eHealthcare system data privacy concept based on Blockchain technology

Dejan B. Cizelj[a], *Tomislav* B. Unkašević[b], *Zoran* Đ. Banjac[c]

Institute VLATACOM, Belgrade, Republic of Serbia

[a] e-mail: dayantcizela@gmail.com,
ORCID iD: https://orcid.org/0009-0003-9785-2524

[b] e-mail: tomislav.unkasevic@vlatacom.com, **corresponding author**,
ORCID iD: https://orcid.org/0000-0002-6456-9250

[c] e-mail: zoran.banjac@vlatacom.com,
ORCID iD: https://orcid.org/0000-0001-8195-8576

DOI: 10.5937/vojtehg71-45589;https://doi.org/10.5937/vojtehg71-45589

FIELD: IT, cryptography, computer sciences
ARTICLE TYPE: original scientific paper

Abstract:

Introduction/purpose: Advances in information and communication technologies have enabled the creation of a symbiotic environment of humans and machines in which humans interact with machines to get better quality of everyday life. In that interaction, environment problems of information security and in particular data privacy are at the forefront. In many countries, there is legal regulation that regulates this problem in terms of securing the goals that must be realized when manipulating private data, and the technology itself is the choice of the creators of information systems. Blockchain technology is one of the methods of choice to ensure the integrity of data and undeniable transactions while digital certificates in conjunction with it enable the realization of data privacy of patients.

Methods: The cryptographic methods of asymmetric cryptography apply blockchain technology and reliable methods of identification in cyberspace, which enables the preservation of data privacy at a high level.

Results: This paper describes the method of patient health data privacy protection in a healthcare system based on digital certificates as an identification method in cyberspace and Blockchain technology as a method for preserving the integrity of transactions and a healthcare information system. The proposed concept enables the separation of private and medical data in such a way that with the accepted principle of patient ownership of medical data, it is possible to achieve primary and secondary use of healthcare data without compromising the patient's privacy.

Conclusions: The concept of identity assignment to every element in the healthcare information system and the organization/storage of data in ac-

cordance with the principles of Blockchain technology proposed in this paper enable the realization of a high level of data privacy in accordance with the European Union General Data Protection Regulation at the international level. In addition, the proposed concept enables the detection of unregistered devices or entities in the system and thus preserves the integrity of the system and increases its overall information security.

Key words: information security, healthcare IS, medical data, primary and secondary usage, asymmetric cryptography, digital signature, Blockchain organization, block structure.

Introduction

Blockchain technology is a mechanism designed to ensure the integrity of large data sets. This technology has experienced its full promotion and affirmation with the launch of the financial system Bitcoin, the first reliable decentralized digital currency in the electronic world. Bitcoin is essentially a digital value/money generation system that uses purpose-designed procedures and communication protocols to manage and exchange the created digital value, Bitcoin. It is important to understand that Bitcoins are digital data, not a physical entity. The developed Bitcoin generation and exchange protocols are based on asymmetric cryptographic systems to ensure the reliability of transactions, their immutability and integrity. The application of electronic signatures and hash functions ensures the reliability of creating Bitcoin and transactions that make payments and exchanges of Bitcoin. Transactions change the ownership of Bitcoin from one entity to another. In this virtual cash transaction, control mechanisms based on electronic signatures and verification of the possession of appropriate private cryptographic keys enable the correct realization of transactions and exchange of values. Defined control mechanisms also prevent the spending of nonexistent money or the multiple use of existing money (double spending). The rules on establishing a consensus regarding the correctness of transactions and the ways of their realization establish mutual trust of individual Bitcoin owners. The basics of the Bitcoin system were first described in the paper (Nakamoto, 2008) in 2008. Bitcoin is the first virtual digital currency system to successfully solve the problem of double spending and establishing trust in a network of mutually distrustful entities.

The model of functioning of the financial system is not unique in everyday life. In the abstract sense, it can be applied to any system in which entities interact with each other and there is no a priori confidence in the correct behaviour, accuracy of the data presented, their integrity during the transaction and later in time. With the advent of Bitcoin and the blockchain technology described in it, for the first time, there was technology that provides a satisfactory solution to this type of problem. This is particularly important for environments where accuracy, consistency, integrity and transparency must be achieved while preserving the privacy of the data of transaction participants.

In this way, by ensuring the integrity and credibility of the data, blockchain technology has enabled the automation of many life and business processes and thus permeates everyday life and the entire reality. In addition to initial applications in finance (Hines, 2020; Smith, 2020; Lee & Deng, 2018), blockchain technology is massively applied in surveillance and management systems based on complex systems of devices with various processing capabilities such as the Internet of Things (Balamurugan et al., 2023; Kumar et al., 2022) and Smart cities (Kumar et al., 2022). In this context, the possibilities of applying blockchain technology in healthcare information systems are particularly emphasized (Shoniregun et al., 2010; Bhushan et al., 2022, 2023). The dominant examples of the application of blockchain technology in information systems of this type relate to:

- Protecting patients' privacy and managing their healthcare data, using various identification, authentication and authorization techniques in patients' private data management procedures (personal identification data, medical data, etc.) in blockchain technology are included in a certain way to ensure the credibility and integrity of the data to the process of its sharing and storage.
- Monitoring supply chains for medical devices and pharmaceutical products has a significant role in healthcare systems. Counterfeiting products and their origin (medical devices and pharmaceuticals) has a significant prevalence in the world. In addition to the consequences of the use of uncertified devices and drugs in the treatment of people and the consequences for their health, financial losses of companies in the healthcare industry are also significant. Therefore, concepts and labeling systems of medical devices and pharmaceutical products have been developed and data on them is stored in appropriate blockchain structures. Each entity in the supply chain can verify

the origin and credibility of each individual product, see for example (Stawicki, 2023).

- For clinical research, it is very important that the data obtained during the research is credible, that during the research data is collected in accordance with current legislation and that the data is stored in such a way that it cannot be changed and its integrity can always be verified. Blockchain technology is enabling these challenges to be overcome and is widely applied in this segment. Some of possible approaches can be seen in (Stawicki, 2023).

Protecting and managing patients' privacy and their data is one of the key challenges in healthcare information systems. This paper presents a concept for solving this problem based on the synergistic application of digital certificate and blockchain technology.

Blockchain technology

The diversity and disparity of terminology in the field of digital currencies makes Blockchain technology equate the digital currency Bitcoin. That is not quite right. Bitcoin technology is more complex and contains Blockchain technology as one of its building blocks. Also, Blockchain technology in the academic literature is defined and described in different ways. For our approach, the most suitable definition is the one based on the Data Structure Theory which defined a blockchain as a linked list of data blocks. Copies of a blockchain list are stored on different computers and the number of copies is not limited. Synchronization between the data contents of list copies and data integrity is realized by execution proprietary designed protocols for blockchain blocks management. Blockchain blocks management assumes rules for new block construction and their registration in the blockchain list. Block construction and management rules are based on cryptographic methods dedicated for data integrity preserving and consequently have the property that the registration of an unverified data block in the blockchain list is an intractable task. Every attempt to falsify the blockchain list by entering an unverified block is easily detectable by applied mechanisms. A high level of data integrity protection in blockchains is achieved by a specific application of hash functions and the cryptographic method of digital signature for digital data.

Such a powerful integrity protection mechanism has experienced its full promotion in data distribution systems in unsafe peer-to-peer (P2P) networks, but a complete solution had to go a few more steps further:

- How to construct a decentralized mechanism for confirming the accuracy of the data included in the candidate block for registration in the blockchain list such that mutually distrustful members of the network have a high degree of confidence in its correctness.
- How to ensure synchronization of blockchain lists stored in different places/devices and the consistent use of data.

Solving these two problems opens the door for the construction of a reliable decentralized system, regarding the correctness and integrity of data blocks, for storing data. Nowadays, decentralized data management provides autonomy for data owners/users and independence from third parties. One of the reasons that speaks in favour of decentralized organization of data and their use lies in the fact that this increases the reliability of the functioning of the system because the cessation of work of one blockchain list holder does not prevent others from participating in business processes that include a blockchain list. In the case of centralized storage, the situation is exactly the opposite. The integrity, decentralization and public availability of a blockchain list are the key characteristics of the immutability of a blockchain list.

These properties are due to the application of the cryptographic mechanisms in Blockchain technology and therefore we will briefly describe the cryptographic mechanisms Blockchain technology is based on.

Blockchain technology and cryptographic mechanisms

In this section, we will briefly describe the cryptographic mechanisms on which Blockchain technology and its power rest. A detailed overview of cryptographic mechanisms, their characteristics and theoretical explanations can be found in (Menezes et al., 1997; Zheng, 2022; Zheng et al., 2023). Additional information and explanation regarding the application of cryptographic techniques in identification and authentication can be found in (Todorov, 2007; Boonkrong, 2021) and (Mamdouh et al., 2021).

Cryptographic hash functions

Informally speaking, hash functions are a class of functions that map data of an arbitrary length in essence to data of a fixed length in bits. The hash function is usually denoted by H, a given data by m and its hash value is denoted by h_m,

$$H(m) = h_m.$$

Interest in this class of functions was expressed in the late 1960s and early 1970s in the context of large data set searches, see (Knuth, 1998), and later found widespread use in cryptology in which numerous researchers dealt with their nature and properties. For cryptology, hash functions which have the following properties are of particular importance:

- For a given value h, it is computationally intractable to find a value, some $H(m) = h$.
- For a given value m_1, it is computationally intractable to find the value m_2 so that $H(m_1) = H(m_2)$.
- It is computationally intractable to find two values m_1, m_2 so that $H(m_1) = H(m_2)$.

The standardized hash functions are, for example, SHA256, SHA2 and SHA3.

Cryptographic transformations

Cryptography deals with the problem of protecting the transmission of messages between two parties in communication, let us call them Alice and Bob, so that the information they exchange is available only to them and to no one else. This is achieved by corresponding message transformations called cryptographic algorithms and the parameters on which the transformation depends are the message being protected, m, and the cryptographic key or keys if there are more than one. The process of transformation by which a message is prepared for sending through a communication channel is called encryption and the result of that transformation is data called a cipher text. The fact that the cipher text that we denote with c is obtained by the transformation of the message m using the cryptographic algorithm E and the cryptographic key k_1 is denoted by

$$E_{k_1}(m) = c.$$

The transformation by which the receiving side is transforming a message c, the cipher text, into its original form by applying the cryptographic key k_2 is called decryption and it is denoted with D

$$D_{k_2}(c) = m.$$

When a $k_1 = k_2$, a cryptographic system is called symmetric and when it is $k_1 \neq k_2$, a system is called asymmetric. A graphical representation of a symmetric cryptographic transformation is shown in Figure 1 and a graphical asymmetric cryptographic transformation is shown in Figure 2.

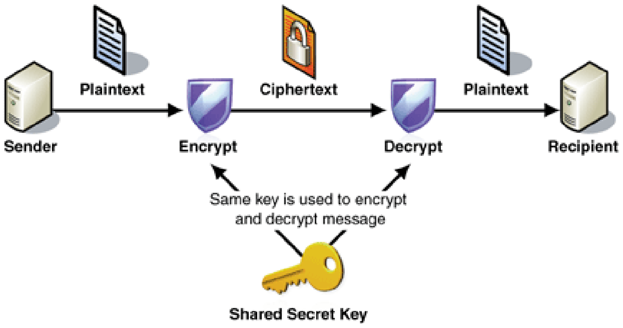


Figure 1 – Symmetric cryptographic transformation
Рис. 1 – Симметричное криптографическое преобразование
Слика 1 – Симетрична криптографска трансформација

Asymmetric cryptographic algorithms

Asymmetric cryptographic algorithms were first described in the work of Diffi and Hellman in 1976 (Diffie & Hellman, 1976) and have revolutionized the cryptographic world. Before the seminal paper of Diffie and Hellman in order to protect the message, the sender and the recipient must securely exchange the cryptographic key they intend to use, otherwise anyone who is able to access their key can find out the contents of the exchanged message. As a consequence, it is not easy to organize the distribution and management of cryptographic keys in symmetric cryptographic systems and especially if the communication networks in which they are applied consist of a large number of participants.

In the case of asymmetric cryptographic algorithms, the encryption and decryption keys are different and the encryption key is usually denoted with p and the decryption key with d. For such systems, the following facts are characteristic:

- When only the encryption key is known, it is not possible to reconstruct the decryption key, and vice versa, and
- Although the decryption key is known, it is not possible to reconstruct the encryption key.

This has brought new possibilities to the cryptographic world.

Let us show this giving one example.

Let Alice want to send Bob a protected message by applying an asymmetric cryptographic algorithm with the encryption and decryption functions E, D, respectively. The procedure proceeds as follows, Figure 2:

- For a given system, Bob constructs his encryption key p_B and the decryption key d_B in the prescribed way.
- On some public directory, Bob publishes his encryption key p_B.
- Alice takes over p_B from the public directory and constructs a cipher c for her message m as
$$c = E_{p_B}(m)$$
- Bob gets c and by applying the deciphering operation D and the key d_b gets
$$m = D_{d_B}(c)$$

Due to the fact that the encryption key can be made publicly known, the name public key is still used in the literature and, for the purpose of keeping the communication secret, the decryption key must be kept secret and therefore it is called a secret or private key.

The security of communication stems from the fact that on the basis of the knowledge of the public key it is not possible to obtain a secret key and decrypt the cipher.

Asymmetric cryptographic algorithms are based on difficult-to-solve mathematical problems:

- The problem of factorization of natural numbers, and
- The problem of discrete logarithms in finite groups.

With this in mind, it follows that asymmetric algorithms by the degree of security they provide fall into the class of practically secure cryptographic

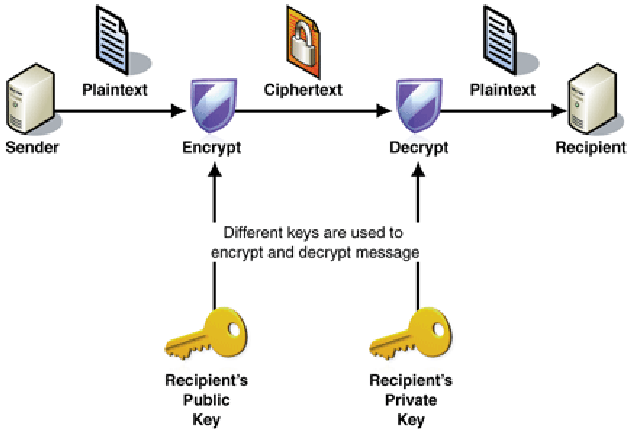


Figure 2 – Asymmetric cryptographic transformation
Рис. 2 – Асимметричное криптографическое преобразование
Слика 2 – Асиметрична криптографска трансформација

algorithms. The methods to compromise them are known, but it is not possible to provide the required resources for the successful execution of these algorithms (Galbraith, 2012).

In today's practice, the most common ones are asymmetric cryptographic algorithms RSA, El Gamal, and Diffie-Hellman as well as the algorithms derived from the arithmetic of points on elliptical curves.

Electronic signature

In addition to advances in the solution for distribution of cryptographic keys, asymmetric algorithms have enabled the definition of the identity of objects involved in transactions in the electronic world as well as verifying the origin and integrity of data involved in transactions. In this way, it is possible to unambiguously identify interactions and their participants in the electronic world.

Declaring the origin of electronic data/documents is carried out by the data/document electronic signature procedure and the verification of the integrity and origin of the document by the verification of the electronic signature procedure. These procedures are based on appropriate asymmetric cryptographic algorithms. Let us call the actors of this process Alice and Bob. Alice has a pair of asymmetric keys appropriate for the electronic signature generation and the verification procedures (p_A, d_A) and wants to send Bob a message m but so that Bob can be sure, upon receipt, that the message was sent by Alice and that the message on the transmission path has not been changed. Alice creates a digital signature for the message m using the procedure for creating an electronic signature

$$Sign\left(m, d_A\right) = sig\left(m\right)$$

and she sends Bob a message $\left(m, sig\left(m\right), p_A\right)$. Bob conducts an electronic signature check for the message he received,

$$Verify\left(m, sig\left(m\right), p_A\right)$$

and if he gets the result that the verification is successful, he knows that the message comes from Alice because it is verified by her public key, the electronic signature verification key, and that the message has not been changed on the transmission path. Bob's belief regarding the origin and integrity of the received message rests on the mathematical fact that the probability of successful verification of an electronic signature created by a certain private key is infinitely small if an inadequate public key is used. The consequence of this fact is that the electronic signature algorithm and its corresponding key pair, in this case, represent a unique set of data and can serve to create Alice's identity in the electronic world. Alice proves her identity to Bob by verifying her electronic signature for the agreed document. This is the basic principle, but there are still many technical details whose considerations are not the subject of this text.

Electronic signature algorithms can be constructed in different ways, to use entire messages or just their hash values. Today, algorithms standardized in (Chen et al., 2023) are most commonly used in practice. The graphical representation of the creation of the electronic signature and its verification is given in Figure 3.

Creation of the Blockchain list

Conceptually, Blockchain is, as we previously stated, a linked list and as such has its beginning, a generic block (the Genesis block), and some number of blocks between the Genesis and the last block added to the list. Each block has a predefined structure.

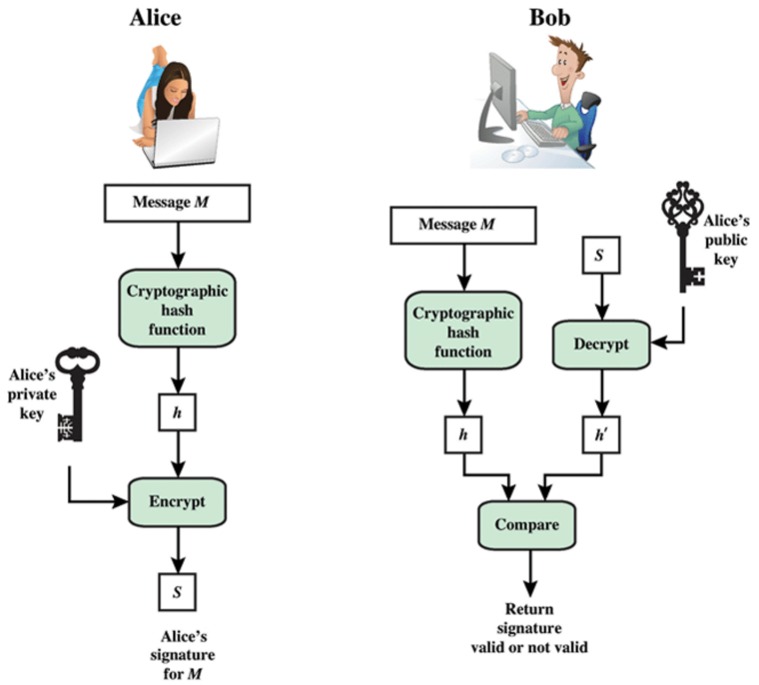


Figure 3 – Generation and verification of the digital signature procedure
Рис. 3 − Процедура генерации и проверки ЭЦП
Слика 3 – Генерисање и провера дигиталног потписа

Block structure

A graphical representation of Blockchain and its block structure is shown in Figure 4.

At the abstract level, every block has two clearly separated parts. The transaction part consists of the digital representation of the transactions between the community members, data are named transactions and each one is electronically signed by the data holder. The block header part consists of the following fields:

- Merkle hash is data calculated over the entire dataset that a block carries but constructed in a specific way that enables fast checking whether or not a piece of data is contained in the transaction part of the block. The details of the construction of Merkle hash value for a single block and its properties can be seen in more detail in (Summers, 2022). One of the key features is that even minimal changes in the

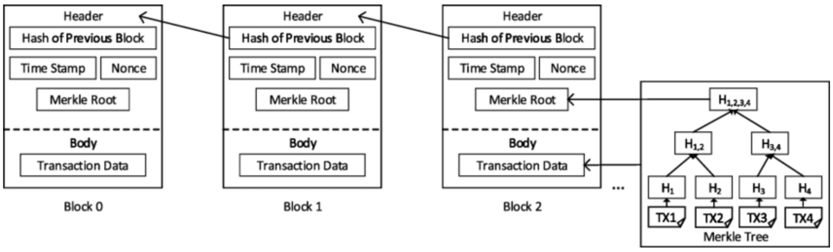


Figure 4 – Blockchain and the block structure, (Liang, 2019)
Рис. 4 – Блокчейн и блочная структура, (Liang, 2019)
Слика 4 – Блокчејн и структура блока, (Liang, 2019)

data result in the newly constructed Merkle hash not matching the previous one, the one that corresponds to the data before the change, and this is evidence of a violation of data integrity within the block.

- Immediate predecessor block header is processed by the defined hash function and the calculated value is entered in the appropriate data field. That value represents the control data for the immediate predecessor block data integrity.
- A timestamp is a data evidence for the block existence in the quoted time that is electronically signed by the time stamp authority.
- The weight-factor, defined in the system, is a random time variant value. It is used for the decision whether the candidate block for registering in the block chain is formed in an appropriate way. Namely, if the block hash value is below the weight-factor value, the block is well formatted and qualified for entering the blockchain. In the opposite case, the registration of the block is rejected.

Creating qualified block for entry in the blockchain list

The data involved in the formation of blocks and transactions may be different in its nature. For the purpose of this description, we will consider that there is a single data source from which to form blocks and pool of transactions, and, eventually, upon a successful procedure, to register a block in a blockchain list.

The pool of transactions is accessible by all entities in the community. Entities that want to try to form a block for registering in the blockchain create the block candidate are usually called miners. The protocol proceeds as follows:

1. The miner selects some number of transactions from the transaction pool and includes them in the transaction part of the block. After that, the miner computes the Merkle hash of the selected transactions, obtains a timestamp as evidence about the time of construction and fills in the timestamp field.
2. From the last block in the blockchain, the miner computes its hash value and fills in the computed value in the Hash Value of Previous Block field.
3. The miner fills in the weight factor field by the current system weight-factor value.
4. Using some random number generator, the miner obtains some value and writes it into a field labelled Nonce.
5. After that, using the defined hash function and the candidate block header, the miner computes the hash value. In the case that the calculated value is lower than the current system weight factor, the miner successfully constructs the eligible block and broadcasts it for verification. In the opposite case, he/she goes back to step 4.

Upon new block candidate broadcasting, the recognition of its novelty procedure for its admission to the blockchain starts by the members of the blockchain community. The community members conduct the eligibility verification procedure as follows:

1. First, the verifier checks whether the Hash Value of Previous Block field contains the hash value of the last block registered in the blockchain. By this check, the verifier prevents incorrect copies of blockchain usage. The negative result assumes that the candidate is rejected for registration.
2. After that, the verifier checks the existence of each individual transaction from the block transaction part in the transaction pool. The absence of any of the selected transactions assumes the rejection of the candidate for registration in the blockchain.
3. The Merkle hash value for the transaction part is calculated by the verifier and compared with the Merkle hash field in the block candidate. If the values are equal, the verification continues; otherwise, the block candidate is rejected.

4. At this stage, the verifier uses a defined hash function over the block candidate header data to obtain the hash value. The obtained value is compared with the system weight factor at the time written in the timestamp field. If the computed value is lower than the appropriate system value, the check is positive; if it is not, the check is negative. If the check is negative, the candidate is discarded.
5. In the case that all checks are fulfilled, the validation of the candidate is successful, the block is entered and registered into the blockchain and the transactions from the transaction part of the block are deleted from the transaction pool.

In the previously described procedure, the criterion for the block candidate eligibility is that its hash value is lower than the current system weight factor. This criterion is the evidence of the effort made by the miner to find a convenient nonce to achieve the declared relation regarding the system defined weight factor, and it is named Proof-of-Work. In digital currency systems, miners obtain financial benefits for successfully created blocks. For different applications of Blockchain technology, various mechanisms are applied to create credible blocks, see (Summers, 2022).

Security of electronic health systems

The turbulent development of technology in the last few decades has led to tremendous advances in the field of Information and Communication Technologies and the possibility of interactive communication between humans and machines. This created a symbiotic community of humans and machines called cyberspace. The new technological environment has brought the possibility of automating many life and business processes and has significantly changed everyday life. One of the areas of everyday life and work that has undergone a significant change by applying technological capabilities is the health care system.

By creating complex information systems connected with various medical devices and means of monitoring the condition of patients, mobile and stationary, and networking of all actors in systemic processes has led to a major change in the way of operation, protocols and treatment. The consequence of these changes is a significant improvement in the quality of services and their results while reducing costs and increasing efficiency. But like any new technology, this one, in addition to its great benefits, also brings significant challenges, especially in the field of managing patients' medical data and preserving their privacy.

Essentially, these problems have their origin in the technology itself and represent the translation of the existing security challenges into a real existing living environment.

Security challenges in information systems

The security of information systems is a complex and extensive issue (Stamp, 2011). Basically, on an abstract level, the challenges that information systems security addresses can be roughly classified into three groups:

- Ensuring the confidentiality of data relating to data protection in such a way that its content is available only to those entities for which it is intended. This applies to all processes of manipulation, processing and transfer of data.
- Ensuring the integrity of the system and data. This includes the ability to detect unauthorized changes to the architecture and structure of the system in relation to the defined structure of the system, when it comes to the system itself, or to detect unauthorized changes in data in relation to its initial correct content.
- Ensuring undeniability for activities in the system. This implies that for each action in the system, it can be unambiguously determined which entity performed it as well as when and what exactly was done.

The previously described information security challenges in the literature are known as the CIA Information Security Triad.

If one looks closely at the requirements of the CIA triad, it is easy to see that for their realization it is necessary that the entities that make up the system, whether passively providing specific functionality or having an active role in it, must be identifiable in a unique way. In other words, each of them must be assigned a unique identity within the system - electronic identity.

Electronic identity

From the very beginning of the development of computer systems, there was a need to distinguish users who use the system by their identification.

Over time, techniques for identifying users in information systems were developed so that today they can be classified into one of three groups. User identification is based on:

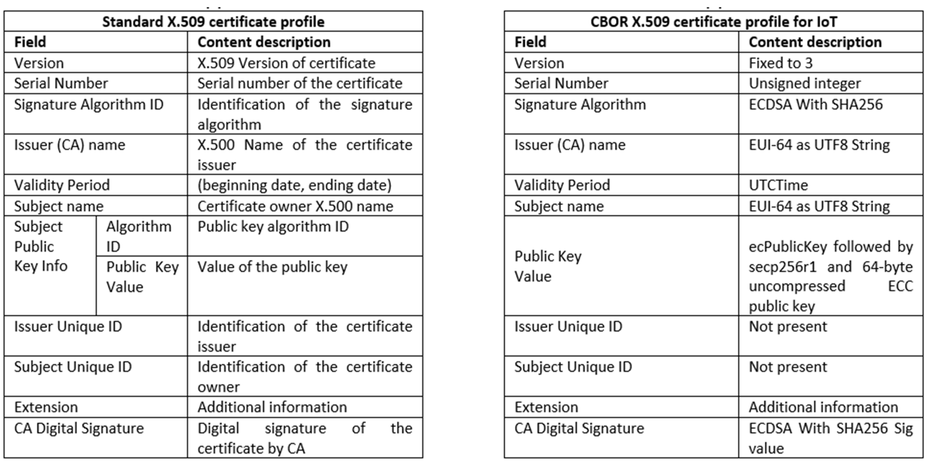
- What the user knows (username and password, etc.)
- What the user owns (electronic certificate, etc.)
- What the user is (fingerprint, iris, other biometric data, etc.)

With the advent of asymmetric cryptography (Diffie & Hellman, 1976), conditions were created for the formation of a system for the unique identification of objects in the digital world through digital certificates and the public key infrastructure (PKI), (Buchmann et al., 2013; Vacca, 2004). The identity of each object is determined by a pair of cryptographic keys, a public one and a secret one, for a chosen asymmetric cryptographic algorithm. The nature of the facility (people, devices, software) and its associated public key within the existing public key infrastructure generates a digital certificate associated with that object. A specific body, the registration authority, within the given PKI infrastructure guarantees for the accuracy of the information included in the digital certificate and, in the case that the application for the issuance of the certificate is correct, forwards it to the competent authority for issuing digital certificates, the Certification Body. A certification body creates a digital certificate for the entity that has requested the issuance of the certificate and guarantees the accuracy of the information contained therein by its digital signature. The architecture, mode of operation and guarantees regarding the issued digital certificates of the certification body are given in the documents of the certification policy, practical rules of operation and internal rules of operation. In order to achieve interoperability in the application of digital certificates as expressions of digital identity, their format and content are standardized through the document of the International Telecommunication Union and the World Organization for Standardization ITU-T X.509, ISO / IEC 9594-8, (Cooper et al., 2008). The main characteristics of certificates generated in accordance with X509 Standard are:

- By their structure, they can be very complex due to recursive definitions in the standard and the analysis of the correctness of the structure and content can be resource demandable.

- Their size, expressed in bytes, is about two kilobytes, in average, which can cause problems while working in resource-limited environments.

For the purpose of creating and using electronic identity in resource-limited environments, Lightweight X.509 Digital Certificates Standard has been created (Forsby et al., 2018) that goes beyond the above-mentioned features and enables the application of digital certificates as methods of identification in resource-limited environments. In Figure 5, the structure and the content of both certificate profiles are presented.



Standard X.509 certificate profile		
Field		**Content description**
Version		X.509 Version of certificate
Serial Number		Serial number of the certificate
Signature Algorithm ID		Identification of the signature algorithm
Issuer (CA) name		X.500 Name of the certificate issuer
Validity Period		(beginning date, ending date)
Subject name		Certificate owner X.500 name
Subject Public Key Info	Algorithm ID	Public key algorithm ID
	Public Key Value	Value of the public key
Issuer Unique ID		Identification of the certificate issuer
Subject Unique ID		Identification of the certificate owner
Extension		Additional information
CA Digital Signature		Digital signature of the certificate by CA

CBOR X.509 certificate profile for IoT	
Field	**Content description**
Version	Fixed to 3
Serial Number	Unsigned integer
Signature Algorithm	ECDSA With SHA256
Issuer (CA) name	EUI-64 as UTF8 String
Validity Period	UTCTime
Subject name	EUI-64 as UTF8 String
Public Key Value	ecPublicKey followed by secp256r1 and 64-byte uncompressed ECC public key
Issuer Unique ID	Not present
Subject Unique ID	Not present
Extension	Additional information
CA Digital Signature	ECDSA With SHA256 Sig value

Figure 5 – X.509 certificate profiles
Рис. 5 − Профили сертификатов X.509
Слика 5 – Профили сертификата X.509

e-Healthcare information security

Health information systems by their nature are very complex in architecture due to heterogeneity of devices that make them up and their functionality. The information security of such systems includes many different aspects of which in this section we will consider the security of medical data.

The introduction of information and communication technologies in health systems resulted in the creation of e-Healthcare systems. They are by their nature network-oriented in the sense that they provide the creation and rapid exchange of health information in order to increase the quality and efficiency of medical services and treatment results. At the heart of any such system there is medical data of patients which can be, by its nature, multimedia, text, image and sound. The user's acceptance of such systems depends largely on patients' confidence in the protection of privacy, integrity and undeniability in the management of their medical data (Singh & Zhou, 2022; Murphy, 2015). Medical data of patients is collected and used by a number of medical professionals from the health care system. This use can be classified as:

1. Primary – when this data is used in the treatment of patients.
2. Secondary – when this data is used for other purposes; for example, for medical research purposes, medical and pharmaceutical statistics, various business and economic records.

The nature of the right to use medical data has changed over time and today it is accepted that the owner of the medical data is the patient from whom the data was collected and that any use of that data, which in terms of scope and content includes the ability to recognize the patient's real identity, requires his explicit consent, (Singh & Zhou, 2022). Therefore, many legislations pay close attention to protecting patient privacy through various legal solutions, e.g. the General Data Protection Rule (GDPR) in the European Union or the Data Privacy Protection Act in the Republic of Serbia.

e-Healthcare data privacy concept based on Blockchain technology

As we mentioned earlier, the security of information systems rests on the ability to know, for every activity undertaken in the system, who and when did it, and this applies to each entity in the system (people, devices, software). Regarding medical information in this system, the basic unit is the electronic health record (EHR) (Shoniregun et al., 2010). The data contained in the EHR is primarily used for medical procedures of the patient to whom the data belong and secondary for medical research needs, medical and pharmaceutical statistics, various business, administrative and economic needs. The need for a strict control of access to the identity of the patient to whom the medical data belongs further emphasizes the requirements for strong and reliable security mechanisms in such systems especially in the management of this data. In order to implement appropriate identification and authorization techniques, it is necessary to establish unambiguous and reliable identification mechanisms.

Identification of entities in the system

In many countries, the transition towards a digitalized society is being implemented and legal solutions define the identification of persons in the electronic world for administrative and business purposes. Consequently, in health insurance, it is customary for persons to be joined by qualified electronic certificates in accordance with X.509v3 Standard which confirms the link between personal and electronic identity. The personal certificate is issued in accordance with the legislation governing this area.

It is common for users to have a smart card in the health insurance system that serves for personal identification in the system, an electronic health-care patient identification document (eHPID). In addition to a digital certificate whose public key represents the electronic identity of the patient, a personal health number (LZB) is also assigned to serve as an identification element in health procedures. The relationship between the public key contained in the electronic certificate and the LZB is such that it is in no way possible to obtain another from one piece of data; for example, an LZB is generated in a random way. Public key pairs and LZBs are kept in a cryptographically protected form in databases with restrictive access rights. The access to this database is possible only with the explicit consent of the patient, which can be expressed by providing the ePHID for inspection and typing the PIN to access this data.

Professional members of the e-Healthcare system possess identification smart cards - the employee electronic healthcare identification card (eEHID).

Issued digital certificates are placed on these identification cards (eHID, ePHID).

For devices, digital certificates are issued in accordance with the Lightweight X.509 Digital Certificates description that is compatible with X509v3 Standard.

Procedure of medical examination, generation and preservation of results

In order to present the security concept of an electronic health system based on blockchain technology and the PKI infrastructure, we will use a simplified scenario of medical examination, creation of medical data and records in the system:

1. Upon arrival at the doctor's office, the patient is identified with the system with his ePHID card and the doctor is identified with his eHID card.
2. If the system does not recognize the patient or the doctor as legitimate entities, the health system issues a report containing the reason for not holding the examination and generates a report that is recorded in the blockchain system records.
3. If the system recognizes both the patient and the doctor as legitimate entities in the health care system, the doctor is allowed to create a new medical report with a system-generated identification ordinal number in which the patient's identity is represented by an LBZ number. The doctor writes in the report anamnesis, ailments, diagnosis and conclusion about medical treatment. The electronic form of the report is digitally signed by the doctor and the system places it in the blockchain for medical reports.
4. If the diagnostic process ended at this level, the physician prescribes the necessary therapy and medications, and the system determines the prescription identification number and forms an electronic form of the prescription that the doctor electronically signs. According to the electronic signature of the prescription, it is placed in the prescription blockchain.
5. If the process of medical care of the patient requires additional examinations or medical interventions, the doctor generates a request with the necessary medical data to which the system assigns an identification number and whose electronic form is digitally signed. The request generated in this way is placed in the blockchain for medical instructions.
6. Each request for additional healthcare examinations is individually digitally signed by the issuing doctor and constitutes a unit medical transaction.

7. The identification numbers of prescriptions, instructions and medical procedures are written into the blockchain, which represents the patient's healthcare history. This blockchain has unique numerical identification and connection with patient's identity and this identification is stored in a specially protecting database.

The described concept of creation and storage of electronic healthcare reports and their usage makes medical data separate from the data on the identity of the patient. The actual identity of the patient can only be obtained by knowing the identification parameter of the user's medical data, which is not feasible because this data is stored in the register of users of the health system, which is a highly protected database with restrictive access policy. A graphical representation of the system is given in Figure 6.

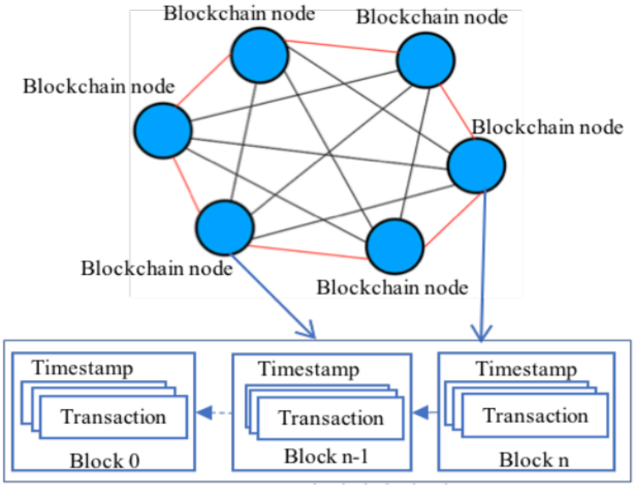


Figure 6 – Graphical presentation of the system structure, (Salman et al., 2019)
Рис. 6 – Графическое изображение структуры системы (Salman et al., 2019)
Слика 6 – Графички приказ структуре система(Salman et al., 2019)

Security analysis

The processes of digital transformation of society and the transition of life processes towards cyberspace inevitably highlight the issues of information security and the preservation of privacy of personal data. Unauthorized access to any individual's personal data can have serious adverse consequences for him or her. The damages can be personal, psychological, business, material and social. By identity theft and access to health data, an individual can be subjected to damage in terms of obtaining employment, premiums of insurance companies and bank loans, and the like. These examples show the importance of preserving the privacy of medical data for an individual in each community.

As we have previously stated, the first and basic element of security is the establishment of a reliable identification system in the electronic health insurance system.

In the proposed concept, each entity that makes up the system (people, devices) has a defined electronic identity in the form of a digital certificate. Digital certificates for persons are issued in the form of a qualified digital certificate in accordance with the legislation of the community in which the system operates. Digital certificates for devices are issued in the Lightweight X.509 Digital Certificates format, which is compatible with X509 Standard and which allows installation on devices with very limited processing resources. This reliable method of identification enables reliable tracking of events in the system and prevents any activities that are inconsistent with the role assigned to the system by the entity. This enables efficient and up-to-date monitoring of the functioning of the system, which brings as an additional benefit the reliability of the functioning of the system as a whole. Additionally, identifying each individual entity in the system makes it possible to verify the integrity of the system and disable access to the system to devices that are not logged as its elements.

The main activity in the health system, including the eHealthcare system, is data collection, its analysis, use and preservation. The system must be designed and implemented in such a way as to enable relatively easy primary and secondary use of this data in accordance with legal regulations. The mechanisms for managing this data must be such as to protect the privacy of the data.

In the proposed concept, this goal is achieved by separating the patient's identification data and his/her medical data. The patient's identification data is stored in a highly secured database with strictly defined and restricted access rights. As identification data in this database, the identification number of the blockchain containing the patient's medical data is stored. The medical data block contains identifiers of the patient's medical procedures and through them a connection among the patient's physical identity and medical data is established. In this way, the separation of identity and content of medical data is achieved.

The primary use of patient data requires access to a secure database to identify a blockchain containing the identifiers of medical procedures and their results for a given patient. This approach requires the patient's explicit consent and can be realized, for example, by physically using an ePHID card and entering a PIN value that testifies that the patient has willingly used the card to access medical data. Regarding to its content, electronic medical data does not contain any references to the identity of the patient, but the connection is established through their randomized numerical identifiers. In this way, the anonymity of the patient is achieved in relation to the content of medical reports.

The integrity of medical data is guaranteed by the electronic signature of the initiator of the medical procedure or the implementer of the procedure and the creator of the results. This guarantees the integrity and immutability of the data at the time of its creation. The integrity and credibility of data over time is guaranteed by storing it in a way that is provided by blockchain technology.

Relationship of the proposed solution concept with some other solutions

Blockchain technology has strongly supported the transformation of healthcare businesses towards paperless business and the cyber world. As in all business and life processes in cyberspace, information security is essential in this segment as well. However, in this sense, Blockchain technology in itself represents one of the building blocks and support for building a data privacy mechanism, but not its essential part. Different concepts for the protection and privacy of health data are applied in the implemented systems of electronic health care with the application of blockchain technology. An exhaustive overview of the solutions described in the literature regarding the methods of identification and authentication of entities in the healthcare information system as well as the protection of privacy in the management of their data can be found in (Fernández-Alemán et al., 2013; Jayabalan & O'Daniel, 2016). In the following paragraphs we will look at two solutions that are based on similar ideas as the solution proposed in this paper, but the ways of realization are different.

The concept described in (Wang et al., 2019) is based on blockchain and cloud technologies. The security of medical data and EHR is ensured by their creator (medical institution + authorized person) encrypting them and additionally encrypting them before placing them in the appropriate space at the storage location in the cloud . The indexes of the generated EHR records are stored in the corresponding blockchain. Encryption mechanisms are such that they enable keyword searches over encrypted data. This concept enables the secondary use of health data, but the mechanism is relatively complex. The owner of the medical data is still the person whose examination created the record and who fully controls the access to that data. The right of access is obtained only with the explicit consent of the data owner. The procedure for accessing the desired data is as follows.

The interested entity sends a list of keywords that relevant records must contain to the EHR creator. The creator sends to the entity a digital patern to search the EHR record space. After finding the requested records, the interested entity addresses the owner of the data, whose identifier it receives after finding the indexes that match the set of keywords, for consent to access the data. If access is granted, the operation of decrypting the EHR data and sending it securely to the interested entity is undertaken.

Theoretically, the weakness of this concept lies in the fact that the patient's privacy is not fully protected. It is possible to create a targeted set of queries by keywords in order to analyze the situation whether a specific patient has a certain type of health problem. The problem lies in the fact that this information is obtained before the right of access to specific medical data.

The concept formulated in (Omar et al., 2019) proposes a solution based on Blockchain technology and cryptographic mechanisms. Cryptographic mechanisms are used to protect privacy and Blockchain technology to store health data. The application of cryptographic methods ensures the anonymity of patients, and Blockchain technology ensures data integrity and immutability .

The solution described in this paper uses usernames and passwords as a method of user identification and authorization. The allowed activities in the system are defined based on the roles assigned to users. Patients have the role of data source and they pass their personal health data to the system in an encrypted form. Entities that use data in the system, data users, require access to data in the system, which is allowed only after successful authentication. The registration authority is responsible for the authentication process . Access and exchange of health data are protected by special cryptographic mechanisms. Each transaction of data stored in the blockchain is marked with a special blockchain identifier, on the basis of which the data contained in the transaction is accessed and this identifier is forwarded to the initiator of the block generation.

In order for the data user to access the data contained in one block of a patient, he/she must have the identifier of that block, which is owned only by the patient as a source of data, so this protocol also implicitly requires the patient's consent to access the data. When the user knows the desired number, he/she turns to the registration authority for the authorization of access to the requested data. If the user's authentication is successful, he/she receives the desired private data of the patient whose data he/she requested.

In relation to the described concept of EHR data management, the concept proposed in this paper has certain security and functional advantages. It refers to the applied identification and authentication mechanism. The method based on digital certificates is organizationally and functionally, in our opinion, less complex in terms of scalability and interoperability. From the functionality point of view, the concept proposed in this work with its data organization, equally easily enables primary and secondary use of medical data without endangering the disclosure of the patient's identity in case of secondary use. In this way, the proposed concept of EHR data organization enables the implementation of an electronic healthcare system in legislative systems with different approaches to the ownership of medical data.

Conclusion

The processes of digital transformation of society and the transition of life processes towards cyberspace inevitably highlight the issues of information security and the preservation of privacy of personal data. Unauthorized access to an individual's personal data can have serious adverse consequences for him or her. The damages can be personal, psychological, business, material and social. Identity theft and access to health data can inflict harm to the person in question in terms of obtaining employment, insurance premiums, bank loans, and the like. These examples show the importance of maintaining the privacy of medical data for the individual in each community and the community as a whole.

This paper presents the concept of object identification and privacy protection based on blockchain technology and the PKI infrastructure. The application of these technologies helps the concept achieve the following goals:

- The use of digital certificates as carriers of electronic identity enables a unique distinction of entities in the system. The application of Lightweight X.509 Digital Certificates enables the identification of devices with limited process capacities, which is significant from the point of view that devices with limited processing capacities (sensors, mobile and wearable devices) also participate in such systems.
- The system of registering events in the system and preserving the history of the system is such that for each activity it is known who did it, and when it was undertaken. This enables the detection of incidents, the analysis of their causation and the definition of prevention procedures.
- The mechanism of separation of identification and medical data enables the primary and secondary use of medical data in accordance with the data privacy regulations.
- Digital signature and blockchain technology enable the integrity of medical data to be preserved both at the time of its creation and over time.

The enumerated security features of the proposed concept enable the implementation of electronic health systems as zero trust information systems (Rais et al., 2024; Kudrati & Pillai, 2022; Garbis & Chapman, 2021) and at the same time ensure compliance with the EU GDPR.

References

Balamurugan, B., Poongodi, T., Manu, M.R., Karthikeyan, S. & Sharma, Y. 2023. *Convergence of Blockchain, AI and IoT: A Digital Platform, 1st Edition*. New York, NY: Chapman & Hall/CRC. ISBN 9780367495305.

Bhushan, B., Rakesh, N., Farhaoui, Y., Nand, P. & Unhelkar, B. 2022. *Blockchain Technology in Healthcare Applications: Social, Economic, and Technological Implications, 1st Edition*. Boca Raton: CRC Press. Available at: https://doi.org/10.1201/9781003224075.

Bhushan, B., Sharma, S.K., Saračević, M. & Boulmakoul, A. 2023. *Blockchain Technology Solutions for the Security of IoT-Based Healthcare Systems: A volume in Cognitive Data Science in Sustainable Computing*. Academic Press. Available at: https://doi.org/10.1016/C2021-0-01904-0.

Boonkrong, S. 2021. *Authentication and Access Control: Practical Cryptography Methods and Tools*. Apress Berkeley, CA. Available at: https://doi.org/10.1007/978-1-4842-6570-3.

Buchmann, J.A., Karatsiolis, E. & Wiesmaier, A. 2013. *Introduction to Public Key Infrastructures*. Heidelberg: Springer Berlin. Available at: https://doi.org/10.1007/978-3-642-40657-7.

Chen, L., Moody, D., Regenscheid, A. & Robinson, A. 2023. Digital Signature Standard (DSS). *Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology*. Available at: https://doi.org/10.6028/NIST.FIPS.186-5.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. & Polk, W. 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Standards Track*. *Tech. rep.* [online]. Available at: https://www.rfc-editor.org/rfc/rfc5280.html [Accessed: 15 July 2023].

Diffie, W. & Hellman, M. 1976. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), pp. 644–654. Available at: https://doi.org/10.1109/TIT.1976.1055638.

Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O. & Toval, A. 2013. Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3), pp. 541–562. Available at: https://doi.org/10.1016/j.jbi.2012.12.003.

Forsby, F., Furuhed, M., Papadimitratos, P. & Raza, S. 2018. Lightweight X.509 Digital Certificates for the Internet of Things. In: *Fortino, G. et al (Eds.) Proceedings of Interoperability, Safety and Security in IoT, Third International Conference, InterIoT 2017, and Fourth International Conference, SaSeIot*. Valencia, Spain, vol. 242. pp.123-133, November 6-7. Cham: Springer. Available at: https://doi.org/10.1007/978-3-319-93797-7_14.

Galbraith, S.D. 2012. *Mathematics of Public Key Cryptography, 1st Edition*. Cambridge University Press. Available at: https://doi.org/10.1017/CBO9781139012843.

Garbis, J. & Chapman, J.W. 2021. *Zero Trust Security: An Enterprise Guide*. Apress Berkeley, CA. Available at: https://doi.org/10.1007/978-1-4842-6702-8.

Hines, B. 2020. *Digital finance: Security tokens and unlocking the real potential of blockchain*. Hoboken, New Jersey: Wiley. ISBN 978-1119756309.

Jayabalan, M. & O'Daniel, T. 2016. Access control and privilege management in electronic health record: a systematic literature review. *Journal of Medical Systems*, 40, art.number:261. Available at: https://doi.org/10.1007/s10916-016-0589-z.

Knuth, D.E. 1998. *The art of computer programming, volume 3: (2nd ed.) sorting and searching*. Redwood City, CA: Addison-Wesley Pub. Co. ISBN 978-0-201-89685-5.

Kudrati, A. & Pillai, B. 2022. *Zero Trust Journey Across the Digital Estate, 1st Edition*. Boca Raton: CRC Press. Available at: https://doi.org/10.1201/9781003225096.

Kumar, V., Jain, V., Sharma, B., Chatterjee, J.M. & Shrestha, R. 2022. *Smart City Infrastructure: The Blockchain Perspective, 1st Edition*. Hoboken, NJ: Willey. ISBN 978-1119785385.

Lee, D. & Deng, R.H. 2018. *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation*. San Diego, CA: Academic Press. Available at: https://doi.org/10.1016/C2015-0-04334-9.

Liang, Y.C. 2019. Blockchain for Dynamic Spectrum Management. In: *Dynamic Spectrum Management*. pp.121-146. Singapore: Springer. Available at: https://doi.org/10.1007/978-981-15-0776-2_5.

Mamdouh, M., Awad, A.I., Khalaf, A.A.M. & Hamed, H. 2021. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Computers & Security*, 111, art.number:102491. Available at: https://doi.org/10.1016/j.cose.2021.102491.

Menezes, A.J., van Oorschot, P.C. & Vanstone, S.A. 1997. *Handbook of Applied Cryptography*. Boca Raton: CRC Press. Available at: https://doi.org/10.1201/9780429466335.

Murphy, S. 2015. *Healthcare Information Security and Privacy, 1st Edition*. New York, NY: McGraw-Hill. ISBN 978-0071831796.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN*, 21 August, pp. 1-9. Available at: https://doi.org/10.2139/ssrn.3440802.

Omar, A.A., Bhuiyan, M.Z.A., Basu, A., Kiyomoto, S. & Rahman, M.S. 2019. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, 95, pp. 511–521. Available at: https://doi.org/10.1016/j.future.2018.12.044.

Rais, R., Morillo, C., Gilman, E. & Barth, D. 2024. *Zero Trust Networks, 2nd Edition*. O'Reilly Media. ISBN 9781492096597.

Salman, T., Zolanvari, M., Erbad, A., Jain, R. & Samaka, M. 2019. Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys and Tutorials*, 21(1), pp. 858–880. Available at: https://doi.org/10.1109/COMST.2018.2863956.

Shoniregun, C.A., Dube, K. & Mtenzi, F. 2010. *Electronic Healthcare Information Security*. New York, NY: Springer. Available at: https://doi.org/10.1007/978-0-387-84919-5.

Singh, A.K. & Zhou, H. 2022. *Medical Information Processing and Security: Techniques and applications*. Institution of Engineering and Technology. Available at: https://doi.org/10.1049/PBHE044E.

Smith, S.S. 2020. *Blockchain, Artificial Intelligence and Financial Services: Implications and Applications for Finance and Accounting Professionals*. Cham: Springer. Available at: https://doi.org/10.1007/978-3-030-29761-9.

Stamp, M. 2011. *Information Security: Principles and Practice*. Hoboken, NJ: Wiley. Available at: https://doi.org/10.1002/9781118027974.

Stawicki, S.P. 2023. *Blockchain in Healthcare: From Disruption to Integration*. Cham: Springer. Available at: https://doi.org/10.1007/978-3-031-14591-9.

Summers, A. 2022. *Understanding Blockchain and Cryptocurrencies: A Primer for Implementing and Developing Blockchain Projects, 1st Edition*. Boca Raton: CRC Press. Available at: https://doi.org/10.1201/9781003187165.

Todorov, D. 2007. *Mechanics of User Identification and Authentication: Fundamentals of Identity Management, 1st Edition*. New York, NY: Auerbach Publications. Available at: https://doi.org/10.1201/9781420052206.

Vacca, J.R. 2004. *Public Key Infrastructure: Building Trusted Applications and Web Services, 1st Edition*. New York, NY: Auerbach Publications. Available at: https://doi.org/10.1201/9780203498156.

Wang, Y., Zhang, A., Zhang, P. & Wang, H. 2019. Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. *IEEE Access*, 7, pp. 136704–136719. Available at: https://doi.org/10.1109/access.2019.2943153.

Zheng, Z. 2022. *Modern Cryptography Volume 1: A Classical Introduction to Informational and Mathematical Principle*. Singapore: Springer. Available at: https://doi.org/10.1007/978-981-19-0920-7.

Zheng, Z., Tian, K. & Liu, F. 2023. *Modern Cryptography Volume 2: A Classical Introduction to Informational and Mathematical Principle*. Singapore: Springer. Available at: https://doi.org/10.1007/978-981-19-7644-5.

Концепция конфиденциальности данных в электронной системе здравоохранения на основе технологии Блокчейн

Деян Б. Цизель, *Томислав* Б. Ункашевич, *Зоран* Дж. Баняц

Институт ВЛАТАКОМ, г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 81.93.29 Информационная безопасность. Защита информации,
28.21.19 Теория кодирования,
49.33.35 Надежность сетей связи и защита информации

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Прогресс в области информационных и коммуникационных технологий позволили создать среду симбиоза между людьми и машинами, в которой люди взаимодействуют с машинами для улучшения качества повседневной жизни. В связи с этим возникают проблемы информационной безопасности, в частности, конфиденциальности данных. Во многих странах существуют правовые рамки, регулирующее этот вопрос с точки зрения целей, которые должны осуществлятся при манипулировании личными данными, а сама технология является выбором создателей информационных систем. Блокчейн технология является одним из предпочтительных методов обеспечения целостности данных и необходимых транзакций, а цифровые сертификаты в сочетании с ней обеспечивают конфиденциальность информации о пациентах.

Методы: С помощью криптографических методов асимметричной криптографии осуществляется блокчейн технология и надежные методы идентификации в киберпространстве, что позволяет сохранять конфиденциальность информации на высшем уровне.

Результаты: В данной статье описывается метод защиты конфиденциальности медицинских данных пациентов в системе здравоохранения, основанный на цифровых сертификатах как методе идентификации в киберпространстве и блокчейн технологии как методе сохранения целостности транзакций и информационной системы здравоохранения. Предлагаемая концепция позволяет разделить личные и медицинские данные таким образом, что при соблюдении права собственности пациента на медицинские данные становится возможным первичное и вторичное использование медицинских данных, не нарушая права пациента на неприкосновенность личных данных.

Выводы: Концепция идентификации объекта в информационной системе здравоохранения и организация/хранение данных в соответствии с принципами блокчейн технологии, предложенными в этой статье, позволяют повысить конфиденциальность информации до международного уровня в соответствии с Общим регламентом защиты данных Европейского Союза. Помимо того, предлагаемая концепция способствует обнаружению незарегистри-

рованных устройств или объектов в системе, таким образом сохраняя целостность системы и повышая ее общую информационную безопасность.

Ключевые слова: информационная безопасность, медицинская информационная система, медицинские данные, первичное и вторичное использование, асимметричная криптография, цифровая подпись, блокчейн организация, блочная структура.

Концепт приватности података у електронском здравственом систему заснован на блокчејн технологији

Дејан Б. Цизељ, *Томислав* Б. Ункашевић, *Зоран* Ђ. Бањац

Институт ВЛАТАКОМ, Београд, Република Србија

ОБЛАСТ: информациони системи, криптологија, рачунарске науке
КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Напредак у информационо-комуникационим технологијама омогућио је стварање симбиотичког окружења људи и машина у којем људи интеракцијом са машинама побољшавају квалитет свакодневног живота. У том контексту, проблеми информационе безбедности и посебно приватности података избијају у први план. У многим земљама постоји законска регулатива којом се тај проблем регулише у смислу обезбеђења циљева који се морају реализовати при манипулацији приватним подацима, а сама технологија је избор креатора информационих система. Блокчејм технологија је једна од метода избора за обезбеђење интегритета података и непорецивости трансакција, док дигитални сертификати у спрези с њом омогућавају остваривање приватности података пацијената.

Методе: Применом криптографских метода асиметричне криптографије реализује се блокчејн технологија и поуздани методи идентификације у сајбер простору, што омогућава очување приватности података на високом нивоу.

Резултати: Овај рад описује концепт заштите приватности података пацијената у здравственом систему. Засно-

ван је на дигиталним сертификатима као методу идентификације у сајбер простору и блокчејн технологији као методу за очување интегритета трансакција и информационог система здравственог осигурања. Предложени концепт омогућава сепарацију приватних и медицинских података тако што је, уз прихваћени принцип власништва пацијента над медицинским подацима, могуће остварити примарну и секундарну употребу медицинских података без угрожавања приватности података пацијента.

Закључак: Концепт идентификације ентитета у здравственом информационом систему и организација/чување података, у складу са принципима блокчејн технологије, који су предложени у овом раду, омогућавају остваривање високог нивоа приватности података у складу са интернационалним документом European Union General Data Protection Regulation. Поред тога, предложени концепт омогућава детекцију нерегистрованих уређаја или ентитета у систему и на тај начин очување интегритета система и повећање његове свеукупне информационе безбедности.

Кључне речи: информациона безбедност, здравствени информациони систем, медицински подаци, примарна и секундарна употреба, асиметрична криптографија, дигитални потпис, блокчејн организација, структура блока.

Paper received on / Дата получения работы / Датум пријема чланка: 21.07.2023.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 30.11.2023.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 01.12.2023.