DOI:10.33942/sit042381 УДК: 004.89

BLOCKCHAIN КОЛДОНУУ МЕНЕН ООРУКАНАНЫН МААЛЫМАТ КООПСУЗДУГУ

Хан А.
PhD доктору, АЛА-ТОО Эл аралык университетинин профессору

Аннотация. *Blockchain технологиясы жасалма интеллект тармагында барган сайын маанилүү ролду ойноп жаткан жаңы демилгелерди жаратууда. Blockchain иштери жана тиркемелери, анын ичинде саламаттыкты сактоо тармагында, өзгөчө электрондук ден соолук жазуулары (EHR) үчүн ар түрдүү. Анткени EHR коргоону талап кылган өтө сезимтал маалыматтарды камтыйт. Protenus Breach Barometer маалыматына ылайык, 2022-жылы 60 миллиондон ашык жазуулар уурдалган же хакердик чабуулдар болгон. Blockchain эгер ишке ашырылса, EHRлердин коопсуздугун, купуялыгын жана жеткиликтүүлүгүн жакшыртат. Блокчейн технологиясы дагы эле салыштырмалуу жаңы болгондуктан, анын EHR менен интеграциясын жакшыртууга мүмкүнчүлүк бар. Бул документ Ethereum негизделген акылдуу келишимдерди, Interplanetary File System (IPFS) жана күчтүү симметриялык шифрлөө аркылуу борборлоштурулган оффлайн сактоону колдонуу менен саламаттыкты сактоонун EHR негизин сунуштайт. Платформа жазуулардын коопсуздугун камсыз кылат жана масштабдуу чечимди сунуштайт.*

Негизги сөздөр: *Электрондук медициналык жазуулар; блокчейн; Эфириум; Планеталар аралык файл системалары*

БЕЗОПАСНОСТЬ БОЛЬНИЧНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙНА

Хан А.
PhD доктор, профессор Международного университета АЛА-ТОО

Аннотация. *Технология блокчейн создает новые инициативы, которые играют все более важную роль в области искусственного интеллекта. Работа над блокчейном и его применение варьируются, в том числе в секторе здравоохранения, особенно для электронных медицинских карт (EHR). Поскольку ЭУЗ содержит высококонфиденциальные данные, требующие защиты. По данным Protenus Breach Barometer, в 2022 году было зарегистрировано, что украдено или взломано более 60 миллионов записей. Блокчейн может повысить безопасность, конфиденциальность и доступность EHR, если он будет реализован. Поскольку технология блокчейна все еще относительно нова, есть возможности для улучшения ее интеграции с EHR. В этом документе предлагается структура EHR в сфере здравоохранения с использованием смарт-контрактов на базе Ethereum, децентрализованного автономного хранилища с использованием межпланетной файловой системы (IPFS) и надежного симметричного шифрования. Платформа обеспечивает безопасность записей и предлагает масштабируемое решение.*

Ключевые слова: *Электронные медицинские карты; блокчейн; Эфириум; Межпланетные файловые системы.*

HOSPITAL DATA SECURITY USING BLOCKCHAIN

Khan Al
PhD Doctor, Professor of ALA-TOO International University

Abstract. *Blockchain technology has been creating new and fresh initiatives, with emerging role in AI since its inception. Work on Blockchain and its application varies, including in the healthcare sector, specifically for electronic health records (EHR). As EHR contains highly confidential data that requires protection. According to Protenus Breach Barometer,in 2022, more than 60 million records were reported stolen / breached. Blockchain has the potential to enhance security, privacy, and availability of EHR if implemented. As blockchain technology is still relatively new, there is room for improvement in integrating it with EHR. This paper proposes a framework for EHR in the healthcare industry using Ethereum-based smart contracts, decentralized off-chain storage utilizing the InterPlanetary File System (IPFS), and robust symmetric encryption. The framework ensures secure records and offers a scalable solution.*

Keywords: *Electronic health records; blockchain; Ethereum; Interplanetary file systems.*

Introduction.

As the role of Artificial Intelligence(AI) is increasing in our well being, more and more diversified means of technology enabled services being offered. From machine learning in disease diagnosis as in the research showed by Al khan [1] to blockchains as an advance method of security, privacy for services and data. The first decentralized blockchain was conceptualized by Satoshi Nakamoto in 2008, though the idea behind the blockchain goes well before this time. Blockchain technology a technique to time-stamp digital documents in such a way that nobody could back-date or offers use cases for banking but also any other business that needs monitoring of transactions. Blockchain is a system that use distributed ledgers to store records of all transactions conducted on the blockchain is made between two blockchain peers, the transaction is recorded and added to the blockchain Each transaction carries an immutable hash signature; this hash and demonstrates how hash signatures function during transactions; combined, they offer a well secured system.signature; this hash and demonstrates how hash signatures function during transactions; combined, they offer a well secured system.

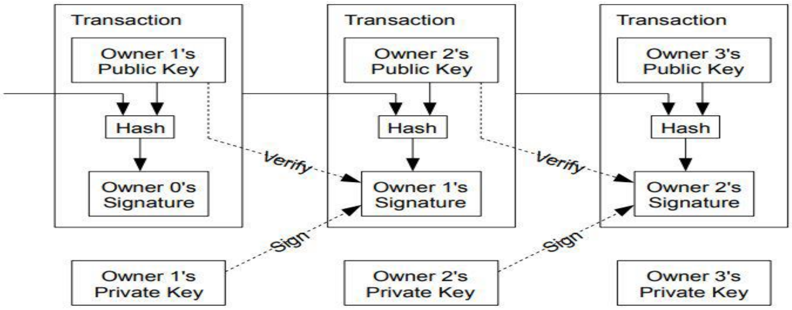

Fig 1: how hash signatures during transactions perform

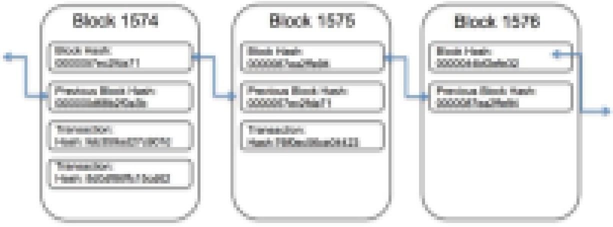

Fig 1.1 shows, how each block is linked together

Over time, blockchain technology has evolved and expanded with numerous new cryptocurrencies emerging. Other than Bitcoin, the Ethereum is second most widely used cryptocurrency which emerged in 2015. With Ethereum, a new blockchain with technology comparable to Bitcoin's system developed that enabled Ethereum incorporated smart contracts, which allow for logical code execution on top of the blockchain[2]. The healthcare industry involves huge amount of data and information that is highly sensitive and makes a storage challenge even for blockchains. The integration of blockchain into such domains can be achieved by storing non-sensitive values on the blockchain, which can then be linked to more sensitive data that is stored off-chain in a database. This is a prevalent scenario for electronic health records, where the actual record data is not stored on the blockchain, but a corresponding hash of the data is saved on the blockchain to create a connection between two points, without revealing the information in point B. It is important to emphasize that to ensure data security, encryption must be implemented on the data before saving it, as an attacker can access the related hash since it is public and retrieve the record, based on the database and smart contract logic.

Blockchain technology offers several significant benefits for hospital data security such as:

Immutable Data: Once data is recorded on a blockchain, it becomes extremely difficult to alter or delete. This immutability ensures the integrity of patient records, preventing unauthorized changes or tampering.

Decentralization: Blockchain operates on a decentralized network of computers, eliminating the need for a single central authority. This reduces the risk of a single point of failure and minimizes the vulnerability to cyberattacks.

Data Transparency: Blockchain provides transparency by allowing authorized parties to view transactions and changes to data. This transparency enhances accountability and trust among stakeholders.

Enhanced Data Privacy: Patient data is encrypted and stored securely on the blockchain. Patients have greater control over their data and can grant or revoke access to healthcare providers as needed, reducing the risk of data breaches.

Data Consistency: The distributed ledger ensures that all participants have access to the same, up-to-date information. This consistency reduces errors and discrepancies in patient records.

Improved Access Control: Blockchain allows for granular access control. Patients can specify who can access their medical records and under what conditions, ensuring that only authorized individuals or entities view sensitive information.

Audit Trails: Blockchain records a comprehensive history of data access and changes. This audit trail makes it easier to track any unauthorized access attempts or data breaches, aiding in forensic investigations.

Interoperability: Blockchain can facilitate interoperability between different healthcare systems and institutions. This seamless data sharing can improve patient care by providing a complete view of a patient's medical history.

Reduced Administrative Overhead: Smart contracts on blockchain can automate administrative tasks, such as claims processing and billing, reducing costs and the risk of errors.

Enhanced Trust: Patients and healthcare providers can have greater trust in the security and integrity of medical data stored on a blockchain. This trust can lead to improved patient outcomes and satisfaction.

Security Against Ransomware: Since blockchain data is decentralized and encrypted, it is less susceptible to ransomware attacks that often target centralized databases.

Regulatory Compliance: Blockchain can assist healthcare institutions in complying with data protection regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in Europe.

Efficient Data Recovery: In the event of data loss or a disaster, blockchain's distributed nature ensures data redundancy and makes recovery more feasible.

Secure Supply Chain Management: Blockchain can be used to track the authenticity and handling of medical supplies and pharmaceuticals, reducing the risk of counterfeit products entering the supply chain.

Research and Clinical Trials: Blockchain can securely manage and share data related to clinical trials and medical research, ensuring data integrity and traceability.

The healthcare deals with large volumes of data, some of which is very sensitive data such as medical histories, diagnoses, vital signs, prescriptions, and so on. In light of technological advancements, the healthcare sector has largely adopted the capabilities of electronic health records (EHR). As of 2022, 96% of all non-federal acute hospitals in the United States have implemented EHR [2]. EHR, in conjunction with well-established health information exchange (HIE) systems, delivers benefits such as lower healthcare expenditures and improved quality of treatment [3]. However, there are several problems when using digital technology to communicate extremely sensitive and personal information. Privacy and security are two important issues because as information becomes more accessible to more health care institutions and general public, it also becomes more prone to data breaching.

Although blockchain technology offers significant opportunities for the healthcare industry, particularly in the realm of electronic health records (EHR), there are still some concerns that need to be addressed. The three major issues are scalability, transparency, and key management. Scalability can be problematic due to the sheer size of EHR data, which can cause slow and lengthy transactions when stored on the blockchain. Transparency is also a concern, as all transactions are public and sensitive information must be kept confidential while still being recorded on the blockchain. To ensure privacy, EHR records must be encrypted; otherwise, they can be accessed by anyone, which is undesirable. As a result, patients and providers must securely store their blockchain account credentials as well as secret keys for encryption and decryption. This can be challenging for individuals without experience in cryptography, putting pressure on both patients and providers to manage their keys securely.

Several common elements can be found in many of the frameworks proposed by others, such as the utilization of intelligent contracts to aid in precise access control, and the use of off-chain storage instead of storing the data on the blockchain. Additionally, the frameworks tend to prioritize a patient-centric approach, where each patient has control over their own access privileges to their electronic health records. Among frameworks mostly make use of centralized databases to store electronic health records. However, this solution has a significant flaw, as a centralized database presents a single point of failure [4]. This means that if a breach occurs, all data is compromised. On the other hand, a distributed/decentralized database may be the preferred option when dealing with highly sensitive data such as electronic health records, as if one file is compromised, it does not necessarily mean that all other files have been compromised. Furthermore, due to the decentralization, it is impractical to modify a file within the decentralized database, as it would require confirmation from several nodes. This provides additional protection for the data stored in the decentralized database. It is crucial to use encryption to keep sensitive data within electronic healthcare records secure, particularly as data breaches in the healthcare field are on the rise. If a hacker gained access to the information in a record, they could potentially commit identity theft and use the information for serious and harmful crimes. However, [5] and [6] do not offer any encryption options for their stored data, which could make their frameworks less secure.

This paper attempts to propose a secure electronic health records efficiently with the use of decentralization. The proposed system makes use of the Ethereum blockchain and the distributed file system InterPlanatery File System (IPFS). Together it creates a scalable decentralized solution for storing and exchanging electronic health records thus enabling a secure framework for Healthcare using blockchain.

Literature review

While blockchain is a rather novel technology, there have been some research and framework proposals for the use of blockchain for securing and exchanging big data in several domains. One of the first major framework proposals for electronic health records and the use of blockchain is MedRec [7]. Furthermore, MedRec makes use of off-chain storage for the records with the help of a local database based on SQL. Ancile and BHEEM are two more framework proposals, which makes use of a similar approach as MedRec. While [8] makes use of two different encryption methods to store and distribute the records. The two methods in use by the Ancile framework is symmetric encryption due to it being more efficient for larger files [9]. However, the encryption during the distribution is done through asymmetric and the use of proxy re-encryption. Proxy re-encryption works as following, person A generates an encryption key which he/she delegates to a proxy. Person B decrypts using his/her private key [10]. Madine et al. [11] presented a blockchain-based patient-centric paradigm for personal health records (PHR). They, like others, employ the Ethereum network and smart contracts to build the access control core of their system. To address scalability difficulties, they employ IPFS in conjunction with proxy re-encryption. The fundamental distinction between the proposed framework is the patient-centric approach. Matos et al. proposed a system architecture and solution for managing electronic health records (EHR) using cloud services and granular access control. The objective was to provide a scalable and secure solution for EHR in which a patient or provider may access the required record from anywhere in the globe. The EHR storage is an intercloud; an intercloud is a method of chaining solitary clouds together to form a mass of clouds, which is then referred to as an intercloud or cloud of clouds. Interclouds provide advantages in that they allow end-to-end privacy for cloud applications and make data migration across providers easier. Matos et al. also define their access control procedure as reliant on authentication and a privilege check. While the system's ultimate purpose was to ensure a patient's privacy, it is nevertheless vulnerable to vulnerabilities that result in a criminal having access to data he or she should not have.

The framework Action-EHR was introduced by Dubovitskaya et al [12]. It operates on the Hyperledger Fabric, a blockchain framework that is private and permissioned, providing enhanced authentication and authorization compared to public blockchains where any node can connect and view transactions. Like the Ethereum network, Hyperledger Fabric enables the creation of smart contracts. Action-EHR utilizes smart contract logic in the same way as other frameworks, with the primary goal of storing state variables related to access control for a patient’s health records. Rather than a local database, Action-EHR employs HIPAA compliant cloud storage. This type of storage ensures that the information stored maintains its confidentiality, integrity, and availability to the best of their ability. Amazon S3 is the specific cloud storage service used in Action-EHR. Before uploading a record to the cloud, it is encrypted using a symmetric key approach. The symmetric key is then encrypted with the public key of the patient and the doctor to whom the patient has granted access. To decrypt the record, the doctor uses their private key to retrieve the symmetric key, which is then used to decrypt the data. The researchers suggest using only a symmetric key to simplify key management. If a patient has multiple doctors with whom they wish to share their records, they only need to upload once. In contrast, the previous approach required separate data uploads for each doctor requiring access. The researchers conclude their paper by stating that the prototype meets medical requirements and that their next step is to establish a test network and evaluate it from the perspective of a real healthcare institution.

Methodology

We shall outline the many features and details of the proposed system and. Also will concentrate on providing a high-level overview of system architecture and design.

The objective is to share and maintain electronic health records in encrypted format. The system's logic and technological stack are transparent and made visible through algorithms and well-explained subtext. The experiment is carried out using design science methodology. There are various needs for a system to function properly, and describing them all would be repetitive. Therefore, the following requirements as being absolutely necessary for developing a safe storage and exchange system for electronic health records are defined, given as:

Entering various details

Right for the patients to access, update/ modify, update the records.

Users and patients to be able to download the records according to the accessing rights assigned.

All data uploaded in encrypted format.

The Tools

The suggested framework is a decentralized application (dApp). The back-end and front-end of the dApp are programmed to be linked through the usage of the Node.js which is a runtime environment for JavaScript. The smart contracts are stored in the framework's backend. The smart contracts were created utilizing the Solidity programming language and the combination of truffle and ganache. Truffle is an Ethereum development framework that facilitates the creation and deployment of smart contracts [13]. Ganache was used as it is a personal Ethereum blockchain that simplifies the testing and execution of smart contract functionality[14].

The front-end is constructed with React.js, a JavaScript framework designed for simple interaction with HTML and JavaScript for designing user interfaces. Furthermore, the front-end requires a cryptocurrency wallet; MetaMask was utilized in this system, and it allows users to connect with an account to the blockchain network, which is required to be present in the system and complete transactions.

System architecture

The architecture for the proposed framework will be reviewed and discussed in this section as shown in Figure 3. The framework has been built and continuously revised as the implementation progressed.

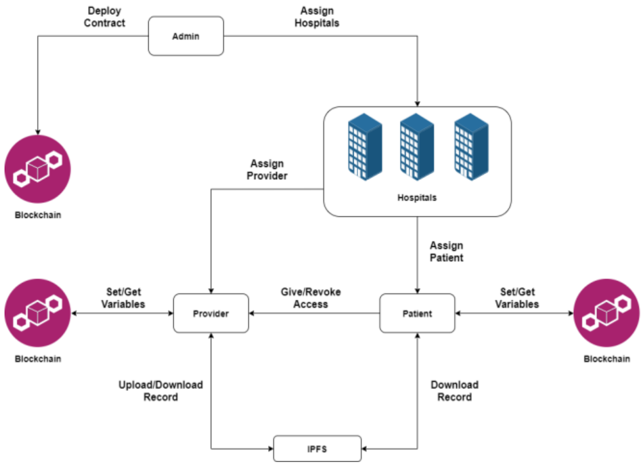

Fig 3: Architecture of proposed framework

Administrator

The Administrator node is the starting node from where the architecture begins. The Administrator node is built and controlled by the smart contract. The Administrator job is to allocate Hospital nodes to certain Ethereum addresses. All other nodes on the blockchain are redundant in the absence of the Administrator node. When the Administrator assigns a hospital or hospitals, the state variables pertaining to the hospital's information, such as hospital name, city, and Ethereum address, are saved on the blockchain. Hospitals assign the Ethereum addresses to either providers or patients; similarly to hospitals, the patient or provider state variables are recorded in the blockchain. The patient node contains identifiers such as Ethereum address, gender and, also contains a list of the users that are allowed to access the patient health records. It is the node’s responsibility to update by giving permission or revoke access from a certain user. Identifiers such as Ethereum Address and Speciality can be found on a provider node. The provider node can generate and edit health records as well as access a patient's previously established health record. The provider must, however, be added to the patient node access list. The important result of combining blockchain with electronic health records is that the data in the records is securely kept. As a result, the treatment of data is critical in any suggested framework for blockchain and health records. In the suggested framework, the first step in creating a record is the patient providing consent to a provider. The provider can now produce a record with the patient's permission; once made, the record is uploaded to IPFS and encrypted with the symmetric encryption technique AES; the hash of the record is generated and stored in the blockchain. If the provider wants to access the record, he or she enters the file's hash and downloads the encrypted version of the record. The record may now be decrypted by the provider or patient using the same key that was produced during the encryption process. This key would have to be kept secure and only shared with the doctors and patients who need access to the record. The framework design is divided into four major tiers which are: the UI layer, the Blockchain layer, the Contract layer, and the Data layer. This subsection will describe the role of each layer in the system beginning at the bottom, as shown in figure 4.6.

The contract layer

The contract layer includes every smart contract that is implemented on the blockchain. The fundamental role of smart contracts is to carry out transactions between two peers on the blockchain where specific conditions must be satisfied for the smart contract's features to properly execute. The idea underpinning smart contracts is designed to create granular access control to the system's numerous transactions in order to prevent illegal access. The following are the numerous transactions that are possible within the system:

1. Addition of node/user.
2. Give/Revoke access to patient’s record.
3. Set hash of patient’s record.
4. Get hash of patient’s record.

Integration and Coding

Algorithm 1 defined the rationale behind the function of adding a hospital, which is available to the administrator node after the smart contracts have been deployed. The method takes three inputs: a MetaMask account’s public key address, a city, and a name. If the functions’s caller is not an administrator, the function is aborted and error message is displayed; also, if the public key assigned is already in the mapping of existing hospitals, the function is cancelled and an error message is displayed. Each hospital node constructed on the blockchain can assign a patient or provider role to a public key. Algorithm 2 adds the provider node, which requires the provider's public key and specialization as input. The public key cannot already be assigned, and the function caller must be a hospital. Algorithm 3 is similar to Algorithm 2 in that it adds a patient node; the reasoning is similar in that the caller of the function must be a hospital and the public key cannot already be assigned. On the addition of a patient node and a provider node to the system, each patient gains the option to grant or revoke access to a provider. By granting access, the provider can set and obtain hashes of a patient's record, but revoking access prevents the provider from setting or retrieving hashes of a patient's record. Algorithm 4 demonstrates when access is granted by utilizing the public key of the provider node to whom access should be granted. By using the same input of a provider's public key, Algorithm 5 determines when access should be canceled. The set hash and get hash functions are the final two algorithms of the smart contract layer. They are straightforward setters and getters that have a role for the Data layer's off-chain storage. Algorithm 6 demonstrates the set hash, which involves a public key and a hash that must be submitted and saved in a patient's list of hashes. Algorithm 7 demonstrates the get hash, which accepts an input of an index and uses a list of hashes to obtain the proper index's hash. Once more, a public key is also utilized as an input. To further generate optimization in the codes and algorithms Machine learning technique was applied for code quality[15].

Blockchain layer

The proposed architecture makes use of Ganache, which enables the creation of a test blockchain network that is comparable to Ethereum Mainnet. In the blockchain layer, every transaction that takes place between two peers is monitored and recorded. using blockchain The deployed smart contracts are held on a separate layer.

Data layer

The proposed architecture uses InterPlanetary File System (IPFS), a distributed file system as off-chain storage. The cryptographic hash of the 21 files that were uploaded to IPFS are provided through a transaction and saved as a patient variable using smart contract logic when a file is uploaded and submitted through the UI layer, as illustrated in Algorithm 6. This hash variable is then utilized when patients or providers want to access a specific record utilizing Algorithm 7 and other UI layer functions.

UI layer

The front-end of the system, which was created using React, is referred to as the UI layer. The UI layer's goal is to make the process easier for users and to get the arguments required for the system's essential tasks. The integration is also included in the UI layer of MetaMask, enabling each node assigned to the system to carry out different operations based on the user's role. Last but not least, when uploading to and downloading from IPFS, the UI layer manages communication with the Data layer (IPFS) and the encryption and decryption of the electronic health information. The process of encryption and decryption is essential to the system. An electronic health record must first be encrypted using AES, and a secret key must be established. This key will later be used for decryption. In order to avoid human mistake and selecting a weak and non-random key, the system uses a random bytes generator to produce the key. The record that the provider wants to upload is automatically encrypted when a key is produced, and the key is printed to the provider. The UI layer then uses an API request to add the file to IPFS. The API response includes a hash, which is then used to use Algorithm 6 to put the hash on the blockchain. Algorithm 8 provides a complete overview of the uploading procedure. When a patient or healthcare provider interacts with a computer, a process comparable to encryption takes place downloads a specific dataset with the intention of decrypting it, but no key is generated.To obtain the correct hash of the record they wish to decrypt and download, the user calls Algorithm 7 in this case. The user is then prompted to download a file that can be correctly decrypted using the same encryption key. Algorithm 9 displays the algorithm for downloading and decrypting the record.

Conclusion

The goal of this project was to employ the innovative technology blockchain to secure electronic health records. The proposed system relies on Ethereum smart contracts, decentralized storage through IPFS, and symmetric encryption to build a solid and resilient solution for securely transferring electronic health information between patients and doctors. It does this by storing reference variables on the blockchain while sensitive information from health records is encrypted and saved off-chain on IPFS, as well as keeping system users secret by limiting the number of IDs each user has. Specific security aspects are discussed and evaluated in the form of research questions, and the overall result demonstrates that the integration of blockchain and distributed off-chain storage provides several benefits that support confidentiality, integrity, availability, privacy, and scalability because big data is stored off-chain.

Bibliography:

1 Al Khan (2022) Machine Learning for Chronic Disease Prediction. CEOS Public. Health. Res. 1(1):101

2 V. Buterin, "Ethereum: A next-generation smart contract and decentralizedapplication platform," 2013. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

3 Pablo RJ, Roberto DP, Victor SU, Isabel GR, Paul C, Elizabeth OR. Big data in the healthcare system: a synergy with artificial intelligence and blockchain technology. J Integr Bioinform. 2021 Aug 18;19(1):20200035. doi: 10.1515/jib-2020-0035. PMID: 34412176; PMCID: PMC9135137.

4 Bhalibar, Kriti and Singh, Abhay and Sharma, Himani and Uphadyay, Ashish and Gupta, Himanshu, Centralize Storage System with Encryption vs Decentralize Storage System Using Blockchain (May 25, 2022). Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022, Available at SSRN: https://ssrn.com/abstract=4119952 or http://dx.doi.org/10.2139/ssrn.4119952

5 Han Y, Zhang Y, Vermund SH. Blockchain Technology for Electronic Health Records. Int J Environ Res Public Health. 2022 Nov 24;19(23):15577. doi: 10.3390/ijerph192315577. PMID: 36497654; PMCID: PMC9739765.

6 A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE Access, vol. 7, pp. 147 782–147 795, 2019

7 D. R. Matos, M. L. Pardal, P. Adão, A. R. Silva, and M. Correia, "Securing electronic health records in the cloud," in Proceedings of the 1st Workshop on Privacy by Design in Distributed Systems, ser. W-P2DS'18. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: https: //doi-org.proxy.lnu.se/10.1145/3195258.3195259.

8 Vanin, F.N.d.S.; Policarpo, L.M.; Righi, R.d.R.; Heck, S.M.; da Silva, V.F.; Goldim, J.; da Costa, C.A. A Blockchain-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach. Sensors 2023, 23, 14. https://doi.org/10.3390/s23010014

9 G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacypreserving framework for access control and interoperability of electronic health records using blockchain technology," Sustainable Cities and Society, vol. 39, pp.
283–297, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210670717310685.

10 Moody D, Peralta R, Perlner R, Regenscheid A, Roginsky A, Chen L. Report on Pairing-based Cryptography. J Res Natl Inst Stand Technol. 2015 Feb 3;120:11-27. doi: 10.6028/jres.120.002. PMID: 26958435; PMCID: PMC4730686.

11 M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," IEEE Access, vol. 8, pp. 193 102–193 115, 2020.

12 A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, and F. Wang, "Action-ehr: Patient-centric blockchain-based

electronic health record data management for cancer care," Med Internet Res, vol. 22, no. 8, p. e13598, Aug 2020

13 Alolayyan, Main & Alyahya, Mohammad & Alalawin, Abdallah & Shoukat, Aftab & Nusairat, Farid. (2020). Health information technology and hospital performance the role of health information quality in teaching hospitals. Heliyon. 6. 10.1016/j.heliyon.2020.e05040.

14 Raghupathi, W.; Raghupathi, V.; Saharia, A. Analyzing Health Data Breaches: A Visual Analytics Approach. AppliedMath 2023, 3, 175-199. https://doi.org/10.3390/appliedmath3010011

15 A. Khan, R. R. Mekuria and R. Isaev, "Applying Machine Learning Analysis for Software Quality Test," 2023 International Conference on Code Quality (ICCQ), St. Petersburg, Russian Federation, 2023, pp. 1-15, doi: 10.1109/ICCQ57276.2023.10114664