerprints. Through this comprehensive approach, the study aims to contribute to the establishment of a secure and scalable framework for medical data protection, resolving the overarching problem identified in the existing literature.

3. The aim and objectives of the study

The aim of the study is to enhance the security of medical data through the development and implementation of advanced authentication mechanisms.

To achieve the aim, the following objectives are accomplished:

– to develop and analyze a two-step authentication model for the protection of medical data with the use of blockchain technology;

– to develop a mathematical model of biometric authentication;

– to develop a biometric authentication module based on fingerprints.

4. Materials and methods

4. 1. Object and hypothesis of the study

The object of the study is the enhancement of security measures in medical data systems, particularly focusing on mitigating the risks associated with unauthorized access and data leakage. The research delves into the vulnerabilities of existing authentication schemes in medical organizations, emphasizing the human factor as a significant contributor to security breaches. The study proposes an advanced two-step authentication scheme that integrates cloud technology and blockchain to fortify the security of patient medical data. The key components of the research object include the design and implementation of a robust authentication system with a specific emphasis on biometric verification through a mobile application.

The research hypothesizes that the integration of cloud technology and blockchain into a two-step authentication scheme can significantly enhance the security of medical data in healthcare information systems. The hypothesis posits that this integrated approach, involving biometrics through a mobile application and cloud encryption keys, will effectively address the human factor vulnerabilities. The two-step authentication is designed to prevent unauthorized access by incorporating biometric verification through a mobile app. Additionally, the use of cloud encryption keys, accessed through the user's biometrics, adds an extra layer of security for decrypting medical data. The practical implementation of a biometric login system using fingerprint recognition in Python with the OpenCV library serves as a validation of the proposed authentication scheme. The successful implementation of this scheme is expected to demonstrate improved security measures against unauthorized access to medical data in healthcare information systems.

4. 2. Research methodology

The analysis of authentication schemes based on blockchain technology in the medical field represents an important step in ensuring the security and reliability of the exchange of medical information [16]. Blockchain allows the creation of a decentralized and continuously updated registry in which the credentials of patients and medical professionals can be stored and verified [17]. This provides a high degree of protection against fraud and unauthorized access to medical information and increases data transparency and reliability. Thanks to blockchain technology, authentication schemes in the healthcare industry can be more efficient and resilient to external threats, improving healthcare quality and patient safety.

The analysis showed that, in most cases, blockchain-based authentication schemes are intended for medical personnel. Rarely, the subjects of blockchain-based authentication schemes are the patients themselves and their loved ones (Table 1).

If we touch upon the systems involved in the authentication scheme and the transmission and storage of medical data, we will notice that medical data is stored in the database of a medical organization while the blockchain is used to authenticate subjects of the system. A web application is most often used for data visualization, but mobile applications are also popular [18] (Table 1).

All the works reviewed use medical devices; in 4 out of 6 cases, they are Internet of Things. Smartphones are predominantly used to transmit data from medical devices (Table 1).

Thus, based on the analyzed data, it is possible to build a classic authentication scheme using blockchain technologies in the medical field (Fig. 1). The subjects of this scheme are patients and medical personnel. The information transfer process begins with the first stage, in which medical readings obtained from the patient's body sensor are transmitted to his smartphone [19]. The next stage, the second, is the transfer of this data via the Internet, where the information can be processed and prepared for further processing. The third stage is the transfer of medical data to the server of a medical organization. In the fourth stage, the server of the medical organization additionally ensures the safety of data by transferring it to the blockchain, which ensures reliable and unchangeable storage of medical information.

Access for medical personnel to this data is ensured at the fifth stage, where they enter a login and password for authentication. Then, at the sixth stage, the login and password are transmitted to the access control system, which interacts with the server of the medical organization, and then, at the eighth stage, makes a request to the blockchain to obtain the data. The ninth stage involves receiving a response from the medical organization's blockchain server; finally, medical data is transmitted to medical personnel in the tenth stage. This complex, multi-step process ensures a high level of security and confidentiality in medical information processing.

Table 1

Comparative analysis of authentication schemes

Publications	[7]	[8]	[9]	[10]	[11]	[12]
Users	Medical staff	Medical staff	Medical staff	Medical staff, patient, close and relatives of the patient	Medical staff	Medical staff, patient
Systems	Web application, DB, blockchain	Web application, mobile application, DB, blockchain	Web application, DB, blockchain	Web application, DB, blockchain	Mobile application, blockchain	Mobile application, DB, blockchain
Use the IoT	Yes	Yes	Yes	Yes	No	No
Use medical devices	Yes	Yes	Yes	Yes	Yes	Yes
Using a smartphone	No	Yes	Yes	Yes	Yes	Yes

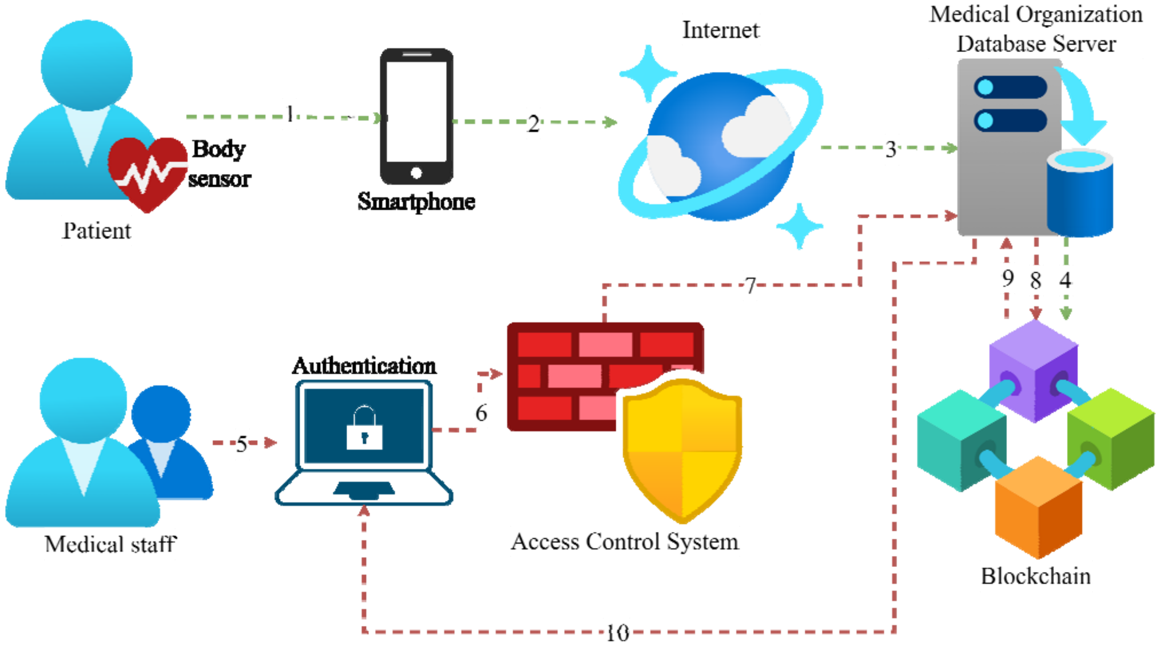

Fig. 1. Classic authentication scheme using blockchain technologies in the medical field

This approach to ensuring the security of patient data minimizes the risks of unauthorized access and ensures the integrity and reliability of medical information, which is important in modern medical practice. The introduction of blockchain technology into an access control system strengthens the level of trust in the digital exchange of medical data and promotes more efficient and secure interaction of medical personnel with information about patient conditions [20].

To study this circuit in more detail, it can be broken down into individual intermediate connections. A medical sensor (sensor) reads the patient's readings and then transmits them to a smartphone (usually via Bluetooth wireless technology) [21]. The mobile application establishes a secure connection in advance, so the medical sensor only needs to find a smartphone in the list of available devices and establish a wireless connection. After that, the sensor will ask for permission to transmit data, and if this device is not blocked in the settings, it will send a confirmation in response. Next, the procedure for transmitting the patient's readings via a secure channel to the smartphone is carried out [19] (Fig. 2).

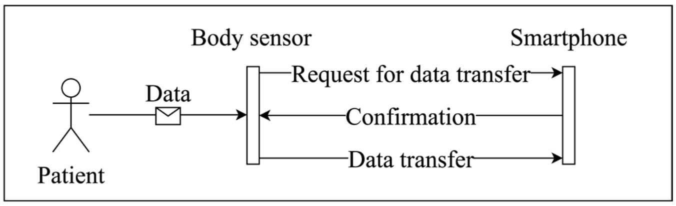

Fig. 2. Transferring patient medical information to a smartphone

The smartphone accumulates the patient's readings and prepares them for sending to the server. Here, the standard procedure for establishing a secure client-server connection via the Internet and transferring medical data to the database server of a medical organization takes place [22] (Fig. 3).

The entire medical database is usually not transferred to the blockchain. In some cases, partial transmission is observed, but more often, a link to the data on the database server and information about who has access to this data is transmitted. Thus, blockchain ensures the integrity and availability of patient medical data. Data transfer is carried out through a node or nodes, with the help of which a new block is created and added to the blockchain according to the established consensus algorithm (Fig. 4) [23].

Accumulating medical data is a one-way process. Gaining access to accumulated data is carried out in the form of a request and response. At the same time, in the first stage, the subject of the system (medical personnel) needs to undergo authentication, and then, when trying to obtain data, his role in the system will be verified with the access data in the blockchain. Only in case of full compliance with the role will the subject be provided with a link to medical data on the database server (Fig. 5).

This scheme for transmitting and storing medical data represents an important modern solution for ensuring the security and reliability of medical information processing and also represents a comprehensive process, starting with the collection of data from medical sensors on patients and ending with providing access to this data to medical personnel. This process is subject to detailed analysis, which reveals the continuity and structure of the stages, starting with sensors on the patient, passing through mobile devices and the Internet, and ending with integration into the blockchain and providing access to data. Researchers and medical organizations widely use this technique, as it provides a high level of security for the transmission and storage of medical data and also maintains the integrity of information and transparency of access.

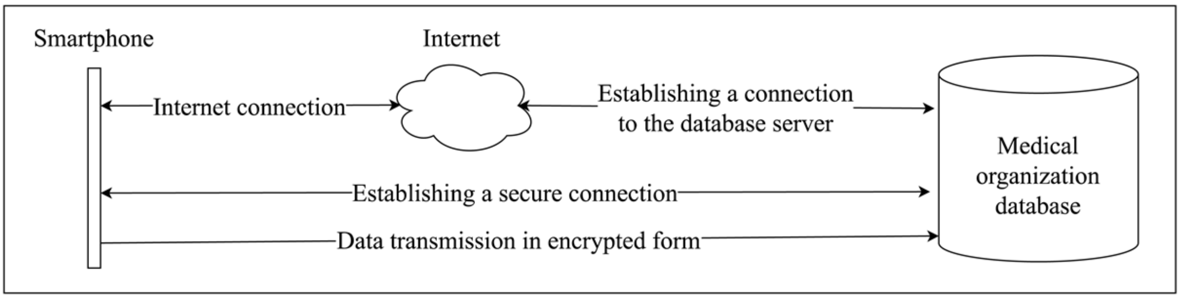
Smartphone
Internet
Internet connection
Establishing a connection to the database server
Medical organization database
Establishing a secure connection
Data transmission in encrypted form

Fig. 3. Transfer of medical data to the server of a medical organization

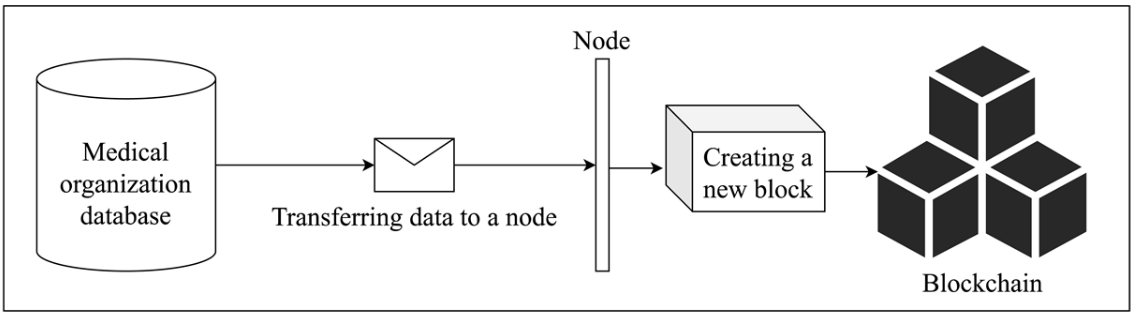

Fig. 4. Transferring data to the blockchain

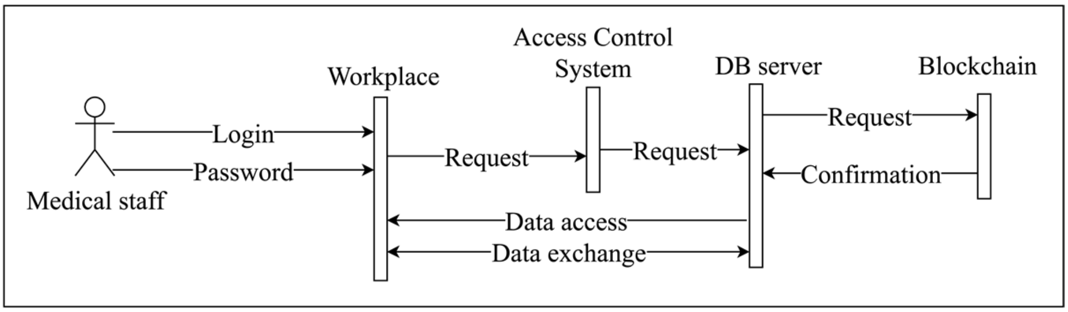

Fig. 5. Gaining access to patient medical data

The key point in this scheme is the use of blockchain technology to ensure the security and integrity of medical data. Blockchain ensures the immutability of records and control over access to this data [24]. The entire procedure is described using modern security standards and principles, making this diagram an important element of modern health information systems that help protect patient privacy and ensure quality care.

5. Results of the study on an improved two-step authentication scheme using blockchain technology in the medical field

5. 1. Development and analysis of a two-step authentication model for the protection of medical data with the use of blockchain technology

The presented classic authentication scheme using blockchain technologies in the medical field certainly has a high level of security. Nevertheless, there is a threat of unauthorized access to patients' medical data if an attacker takes possession of medical personnel logins and passwords [25]. In this case, the scheme in question will mistake the attacker for medical personnel and provide access to medical data. The reason for this is the human factor, along with the one-step authentication procedure. This paper does not consider the elimination of the risk associated with the human factor.

To conduct the study, a proposed conceptual solution will reduce the risks of unauthorized access by establishing two stages of authentication and using cloud digital signatures for cryptographic protection of medical data (Fig. 6).

A cloud electronic signature is a computing system through which the certificate owner, via the Internet, gains access to the processes of creating and confirming an electronic signature and using the key for the necessary purposes. User certificates are stored on a special device – HSM (Hardware Secure Module) [26].

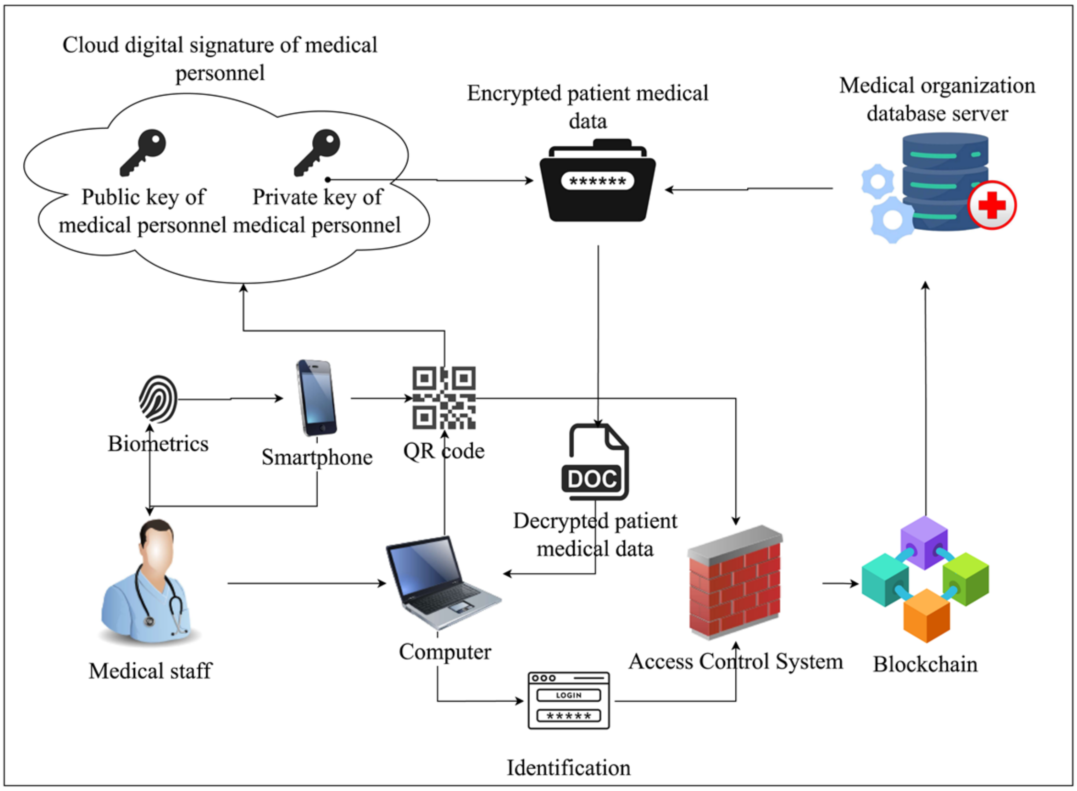
Cloud digital signature of medical personnel
Public key of medical personnel
Private key of medical personnel
Encrypted patient medical data
******
Medical organization database server
Biometrics
Smartphone
QR code
DOC
Decrypted patient medical data
Medical staff
Computer
Access Control System
Blockchain
LOGIN
*****
Identification

Fig. 6. A two-step authentication scheme using blockchain technology in the medical field

The presented model provides the double protection of medical data. The first level of protection is a two-step authentication [27]. This procedure involves the use of a smartphone by medical personnel to confirm their identities after standard authentication, where the user enters a login and password. If an attacker obtains the logins and passwords of medical personnel, the second stage of authentication will make it difficult to access medical data since successful authentication requires identity confirmation via a QR code in the mobile application. The access control system generates the QR code, and the mobile application identifies the user using biometrics [28].

The second level of protection involves encrypted storage of access links to medical data in the blockchain. In this case, an asymmetric encryption algorithm is used. At the same time, it should be noted that data is encrypted with a symmetric encryption algorithm and stored in the medical organization's database. Encryption and decryption of access links are carried out using private and public keys of cloud digital signatures [29, 30]. Medical personnel gain access to cloud storage when confirming their identity via a QR code in the mobile application. This eliminates the risk of unauthorized access to medical data if an attacker obtains access links illegally.

Thus, the two-step authentication scheme using blockchain technology ensures high medical data security by reducing the risks of unauthorized access and cryptographic protection of data access links in the medical organization's database.

In the proposed two-step authentication scheme with blockchain technology, biometric authentication is essential in the first step. Biometric systems have become widespread in image recognition based on fingerprints, significantly influencing the increase in systems' security level [31]. In this pilot study, fingerprint-based biometric authentication was carried out, as well as a comparison of images based on their level of proximity. This step is the first stage of the proposed scheme.

5. 2. Development of a mathematical model of biometric authentication

A mathematical model of biometric authentication based on an algorithm using fingerprint biometric data can be presented as follows:

Designation:

– F_S as a set of characteristics (features) of a fingerprint obtained from an image stored in a database;

– F_T as a set of characteristics (features) of a fingerprint obtained from the tested image;

– N_{match} as a good number of counties (obtained from the compare_features function);

– *Threshold* as a threshold value to improve authentication performance.

Mathematical model:

1. Preprocess function: Converts the fingerprint image into a unified format, making it suitable for subsequent processing. The mathematical model for this step can be represented as:

$$F_{img} = preporocess\left(I_{fp}\right), \quad (1)$$

where I_{fp} is the fingerprint image, F_{img} is the preprocessing result representing the characteristics of the image.

2. Extract_features: Extracts the main features of the switch fingerprint image. The mathematical model for this step can be represented as:

$$F_s = extract\_features\left(F_{img}\right), \quad (2)$$

where F_S is the extracted image features representing the features of the switch fingerprint in the database.

3. Compare_features: Compares the features of the fingerprint being tested with the stored data and determines the number of feature groups. The mathematical model for this step is:

$$N_{match} = compare\_features\left(F_T, F_S\right), \quad (3)$$

where N_{match} is the number of feature groups between the pointer fingerprint being tested and the data being stored.

4. Authentication Process: Uses the number of parliament representatives and a threshold value to determine whether authentication is successful. If N_{match}=*Threshold*, the authentication process is considered successful; otherwise, the authentication process is considered unsuccessful.

The mathematical model represents the steps of biometric fingerprint authentication using the functions of preprocessing, evidence detection, comparative evidence and threshold-based authentication process.

5. 3. Development of a biometric authentication module based on fingerprints

In the first stage, we create a fingerprint database using specialized devices (sensors) that read and save fingerprint images.

In the second stage, image preprocessing is performed. Fingerprints can have different resolutions, lighting, and other parameters. Before authentication, it is necessary to carry out a number of preprocessing operations:

– bringing the image to a standard size;

– improving image quality.

The third stage is feature extraction. After the image is preprocessed, the next step is to extract key features (minutiae) from it.

The fourth stage is a comparison of features. After the features are extracted from the image, they are compared with the features of the generated database.

The algorithm of the biometric fingerprint authentication module is presented in Fig. 7.

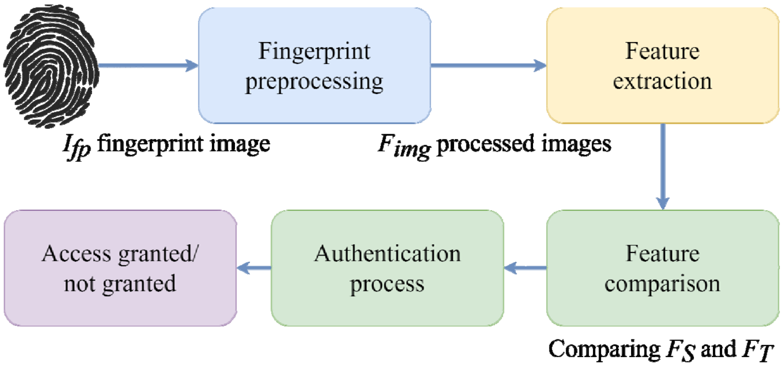
Fingerprint preprocessing
Feature extraction
I_{fp} fingerprint image
F_{img} processed images
Access granted/ not granted
Authentication process
Feature comparison
Comparing F_S and F_T

Fig. 7. Biometric authentication algorithm based on fingerprints

An example of implementation in Python using the OpenCV library [32]:

```
import cv2
import numpy as np
# Preprocessing
```

```
def preprocess(fingerprint_path):
        img=cv2.imread(fingerprint_path, cv2.IMREAD_GRAYSCALE)
        img=cv2.resize(img, (400, 400))
        img=cv2.threshold(img, 100, 255, cv2.THRESH_BINARY)
        return img
# Feature extraction
def extract_features(img):
        sift=cv2.SIFT_create()
        keypoints, descriptors=sift.detectAndCompute(img, None)
        return descriptors
# Comparison of features
def compare_features(test_features, stored_features):
        bf=cv2.BFMatcher()
        matches=bf.knnMatch(test_features, stored_features, k=2)
        good_matches=[m for m, n in matches if m.distance < 0.7 * n.distance]
        return len(good_matches)
# Usage
stored_img=preprocess("stored_fingerprint.jpg")
stored_features=extract_features(stored_img)
test_img=preprocess("test_fingerprint.jpg")
test_features=extract_features(test_img)
match_count=compare_features(test_features, stored_features)
threshold=50

if match_count > threshold:
        print("Authenticated successfully!")
else:
        print("Authentication failed!").
```

Fig. 8 shows fingerprints.

The results of the conducted study highlighted the remarkable uniqueness and viability of fingerprint patterns as a means of biometric authentication within mobile applications. The significance of the robust security measures cannot be overstated. The research showed that fingerprint patterns offer an unparalleled level of individual distinctiveness, making them a highly dependable and secure method for user authentication. It has important implications for healthcare, ensuring that only authorized individuals can access and manage their health information. Therefore, using fingerprint authentication represents an essential step forward in ensuring data integrity and privacy for users in health-related applications.

6. Discussion of the results of the study on an advanced two-step authentication scheme in healthcare

In this study, an advanced two-step authentication scheme was devised to counter unauthorized access to medical data, integrating biometric authentication, cloud digital signatures, access control systems, and blockchain technology. The first level involved personality identification using smartphones, while the second level focused on safeguarding encrypted links to medical data through an asymmetric encryption algorithm and blockchain. The potential effects of implementing this scheme extend beyond enhanced user experiences to a transformative impact on healthcare system users. They are empowered to autonomously manage the security of their medical data from their workplaces. With the incorporation of biometrics, cloud digital signatures, and blockchain, the scheme is poised to significantly reduce vulnerabilities to unauthorized access, providing users with a streamlined and secure authentication process.

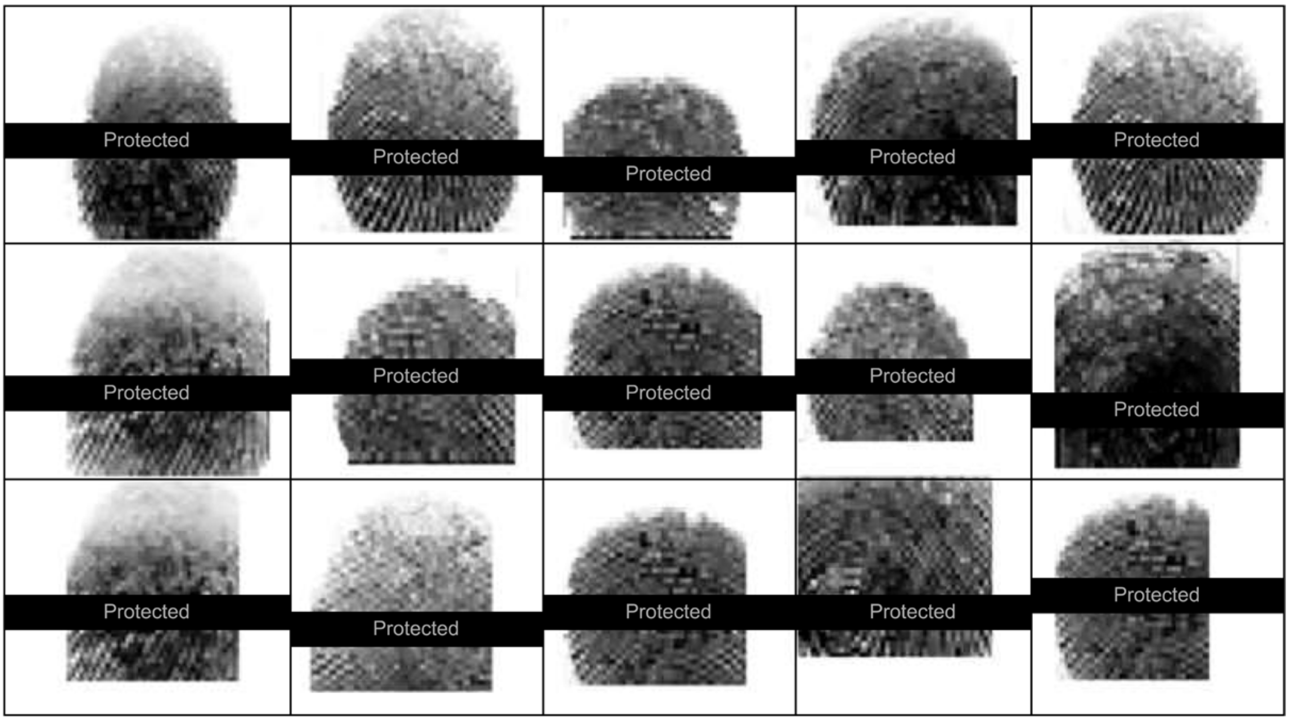

Fig. 8. Fingerprints

In the research outcomes regarding the improved two-step authentication scheme using blockchain technology in the medical field, the classic authentication scheme was critiqued for its vulnerability if an attacker acquires medical personnel logins and passwords. To address this, the proposed solution introduces a two-step authentication process and employs cloud digital signatures for cryptographic protection.

The model not only offers double protection through biometric authentication via smartphones and encrypted storage of access links in the blockchain but also emphasizes the need for robust security in healthcare data (Fig. 6). The mathematical model for biometric authentication, particularly based on fingerprint data, provides a standardized approach encompassing preprocessing (1), feature extraction (3), feature comparison (4), and an authentication process. This model enhances the reliability of the two-step authentication scheme by establishing a systematic and secure method for authenticating users based on unique fingerprint characteristics.

The development of a biometric authentication module based on fingerprints involves multiple stages, including creating a fingerprint database, image preprocessing, feature extraction, and feature comparison (Fig. 7). The demonstrated algorithm, implemented in Python using the OpenCV library, showcases the efficacy of fingerprint patterns as a secure means of user authentication. The results underscore the remarkable uniqueness and viability of fingerprint patterns, emphasizing their unparalleled level of individual distinctiveness (Fig. 8). This characteristic makes fingerprints a highly dependable and secure method for user authentication, particularly in healthcare applications. The research contributes to the foundation of a healthcare ecosystem where individuals confidently engage with their medical records, fostering increased user autonomy and data security.

The limitation of this study is related to the algorithms used to form public and private keys for encrypted medical data. How they will be formed and how all encryption and decryption mechanisms are implemented are still not completely defined. In addition, the mathematical model and its specifications, which are crucial in the authentication process, should be carefully observed. Nevertheless, there are some drawbacks connected with the insufficient database of fingerprints that create some barriers to further improving the accuracy of the authentication process.

Although the proposed scheme gives different advanced features for the protection of medical data, it uses a limited key formation method. Therefore, it is essential to build the proper methods of key formation when the authentication scheme is improved. Only a fingerprint recognition approach is utilized in the first step of the scheme's authentication mechanism, leaving other biometric ways away. In the future, other popular biometric authentication mechanisms can be realized. They include facial recognition, voice recognition, behavioral biometrics, and others.

The conducted practical experiments highlighted the importance of the proposed scheme and the significance of the robust measures for defining security patterns of fingerprint recognition. The programming code has been adapted to process the fingerprints rapidly and accurately. The code is adapted well for the task, but it is also necessary to improve it when new functionality features are added. This is important in the field of medical care as access to confidential data is well secured. Although the proposed authentication scheme is significant, there are still several steps that can be the development of the work:

– development of an access control system based on two-step authentication using a QR code;

– development of cloud storage of electronic keys of medical personnel to ensure the confidentiality of patient medical data;

– integrating an access control system with blockchain to ensure the integrity of stored medical data on the server.

7. Conclusions

1. The proposed solution is based on establishing two-step authentication and using cloud digital signatures to ensure the security of medical data in the context of blockchain technologies in the medical field. Two-step authentication, which requires identity verification via a QR code and the use of biometrics, effectively reduces the risk of unauthorized access, minimizing the vulnerability associated with the potential for attackers to obtain logins and passwords. In addition, the encrypted storage of access links in the blockchain, combined with a cloud digital signature, ensures cryptographic data protection and eliminates the risk of unauthorized access. These technological methods create double protection, ensuring a high level of security of medical data based on reducing the risks of unauthorized access and the use of cryptographic protection of data access channels in the medical organization's database.

2. The mathematical model of fingerprint-based biometric authentication provides a feature comparison method based on the number of good matches between the extracted stored and tested fingerprints. This allows the degree of similarity of biometric data to be determined, providing a practical approach to identity verification. Within the framework of this model, the problem of assessing the similarity of unique biometric characteristics of fingerprints using a threshold value is solved, which ensures the authentication process based on the quantitative interpretation of matching features and solves the problem of identity verification with high accuracy with the correct selection of the matching threshold.

3. The presented software code implements fingerprint-based biometric authentication using images to extract and match unique features. The results of this approach allow us to determine the success of authentication based on the threshold value of feature comparison. If the number of good matches between the stored and tested fingerprints exceeds the specified threshold, the message "Authenticated successfully!" is displayed. Otherwise, "Authentication failed!" is shown. This method provides efficient identity verification based on unique fingerprint biometric data.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship, or otherwise, that could affect the research and its results presented in this paper.

Financing

This research was carried out within the framework of the project AP19675957 "Research and development of a system for medical data protection using blockchain technology and artificial intelligence methods", which is being implemented at the Institute of Information and Computer Technologies.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors have used artificial intelligence technologies within acceptable limits to provide their own verified data, which is described in the research methodology section.

References

1. Jansen, W. (2003). Authenticating users on handheld devices. Canadian Information Technology Security Symposium, 1–12. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50736
2. O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91 (12), 2021–2040. doi: https://doi.org/10.1109/jproc.2003.819611
3. Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., Hussain, F. K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. Internet of Things, 23, 100844. doi: https://doi.org/10.1016/j.iot.2023.100844
4. Barkadehi, M. H., Nilashi, M., Ibrahim, O., Zakeri Fardi, A., Samad, S. (2018). Authentication systems: A literature review and classification. Telematics and Informatics, 35 (5), 1491–1511. doi: https://doi.org/10.1016/j.tele.2018.03.018
5. Addobea, A. A., Li, Q., Obiri, I. A., Hou, J. (2023). Secure multi-factor access control mechanism for pairing blockchains. Journal of Information Security and Applications, 74, 103477. doi: https://doi.org/10.1016/j.jisa.2023.103477
6. Al-Shareeda, M. A., Saare, M. A., Manickam, S. (2023). The blockchain internet of things: review, opportunities, challenges, and recommendations. Indonesian Journal of Electrical Engineering and Computer Science, 31 (3), 1673. doi: https://doi.org/10.11591/ijeecs.v31.i3.pp1673-1683
7. Zhou, B., Zhao, J., Chen, G., Yin, Y. (2023). Security Authentication Mechanism of Spatio-Temporal Big Data Based on Blockchain. Applied Sciences, 13 (11), 6641. doi: https://doi.org/10.3390/app13116641
8. Mohammed, Z. H., Chankaew, K., Vallabhuni, R. R., Sonawane, V. R., Ambala, S., S, M. (2023). Blockchain-enabled bioacoustics signal authentication for cloud-based electronic medical records. Measurement: Sensors, 26, 100706. doi: https://doi.org/10.1016/j.measen.2023.100706
9. Li, C., Jiang, B., Guo, Y., Xin, X. (2023). Efficient Group Blind Signature for Medical Data Anonymous Authentication in Blockchain-Enabled IoMT. Computers, Materials & Continua, 76 (1), 591–606. doi: https://doi.org/10.32604/cmc.2023.038129
10. Chen, F., Tang, Y., Cheng, X., Xie, D., Wang, T., Zhao, C. (2021). Blockchain-Based Efficient Device Authentication Protocol for Medical Cyber-Physical Systems. Security and Communication Networks, 2021, 1–13. doi: https://doi.org/10.1155/2021/5580939
11. Li, C.-T., Shih, D.-H., Wang, C.-C., Chen, C.-L., Lee, C.-C. (2020). A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System. IEEE Access, 8, 173904–173917. doi: https://doi.org/10.1109/access.2020.3025898
12. Gibson, A., Thamilarasu, G. (2020). Protect Your Pacemaker: Blockchain based Authentication and Consented Authorization for Implanted Medical Devices. Procedia Computer Science, 171, 847–856. doi: https://doi.org/10.1016/j.procs.2020.04.092
13. Shi, S., Luo, M., Wen, Y., Wang, L., He, D. (2022). A Blockchain-Based User Authentication Scheme with Access Control for Telehealth Systems. Security and Communication Networks, 2022, 1–18. doi: https://doi.org/10.1155/2022/6735003
14. Shukla, S., Thakur, S., Hussain, S., Breslin, J. G., Jameel, S. M. (2021). Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model. Internet of Things, 15, 100422. doi: https://doi.org/10.1016/j.iot.2021.100422
15. Alzubi, J. A. (2021). Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare. Computer Communications, 170, 200–208. doi: https://doi.org/10.1016/j.comcom.2021.02.002
16. Yazdinejad, A., Srivastava, G., Parizi, R. M., Dehghantanha, A., Choo, K.-K. R., Aledhari, M. (2020). Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. IEEE Journal of Biomedical and Health Informatics, 24 (8), 2146–2156. doi: https://doi.org/10.1109/jbhi.2020.2969648
17. Xiang, X., Wang, M., Fan, W. (2020). A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems. IEEE Access, 8, 171771–171783. doi: https://doi.org/10.1109/access.2020.3022429
18. Tao, Q., Liu, S., Zhang, J., Jiang, J., Jin, Z., Huang, Y. et al. (2023). Clinical applications of smart wearable sensors. IScience, 26 (9), 107485. doi: https://doi.org/10.1016/j.isci.2023.107485
19. Altay, A., Learney, R., Güder, F., Dincer, C. (2022). Sensors in blockchain. Trends in Biotechnology, 40 (2), 141–144. doi: https://doi.org/10.1016/j.tibtech.2021.04.011
20. Rouhani, S., Deters, R. (2019). Blockchain based access control systems: State of the art and challenges. IEEE/WIC/ACM International Conference on Web Intelligence. doi: https://doi.org/10.1145/3350546.3352561

21. Thapliyal, S., Wazid, M., Singh, D. P., Das, A. K., Shetty, S., Alqahtani, A. (2023). Design of Robust Blockchain-Envisioned Authenticated Key Management Mechanism for Smart Healthcare Applications. IEEE Access, 11, 93032–93047. doi: https://doi.org/10.1109/access.2023.3310264
22. Tanwar, S., Parekh, K., Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. doi: https://doi.org/10.1016/j.jisa.2019.102407
23. Aliya, B., Olga, U., Yenlik, B., Sogukpinar, I. (2023). Ensuring Information Security of Web Resources Based on Blockchain Technologies. International Journal of Advanced Computer Science and Applications, 14 (6). doi: https://doi.org/10.14569/ijacsa.2023.0140689
24. Basori, A. A., Ariffin, N. H. M. (2022). The adoption factors of two-factors authentication in blockchain technology for banking and financial institutions. Indonesian Journal of Electrical Engineering and Computer Science, 26 (3), 1758. doi: https://doi.org/10.11591/ijeecs.v26.i3.pp1758-1764
25. Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., Lymberopoulos, D. (2020). A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). Transactions on Emerging Telecommunications Technologies, 33 (6). doi: https://doi.org/10.1002/ett.4049
26. Gowda, N. C., Shaw, S. et al. (2023). Digital Signatures in Digital Communications: A Review. International Journal of Computational Learning & Intelligence, 2 (2), 76–86. doi: https://doi.org/10.5281/zenodo.7920995
27. Nysanbayeva, S., Wójcik, W., Ussatova, O. (2019). Algorithm for generating temporary password based on the two- factor authentication model. Przegląd Elektrotechniczny, 1 (5), 103–107. doi: https://doi.org/10.15199/48.2019.05.25
28. Indriyawati, H., Winarti, T., Vydia, V. (2021). Web-based document certification system with advanced encryption standard digital signature. Indonesian Journal of Electrical Engineering and Computer Science, 22 (1), 516. doi: https://doi.org/10.11591/ijeecs.v22.i1.pp516-521
29. Yenlik, B., Olga, U., Rustem, B., Saule, N. (2020). Development of an automated system model of information protection in the cross-border exchange. Cogent Engineering, 7 (1), 1724597. doi: https://doi.org/10.1080/23311916.2020.1724597
30. Mehbodniya, A., Webber, J. L., Neware, R., Arslan, F., Pamba, R. V., Shabaz, M. (2022). Modified Lamport Merkle Digital Signature blockchain framework for authentication of internet of things healthcare data. Expert Systems, 39 (10). doi: https://doi.org/10.1111/exsy.12978
31. Glover, J. D., Sudderick, Z. R., Shih, B. B.-J., Batho-Samblas, C., Charlton, L., Krause, A. L. et al. (2023). The developmental basis of fingerprint pattern formation and variation. Cell, 186 (5), 940-956.e20. doi: https://doi.org/10.1016/j.cell.2023.01.015
32. Sugadev, M., Sreekar, B. V. S. S., Velan, B. (2020). Development of open-CV framework for minutiae Extraction and matching of fingerprints. 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT). doi: https://doi.org/10.1109/icssit48917.2020.9214209