IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A BLOCKCHAIN-BASED PRIVACY AND ACCESS CONTROL FOR ENHANCED EHR SECURITY

[1]Ganta Santosh,[2]Prof.K.Venkata Rao
[1]M. Tech Student, [2]Professor
[1,2]Department of CS & SE, AUCE, Andhra University, Visakhapatnam

ABSTRACT:
An Electronic Health Record (EHR) represents a digital rendition of a patient's complete medical history, meticulously maintained by healthcare providers. The sharing of EHRs plays a pivotal role in healthcare, facilitating seamless communication among different medical institutions. However, the prevalent use of cloud-based EHR sharing systems raises concerns regarding patient privacy and data security. The centralization of data in cloud servers can potentially expose sensitive information to vulnerabilities.Blockchain technology emerges as a promising solution to address these challenges, owing to its distinctive attributes of decentralization and tamper resistance. This paper advocates for the adoption of Blockchain-Based Privacy and Access Control to enhance EHR security. The primary objective of this proposal is to implement blockchain technology for EHRs, ensuring the secure storage of electronic records while precisely defining access permissions for authorized users.
To achieve this, we employ a Hybrid Encryption approach, combining Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) techniques for sharing medical records securely. Additionally, we model the relationships between EHR owners and EHR users using smart contracts, which operate within the Ethereum blockchain ecosystem. These smart contracts facilitate the enforcement of access control policies, ensuring that only authorized individuals can access and modify EHR data.Our evaluation of the proposed system centers on the efficiency of encryption and decryption processes, measuring the time required to safeguard and retrieve EHR data. By integrating blockchain technology, we aim to establish a robust and secure framework for managing electronic health records, safeguarding patient privacy, and enhancing data security in the healthcare sector.

Keywords: Ethereum Blockchain, EHR, Hybrid Encryption.

1. INTRODUCTION:

An Electronic Health Record (EHR) comprises an individual's comprehensive health-related data, encompassing personal information, medical images, medical conditions, and medication history. Sharing EHRs holds the potential to benefit both patients and healthcare institutions in several significant ways, as outlined in HIMSS (2006). It can facilitate medical research, enable cross-border cooperation among healthcare providers, and establish robust regulations and standards to promote secure EHR sharing, instill trust among medical entities, enhance patient care, and advance medical science.
However, the increasing reliance on cloud storage for EHRs, with its associated advantages, also introduces security challenges that hinder the widespread adoption of cloud-based e-health applications, as noted by Abukhousa et al. (2012). Despite the broader availability of EHRs, their utilization remains limited due to security concerns, as indicated by Sauermann et al. (2013). Technological hurdles persist, impeding EHR sharing and complicating its implementation. Consequently, one of the most significant challenges in healthcare systems today revolves around securely sharing medical data. This sharing paradigm gives rise to numerous privacy and security issues, potentially impeding its widespread acceptance, as discussed by Boumezbeur and Zarour (2018). The

sensitive nature of this data makes patients and medical organizations wary of sharing it, emphasizing the need for protection against unauthorized access. Security concerns include safeguarding the secure sharing of EHRs among patients and various healthcare services within cloud environments. Unauthorized access to EHRs without patient consent poses significant risks, compromising data privacy, security, and the integrity of cloud-based e-health systems. Additionally, patients may face challenges in monitoring and managing their cloud-based health records shared by healthcare providers. Therefore, proposing suitable access control solutions for EHR sharing within cloud environments becomes imperative.

In recent times, the adoption of blockchain technology has emerged as a significant development in enhancing medical and e-health services. Satoshi Nakamoto initially introduced blockchains through the popular cryptocurrency Bitcoin (Shuaib et al., 2014). Blockchains operate on a decentralized architecture and consist of an open and distributed ledger that records transactions efficiently, verifiably, and permanently (Rajput et al., 2019). Individual transactions are organized as interconnected blocks within a single chain, with each transaction being authenticated by a network of interconnected validating nodes before being appended to the blockchain (Siddiqui et al., 2020a; Siddiqui et al., 2020b). Unlike traditional databases, blockchains enable members in a distributed network to exchange electronic currency without the need for a centralized, trusted third party (Agbo et al., 2019; Hardin and Kotz, 2019). Transaction validation is decentralized and relies on validators, typically miners, eliminating the need for centralized intermediaries (Hölbl et al., 2018).

Blockchain technology's immutability and use of cryptographic functions for secure communication make it well-suited for secure EHR information sharing (Gordon and Catalini, 2018; Catalini and Gans, 2020). This technology has the potential to revolutionize the healthcare system in various aspects, including secure EHR exchange and data access control among different medical institutions to enhance privacy and data protection (Mayar et al., 2020). It offers a promising approach to collaborative clinical decision-making in telemedicine and precision medicine (Cheng et al., 2018) and has the potential to transform the exchange of health information (HIE) by making EHRs more secure and efficient. As a result, numerous blockchain companies, such as HealthNautica, Factom, Capital One, and Gem, are actively collaborating to leverage blockchain technology for preserving medical data.

This article proposes a privacy-preserving EHR sharing scheme that combines cloud storage and blockchain technology. Cryptography plays a vital role in securing and safeguarding users' personal information within this proposal. In this scheme, original EHRs are securely uploaded to the cloud in an encrypted format, with only signature and encryption keys retained on the blockchain. Smart contracts, responsible for managing access control, facilitate secure data sharing among users. Patients retain full control over their EHRs within this new system, ensuring that users and healthcare providers can practically utilize the data without compromising patient privacy. The primary contributions of this paper can be summarized as follows:

1. Proposing a blockchain-based cryptographic and access control scheme for EHR sharing, leveraging Ethereum smart contracts.
2. Utilizing a combination of symmetric and asymmetric encryption algorithms to secure EHRs and secret keys, ensuring confidentiality and privacy.
3. Implementing smart contracts within the proposed scheme to manage user access control, ensuring that data owners maintain control over who can access their health records.

Performance analysis of the proposed framework using cloud computing usability tests conducted on the Google Storage Platform (GSP) and Ethereum blockchain with Solidity for smart contract implementation, demonstrating the feasibility of the suggested approach.

The remainder of this paper is structured as follows: Section 2 provides an overview of related work, while Section 3 delves into the system architecture, workflow, and smart contract details. Section 4 offers a comprehensive analysis and discussion of the proposal's performance. Finally, Section 5 concludes the paper.

2. LITERATURE SURVEY

Li et al. (2018) introduced a novel Data Preservation System (DPS) built upon blockchain technology, providing a secure storage solution that ensures data integrity and verifiability while safeguarding user privacy. The DPS harnesses data storage mechanisms and cryptographic algorithms to bolster security.Thwin and Vasupongayya (2019) proposed an access control model for Personal Health Records (PHRs) leveraging blockchain. Their approach employs proxy re-encryption and cryptographic techniques to uphold confidentiality. Encrypted records are stored in the cloud, while metadata resides on the blockchain. Notably, the data sharing process relies on an intermediary, a proxy server responsible for re-encryption and key management, adding an extra layer of security.

Wang et al. (2018) presented a secure Electronic Health Record (EHR) system based on blockchain technology and a cryptosystem mechanism. This system offers fine-grained access control, ensuring authentication and confidentiality of cloud-stored EHR medical data. They introduced a novel cryptographic technique called hybrid attribute/identity-based encryption and signature (C-AB/IB-ES). Attribute-Based Encryption (ABE) and Identity-Based Encryption (IBE) are used for data encryption, while Identity-Based Signature (IBS) is employed for digital signatures.

HBasechainDB (Sahoo and Baruah, 2018) is a scalable blockchain framework integrated with the Hadoop database. It leverages blockchain pipelining and federated consensus to create blocks. The blockchain framework, although dependent on Hadoop, stores blocks in the Hadoop database, enhancing scalability. This study highlights the potential of combining blockchain with other scalable platforms to address scalability challenges while exploring data stored within the blockchain.Xia et al. (2017) proposed a blockchain-based Data Sharing (BBDS) scheme focused on access control policies for sensitive health data. The BBDS emphasizes identity-based authentication to enhance healthcare system efficiency. It employs cryptographic techniques within a blockchain network to reinforce security measures, ensuring the integrity and confidentiality of shared health data.

3. METODOLOGY

3.1 Proposed System:

The objective of the proposal is to implement EHR blockchain technology and ensure that electronic records are safely stored by specify access permissions for users. We use Hybrid Encryption techniques (AES + ECC) for sharing medical records and We model the relationships between the EHR owner and EHR user using smart contracts through the proposed system on the Ethereum blockchain.

3.2 System Architecture:

The system architecture of the proposed privacy-preserving and access control scheme for sharing Electronic Health Records (EHRs) using blockchain technology (BAcP-EHR) is depicted in Figure 1. This architecture ensures the secure sharing of EHR data while preserving privacy and access control.

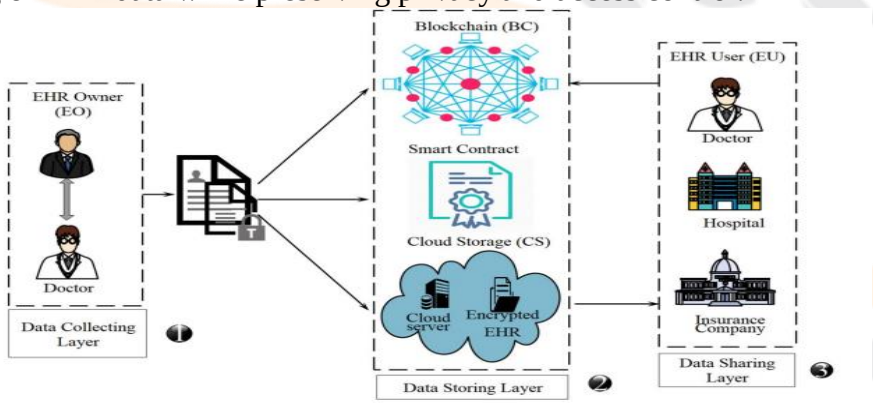

Figure 1: Proposed System Architecture

3.2.1 Encryption and Cloud Storage:

EHR data is first encrypted using the EHR owner's secret key to maintain confidentiality.The encrypted EHR is then securely stored in cloud storage, transmitted via a secure socket layer (SSL) to ensure data protection. To enhance security, the secret key is further encrypted using a public key.

3.2.2 Blockchain Component: The encryption key, along with all essential information, is stored on the blockchain for authentication purposes. The blockchain component is responsible for storing smart contracts, EHR signatures, and encrypted keys.

3.2.3 Three-Layered Framework: The proposed framework comprises three layers:

Data Collecting Layer: This layer involves patients visiting healthcare providers for treatment. The primary entity in this layer is the EHR owner (EO), who owns the EHR data to be shared. The EO has complete control over their EHR and can establish access control policies, granting or denying access permissions to others as needed.

Data Storing Layer: This layer includes two entities:

Cloud Storage (CS): The cloud repository stores the encrypted EHRs uploaded by the EO.

Blockchain (BC): The blockchain serves as a repository for smart contracts, EHR signatures, and encrypted keys.

Data Sharing Layer: In this layer, the EHR user (EU) is an entity that can be an individual (e.g., patient, doctor) or an organization (e.g., hospital, health insurance company, medical research institute). They access the patient's EHRs for various legitimate purposes.

3.2.4 Overall Architecture Workflow:

Step 1: Interactions between the patient and their healthcare provider generate primary data, including patient records, current medical issues, and other physiological information.

Step 2: The EHR owner uploads the encrypted EHR to cloud storage. Simultaneously, the encrypted keys and other essential information are transmitted to the blockchain.

Step 3: The EHR user sends a request to the blockchain to access the EHR, retrieve it, and subsequently decrypt it for legitimate use.

This architecture ensures secure EHR sharing, where the EHR owner maintains control over their data, and authorized users can access and use the EHRs while preserving data privacy and security.

3.3 System Workflow:

The proposal enables EHR owners to control their own EHRs. Based on cryptography techniques and blockchain technology, it performs privacy-preserving EHR sharing through the following steps.

3.3.1 System setup: To implement the Hybrid Encryption scheme, users should register unique accounts and create their keys. First, a symmetric key (SK) 128 bits in length is generated for each EO. The SK is the output of the hash function (SHA-1) employed by the SUN provider's pseudo-random number generation (PRNG) algorithm termed SHA1PRNG. The hash function is used to generate a stream of random numbers. The SK of an advanced encryption standard (AES) is used to encrypt the EHR. Each user in the blockchain obtains key pairs (PuK, PrK) by hashing a random number (RN) utilizing the 256-bit SHA-1 hash function to complete data sharing transactions. The key pair of the ECC asymmetric key encryption was used to encrypt SK and sign the original EHR.

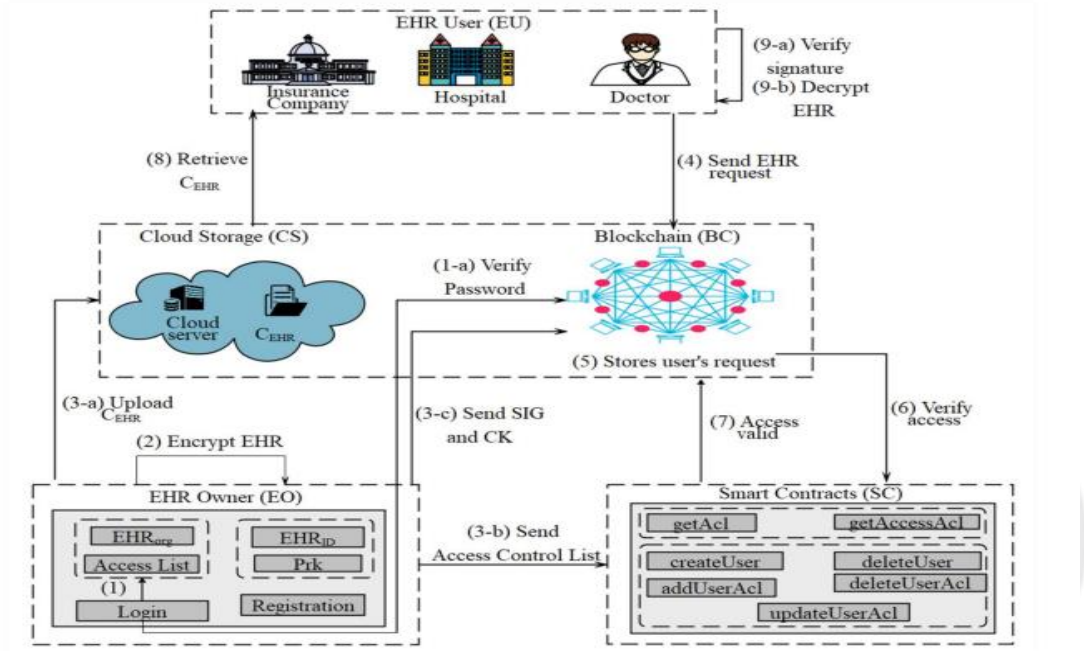

Figure 2: Workflow of proposed system

3.3.2 Data storing: After generating all the keys, the EO encrypts the EHR using the SK to get the ciphertext CEHR, then encrypts his/her symmetric encryption key using the public key PuK to get the ciphertext key CK, as shown in Equations (1) – (2).

$$C_{EHR} = Enc_{EHR}(EHR_i\ (i \in [1;8]), SK) \quad (1)$$

$$C_K = Enc_{Key}(SK, PuK) \quad (2)$$

After that, he/she creates a hash of the encrypted EHR to be signed using Equation (3), where MD is the message digest. The private key is then used to sign the MD, and the encrypted hash is the digital signature (SIG). When the signature algorithm is completed, the EO sends the encryption EHR (CEHR) to the cloud storage, as described in Equation (4).

$$MD = H(C_{EHR}) \quad (3)$$
$$SIG = (MD, PrK) \quad (4)$$

Then, he/she sends both SIG and encrypted keys (C_K) to the blockchain. Besides, he/she sends the access permissions to the smart contract as presented in 3.5 below. For example, all users' public keys are stored in the system database. If B (the owner) wants to share data with C (add C to the list of approved users), the SK will be re-encrypted with the public key of C. When C needs to access data, he/she can decrypt them using its private key. Because only C has access to C's private key, no one else can decrypt the data. The storage process is shown in Algorithm 1

Algorithm 1. Data storing level.
1: Input EHRi, Access control, PuK, PrK, SK, SHA-2
2: For each EHR data do
3: Use SK to encrypt EHR $C_{EHR} = Enc_{EHR}$ (EHRi (i∈ [1 ;8]), SK).
4: Use PuK to encrypt SK, $C_K = Enc_{Key}$ (SK, PuK).
5: Use SHA-2 to create MD on encrypted EHR, MD= H(EncEHR).
6: Use PrK to sign MD, SIG = (MD, PrK).
7: Store user's Puk in the system's database.
8: Upload C_{EHR} to the CS.
9: Upload C_K and SIG to the BC.
10: End for;
11: Output C_{EHR}, C_K, SIG.

3.3.3 Data sharing: The EHR owner predefines access rights in smart contracts, such as access privileges, access actions and access rights (e.g., read, write), to ensure the secure sharing of EHR. The smart contract is activated immediately before the access condition is met, which will ensure the validity and fairness of the sharing of data to implement the corresponding procedure. The process of EHR sharing consists of the following two sections:

A.Blockchain access:

EHR access request: The EU initiates a blockchain network EHR exchange request (Req) transaction. The access target (ID), access EHRi and PrK must be included in the request, as shown in Equation (5). The blockchain receives the transaction request and verifies the EU's identification. Only the EU is fair, and the transaction data will be stored in the blockchains.

$$Req = (ID \| EHR_i \| PrK);\ i \in [1\ ;8]) \quad (5)$$

Execution of the smart contract: If the Req is valid, the SK will be decrypted using the EU's private key and sent to the user, as described in Equation (6).

$$SK = Dec_{CK}\ (CK, PrK) \quad (6)$$

B. Cloud storage EHR sharing: As seen in Algorithm 2, the EU will recover the EHRi from the cloud. Then, to achieve the integrity and authenticity of the EHR, the EU creates a hash of the encrypted EHR, MD2, as shown in Equation (7). Then, he/she uses the EO's public key to decrypt the SIG; the result of the decryption is shown in Equation (8).

$$MD_2 = H(C_{EHR}) \quad (7)$$
$$Dec_{SIG} = (SIG, PK) \quad (8)$$

If this decrypted MD matches MD2, the signature is correct, and the EU will decrypt the EHR and perform its access action, as described in Equation (9). If not, the user can inform the system that the data may have been changed.

$$EHR_i = Dec_{CEHR}\ (C_{EHR}, SK) \quad (9)$$

Algorithm 2. Data sharing level.
1: Input SK, PrK.
2: If Req is not valid then
3: 'return failure'.
4: Else
5: Decrypt EncKey, SK= DecCK (Ck, PrK).
6: Retrieve CEHR from the CS.

7: Create MD_2= H(C_{EHR}).
8: Decrypt SIG, Dec_{SIG}= (SIG, PK) to get the MD.
9: IF the two MD do not match then
10: 'return failure'.
11: Else
12: Decrypt C_{EHR}, EHR_i= Dec_{CEHR} (CEHR, SK).
13: End If
14: End If
13: Output EHR_i

4. RESULTS

We initially conducted tests to measure the time required for encrypting and decrypting blockchain data for various sizes of Electronic Health Records (EHRs). Figure3 illustrates the encryption and decryption process times for Thwin and Vasupongayya (2019), Wang et al. (2018), and our Hybrid Encryption scheme. Notably, the Hybrid Encryption scheme exhibits consistent time efficiency, regardless of the EHR size.

We proceeded to compare our test results of encryption and decryption time consumption with those of Thwin and Vasupongayya (2019) and Wang et al. The comparative outcomes are depicted in Figure 4 and Figure 5, revealing that our scheme boasts faster encryption and decryption processes. Particularly, when dealing with large EHRs containing substantial image files like X-rays and CT scans, our scheme significantly outperforms Thwin and Vasupongayya (2019) and Wang et al. (2018), making it a more suitable choice for securing health record data.

Work	Work Wang et al. (2018)		Thwin and Vasupongayya (2019)		Hybrid Encryption	
File size	Encryption	Decryption	Encryption	Decryption	Encryption	Decryption
128 KB	0.366	0.162	0.092	0.0032	0.017	0.0009
512 KB	0.371	0.170	0.094	0.0064	0.018	0.0011
2 MB	0.376	0.180	0.101	0.0166	0.019	0.0054
8 MB	0.423	0.226	0.142	0.0592	0.059	0.0315
32 MB	0.593	0.405	0.303	0.2383	0.109	0.1055

Figure 3: Encryption and Decryption comparison

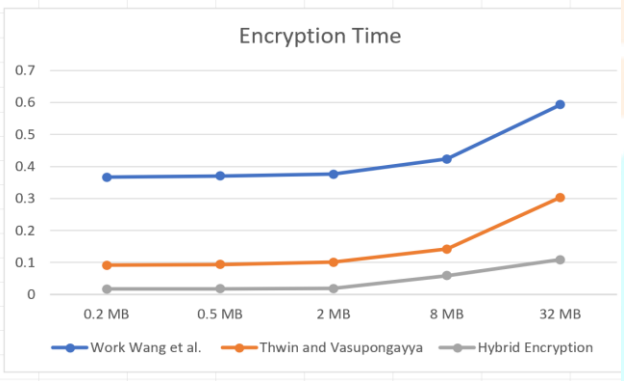

Figure 4: Encryption Process comparison

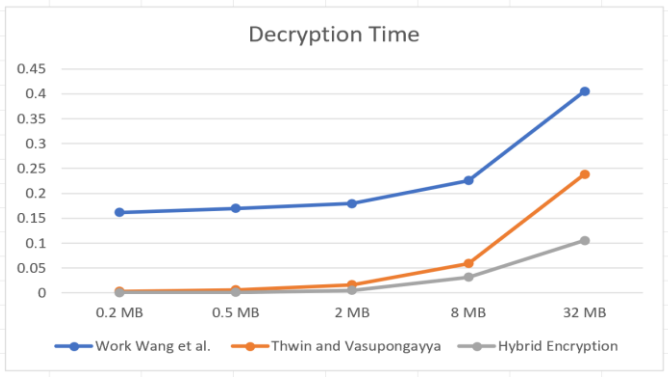

Figure 5: Decryption process comparison

5. CONCLUSIONS:

This paper presents a blockchain-based access control scheme aimed at preserving the privacy of electronic health records (EHRs), with a focus on achieving privacy, confidentiality, integrity, and access control. The system leverages Ethereum blockchain technology and cloud storage to ensure secure storage of electronic records by defining precise user access rules. Initially, a framework for EHR sharing among various entities is proposed, with cloud storage housing encrypted EHRs, and EHR signatures stored on the Ethereum EHR blockchain. Access controls for EHRs are established through Ethereum blockchain smart contracts to facilitate efficient and secure access. The scheme employs both symmetric and asymmetric encryption techniques to ensure data confidentiality while enabling privacy-preserving data sharing. Implementation on the Ethereum platform is carried out, with performance evaluation demonstrating the scheme's

security objectives. Future work includes exploring extensions and enhancements to the system, such as the development of a blockchain-based fraud detection system in healthcare.

7. REFERENCES

[1] AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health Cloud: Opportunities and Challenges. Future internet, 4(3),621–645. https://doi.org/10.3390/fi4030621

[2] Abunadi, I., & Kumar, R. L. (2021). BSF-EHR: blockchain security framework for electronic health records of patients.Sensors, 21(8), Article no. 2865. https://doi.org/10.3390/s21082865

[3] Agbo, C., Mahmoud, Q., & Eklund, J. (2019). Blockchain Technology in Healthcare: A Systematic Review. Healthcare, 7(2),56. https://doi.org/10.3390/healthcare7020056

[4] Boumezbeur, I., & Zarour, K. (2018). Privacy Preserving Requirements for Sharing Health Data in Cloud. In InternationalConference Europe Middle East & North Africa Information Systems and Technologies to Support Learning (pp. 412-423).Springer. https://doi.org/10.1007/978-3-030-03577-8_46

[5] Capitalone. (2022). Capital main page. https://www.capitalone.com/Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. Communications of the ACM, 63(7), 80–90.https://doi.org/10.1145/3359552

[6] Chen, L., Lee, W.K., Chang, C.C., Choo, K.K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronichealth record sharing. Future generation computer systems, 95, 420–429. https://doi.org/10.1016/j.future.2019.01.018

[7] Cheng, E. C., Le, Y., Zhou, J., & Lu, Y. (2018). Healthcare services across China–on implementing an extensible universallyunique patient identifier system. International Journal of Healthcare Management, 11(3), 210–216.https://doi.org/10.1080/20479700.2017.1398388

[8] Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-DrivenInteroperability. Computational and Structural Biotechnology Journal, 16, 224–230.https://doi.org/10.1016/j.csbj.2018.06.003

[9] Hardin, T., & Kotz, D. (2019). Blockchain in health data systems: A survey. In 2019 sixth international conference on internet of Things: Systems, management and security (pp. 490-497). IEEE. https://doi.org/10.1109/IOTSMS48152.2019.8939174

[10] HealthData.gov. (2022) Washington: Department of health and human services. https://www.va.gov/bluebutton

[11] HealthNautica. (2022). HealthNautica main page. https://www.healthnautica.com/comppages/index.aspHIMSS. (2020). Digital health. https://www.himss.org/resources/personal-health-records-electronic-health-records-key-indiasnational-digital-health

[12] Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain inhealthcare. Symmetry, 10(10), 470. https://doi.org/10.3390/sym10100470

[13] Khalaf, O. I., Abdulsahib, G. M., Kasmaei, H. D., &Ogudo, K. A. (2020). A New Algorithm on Application of BlockchainTechnology in Live Stream Video Transmissions and Telecommunications. International Journal of E-Collaboration, 16(1),16–32. https://doi.org/10.4018/ijec.2020010102

[14] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-Based Data Preservation System for Medical Data.Journal of Medical Systems, 42(8). https://doi.org/10.1007/s10916-018-0997-3

[15] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobilehealthcare applications. In 2017 IEEE 28th annual

international symposium on personal, indoor, and mobile radiocommunications (pp. 1-5). IEEE. https://doi.org/10.1109/PIMRC.2017.8292361

[16] Mayer, A. H., da Costa, C. A., & Righi, R. da R. (2020). Electronic health records in a Blockchain: A systematic review. HealthInformatics Journal, 26(2), 1273–1288. https://doi.org/10.1177/1460458219866350

[17] Pournaghi, S. M., Bayat, M., &Farjami, Y. (2020). MedSBA: a novel and secure scheme to share medical data based onblockchain technology and attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing,11(11), 4613–4641. https://doi.org/10.1007/s12652-020-01710-y

[18] Qin, Q., Jin, B., & Liu, Y. (2021). A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based onConsortium Blockchain. BioMed Research International, 1–14. https://doi.org/10.1155/2021/6676171

[19] Ramani, V., Kumar, T., Bracken, A., Liyanage, M., &Ylianttila, M. (2018). Secure and efficient data accessibility inblockchain based healthcare systems. In 2018EEE Global Communications Conference (pp. 206-212). IEEE.https://doi.org/10.1109/GLOCOM.2018.8647221

[20] Alam, S., Ahmad Reegu, F., Daud, S. M., & Shuaib, M. (2021). Blockchain-Based Electronic Health Record System forEfficient Covid-19 Pandemic Management. https://doi.org/10.20944/preprints202104.0771.v1

[21] Sahoo, M. S., & Baruah, P. K. (2018). HBasechainDB – A Scalable Blockchain Framework on Hadoop Ecosystem. In AsianConference on Supercomputing Frontiers (pp. 18–29). Springer. https://doi.org/10.1007/978-3-319-69953-0_2

[22] Sauermann, S., Frohner, M., Urbauer, P., Forjan, M., Pohn, B., Drauschke, B.A., & Mense, A. (2013). The adolescence ofelectronic health records: Status and perspectives for large scale implementation. Acta Informatica Pragensia, 2(1), 30–38. https://doi.org/10.18267/j.aip.11

[23] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. IEEE Access, 7, 147782–147795.https://doi.org/10.1109/ACCESS.2019.2946373

[24] Shuaib, K., Saleous, H., Shuaib, K., & Zaki, N. (2019). Blockchains for secure digitized medicine. Journal of personalizedmedicine, 9(3), Article no. 35. https://doi.org/10.3390/jpm9030035

[25] Shuaib, M., Daud, S. M., Alam, S., & Khan, W. Z. (2020). Blockchain-based framework for secure and reliable land registrysystem. Telkomnika, 18(5), 2560–2571. https://doi.org/10.12928/TELKOMNIKA.v18i5.15787

[26] Siddiqui, S. T., Ahmad, R., Shuaib, M., & Alam, S. (2020). Blockchain security threats, attacks and countermeasures. Indvances in Intelligent Systems and Computing (pp. 51-62). Springer. https://doi.org/10.1007/978-981-15-1518-7_5

[27] Thwin, T. T., &Vasupongayya, S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal HealthRecord Systems. Security and Communication Networks, 2019, 1–15. https://doi.org/10.1155/2019/8315614

[28] Wang, H., & Song, Y. (2018). Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. Journalof Medical Systems, 42(8). https://doi.org/10.1007/s10916-018-0994-6

[29] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). Bbds: Blockchain-based data sharing for electronic medicalrecords in cloud environments. Information, 8(2), Article no. 44. https://doi.org/10.3390/info8020044

[30] Zhang, A., & Lin, X. (2018). Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via ConsortiumBlockchain. Journal of Medical Systems, 42(8). https://doi.org/10.1007/s10916-018-0995-5

[31] Zhao, Y., Cui, M., Zheng, L., Zhang, R., Meng, L., Gao, D., & Zhang, Y. (2019). Research on electronic medical recordaccess control based on blockchain. International Journal of Distributed Sensor Networks, 15(11), 155014771988933.https://doi.org/10.1177/1550147719889330