Proceedings of the 10th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects»

(September 19-20, 2024). Rome, Italy

No 217

INFORMATION AND WEB TECHNOLOGIES

DOI 10.51582/interconf.19-20.09.2024.023

Model of a decentralised medical card exchange system based on blockchain technology

Shmatko Oleksandr[1], Gamayun Igor[2], Gorbach Tetiana[3]

[1] PhD, Associate Professor;
Technical University «Metinvest Polytechnic» LLC; Ukraine

[2] Doctor of Technical Science, Professor;
National Technical University «Kharkiv Polytechnic Institute»; Ukraine

[3] PhD, Associate Professor;
National Technical University «Kharkiv Polytechnic Institute»; Ukraine

Abstract.
In the current era of digitalisation, data protection is emerging as a critical issue across many industries, particularly within the healthcare domain. Given the crucial importance of patient data, it is imperative to establish dependable systems to protect it. Unauthorised access can lead to potentially harmful exploitation. This paper examines the variable. The data security environment in the healthcare industry exposes the weaknesses of conventional storage solutions. This work proposes a conceptual framework for the system that facilitates the collection, storage, and exchange of electronic data (electronic health records, or EHR). The research analyses blockchain technology as an innovative method for addressing security issues in the transmission of sensitive medical information. The objective of this study is to guarantee a dependable flow of medical data between medical institutions and other participants; the objective is to improve the confidentiality, integrity, and availability of this data. We will achieve this objective by creating and implementing software components that offer secure platforms for medical information transmission through blockchain technology. The study centres on the development of technologies that enable the seamless transfer of medical information. Collaboration among healthcare professionals, experts, and patients is essential to guaranteeing the confidentiality, integrity, and availability of this data. This research focusses on the methodologies and technologies used in the design and development of software components. They are crucial for establishing and preserving secure systems for sending medical data. The aforementioned components include software specifically developed for encryption, authentication, and authorisation, as well as techniques to guarantee error tolerance and data restoration. Results. This work presents a decentralised system concept for the collection, storage, and exchange of Electronic Health Records (EHR). In conclusion. In the healthcare industry, the findings of this study underscore the revolutionary capacity of blockchain technology to rethink data security norms. The suggested paradigm establishes a safe, transparent, and efficient platform for the management of electronic health records (EHR). Not only does it increase the security and integrity of medical data, but it also greatly enhances the quality of medical care and has a positive impact on patient treatment results. As we progress, the use of decentralized systems leveraging blockchain technology in healthcare offers a highly

INFORMATION AND WEB TECHNOLOGIES

promising trajectory. The resolution of intricate issues pertaining to data security and privacy is now underway, thereby facilitating progress. The aim is to establish a healthcare ecosystem that is both sustainable and focused on the needs of patients.

Keywords:
blockchain technology
electronic medical cards
smart contracts
Ethereum
MetaMask
architectural paradigms

Proceedings of the 10th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects»

(September 19-20, 2024). Rome, Italy

No 217

INFORMATION AND WEB TECHNOLOGIES

Introduction.

The volume of patient diagnostic data and the number of medical information systems (MIS) are experiencing significant growth. Consequently, the quantity of digitally stored patient information is increasing [1, 2]. The demand for enhanced functionality within these systems is also on the rise.

Despite MIS's widespread adoption in Ukraine, primary care is currently its only application. A considerable number of medical professionals continue to rely on paper-based records in their practice.

Ukraine is currently implementing eHealth, an electronic healthcare system that aims to protect patients' rights to high-quality medical care and enhance patient-physician interactions by automating processes, maintaining medical records, and managing medical information electronically.

eHealth is comprised of a central database and a diverse array of management information systems. The central database in Ukraine ensures transparency in healthcare expenditures and facilitates paperless information flow, gradually transitioning to electronic record-keeping, including electronic prescriptions, medical cards, and certificates. This system aims to create new electronic services, foster a business-friendly environment, promote innovative medical products, and advance the medical IT market as a whole.

Through rapid access to comprehensive patient information, physicians gain a holistic view of an individual's health status, with a complete electronic medical history aiding in accurate diagnosis. Remote access is available for the majority of medical services. The eHealth system has fundamentally altered the funding model for medical institutions, operating on the principle that "money follows the patient." This system enables monitoring of state fund utilization efficiency.

Initially, eHealth will encompass primary care: general practitioners, internists, and pediatricians. Patients sign declarations with their chosen physicians, who then register them in the system. This process facilitates state reimbursement for each physician's patient care.

Electronic health records (EHR), shared across various

INFORMATION AND WEB TECHNOLOGIES

levels of the healthcare system, have made protecting patients' rights to medical data confidentiality increasingly complex. This enhanced connectivity among diverse users of medical data amplifies the risk of breaches, posing a significant threat to healthcare institutions. Given the sensitive nature of medical records, any confidentiality breach can lead to severe consequences, including defamation, discrimination, and unwarranted stress for both patients and caregivers. Ensuring the privacy and integrity of medical records necessitates stringent access control to EHRs, as well as the preservation of their integrity to prevent unauthorized alterations or destruction [3].

In light of the inherent vulnerabilities in existing systems, the study [4] delineates a security framework to create a protected, adaptable, and reliable EHR system, addressing the urgent need for advanced security measures. The authors synthesise extant EHR security research, highlighting various security strategies encompassing administrative, physical, and technical safeguards necessary to protect the complex healthcare ecosystem. Despite these advancements, there remains a clear need for superior, institution-specific security solutions that meet the evolving requirements of future healthcare organisations.

Several studies [5-8] contribute to this discourse by presenting frameworks and models that address the multifaceted security challenges in healthcare information systems. For instance, [9] proposes a conceptual framework that underscores the disparities in security methodologies across different hospitals and advocates for ethical management of electronic medical records across the healthcare spectrum. Meanwhile, the research in [10] underscores that HIPAA compliance is the cornerstone of ensuring medical information security, implying comprehensive adherence to these guidelines as a standard for healthcare organizations. Other materials [11-13] propose client-server models and their investigations in medical data exchange systems. [13] The authors provide insights into mitigating insider threats in medical institutions, utilizing attack tree tools for detailed analysis of potential security breaches.

INFORMATION AND WEB TECHNOLOGIES

Innovative solutions, such as the smart contract-based access control model [14], offer a framework structure for reducing the risks of hacker attacks. Equally noteworthy is the proposed cloud data storage architecture [15], which can provide an enhanced degree of security for information outsourcing in a cloud computing environment involving numerous independent cloud providers. The framework incorporates double encryption and data fragmentation methods, ensuring secure information dissemination in a multi-cloud environment. The study [16] proposes a hybrid architecture for accessing patient records while preserving confidentiality in a cloud system. The proposed framework allows patients to manage access to their medical records, facilitating seamless data exchange between medical institutions while ensuring emergency access protocols are available.

The authors of [17] examine the distributed ledger technology (DLT) known as IOTA. IOTA addresses blockchain scalability and performance issues by utilizing a Directed Acyclic Graph (DAG) structure, which facilitates parallel transaction addition. This innovation significantly reduces transaction confirmation time and allows for processing an unlimited number of transactions simultaneously. The Masked Authenticated Messaging (MAM) protocol in IOTA ensures secure transmission of encrypted data streams in the form of transactions.

Analysis of recent research underscores the necessity of implementing advanced, specially designed security measures to strengthen the integrity and confidentiality of EHR systems, thereby protecting patient privacy and enhancing the resilience of healthcare information systems against emerging threats.

The issue of designing and developing information systems for collecting, storing, and processing electronic medical records based on blockchain technology is of significant relevance, according to the analysis of recent research and publications.

The objective of this study is to enhance the confidentiality, integrity, and availability of medical data, as well as to ensure reliable exchange of this data between

INFORMATION AND WEB TECHNOLOGIES

medical institutions and other stakeholders through the design and development of software components for creating secure medical information transmission systems based on blockchain technology.

Main part.

The traditional approach to storing and processing medical data involves centralising data storage in the cloud, which raises significant concerns regarding data access security and control. In the healthcare sector, where patient data is both critical and confidential, ensuring robust security measures for cloud-stored information is of paramount importance [18]. Patients should have the right to dictate access permissions to their data, necessitating the creation of a secure and controlled environment for cloud data storage.

To address these security challenges, the authors of this study have turned to the proven capabilities of blockchain technology. Among the multitude of blockchain platforms, Ethereum stands out due to its exceptional security features, making it the preferred choice for this application. The reasons for selecting Ethereum include:

1. Established Ethereum Network: With its extensive track record, the Ethereum network is both large-scale and time-tested, providing a reliable and secure foundation for applications.

2. Functionality and Smart Contracts: Ethereum's rich feature set, particularly its support for smart contracts, ensures secure and decentralised data storage, making it an ideal choice for our system.

3. Active Community Support: Ethereum benefits from a robust and active community that continually explores innovative ways to enhance the technology.

The authors have utilized these advantages to create an Ethereum-based smart contract that aims to enhance communication between patients and physicians. This smart contract streamlines the process of physician oversight of their patients, enhancing the efficiency and security of patient-doctor interactions.

The proposed system's conceptual architecture integrates blockchain technology into the medical data exchange system,

INFORMATION AND WEB TECHNOLOGIES

as shown in Figure 1. This architecture represents a significant advancement in the secure management and exchange of medical information, addressing the critical needs of data confidentiality, integrity, and accessibility in the healthcare sector.

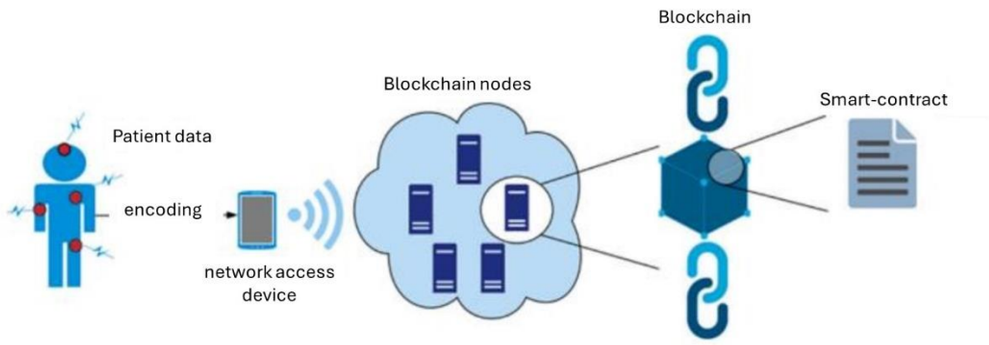

Figure 1
The proposed system's conceptual architecture

In the proposed model, patient data is securely encrypted and stored in the cloud, ensuring that confidential information remains protected throughout the storage and exchange process.

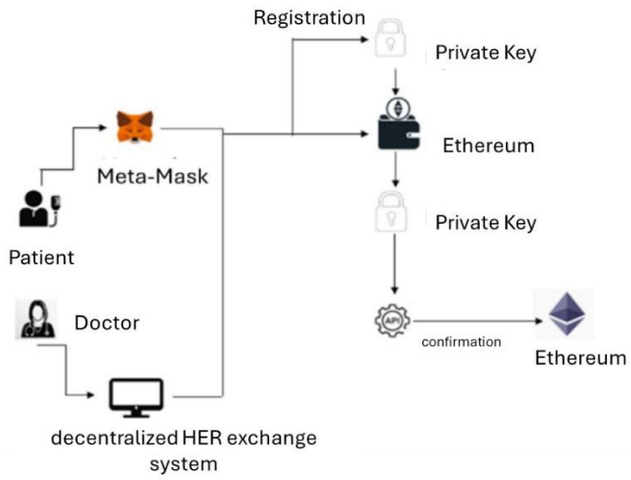

Figure 2
The system's operational schema

INFORMATION AND WEB TECHNOLOGIES

Figure 2 illustrates the system's operational schema whenever a patient chooses to view medical records via MetaMask or the decentralized EHR exchange system website. By accessing the private key from the Ethereum wallet, the user automatically logs into the system. The Ethereum wallet serves as a cold storage wallet, resulting in a significantly lower risk of compromise compared to hot wallets. Furthermore, if a device is lost, patients can simply be issued a new one without incurring penalties for losing their medical records. The wallet can be utilized for signing any documents or for other identity verification needs. This wallet can also be employed for multi-party patient verification. It can be used to create a role-based record access control system, as well as a blockchain-based distributed ownership identification system. In cases of emergency medical care, a similar multi-party mechanism for obtaining permissions to access patient records can be implemented.

The proposed design consists of four main components: User Application, Blockchain Handshake Protocol, Cloud Storage, and Public Blockchain Network. The system serves as a virtual representation with dual purposes. Firstly, it provides users access to application interfaces. Physicians and patients are the two types of users in our system. Each user has a specific function, resulting in the user application providing different user interfaces depending on the user's role. Secondly, based on user input, the user application generates an initial transaction. For confirmation purposes, the transaction is sent to the blockchain handshake protocol. Finally, the user interface establishes communication between users and the blockchain handshake protocol. A fundamental component of the proposed architecture is the Blockchain Handshake (BH) protocol. This component connects the database server, blockchain network, and cloud-based medical records system, which acts as a shell. The proposed architectural model utilizes the Ethereum blockchain network. The distributed ledger connecting blockchain nodes is known as the public blockchain network. Blockchain nodes are miners responsible for updating the blockchain based on a decision-making method. Alternatively, blockchain nodes accept transactions and use the network's

smart contracts for authentication.

In the proposed design, the cloud provides two services analogous to those offered by existing cloud services:

1. EHR Administration Systems: The EHR administration system is hosted as an initial service.

2. Data Storage: This is the subsequent service. All medical records can be stored in the database.

The EHR administration system accepts transactions from the blockchain handshake protocol, performs all related duties, and ultimately stores them in the cloud database. In response to user access requests, the cloud provides the necessary data.

This architecture represents a significant advancement in secure medical data management and exchange, addressing critical needs for data confidentiality, integrity, and accessibility in the healthcare sector. The integration of blockchain technology with cloud storage and user-friendly interfaces creates a robust system for managing electronic health records while maintaining patient privacy and data security.

Conclusions.

Data security is becoming increasingly recognized in the healthcare sector. Therefore, to overcome this problem, the paper suggests using blockchain technology to ensure privacy. The proposed architecture model of medical data exchange systems is primarily designed for remote patient care and prioritizes the protection of patients' confidential medical records. er proposes an Ethereum-based blockchain, which is considered one of the most effective methods used to ensure data security. The proposal also suggests using asymmetric cryptography for data hashing, enhancing transaction security compared to other systems.

References:

[1] Левківський, В. Л. (2023). Аналіз структури та функціональних можливостей медичних інформаційних систем україни.

[2] Bedianashvili, g., Zhosan, h., & lavrenko, s. (2022). Modern digitalization trends of Georgia and Ukraine. Scientific Papers Series Management, Economic Engineering in Agriculture & Rural Development, 22(3).

[3] Корчинський, І. О., & Фірман, Н. А. (2022). Цифрова медицина:

INFORMATION AND WEB TECHNOLOGIES

особливості та проблеми становлення в Україні. Цифрова економіка та економічна безпека, (1 (01)/), 100-105.
[4] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177-183.
[5] Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & security, 97, 101966.
[6] Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications, 153, 311-335.
[7] Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine, 129, 104130.
[8] Mayer, A. H., da Costa, C. A., & Righi, R. D. R. (2020). Electronic health records in a Blockchain: A systematic review. Health informatics journal, 26(2), 1273-1288.
[9] Goodman, K. W. (2020). Ethics in health informatics. Yearbook of medical informatics, 29(01), 026-031.
[10] Yigzaw, K. Y., Olabarriaga, S. D., Michalas, A., Marco-Ruiz, L., Hillen, C., Verginadis, Y., ... & Chomutare, T. (2022). Health data security and privacy: Challenges and solutions for the future. Roadmap to Successful Digital Health Ecosystems, 335-362.
[11] Ismail, L., Materwala, H., & Sharaf, Y. (2020, October). Blockhr-a blockchain-based healthcare records management framework: performance evaluation and comparison with client/server architecture. In 2020 International symposium on networks, computers and communications (ISNCC) (pp. 1-8). IEEE.
[12] Li, W., Wang, S., Xie, W., Yu, K., & Feng, C. (2023). Large scale medical image online three-dimensional reconstruction based on WebGL using four tier client server architecture. Information Visualization, 22(2), 100-114.
[13] Xu, L., Xu, C., Liu, J. K., Zuo, C., & Zhang, P. (2020). Building a dynamic searchable encrypted medical database for multiclient. Information Sciences, 527, 394-405.
[14] Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. IEEE Internet of Things Journal, 8(7), 5914-5925.
[15] Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108.
[16] Guo, H., Li, W., Nejad, M., & Shen, C. C. (2022). A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms. IEEE Transactions on Network and Service Management.
[17] Golubnychy, D., Kolomiytsev, O., Tretyak, V., Kliuchka, Y., &

INFORMATION AND WEB TECHNOLOGIES

Rybalchenko, A. (2022). Архітектура системи обміну медичними даними пацієнтів з лікарями на основі IOTA. Системи управління, навігації та зв'язку. Збірник наукових праць, 1(67), 57-61.

[18] Ключка, Я. О., Шматко, О. В., Євсеєв, С. П., & Милевський, С. В. (2021). Peculiarities of blockchain technology introduction in the field of healthcare: current situation and prospects. Системи обробки інформації, (1 (164)), 33-44.

[19] Rghioui, A., Lloret, J., Harane, M., & Oumnad, A. (2020). A smart glucose monitoring system for diabetic patient. Electronics, 9(4), 678.

[20] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500.

[21] Khang, A., Hahanov, V., Litvinova, E., Chumachenko, S., Hajimahmud, A. V., Ali, R. N., ... & Anh, P. T. N. (2023). The Analytics of Hospitality of Hospitals in a Healthcare Ecosystem. In Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem (pp. 39-61). CRC Press.