INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 56-63

e-ISSN : 2583-1062

Impact Factor: 5.725

EFFICIENT MEDICAL RECORD SYSTEM USING HYBRID BLOCKCHAIN TECHNOLOGY

Ashish Thomas[1], M. Saravanakumar[2]

[1]Dept of CSE, PG Scholar, Rathinam college of arts and science, Coimbatore, India.

[2]Dept of CSE, Senior Faculty, Rathinam college of arts and science, Coimbatore, India.

DOI: https://www.doi.org/10.58257/IJPREMS33110

ABSTRACT

Interoperability, patient privacy, and data security are major issues facing the healthcare sector. In order to tackle these problems, the system uses hybrid blockchain technology to offer a novel method of maintaining medical records. Because of blockchain technology's decentralization, security, privacy, and confidentiality, the healthcare industry stands to gain greatly from it.

In order to provide a safe, scalable, and interoperable platform for medical record management, the proposed system combines the advantages of public and private blockchains. Patient information in this system is kept on a private blockchain, ensuring access control and privacy. Access to the patient's medical history is restricted to authorized healthcare providers, enhancing confidentiality and regulatory compliance. On the other hand, a public blockchain is utilized for managing data transactions, enabling secure and efficient data sharing between different healthcare institutions.

This hybrid blockchain-based medical record system offers several advantages. It ensures data integrity, traceability, and immutability, reducing the risk of data breaches and unauthorized alterations. The system allows patients to have more control over their medical data and provides a transparent audit trail for all data access and modifications. Moreover, it promotes interoperability between healthcare providers, making it easier to exchange patient information and improve the quality of care.

Keywords: Blockchain, public and private blockchains, data security, medical record, confidentiality and decentralization

1. INTRODUCTION

The healthcare industry has long struggled with issues related to the management of medical records, including data security, interoperability, and patient privacy. In response to these challenges, this paper outlines the practical implementation of a Medical Record System using a Hybrid Blockchain Technology. The system will leverage both public and private blockchain components to create a secure, scalable, and interoperable platform for managing medical records. The primary objective of this paper is to successfully implement a cuttingedge Medical Record System by leveraging the capabilities of Hybrid Blockchain Technology. This entails combining the strengths of both public and private blockchain

components to create a sophisticated and robust platform for managing medical records. The overarching goal is to address longstanding challenges within the healthcare industry, including issues related to data security, interoperability, and patient privacy. Through the implementation of this Hybrid Blockchain-based system, the paper aims to establish a secure, scalable, and interoperable solution that enhances the efficiency and integrity of medical record management within the healthcare ecosystem.

2. PROBLEM STATEMENT

Electronic Health Record (EHR) systems have indeed become integral components in healthcare settings worldwide, revolutionizing the way patient information is managed and healthcare services are delivered. The widespread adoption of EHR systems can be attributed to a multitude of benefits, with security enhancement and cost-effectiveness being key drivers. The fundamental objective of Electronic Health Record (EHR) systems is to offer secure, tamper-proof, and easily shareable medical records across diverse platforms. While the initial motivation behind implementing EHR systems in healthcare was to enhance the quality of healthcare delivery, several challenges have been encountered, and certain expectations haven't been fully met.

Certainly, Electronic Health Record (EHR) systems, while offering numerous benefits, have encountered challenges and problems that warrant attention and improvement. Here are some issues faced by EHR systems:

2.1 Interoperability

It serves as a conduit for disparate information systems to share data effectively. The exchanged information must be not only transferable but also readily applicable for subsequent use. An integral facet of Electronic Health Record (EHR) systems is their Health Information Exchange (HIE) or the broader aspect of data sharing. As EHR systems proliferate across diverse hospital settings, they exhibit varying terminologies, technical nuances, and functional capacities, lacking a universally standardized framework. Furthermore, at a technical level, the exchanged medical records need to be interpretable, ensuring that the gleaned information can be effectively utilized for downstream purposes.

2.2 Data Breaches

The healthcare sector faces significant challenges, particularly in the realm of data breaches within Electronic Health Record (EHR) systems. A study analyzing EHR data breaches revealed that since October 2009, approximately 173 million data entries have been compromised. Cybersecurity threats against hospitals are escalating, as noted by Argaw et al indicating a rising trend in cyber-attacks on healthcare institutions. Substantial research has been conducted in this domain, highlighting the urgency to address these vulnerabilities.

Furthermore, many existing EHR systems encounter issues such as inefficiency, poor adaptation, and negative consequences on information processing, necessitating a platform transformation that prioritizes patient-centric care. Blockchain emerges as a viable solution, offering security, transparency, and data integrity for patients' medical records.

This paper proposes a decentralized framework to store patients' medical records securely and provide access to authorized individuals, including healthcare providers and patients. To address blockchains scalability limitations, an off-chain scaling method is suggested, utilizing an underlying medium for storing large volumes of data. The overarching goal is to mitigate information asymmetry and combat data breaches prevalent in current EHR systems.

2.3 Information Asymmetry

The primary concern raised by critics in the healthcare sector today is information asymmetry, where one party possesses more accessible information than the other. In the context of Electronic Health Record (EHR) systems and the broader healthcare industry, this issue is evident as doctors or hospitals hold exclusive access to patients' records, creating a centralized system. Patients, on the other hand, face a cumbersome and lengthy process when attempting to retrieve their medical records, with control limited to healthcare organizations.

3. BLOCKCHAIN TECHNOLOGY AND ITS DEPENDENCIES

Nakamoto initially introduced blockchain technology in his groundbreaking work on digital currency, specifically Bitcoin. The primary purpose was to address the double-spending issue within the Bitcoin system. However, this innovative technology quickly found applications beyond cryptocurrencies. Blockchain, essentially a chain of interconnected blocks, continually expands by recording transactions. Its decentralized nature ensures information distribution with shared ownership of data.

In this platform, transactions are grouped into blocks, and each block is secured through hashing. These blocks are then managed by peer-to-peer networks. The advantages of blockchain include enhanced security, anonymity, and data integrity without the need for third-party intervention. Given these benefits, it becomes a viable option for storing sensitive data such as patients' medical records. The healthcare industry, prioritizing the security of medical data, has recognized the potential of blockchain technology. Several researchers have endorsed the feasibility of incorporating blockchain in healthcare solutions.

3.1. Architecture

1. To grasp the blockchain architecture, refer to Figure 1, illustrating the comprehensive process of a user-initiated transaction within the blockchain network:

When a user initiates a new transaction on the blockchain network, it triggers the creation of a new block. Within the blockchain, blocks serve as repositories for transactions, and these blocks are distributed to all connected nodes in the network.

The transaction enclosed within the newly formed block is broadcasted to every node in the network. All nodes possess a copy of the complete blockchain, aiding in the verification process.

Upon receiving the broadcasted block, each node scrutinizes it to ensure there has been no tampering. Successful verification confirms the block's authenticity, and nodes incorporate the verified block into their individual copies of the blockchain.

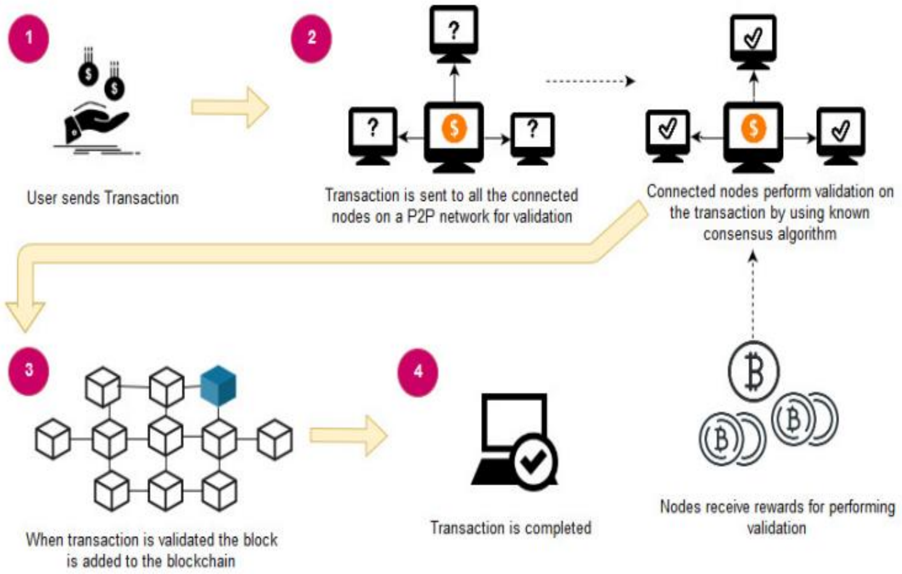

1
User sends Transaction
2
Transaction is sent to all the connected nodes on a P2P network for validation
Connected nodes perform validation on the transaction by using known consensus algorithm
3
When transaction is validated the block is added to the blockchain
4
Transaction is completed
Nodes receive rewards for performing validation

Figure 1. An overview of blockchain architecture.

2. The process of adding a block to the blockchain involves nodes reaching a consensus, collectively deciding which blocks are deemed valid for inclusion and which are not. This validation is executed by connected nodes employing established algorithms to verify transactions and authenticate the sender within the network. Upon successful validation, the validating node is rewarded with cryptocurrency. This validation process is commonly referred to as mining, and the node performing this function is known as a miner.

3. Completion of the validation process, the validated block is added to the blockchain.

4. Once the entire validation process is concluded, the transaction is considered completed.

3.2 Key features of blockchain

3.2.1 Decentralization

Blockchain ensures the distribution of information across the network, eliminating centralization. Control over information is decentralized and managed through consensus achieved by the collective input of connected nodes. Previously centralized data is now handled by multiple trusted entities.

3.2.2 Data transparency

Data transparency relies on trust-based relationships between entities. In blockchain, data or records are not concentrated in a single location, and control is not vested in a singular node. Instead, data is distributed across the network, promoting shared ownership and ensuring transparency and security against third-party interference.

3.2.3 Security and privacy

Blockchain employs cryptographic functions, such as the SHA-256 algorithm, to enhance security for connected nodes. The SHA-256 cryptographic algorithm is applied to the hashes stored in blocks, ensuring data integrity. Cryptographic hashes, being strong one-way functions, generate checksums for digital data that resist data extraction. This decentralized platform, fortified by cryptographic measures, makes blockchain an appealing choice for privacy protection in various applications.

3.3 Public vs private blockchain frameworks

Distinctions exist between public and private blockchain frameworks. Public implementations allow anyone to participate, making the network open to all. In contrast, private blockchains involve known participants. In public versions, incentives are often in place to encourage widespread participation. Bitcoin, the world's largest public blockchain, serves as a prominent example of this approach.

In a private blockchain, all participants are identified, and entry requires an invitation. Private Blockchains typically operate on a permissioned network, further restricting participation. For instance, a regulatory authority might issue licenses to control entry into the network, illustrating an example of a private blockchain implementation.

4. PROPOSED SYSTEM

Medical Record System using Hybrid Blockchain Technology, the results indicate a transformative enhancement in healthcare data management, exemplified by heightened security measures, seamless interoperability, and improved patient privacy.

The hybrid blockchain architecture, incorporating both public and private components, leveraging cryptographic features to safeguard against unauthorized access and data breaches. The integration with existing healthcare systems demonstrates a significant leap forward in interoperability, fostering seamless data exchange among healthcare providers, insurers, and regulatory bodies.

The privacy-centric features embedded within the smart contracts ensure confidentiality, empowering patients with control over their medical data and addressing concerns related to privacy breaches.

The user-friendly interface has streamlined interactions for healthcare professionals, administrators, and patients, ensuring accessibility and ease of use.

5. USAGE SCENARIO FOR PROPOSED FRAMEWORK

The Administrator and the User are the two primary entities in the system. For our suggested paradigm, users are further classified as either patients or doctors. The system administrator, a member of the administrative staff of the hospital, assigns roles to these users. The administrator has been tasked with setting the level of access that the doctor and patient, the two primary users of our system, can have. The administrator's role assignment would be the initial action, and it would include the role name and the account address of the user to whom the role is being assigned. Each person utilizing the proposed system would be assigned a role name and account address. The role name and account address are therefore saved in a roles list once the administrator assigns this user a role, as needed for validation in subsequent phases.

After roles are assigned, now when a user wants to perform some operations on the proposed system he would at first request to perform them. The system would verify the user role name and account address from the Roles List and allows them accordingly to perform those functions after validation returns success. After the functions are performed the system would store the information on the Ethereum Blockchain that would perform transactions for

that information. Once the transaction is confirmed the system receives the message of success from the blockchain layer that users can view on the DApp browser on which the whole proposed framework is being visible.

4.2 Block diagram for proposed system

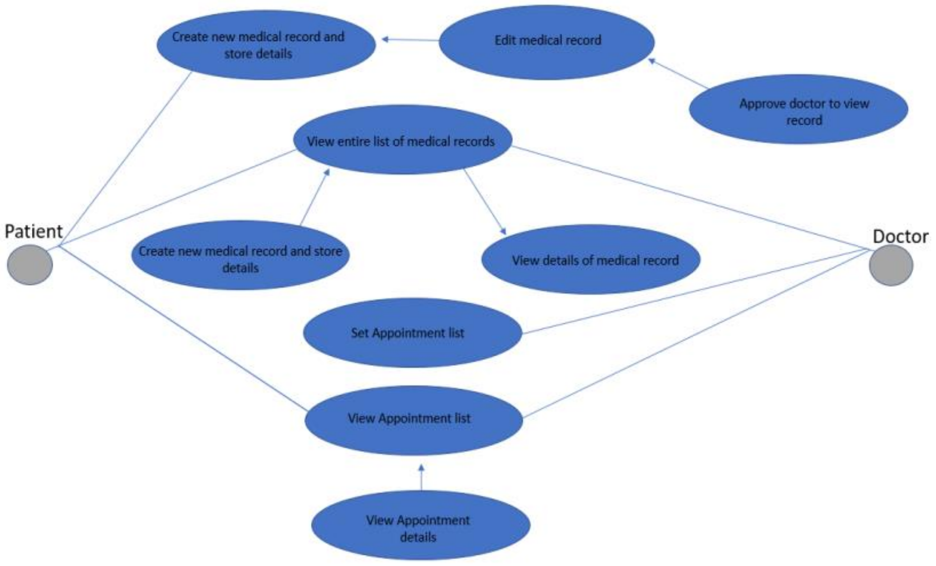

Create new medical record and store details
Edit medical record
Approve doctor to view record
View entire list of medical records
Patient
Create new medical record and store details
View details of medical record
Doctor
Set Appointment list
View Appointment list
View Appointment details

Figure 2. Medical Record System Data Flow Diagram

4.3 Comparison of Proposed Framework with Related Work

The parameters that are present in our framework and are used for comparison with the related work in this domain. While ensuring the presence of these parameters in the framework it is also considered that it would not compromise the security and privacy of the system.

4.3.1 Scalability:

Put more simply, scalability is the information system's capacity to continue operating as intended as its storage capacity rises or falls. Scalability is a problem with blockchain technology that requires an ongoing solution. when the volume or size of data on the blockchain grows. As the patient's data stored on the blockchain includes the patient's basic information in addition to the IPFS hash—that is, the off-chain scaling solution utilized in our suggested system framework—we employed the off-chain storage method in our proposed system.

4.3.2 Content-Addressable Storage:

Content-addressable storage refers to the off chain storage mechanism of IPFS used in the proposed framework. The

sensitive record of patient is stored on the IPFS, which ensures that a hash of the stored record is generated. That hash is now stored in the blockchain and is accessed when needed by the doctors and patients. The IPFS generates the

cryptographically secure hash which ensures the security of the data being stored on it. And this also ensures security in our proposed framework.

4.3.3 Integrity:

A system's integrity is determined by how trustworthy it is and how reliable and temperature-proof its information storage is. This blockchain-based method makes sure that this feature is not jeopardized. This system's storage of data is unaltered and unaltered by unwanted access. Furthermore, only the individuals involved—doctor and patient—have access to the information.

4.3.4 Access Control:

Using the Role-based access mechanism, this framework

makes sure that every entity of the system is assigned role. Any third party who is not authorized to have access to the system would not be able to access the system. This system provides a two core security as firstly blockchain technology in itself is secure and uses certain protocols and mechanism to keep itself secure from third-part intrusions.

4.3.5 Information Confidentiality:

The patient medical records stored on the blockchain should be secured from any third party access to ensure the confidentiality of the patients' record. The patient's data include the important information of patient such as the patient medical history, blood group, records, lab results, X-rays reports, MRI results and many other related results and reports.

4.4 Experimental Setup

We have tested the suggested framework's functionality using the following configurations in our experiments:

- Intel Core i7-6498DU CPU @ 2.50GHz 2.60 GHz processor
- And 8.00 GB of memory with Windows 64-bit OS (version 10)

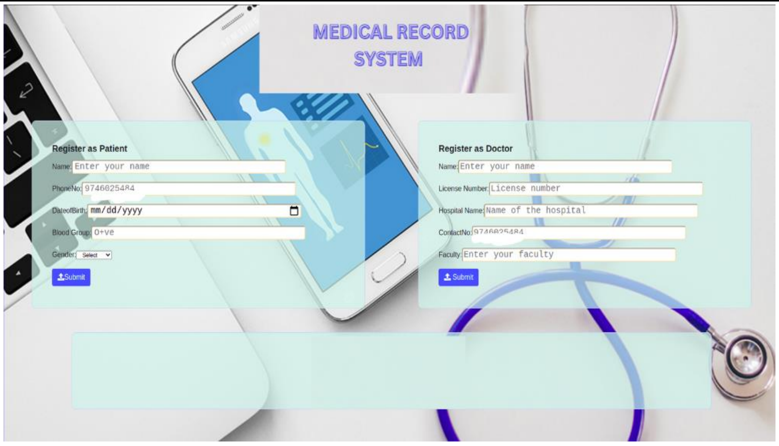
We used Ethereum Solidity programming language to create our suggested framework. To build code for smart contracts, Ethereum provides the Solidity language, which encapsulates Python and JavaScript..

6. IMPLEMENTATION

In the development and deployment of a hybrid medical record system, the integration of both public and private blockchains is a strategic approach aimed at optimizing the management of patient information within the healthcare ecosystem. This comprehensive implementation entails the incorporation of a decentralized and transparent public blockchain, which serves as a foundational framework for facilitating seamless accessibility and interoperability of patient data across diverse healthcare providers. By leveraging the decentralized nature of the public blockchain, this hybrid system promotes a standardized and secure exchange of medical records, fostering a cohesive and interconnected healthcare network.

Simultaneously, the inclusion of a private blockchain component is pivotal in ensuring a heightened level of security and controlled access to sensitive patient information. The private blockchain operates within a permissioned framework, restricting entry only to authorized entities such as healthcare professionals and institutions. This dual-layered blockchain architecture not only fortifies data integrity but also safeguards patient privacy, mitigating the risk of unauthorized access and potential breaches.

Through this hybrid approach, the medical record system achieves a delicate balance between the transparency and accessibility afforded by the public blockchain and the heightened security and restricted access provided by the private blockchain.



MEDICAL RECORD SYSTEM

Register as Patient

Name: Enter your name

PhoneNo: 9746025484

DateofBirth: mm/dd/yyyy

Blood Group: O+ve

Gender: Select

Submit

Register as Doctor

Name: Enter your name

License Number: License number

Hospital Name: Name of the hospital

ContactNo: 9746025484

Faculty: Enter your faculty

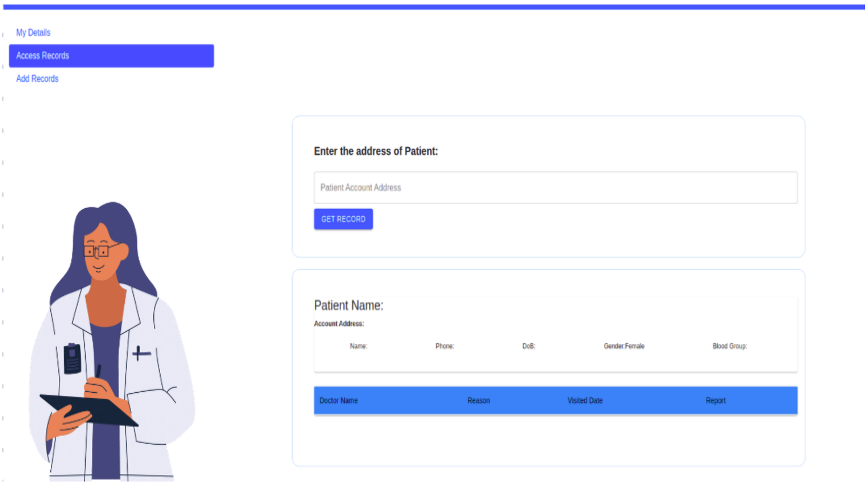
Submit

Figure 3. Home page of medical record system

The home page of the blockchain-based medical record system serves as the central gateway to a secure and efficient platform, seamlessly integrating patient and doctor details. Within the patient details section, users encounter a comprehensive interface where essential personal information is stored with the utmost privacy and integrity. This includes the patient's name, contact number, date of birth (DOB), and blood group. Leveraging the robust security features of blockchain technology, these details are encrypted and decentralized, ensuring transparency, immutability, and tamper-proof storage.

Simultaneously, the doctor details section offers a comprehensive repository of healthcare professionals' information. This encompasses the doctor's name, license details, affiliated hospital name, and contact number. The incorporation of blockchain technology in storing doctor details guarantees a secure and verifiable record, bolstering trust and accuracy in the healthcare ecosystem.

Users navigating the home page are presented with an intuitive and user-friendly interface, facilitating easy access to patient and doctor information while upholding the highest standards of data security and privacy. The blockchain backbone of the system ensures that patient and doctor details are not only readily accessible but also resistant to unauthorized alterations, fostering a dependable and transparent medical record management system. This innovative approach enhances the overall efficiency of healthcare interactions, streamlining patient care and medical workflows.



Enter the address of Patient:

Patient Account Address

GET RECORD

Patient Name:

Account Address:

Name:	Phone:	DoB:	Gender:Female	Blood Group:

Doctor Name	Reason	Visited Date	Report

Figure 4. Access records of patients

Access records within a medical record system leverage blockchain technology to compile a comprehensive dataset documenting patient interactions with healthcare providers, containing personal details like name, date of birth, and contact information, alongside visit specifics, reasons for access, gender, blood type, and pertinent medical reports. This blockchain-based system ensures heightened patient privacy and security through cryptographic techniques, enabling secure and immutable storage of sensitive medical data. It also facilitates seamless care continuity by allowing authorized healthcare professionals instant access to pertinent patient information across various healthcare settings. Furthermore, the transparent and decentralized nature of blockchain enhances medical research support by enabling anonymized data sharing while maintaining patient confidentiality, thereby fostering collaboration and innovation in healthcare research endeavors.

7. CONCLUSION

In this system it shows how blockchain technology can be useful for healthcare sector and how can it be used for electronic health records. Despite the advancement in healthcare sector and technological innovation in EHR systems they still faced some issues that were addressed by this novel technology, i.e., blockchain. We present a framework that combines granular access rules for individual data with secure record storage. It makes a system that is simpler for consumers to operate and comprehend. Additionally, given the framework makes use of IPFS's off-chain storage feature, it suggests steps to guarantee that the system addresses the issue of data storage. Additionally, because only connected and trustworthy parties have access to medical records, role-based access helps the system as a whole. This also addresses the EHR system's information asymmetry issue.

8. FUTURE WORKS

As the medical record system leveraging hybrid blockchain technology undergoes further development, it is imperative to prioritize several key aspects. Firstly, an emphasis should be placed on fortifying security measures to safeguard the confidentiality and integrity of sensitive medical data. Simultaneously, efforts should be directed towards achieving seamless interoperability with established healthcare standards, such as HL7 and FHIR, facilitating unhindered data exchange across diverse healthcare systems. Furthermore, the ongoing refinement of the system necessitates the creation of a user-friendly interface, ensuring that healthcare professionals can effortlessly access and update medical records.

9. REFERENCES

[1] G. Jetley and H. Zhang, ‘‘Electronic health records in IS research: Quality issues, essential thresholds and remedial actions,’’ Decis. Support Syst., vol. 126, pp. 113–137, Nov. 2019.

[2] K. Wisner, A. Lyndon, and C. A. Chesla, ‘‘The electronic health record’s impact on nurses’ cognitive work: An integrative review,’’ Int. J. Nursing Stud., vol. 94, pp. 74–84, Jun. 2019.

[3] M. Hochman, ‘‘Electronic health records: A ‘‘Quadruple win,’’ a ‘‘quadruple failure,’’ or simply time for a reboot?’’ J. Gen. Int. Med., vol. 33, no. 4, pp. 397–399, Apr. 2018.

[4] Q. Gan and Q. Cao, ‘‘Adoption of electronic health record system: Multiple theoretical perspectives,’’ in Proc. 47th Hawaii Int. Conf. Syst. Sci., Jan. 2014, pp. 2716–2724.

[5] T. Vehko, H. Hyppönen, S. Puttonen, S. Kujala, E. Ketola, J. Tuukkanen, A. M. Aalto, and T. Heponiemi, ‘‘Experienced time pressure and stress: Electronic health records usability and information technology competence play a role,’’ BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 160, Aug. 2019.

[6] M. Reisman, ‘‘EHRs: The challenge of making electronic data usable and interoperable.,’’ PT, vol. 42, no. 9, pp. 572–575, Sep. 2017.

[7] W. W. Koczkodaj, M. Mazurek, D. Strzałka, A. Wolny-Dominiak, and M. Woodbury-Smith, ‘‘Electronic health record breaches as social indicators,’’ Social Indicators Res., vol. 141, no. 2, pp. 861–871, Jan. 2019.

[8] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, ‘‘The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review,’’ BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 10, Dec. 2019.

[9] A. McLeod and D. Dolezel, ‘‘Cyber-analytics: Modeling factors associated with healthcare data breaches,’’ Decis. Support Syst., vol. 108, pp. 57– 68, Apr. 2018

[10] 10.Coventry and D. Branley, ‘‘Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,’’ Maturitas, vol. 113, pp. 48–52, Jul. 2018.

[11] ‘‘The future of health care cybersecurity,’’ J. Nursing Regulation, vol. 8, no. 4, pp. S29–S31, 2018

[12] D. Spatar, O. Kok, N. Basoglu, and T. Daim, ‘‘Adoption factors of electronic health record systems,’’ Technol. Soc., vol. 58, Aug. 2019,

[13] S. Nakamoto, Bitcoin: A Peer-to-Peer Electrnic Cash System. 2008,

[14] W. J.Gordon and C. Catalini, ‘‘Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,’’ Comput. Struct. Biotechnol. J., vol. 16, pp. 224–230, Jan. 2018.

[15] A. Boonstra, A. Versluis, and J. F. J. Vos, ‘‘Implementing electronic health records in hospitals: A systematic literature review,’’ BMC Health Services Res., vol. 14, no. 1, Sep. 2014, Art. no. 370.

[16] T. D. Gunter and N. P. Terry, ‘‘The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions,’’ J. Med. Internet Res., vol. 7, no. 1, p. e3, Jan./Mar. 2005.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ‘‘An overview of blockchain technology: Architecture, consensus, and future trends,’’ in Proc. IEEE Int. Congr. Big Data (BigData Congr.), Jun. 2017, pp. 557–564.

[18] C. Pirtle and J. Ehrenfeld, ‘‘Blockchain for healthcare: The next generation of medical records?’’ J. Med. Syst., vol. 42, no. 9, p. 172, Sep. 2018.

[19] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, ‘‘Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives,’’Cryptography, vol. 3, no. 1, p. 3, Jan. 2019.

[20] J. Eberhardt and S. Tai, ‘‘On or off the blockchain? Insights on offchaining computation and data,’’ in Proc. Eur. Conf. Service-Oriented Cloud Comput., Oct. 2014, pp. 11–45.