IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Ehr (Electronic Health Records) Management System Using Blockchain

Prof. Mohammad Sharique Sandip Institute of Technology and Research Centre Savitribai Phule Pune University Maharashtra, India

Atharva Sajgure Sandip Institute of Technology and Research Centre Savitribai Phule Pune Nashik, University Nashik, Maharashtra, India

Swapnil Singh Sandip Institute of Technology and Research Centre Savitribai Phule Pune University Nashik, Maharashtra, India

Vedant Patil Sandip Institute of Technology and Research Centre Savitribai Phule Pune University Nashik, Maharashtra, India

Sneha Joshi Sandip Institute of Technology and Research Centre Savitribai Phule Pune University Nashik, Maharashtra, India

Abstract:

Electronic healthcare records (EHR) play a crucial role in modern healthcare systems, providing a comprehensive digital repository of patient information. However, ensuring the security, privacy, and interoperability of EHR remains a significant challenge. Blockchain technology has emerged as a potential solution to address these challenges by leveraging its decentralized, transparent, and immutable nature. This research paper explores the application of blockchain technology in enhancing EHR systems. It begins with an overview of EHR and highlights the existing security and privacy concerns associated with traditional systems. The paper then provides a comprehensive understanding of blockchain technology, focusing on its key features, such as decentralization, immutability, and cryptographic security, that make it well-suited for EHR management. The benefits of implementing blockchain in EHR systems, including enhanced data security, auditability, and patient control over their data, are examined. Furthermore, the paper proposes a framework for implementing blockchain in EHR, outlining the key considerations, such as data encryption, access control, interoperability, and consent management. Real-world case studies and pilot projects that have implemented blockchain for EHR management are presented to illustrate the feasibility and effectiveness of this technology. The technical aspects of blockchain integration, including consensus mechanisms, smart contracts, and scalability, are also discussed. The paper concludes by addressing the challenges and future directions of utilizing blockchain in EHR systems, including regulatory compliance, standardization, and integration with existing healthcare infrastructure. Overall, this research paper contributes to the understanding of blockchain technology's potential in improving the security, privacy, and interoperability of electronic healthcare records, offering valuable insights to healthcare organizations, policymakers, and researchers interested in adopting blockchain for EHR management.

Keywords: Blockchain, Ethereum, SHA-256 algorithm, decentralization, electronic health records, and scalability.

Introduction

Background

Electronic healthcare records (EHR) have revolutionized the way healthcare information is stored, accessed, and shared. EHR systems provide numerous advantages over traditional paper-based records, including improved data accuracy, accessibility, and efficiency in healthcare delivery. However, the increasing digitization of healthcare data has raised concerns regarding data security, privacy breaches, and the interoperability of EHR systems. Unauthorized access, data tampering, and data silos pose significant risks to patient privacy and the integrity of healthcare records

The goal of this project is to provide a user friendly and cost-effective application. A big advantage of this project is security. A secure system is more important to be trustworthy. Electronic Health Records (EHR) provides a convenient medical record storage service that allows traditional paper medical records to be accessed electronically over the Internet. The system is designed to give a patient control over the generation, management, and sharing of her EHR with family, friends, healthcare providers, and other authorized data users. Furthermore, if healthcare researchers and providers of such services can access these EHRs from anywhere, it is hoped that the Healthcare Solutions Transition Program will be achieved. However, in the current situation, the patient distributes her ePA to different regions. During a life event in which the EHR will be moved from her one service provider database another. A blockchain is a decentralized database in which blocks of data are linked in chronological order. In the healthcare industry, there are various parties that need to jointly manage an individual's EHR blockchain (in a consortium blockchain model), including: B. Medical professionals, hospitals, insurance departments, etc. Electronic records systems are designed to be proprietary and centralized. This means you have a single vendor to control your code base, database, and system output while providing monitoring tools. It is difficult for a centralized system to gain the trust of patients, physicians and hospital administrators. An independently verifiable open-source system solves this problem. Cryptographic ownership on the blockchain network ensures patient privacy. Data integrity and integrity prevent medical data from being tampered with. Blockchain can be thought of as a distributed database that stores data on each network node to avoid outage issues. Therefore, it improves stability, consistency, and resistance to attacks. The problem of distributed denial of service (DDOS) attacks in traditional centralized frameworks can be solved by blockchain technology.

Electronic medical record (EMR) system. However, hospitals face several issues related to medical record security, data user ownership, data integrity, and more. The solution to these problems is to use new technology. User Classes and Functionality: The application mainly has his three types of users: administrators, patients and doctors. A user connects his girlfriend's Meta Mask wallet to the application and logs into the application.

1. Administrators - Administrators can register users as patients or doctors. The user's girlfriend's Meta Mask wallet address is used to identify the identity.

2. Patients – Patients are the owners of their data and can grant or revoke permission from doctors and other medical institutions such as hospitals, laboratories and health insurance companies.

3. Physician - Physicians can add, edit, view, or delete medical records for patients granted access to medical records.

BLOCKCHAIN TECHNOLOGY

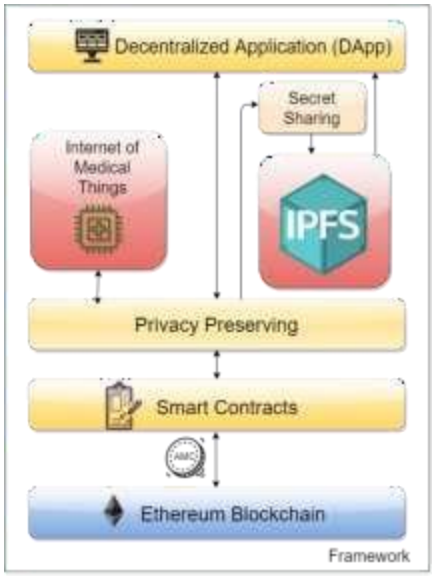
Definition: A blockchain is a distributed database or ledger that is stored among the nodes of a computer network. It is a peer-topeer or P2P, distributed database that stores the ongoing transactions on the blockchain in a way that the records remain distributed, decentralized an immutable.

The transactions are stored in the form of blocks chained using cryptography. Each block stores the hash of data in the previous block, except for the starting block, forming a chain of block, hence called genesis block. Every user on the blockchain owns a public key of the user is visible to everyone, others can use the users public key to send transactions, while private key is private to the user and should be kept secret. If a user loses access to his private key, he can no longer access his account or the funds in his account. Every transactions on the blockchain needs to be signed by the private key of the sender, which authenticates the transactions and protects it from tampering.

PROBLEM STATEMENT

The current healthcare solution for storing and sharing medical records is highly sensitive electronic medical records. Due to the lack of reliable and trustworthy health data sharing mechanisms, the majority of EHR data sharing still occurs by mail. This results in significant delays in patient treatment and many other reasons For patients, the decision to participate in a clinical trial is a complex decision, often with unknown and potential medical benefits. The advantages and disadvantages must be weighed side impact risk. The solution is for patients to own their data in order to find suitable and efficient treatments. Different hospitals and medical facilities have different systems. Therefore, integration and interoperability issues result. Blockchain features a decentralized system that provides cryptographic guarantees for data integrity, security, privacy, and data access smart contracts. Some EHR management literature addresses these issues by proposing a centralized framework and system for sharing his EHR across cloud infrastructures. While these frameworks provided solutions to many of the above challenges, they were plagued by limitations especially around transparency, data ownership, and privacy. Natural disasters present new challenges as health departments need to be prepared and able to respond quickly to crises. This is one of the arguments for how decentralized EHR management and information replication and distribution can guarantee improved performance and availability in disaster situations compared to centralized models.

SYSTEM ARCHITECTURE



Ethereum – The Ethereum blockchain is often touted as the “computer of the world”. This is because it is globally accessible deterministic state machine managed by a peer-to-peer network of nodes. His state changes in this state machine follow consensus rules followed by peers in the network. Smart Contract – A smart contract is a program that runs on the Ethereum blockchain, defines the logic behind state changes that occur on the blockchain

Ethereum Virtual Machine (EVM) – The EVM is responsible for executing smart contracts and the handles state changes that occur in this globally accessible state machine. Provider – A node on the blockchain that you connect to interact with the blockchain is called a provider. Each provider implements the JSON-RPC (Remote Procedure Call) protocol. It defines various data structures and their processing rules, and uses JSON (RFC 4627) as the data format.

Signer (Meta Mask) – After connecting to the blockchain, you can read the state of the blockchain. However, to write to the blockchain state, you need to perform a transaction that must be signed with theprivate key. This is where Meta Mask comes into play. Meta Mask stores the user's girlfriend's private key in the browser and calls Meta mask each time the frontend asks the user to sign a transaction. Frontend – Defines the UI logic that the user interacts with. It also communicates application logic defined in smart contracts.

IPFS – IPFS (Interplanetary File System) is a distributed file system for storing and accessing data. The IPFS system distributes and stores data over a peer-to-peer network. This makes it easy to get the data when you need it.

SYSTEM REQUIREMENTS

Database Requirements –

· Firebase

· NoSQL Database

· Node JS

.

Ganache

· JSON

· Git, GitHub

· VS Code

· NPM

Hardware requirements—

RAM: Hard Disk: 1 GB or more

·Processor: 64-bit, single 2.5 GHz minimum per **Brief description of** core, core speed.

Software Requirements –

· Operating System: Windows 10 (64- bit) or later / Linux / Mac OS

· Languages: O

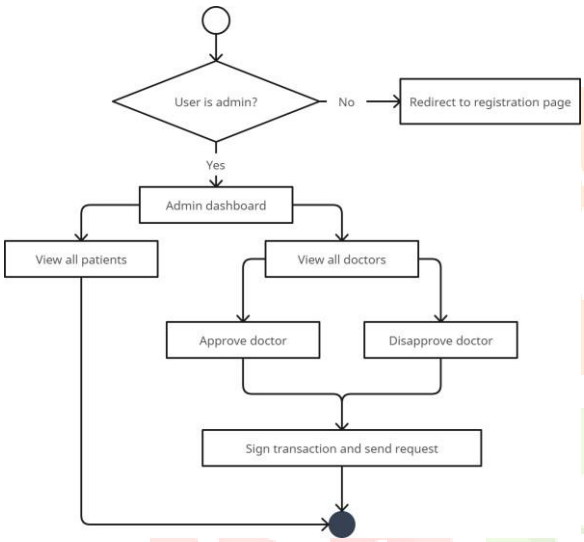
Solidity o

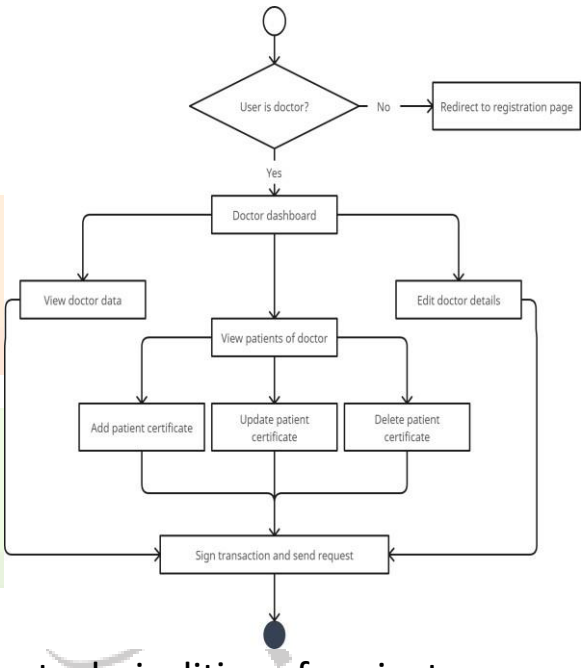
TypeScript o HTML

o CSS o Sass o

JavaScript · Angular

JS





technicalities of project

Activity Diagrams Encryption mechanism

Steps:

1. File object received from <input type=”file” /> is converted to data url using FileReader().readAsDataURL(File), which directly gives a data url that is be put in <iframe /> tag to display the data.

2.The output from FileReader().readAsDataURL(File) is encrypted using utf-8 to hex encryption, which can then be decrypted using hex to utf-8 decryption.

Type of encryption used:

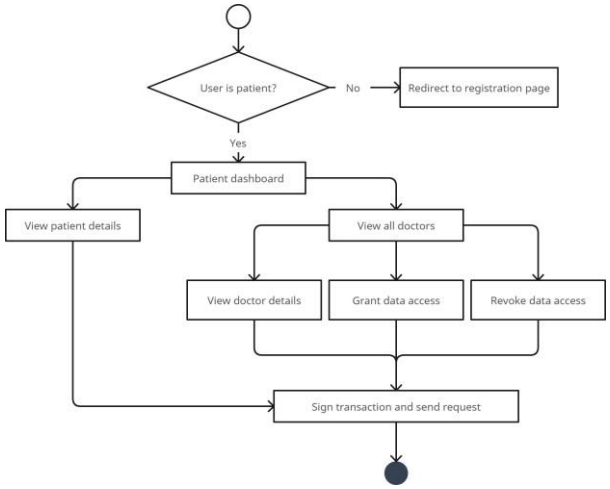
1. Suppose, we have a patient X and doctor A, B and patient X wants to give access only to doctor A while also himself having the access to data.
2. Asymmetric cryptography uses receivers public key to encrypt data, but using this way only one person at a time can access the data, i.e. either the patient can access his own data or a doctor can access patient's data, which is not a feasible solution.
3. So, here we are going to use hybrid encryption, the data is encrypted using a symmetric key, then the symmetric key is encrypted using accessor's public keys separately and stored along with the encrypted files.

```
encrypt(data, S)  encrypt(S, X_pubkey)
send to X    encrypt(S, A_pubkey) send
to A  decrypt(S, X_privkey) X gets key
S
decrypt(S, A_privkey) A gets key S
decrypt(data, S)
```

Upgradable smart contracts

Upgradable smart contracts

By design of the blockchain, smart contracts are immutable. While a software quality highly depends on the ability of upgrade to mitigate



the bugs and security vulnerabilities and introduce new features, smart contracts are made upgradable using proxy contracts.

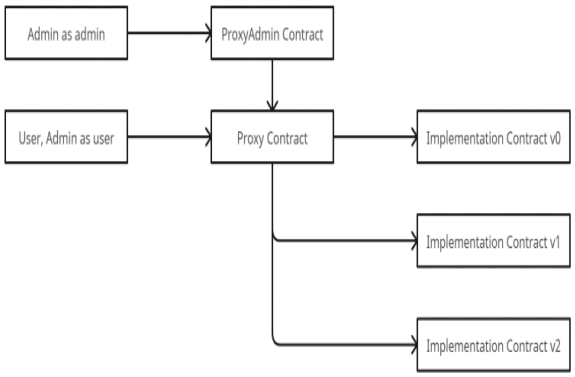
- Idea behind proxy contract is to deploy a wrapper contract (proxy contract) that

stores the state of the contract and the address of latest implementation of dApp contract.

- While all the state variables lies in the proxy contract, the implementation contract contains the logic to update those variables, which is achieved through low level operation delegatecall.

- The function allows a contract to call function of another as if it were its own. This means that the called (implementation) contract can access the storage of caller (proxy) contract. Any changes to variables will be made to proxy contract.

OpenZeppelin



Proxy Contract: Proxy contract is responsible for storing the state variables of smart contract, storing the address of latest implementation contract and delegating the incoming calls to Implementation contracts.

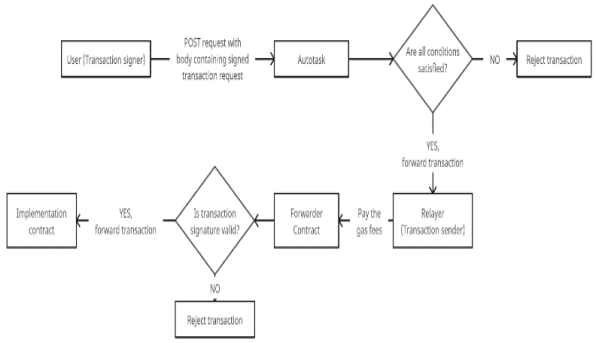
ProxyAdmin Contract: Every function that is part of a contract's public ABI is identified, at the bytecode level, by a 4-byte identifiers. The functions in Proxy contract and implementation contract sometimes may have the same identifier resulting in clashing of functions. To deal with this issue OpenZeppelin Transparent Proxy Pattern, uses and extra contract called ProxyAdmin Contract. So proxy contract delegates all the calls that are not forwarded from the ProxyAdmin contract, even if the sender address is the admin of contract.

Implementation contract: Implementation contract is the actual implementation of dApp contract.

Meta-transactions (Gas less transactions)

To perform transactions on blockchain users need to pay gas fees which contributes to difficulty in user onboarding and less users being interested in using the application, as currently not many target users of application own the cryptocurrency required to pay the fees.

Solution to this problem is integration of meta transactions into application which facilitates the users by paying the transaction fees for them while maintaining the security and privacy by requiring the users to sign the transactions.



Autotask: Autotask is a OpenZeppelin Defender service that allows you to run

conde snippets on a regular basis, via web hooks or in response to a transaction. The service integrates with Relay service and hence can send transaction on-chain through relayer. Here, it checks if the transaction sender satisfies all the conditions and forwards the transaction to relayer accordingly.

Relayer: A relayer is simply a pair of public and private key with a public address on blockchain provided by OpenZeppelin Defender. It is exposed for usage through its API key and API secret. The relayer here is responsible for send the transaction onchain through forwarder.

Forwarder Contract: Forwarder is a contract that checks for the integrity of message received from the transaction signer i.e. user. It verifies the transaction message against the transaction signature to validate the message. This is done to restrict the autotask or relayer from making any changes to the message before forwarding.

Implementation Contract: Implementation contract is where the users transaction request is executed. And the resulting transaction is sent back from autotask to the transaction signer (users) as an HTTP response to post request.

Innovation of Invention

The innovation of this invention lies in the shift of access control of EHRs from centralized organizations to individual patients. By utilizing the decentralization of blockchain and distributed file system of IPFS, the platform provides a transparent, tamper-proof, and trustless environment for patients to share their medical data with their doctors.

While today's traditional EHR systems store data and manage access control through a centralized server in healthcare centers, patients have to trust these organizations and their trust-based contracts for maintaining the security and privacy of their data.

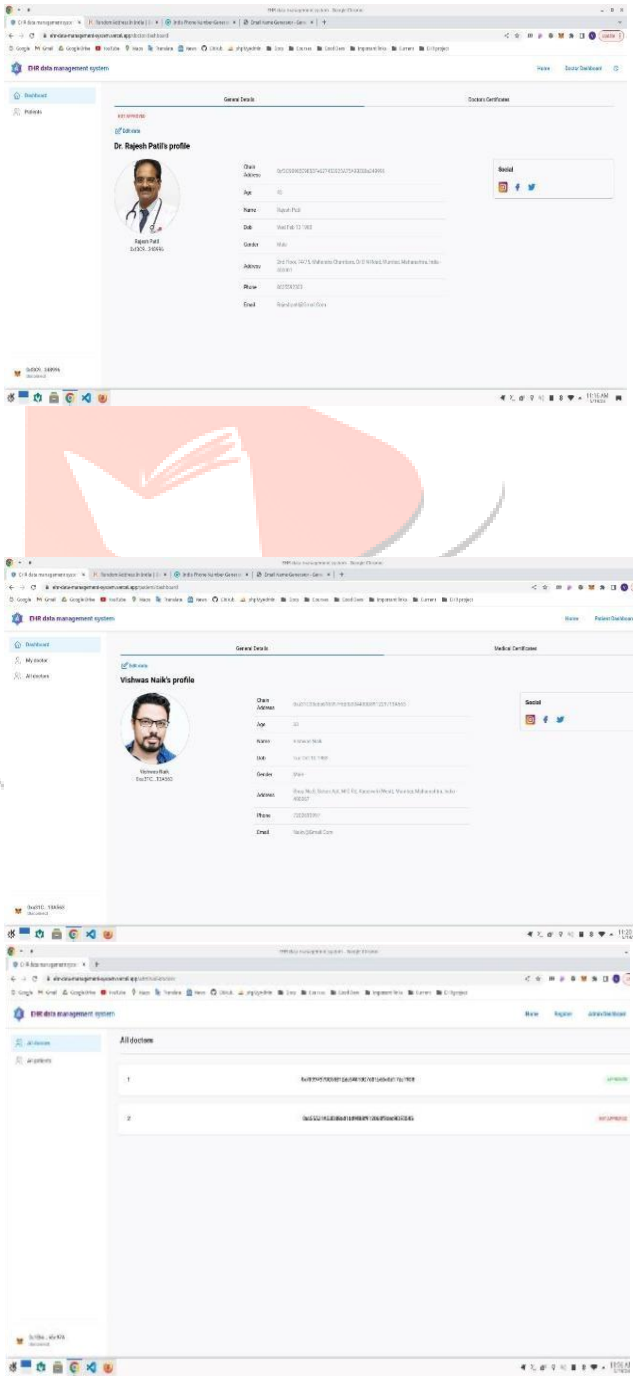
On the other hand, our system takes a

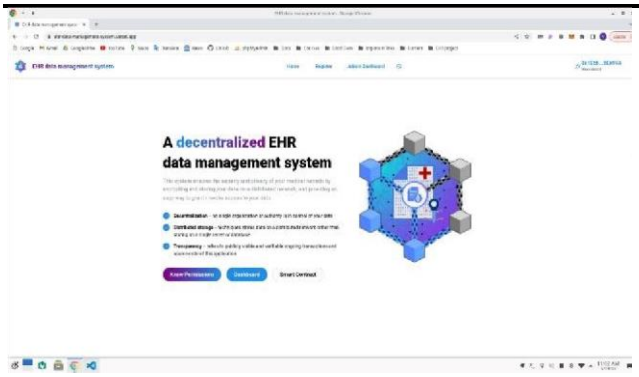
completely different approach. With our platform, both storage and access control is decentralized and transparent. The application executes in a trustless and verifiable environment powered by mathbased smart contracts on EVM based blockchain where users can see the code of contract managing the access control and can view exactly how the data is stored on distributed IPFS network. In addition to distributed storage, the encryption and decryption of data is done using the user's and his trusted party's public and private key pairs so none other than user and his trusted parties can decrypt the data. The application provides patients with complete control over their medical data, while ensuring that their records remain secure and private.

Moreover, the upgradability of contract ensures that the smart contract can be updated to mitigate bugs and security vulnerabilities, and new features can be added without losing the user data and without a need for users to shift to a different contract. Also, the gas-less transaction feature eliminates the need for users to hold cryptocurrency, simplifying the user onboarding process and increasing their interest in the application.

Overall, this invention presents a unique and innovative solution to the challenges faced by the healthcare industry in the secure storage and sharing of medical data.

OVERVIEW





CONCLUSION AND FUTURE WORK

In this study, a systematic literature review regarding EHRs within a Blockchain was conducted, with the objective of identifying and discussing the main issues, challenges, and possible benefits from Blockchain adoption in the healthcare field. The application of Blockchain has exceeded the scope of the field of economics and we have highlighted Blockchain's potential for the healthcare area, while also revealing that it still highly depends on the acceptance of the new technology within the healthcare ecosystem.

Analyzing the results that were obtained from the literature review, we conclude that Blockchain technology might be a future suitable solution for common problems in the healthcare field, such as HER interoperability, establishing sharing trust between healthcare providers, auditability, privacy, and granting of health data access control by patients, which would enable them to choose whom they want to trust and with whom to share their medical records. However, additional research, trials, and experiments must be carried out to ensure that a secure and established system is implemented prior to using Blockchain technology on a large scale in healthcare, since a patient's health data are personal, highly sensitive, and critical information.

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. WoodburySmith, ''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. EshayaChauvin, 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, ‘‘Cyberanalytics: Modeling factors associated with healthcare data breaches,’’ Decis. Support Syst., vol. 108, pp. 57–68, Apr. 2018.

10. L. Coventry and D. Branley, ‘‘Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,’’ Maturitas, vol. 113, pp. 4852, 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, Art. no. 101144.

13. S. Nakamoto, Bitcoin: A Peer-to-Peer Electrnic Cash System. 2008, pp. 1–9. 14. W. J. G 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.

14. W. J. Gordon and C. Catalini, ‘‘Blockchain technology for healthcare: Facilitating the transition 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,