UDC 004.056 **DOI 10.52167/1609-1817-2024-130-1-332-343**

O. Ussatova[1,4], Sh. Makilenov [2,3]✉, S. Amanzholova[3], S. Dikhanbayev [3], N. Ussatov[1,5]
[1] Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan
[2] Al-Farabi Kazakh National University, Almaty, Kazakhstan
[3] International Information Technology University, Almaty, Kazakhstan
[4] Almaty University of Energy and Communications named after G. Daukeyev, Almaty, Kazakhstan
[5] Turan University, Almaty, Kazakhstan
E-mail: shakirt.makilenov@gmail.com

DEVELOPMENT OF A SYSTEM FOR LOGGING USER ACTIONS IN A HEALTH INFORMATION SYSTEM

`

Abstract. Protecting medical data is of utmost importance in today's healthcare environment, where information confidentiality and secure storage play a key role. Medical records are a critical asset around which the entire medical practice is built, and a breach of their integrity or confidentiality can have serious consequences for patients and the healthcare system as a whole. Problems associated with journaling (logging) actions in medical organizations are integral and relevant. Medical records are at risk of illegal changes, lack of transparency, and vulnerabilities to various types of cyber-attacks. In this context, the relevance of logging user activities in the healthcare system becomes undeniable. This article proposes the development of a module for logging the actions of medical personnel in medical institutions. The purpose of this module is to create a reliable system for tracking and recording the activities of healthcare professionals, which will allow healthcare institutions to maintain detailed and reliable records of interactions between doctors and patients, treatment procedures performed, diagnoses, prescriptions and other important medical actions. This module not only ensures the accuracy and transparency of medical records, but also plays an important role in enhancing patient safety and improving the quality of care. Additionally, it provides comprehensive auditing of each patient's medical history, making it a valuable resource for internal audits, regulatory compliance, and legal documentation support. This module is designed with a deep understanding of healthcare workflows as well as strict data privacy regulations such as HIPAA (Hardware Portable and Affordable Health Act). It is an advanced software solution that can be tailored to the specific needs of various healthcare organizations, be it small clinics or large hospitals. The module provides scalability and adaptability, making it a powerful tool for maintaining the reliability and security of medical data in the healthcare industry.

Keywords. Logging, audit trail, blockchain, medical data protection, healthcare system, compliance.

Introduction.

In today's healthcare environment, maintaining confidentiality and protecting medical data faces threats of information leakage, which creates serious risks for patients and the healthcare system itself[1]. Security incidents, such as unauthorized access to data, alteration of records, or even cyberattacks on system data, indicate the relevance of data privacy issues in the medical field [2][3].

In connection with this, an urgent challenge is the development of effective methods for ensuring the safety and security of storing medical data, including recording user actions in healthcare information support [4]. Logging of user activities is the recording of the process and identification of various actions performed in the system, such as accessing data, changes in patient records, or performing certain procedures [5]. This allows you not only to control, but

also to analyze the actions of personnel, healthcare and other system participants, providing a higher level of security and transparency.

Logging user activity in a healthcare system is critical to ensuring the accuracy of medical data, controlling access, and preventing potential security threats. Traditional logging methods may have disadvantages, such as vulnerabilities in data storage conditions or lack of changes in historical history [6]. This opens the door to innovative technologies such as blockchain to provide more reliable and secure logging in the home healthcare industry [7].

The application of blockchain technology in healthcare represents a promising approach to solving user activity logging problems. Blockchain provides immutable resistance to change and a high level of trust due to its decentralized and encrypted nature [7]. This allows the creation of secure, permanent logs of user activity while preserving the integrity of the information, which is important for ensuring the security of medical data [8].

Using blockchain technology to monitor activities in portable medical equipment represents an important step towards creating transparent, reliable and secure audit processes. This technology allows healthcare systems to not only enroll users, but also ensure privacy and transparency of health data, improve the security of patient information and improve overall system efficiency.

Related work.

The article [9] discusses the SmartWalk system for monitoring the physical activity of people and controlled by medical workers. The article presents the results of a study of SmartWalk security services, such as authentication, authorization, symmetric and asymmetric key cryptography, critical transaction verification and logging using blockchain technology. In this research work, logging is used to verify data integrity when authenticating through a trusted third party.

The article [10] presents the results of a study of a logging procedure using blockchain to ensure secure transmission of data from body sensors via a smartphone to a medical server. The data transfer process involves additional witnesses who record packets in a secure form for auditability.

In [11], the authors show how to efficiently perform complex audit queries on access log data stored in blockchains using additional key-value stores. To effectively utilize the key value storage mechanism, the authors applied various techniques and optimizations such as sharding, simple data duplication, and batch loading, keeping in mind the required competitor query types and interface.

Paper [12] proposes the use of mixed block blockchain to support immutable journaling and editable blocks. This means that editable blocks storing patient data and non-editable logging blocks are generated alternately.

Article [13] presents the results of a study of the logging and auditing component within the REST (Representational state transfer) architecture used on the SOCIAL (Social Cooperation for Integrated Assisted Living) platform. The use of cryptographically secure blockchain technology allows you to store events and data blocks in a specialized database. Audit processes access stored events and blocks to determine relevant data, and three separate processes are considered: log insertion, log consensus, and log auditing. Log insertion is activated when an event occurs in the SOCIAL platform service and involves sending data describing the event to the log service in the form of an HTTP (HyperText Transfer Protocol) request with the event inserted into its request body in the form of a JSON (JavaScript Object Notation) object.

Materials and methods.

A commercial solution for the gathering, inspection, and reporting of logs is provided by log management systems. These systems offer storage options and a configuration interface for managing log collection, and frequently let administrators set log retention limits for specific log

sources [14]. Log management systems include nonrepudiation features to guarantee log file integrity during the collection process. This entails «signing» logs with a calculated hash that can subsequently be used as a checksum on the files. These logs can be gathered, examined, and searched. The systems can also produce prefiltered reports, enabling users to present log data customized for particular functions or purposes.

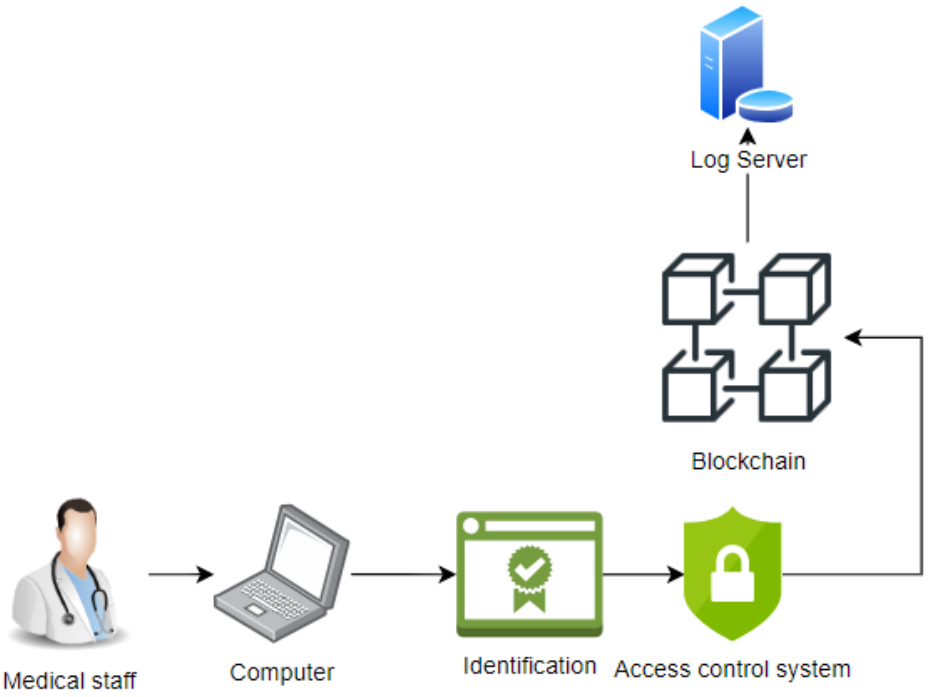

Figure 1 - Logging process with using blockchain in medical organization

Figure 1 describes the Logging the activity of doctors using blockchain in medical organizations. It can enhance transparency, security, and accountability in healthcare. Here's a step-by-step description of the process:

1) Medical organizations need to first identify the need for logging doctors' activities. This can be for various reasons such as ensuring the accuracy of medical records, tracking prescription history, monitoring access to patient data [15].

2) Doctors' identities should be verified on the blockchain network. This might involve using cryptographic keys or digital certificates to ensure that only authorized personnel can participate. Each activity performed by doctors, such as patient consultations, surgeries, prescription issuance, and updates to medical records, should be logged on the blockchain. The data should be time-stamped to establish a clear chronological order.

3) Depending on the blockchain network, a consensus mechanism (e.g., Proof of Work, Proof of Stake, or a private consensus algorithm) ensures that the recorded data is agreed upon by network participants. Sensitive patient data must be protected. Implement encryption mechanisms to ensure that only authorized personnel can access certain information. This should be balanced with the need for transparency and accountability [16].

4) Implement role-based access controls. Doctors, nurses, administrators, and other staff should have different levels of access and permissions. Blockchain can maintain and enforce these access rules. One of the core features of blockchain is immutability.

In terms of implementation, a java project was created. The peculiarity of this project is that with the help of this project we will be able not only to create blocks based on the blockchain, but also to verify all blocks.

```
public class Main {

    public static void main(String[] args) {
        BlockFactory blockFactory = new StandardBlockFactory();
        BlockchainValidator blockchainValidator = new BlockchainValidatorImpl();
        Blockchain blockchain = BlockchainImpl.getInstance(blockchainValidator);
        Miner miner = new MinerImpl(blockchain, blockFactory);
        miner.mine();
        blockchain.getBlocks().forEach(System.out::println);
    }
}
```

This code snippet from main class of the project sets up the basic structure of the blockchain with a black factory, a blockchain validator and a miner. This means a new black color, and then output all the blocks in the blockchain to the console.
This is the output from the program (Figure 2).

```
Block:
Created by miner # 0
Id: 1
Timestamp: 1697678532044
Magic number: -5426026794296243079
Hash of the previous block:
0
Hash of the block:
cc3775a7beef0b4555b2dc3978cc38a58d04428f6e5c92a60638ac03ac51e003
Block was generating for 0 seconds
N was increased to 0
```

Figure 2 – Program output

«Block: Created by miner # 0»: This line indicates that a new block has been created by miner number 0. In a blockchain, miners are responsible for creating new blocks through a process called mining. ***«Magic number: -5426026794296243079»*** is a value associated with the block. In some blockchain systems, a magic number can be used for various purposes, including version identification or security checks. ***«Hash of the previous block: 0»***: This line indicates that this block is the first block in the blockchain (the genesis block), as its «previous block» hash is 0. In subsequent blocks, this would reference the hash of the previous block in the chain.

«Hash of the block:

cc3775a7beef0b4555b2dc3978cc38a58d04428f6e5c92a60638ac03ac51e003»: This is the cryptographic hash of the current block. In a blockchain, each block contains the hash of the previous block, which ensures the integrity and immutability of the blockchain. ***«N was increased to 0»*** is likely related to a mechanism used in the blockchain to adjust the difficulty of mining. The value of «N» is being increased to 0, which may indicate that the mining difficulty has been lowered for the next block generation.

In generally, the output provides detailed information about a single block in a blockchain, including its creation, identification, timestamp, hash values, and a change in a parameter related to mining difficulty (N). This information is crucial for maintaining the integrity and transparency of the blockchain ledger.

```
public interface BlockchainValidator {
   void validateBlockchain(Blockchain blockchain) throws InvalidBlockchainException;
   void validateBlock(Block block, Block prevBlock) throws InvalidBlockchainException;
}
```

This interface is used to specify the methods that a class implementing it must provide for validating a blockchain and its individual blocks. Here's an explanation of the two methods defined in the interface:

validateBlockchain(Blockchain blockchain) throws InvalidBlockchainException:

InvalidBlockchainException: This method is used to validate the entire blockchain for consistency and integrity. It takes a single parameter, blockchain, which represents the blockchain to be validated. Implementations of this method should check that the blocks in the blockchain are linked correctly, that their data is consistent and follows the rules of the blockchain protocol, and that there are no unauthorized changes or tampering with the blockchain data.

The second method Similar to the first method and Implementations of this method should verify that the new block's data is correctly linked to the previous block (via its hash or other means), that the block's data adheres to the rules of the blockchain protocol, and that there are no unauthorized changes or tampering with the block's data.

Mathematical model of the project.

Developing a mathematical model for logging user actions in a health information system involves quantifying various aspects of the system's behavior. In this model, we'll focus on tracking user actions and generating log entries. Let's use mathematical notations to describe this process.

Let:

- U be the set of users in the health information system.
- A be the set of possible user actions, such as «View Patient Record,» «Update Medication,» «Add Diagnosis,» etc.
- T be the set of discrete time intervals, where $t \in T$ represents a specific time interval.

We want to create a mathematical model that tracks user actions and generates log entries. We can use a binary matrix M to represent this system, where each entry is a binary variable, indicating whether user u performed action a during time interval t.

1. Objective Function:

We aim to maximize the effectiveness of logging user actions while minimizing the impact on system performance. Define the objective function as follows:

$$\text{Maximize } \sum_{u \in U} \sum_{a \in A} \sum_{t \in T} M_{u,a,t}. \quad (1)$$

This objective function represents the total number of logged user actions over all users, actions, and time intervals.

2. Constraints:

a. Data Retention Constraints:

- Define a parameter $(D_{a,t})$representing the maximum allowable data retention period for action (a) at time (t).
- Ensure that actions are retained in the log for a duration not exceeding $(D_{a,t})$:

$$[\sum_{u\in U} M_{u,a,t} \leq D_{a,t} \quad \forall a \in A, \forall t \in T]. \tag{2}$$

b. Resource Constraints:

- Define a parameter (R_t) representing the maximum resource allocation for logging at time (t).

- Ensure that the total number of logged actions at time \(t\) does not exceed the resource limit:

$$[\sum_{u\in U} \sum_{a\in A} M_{u,a,t} \leq R_t \quad \forall t \in T]. \tag{3}$$

c. Consistency Constraints:

- Ensure that if a user performs an action, it is logged:

$$[M_{u,a,t} \leq M_{u,a',t} \quad \forall u \in U, \forall a, a' \in A, \forall t \in T]. \tag{4}$$

3. Binary Decision Variables:

- $(M_{u,a,t})$is a binary variable, indicating whether user (u) performed action (a) during time interval (t).

4. Log Entry Generation:

- The log entries are generated based on the (M) matrix. For each$(M_{u,a,t})$ equal to 1, a log entry is created, documenting the user action, user ID, and timestamp.

This mathematical model provides a framework for optimizing the logging of user actions in a health information system while respecting data retention limits and resource constraints.

Results.

The implementation of blockchain technology for logging the actions of doctors in medical organizations yields several important results and has a transformative impact on healthcare operations. Before the introduction of blockchain technologies into the project, a static code analysis was carried out.

Язык	Продолжительность анализа	Строки кода	Уязвимости					Статус
Config files	0:00:03	60985	0	0	9	2	11	завершено
JavaScript	0:01:28	36483	3	0	100	8	111	завершено
TypeScript	0:00:02	904	0	0	0	0	0	завершено
HTML5	0:00:01	1	0	0	0	0	0	завершено

Figure 3 - Statistics on programming languages

The report typically assigns severity levels to the identified issues, such as critical, high, medium, or low, to help prioritize and focus on the most critical vulnerabilities. According to the results from Figure 4, before the introduction of blockchain technology, the estimate of this project was 3.2/5. There were critical vulnerabilities in 3 places.

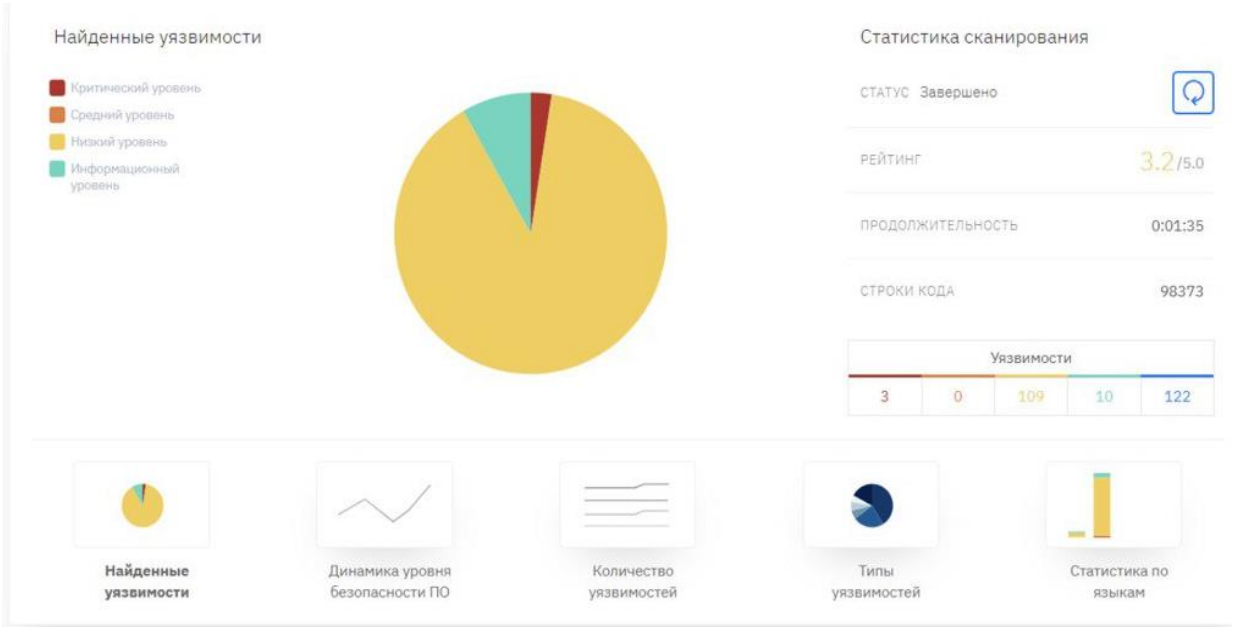

Figure 4 - Graph of results before Blockchain Implementation

One of the most significant improvements is in data security and privacy. Blockchain cryptographic techniques and decentralized architecture ensure that data stored on the blockchain is highly secure and resistant to tampering. This is particularly vital in healthcare sector.

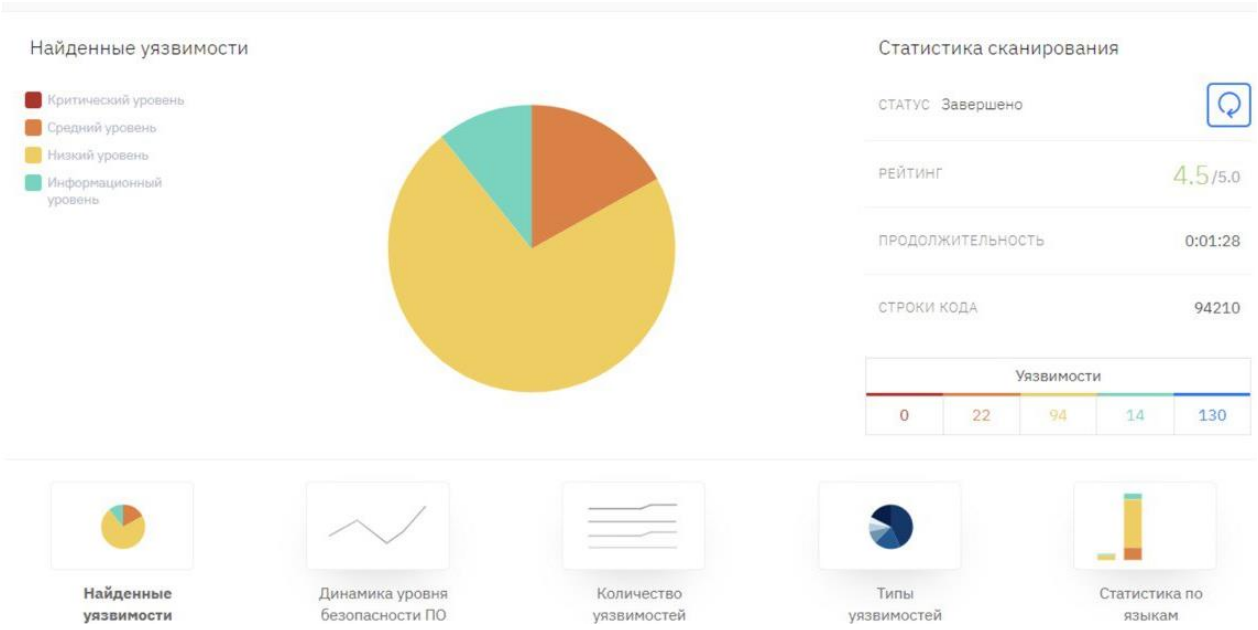

Figure 5 - Graph of results before Blockchain Implementation

According to Figure 5, you can see the result after the introduction of blockchain technology. The code security score was 4.5 out of 5. As you can see, critical vulnerabilities have been fixed with the introduction of technologies.

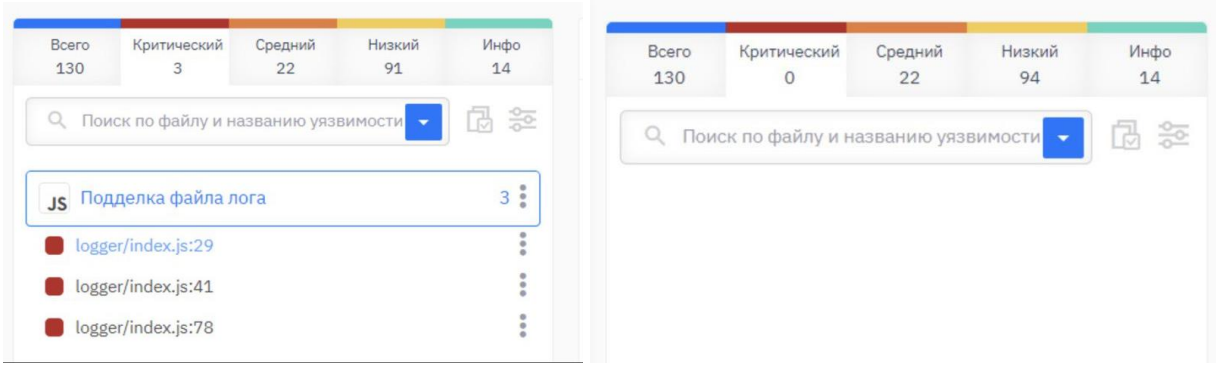

Figure 6 - Detailed results of vulnerabilities before and after implementation

The above description outlines the types of vulnerabilities identified through static code analysis. The majority of the vulnerabilities were associated with Log file tampering. Additionally, vulnerabilities related to network activity and cross-site request forgery were also identified. Forgery of log files is a significant security concern, and the use of blockchain technology can provide a robust solution to address this vulnerability. Blockchain's inherent characteristics, including immutability and transparency, make it a powerful tool for preventing log file forgery.

With using blockchain to prevent log file forgery provides a robust solution that enhances the security and integrity of log data. It safeguards against unauthorized modifications, provides transparency, and supports reliable audit trails.

Discussion

The development and implementation of blockchain technology for logging the actions of doctors in medical organizations represent a significant step forward in healthcare data management. While the advantages of enhanced transparency, data integrity, and improved patient care are evident, several challenges and future directions must be considered to ensure the successful integration of this innovative technology into the healthcare ecosystem.

1. Integration Challenges:

One of the primary challenges is the integration of blockchain into existing healthcare systems. Many medical organizations have well-established electronic health record (EHR) systems and processes. Adapting to blockchain technology while minimizing disruption to ongoing operations is a complex task. Solutions that facilitate seamless integration are essential [17].

2. Scalability Concerns:

Healthcare organizations generate vast amounts of data daily. Ensuring that the blockchain can scale to accommodate this growing volume of data is crucial. Scalability solutions must be developed to prevent congestion, bottlenecks, and the potential for delayed patient care due to slow data processing.

3. Data Ownership and Consent:

Determining data ownership and obtaining patient consent for data usage are crucial ethical and legal considerations. Patients have a right to know how their medical data is being utilized and should have control over its use. Addressing these issues requires a thoughtful approach to consent management and data access.

As the adoption of blockchain technology for logging doctor actions in medical organizations advances, it is vital to address these challenges and seize the opportunities for improvement. The ultimate goal is to harness the potential of blockchain to improve patient care, ensure data security and privacy, and streamline healthcare processes. By working

collaboratively, medical organizations, technology providers, and regulators can unlock the full potential of this groundbreaking technology in healthcare.

Conclusions.

In the rapidly changing field of healthcare, creating systems to record the actions of doctors in healthcare organizations using blockchain technology is a significant step forward. This innovative approach promises to change the way healthcare data is recorded, stored and accessed.

The advantages of this development are evident, with transparency, data integrity, and regulatory compliance being at the forefront. Blockchain's transparent ledger ensures that every action taken by medical professionals is documented securely, creating an immutable record. This not only fosters accountability but also provides the foundation for informed, data-driven decision-making.

However, like any technological advancement, the integration of blockchain into healthcare is not without its challenges. The need for seamless integration into existing systems, scalability to accommodate the ever-expanding volume of medical data, and the complexities of regulatory compliance are just a few of the hurdles to overcome. Privacy and security concerns must also be addressed to safeguard patient data and maintain trust in the healthcare system.

In conclusion, the development of systems for logging the actions of doctors in medical organizations through blockchain is not merely a technological upgrade; it is a paradigm shift in healthcare data management. The ultimate vision is a healthcare ecosystem that prioritizes patient care, data security, and efficiency. As healthcare organizations, technology providers, and regulatory bodies work together, the full potential of blockchain will be harnessed, ushering in a new era of excellence in healthcare data management. This transformation is not just a possibility; it is a shared commitment to a healthier, more secure future for patients and medical professionals alike.

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

REFERENCES

[1] Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare, 2(3), 1-44.

[2] Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. IEEE Access, 7, 183339-183355.

[3] 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.

[4] Nysanbayeva, S., Wójcik, W., & Ussatova, O. (2019). Algorithm for generating temporary password based on the two-factor authentication model. Przegląd Elektrotechniczny, 5, 101-106.

[5] Elangovan, D., Long, C. S., Bakrin, F. S., Tan, C. S., Goh, K. W., Yeoh, S. F., ... & Ming, L. C. (2022). The use of blockchain technology in the health care sector: systematic review. JMIR medical informatics, 10(1), e17278.

[6] Ali, A., Khan, A., Ahmed, M., & Jeon, G. (2022). BCALS: Blockchain-based secure log management system for cloud computing. Transactions on Emerging Telecommunications Technologies, 33(4), e4272.

[7] 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).

[8] Kumar, R., Arjunaditya, Singh, D., Srinivasan, K., & Hu, Y. C. (2022, December). AI-powered blockchain technology for public health: A contemporary review, open challenges, and future research directions. In Healthcare (Vol. 11, No. 1, p. 81). MDPI.

[9] Bastos, D., Ribeiro, J., Silva, F., Rodrigues, M., Rabadão, C., Fernández-Caballero, A., ... & Pereira, A. (2021). Security Mechanisms of a Mobile Health Application for Promoting Physical Activity among Older Adults. Sensors, 21(21), 7323.

[10] Chinaei, M. H., Gharakheili, H. H., & Sivaraman, V. (2021). Optimal witnessing of healthcare IoT data using blockchain logging contract. IEEE Internet of Things Journal, 8(12), 10117-10130.

[11] Ozdayi, M. S., Kantarcioglu, M., & Malin, B. (2020). Leveraging blockchain for immutable logging and querying across multiple sites. BMC Medical Genomics, 13, 1-7.

[12] Hylock, R. H., & Zeng, X. (2019). A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study. Journal of medical Internet research, 21(8), e13592.

[13] Rosa, M., Faria, C., Barbosa, A. M., Martins, A. I., Almeida, A. F., & Rocha, N. P. (2019). A platform of services to support community-dwelling older adults integrating FHIR and complex security mechanisms. Procedia Computer Science, 160, 314-321.

[14] Doll, H. (1949). Introduction to induction logging and application to logging of wells drilled with oil base mud. Journal of Petroleum Technology, 1(06), 148–162. https://doi.org/10.2118/949148-g

[15] Landolsi, T., Al-Ali, A. R., & Al-Assaf, Y. (2007). Wireless stand-alone portable patient monitoring and logging system. Journal of Communications, 2(4). https://doi.org/10.4304/jcm.2.4.65-70

[16] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

[17] Hong, L., & Hales, D. N. (2021). Blockchain performance in supply chain management: application in blockchain integration companies. Industrial Management and Data Systems, 121(9), 1969–1996. https://doi.org/10.1108/imds-10-2020-0598

Ольга Усатова, PhD, ҚР ҒЖБМ ҒК Ақпараттық және есептеуіш технологиялар институты, Ғ.Дәукеев атындағы Алматы энергетика және байланыс университеті, Алматы, Қазақстан, olgaussatova@gmail.com

Шәкірт Макиленов, докторант, әл-Фараби атындағы Қазақ Ұлттық Университеті, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан, shakirt.makilenov@gmail.com

Сауле Аманжолова, т.ғ.к., Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан, shokataeva@gmail.com

Сұңқар Диханбаев, магистрант, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан, suna555111@gmail.com

Никита Усатов, студент, ҚР ҒЖБМ ҒК Ақпараттық және есептеуіш технологиялар институты, Тұран университеті, Алматы, Қазақстан, usatov.nikita2242@gmail.com

ДЕНСАУЛЫҚ САҚТАУ АҚПАРАТТЫҚ ЖҮЙЕСІНДЕГІ ПАЙДАЛАНУШЫЛАРДЫҢ ӘРЕКЕТТЕРІН ЖҮРГІЗУ ЖҮЙЕСІН ӘЗІРЛЕУ

Аңдатпа. Медициналық деректерді қорғау ақпараттың құпиялылығы мен қауіпсіз сақтау маңызды рөл атқаратын қазіргі денсаулық сақтау ортасында өте маңызды. Медициналық жазбалар бүкіл медициналық тәжірибе жинақталған маңызды актив болып табылады және олардың тұтастығын немесе құпиялылығын бұзу пациенттер мен тұтастай алғанда денсаулық сақтау жүйесі үшін ауыр зардаптарға әкелуі мүмкін. Медициналық ұйымдардағы әрекеттерді журналға (тіркеуге) байланысты мәселелер біртұтас және өзекті болып табылады. Медициналық жазбалар заңсыз өзгерістерге, ашықтыққа және кибершабуылдардың әртүрлі түрлеріне осалдықтарға ұшырау қаупіне ұшырайды. Осы контекстте денсаулық сақтау жүйесіндегі пайдаланушы әрекеттерін тіркеудің өзектілігі даусыз болады. Бұл мақалада медициналық мекемелердегі медицина қызметкерлерінің іс-әрекеттерін тіркеу модулін әзірлеу ұсынылады. Бұл модульдің мақсаты денсаулық сақтау мекемелеріне дәрігерлер мен пациенттер арасындағы өзара әрекеттесулердің, орындалған емдеу процедураларының, диагностикалардың, рецепттердің және басқа да маңызды медициналық шаралардың егжей-тегжейлі және сенімді жазбаларын жүргізуге мүмкіндік беретін денсаулық сақтау мамандарының қызметін қадағалау және тіркеудің сенімді жүйесін құру болып табылады. әрекеттер. Бұл модуль медициналық жазбалардың дәлдігі мен ашықтығын қамтамасыз етіп қана қоймайды, сонымен қатар пациенттердің қауіпсіздігін арттыруда және медициналық көмек сапасын арттыруда маңызды рөл атқарады. Бұған қоса, ол әрбір пациенттің ауру тарихының жан-жақты аудитін қамтамасыз етеді, бұл оны ішкі аудиттер, нормативтік талаптарға сәйкестік және құқықтық құжаттаманы қолдау үшін құнды ресурсқа айналдырады. Бұл модуль денсаулық сақтаудың жұмыс процестерін терең түсінумен, сондай-ақ HIPAA (Аппараттық портативті және қолжетімді денсаулық туралы заң) сияқты деректердің құпиялылығының қатаң ережелерімен жасалған. Бұл шағын емханалар немесе ірі ауруханалар болсын, әртүрлі денсаулық сақтау ұйымдарының нақты қажеттіліктеріне бейімделуі мүмкін кеңейтілген бағдарламалық құрал шешімі. Модуль денсаулық сақтау саласындағы медициналық деректердің сенімділігі мен қауіпсіздігін қолдаудың қуатты құралына айналдыра отырып, ауқымдылық пен бейімделуді қамтамасыз етеді.

Түйінді сөздер. Тіркеу, аудит, блокчейн, медициналық деректерді қорғау, денсаулық сақтау жүйесі, комплаенс.

Ольга Усатова, PhD, Институт информационных и вычислительных технологий КН МНВО РК, Алматинский университет энергетики и связи имени Г. Даукеева, Алматы, Казахстан, olgaussatova@gmail.com

Шакирт Макиленов, докторант, Казахский национальный университет имени аль-Фараби, Международный университет информационных технологий, Алматы, Казахстан, shakirt.makilenov@gmail.com

Сауле Аманжолова, к.т.н., Международный университет информационных технологий, Алматы, Казахстан, shokataeva@gmail.com

Сункар Диханбаев, магистрант, Международный университет информационных технологий, Алматы, Казахстан, suna555111@gmail.com

Никита Усатов, студент, Институт информационных и вычислительных технологий КН МНВО РК, Университет Туран, Алматы, Казахстан, usatov.nikita2242@gmail.com

РАЗРАБОТКА СИСТЕМЫ ЛОГИРОВАНИЯ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ЗДРАВООХРАНЕНИЯ

Аннотация. Защита медицинских данных приобретает важнейшее значение в современной сфере здравоохранения, где конфиденциальность информации и надежность ее хранения играют ключевую роль. Медицинские записи представляют собой критически важный актив, вокруг которого строится вся медицинская практика, и нарушение их целостности или конфиденциальности может иметь серьезные последствия для пациентов и системы здравоохранения в целом. Проблемы, связанные с журналированием (логированием) действий в медицинских организациях, неотъемлемы и актуальны. Медицинские записи подвергаются риску незаконных изменений, их недостаточной прозрачности и уязвимостям перед различными видами кибератак. В этом контексте, актуальность журналирования действий пользователей в системе здравоохранения становится неоспоримой. В данной статье предлагается разработка модуля протоколирования действий медицинского персонала в медицинских учреждениях. Целью этого модуля является создание надежной системы отслеживания и регистрации деятельности медицинских работников, что позволит учреждениям здравоохранения вести подробные и надежные записи о взаимодействии врачей и пациентов, проведенных процедурах лечения, диагнозах, назначениях и других важных медицинских действиях. Этот модуль обеспечивает не только точность и прозрачность медицинских записей, но также играет важную роль в повышении безопасности пациентов и улучшении качества медицинской помощи. Кроме того, он предоставляет возможность всестороннего аудита истории болезни каждого пациента, что делает его ценным ресурсом для внутренних проверок, соблюдения нормативных требований и поддержки юридической документации. Этот модуль разрабатывается с учетом глубокого понимания медицинских рабочих процессов, а также строгих правил конфиденциальности данных, таких как HIPAA (Закон о портативной и доступной медицинской информации). Он представляет собой передовое программное решение, способное быть адаптированным к конкретным потребностям различных медицинских организаций, будь то небольшие клиники или крупные больницы. Модуль обеспечивает масштабируемость и адаптируемость, что делает его мощным инструментом для поддержания надежности и безопасности медицинских данных в сфере здравоохранения.

Ключевые слова. Логирование, аудит, блокчейн, защита медицинских данных, система здравоохранения, комплаенс.

****