International Journal of Reliable and Quality E-Healthcare
Volume 11 • Issue 2

An Extensive Survey on Blockchain-Based Electronic Health Record Systems

Pranab Kumar Bharimalla, KIIT University, India*
https://orcid.org/0000-0002-9952-8096

Satya Ranjan Dash, School of Computer Engineering, KIIT University, India
https://orcid.org/0000-0002-7902-1183

Hammad S. Choudhury, Infosys Ltd., USA
https://orcid.org/0000-0003-1594-7582

ABSTRACT

Healthcare systems around the world are beset by problems due to the lack of effective communication. Significant problems relating to patient medical record access, transition, and storage have persisted due to the lack of resources to adequately interact and track records between all main participants. To overcome this challenge, a nationwide electronic health record (EHR) solution may be utilized. To further enhance EHR efficiency, blockchain technology can be used to improve security, performance, and cost. In this survey, various literature proposing blockchain-based EHR systems are discussed, along with their benefits and potential research gaps. Also, the authors proposed a comprehensive architecture that could bridge all the gaps.

KEYWORDS

Blockchain, Cloud Computing, EHR, Electronic Healthcare System, NLP

INTRODUCTION

The lack of reliable medical records for patients is a serious issue faced by many healthcare systems in both developing and developed countries. The current medical data management system oriented by medical institutions does not guarantee the integrity and reliability of patient data (Chen et al., 2019). As demand for care increases, the need for efficient resource delivery is indispensable. For healthcare systems reliant on obsolete methods, the implementation of an Electronic Health Record (EHR) system will help rectify issues dealing with human error, fraud, coordination, and trust. EHR is a digital repository of medical data which can be securely accessed and shared in real-time. EHR systems allow healthcare providers to serve patients effectively by having quick access to reliable information, but the added convenience comes at a cost of privacy.

EHR systems along with other technological innovations such as social media, smartphones, smart sensors, cloud computing, IoT devices, etc. are being increasingly used to improve everyday life but are collecting sensitive data at an unprecedented rate. The amount of generated data will continue

DOI: 10.4018/IJRQEH.299960
*Corresponding Author

to expand as more people venture into the digital space. The importance of privacy protection is realized due to bolder attacks by cybercriminals to capture confidential information during this data surge. Blockchain can be used to safeguard the security of highly sensitive medical data. Blockchain technology ensures that the effort required to alter records (e.g., to commit fraud, etc.) always exceeds the benefits or gains resulting from attempts to alter records (Seitz et al., 2017). Blockchain technology enables EHR systems to withstand intelligent attacks by integrating efficient security measures.

Blockchain technology is transforming how transactions between two untrusted parties are processed. At any stage of a transaction, Blockchain will mitigate confidentiality and security issues, such as third-party trust, implying that with the introduction of Blockchain technology, all intermediaries or third parties are eliminated (Tanwar et al., 2020). Blockchain is a decentralized data structure eliminating a third party's need to validate a transaction. When integrated into EHR systems, Blockchain provides key security upgrades such as prevention of illegal alterations of data through distributed ledger technology, secure and efficient transactions validated through clever algorithms, and reduced operations cost.

This survey provides an in-depth analysis of numerous pieces of literature proposing Blockchain-based EHR systems. The writings were evaluated based on key factors such as the architecture, algorithm, data sharing from existing local EHR systems, real-life implementation, and performance evaluation. In addition, the survey focuses on the proposal of practical features such as integration with cloud storage, patient management of medical records, involvement of key healthcare participants, integration with unique patient and institution identifiers, and availability of a user interface. In the next section, the related works are discussed along with a detailed comparison of key works followed by research gaps, proposed high-level architecture, and the conclusion.

RELATED WORKS

Many patient-centric, permission-based Blockchain EHR schemes have been suggested in the literature since the introduction of Blockchain platforms such as Hyperledger Fabric, Ethereum, and Azure Blockchain Workbench.

Intending to improve security and privacy, Tanwar et al. introduced a permission based EHR sharing scheme (Tanwar et al., 2020). They also introduced a smart contract-based architecture access control policy algorithm and a system performance optimization mechanism. However, the reusability of current healthcare records held in individual hospital files is ignored in this report. On the other hand, Dubovitskaya, et al. suggested a Blockchain-based permissioned EHR framework that can integrate data from local standalone EHR systems in different hospitals or clinics. The system suggested storing metadata and providing access only via Blockchain, with real health records being stored in the cloud (Dubovitskaya et al., 2020). Although this is a novel idea, actual patient sensitive EHR data is stored in the cloud and does not benefit from the immutability that Blockchain provides. The system proposed by Tanwar et al. was strengthened by Singh, Akhilendra Pratap, and his fellow researchers, who added a few additional modules such as chemist, insurance, and doctor's appointment (Singh et al., 2020). Despite the authors' systematic approach, the study overlooks data scalability and interoperability with existing EHR and healthcare databases. (Chen et al., 2019) proposed a Blockchain-based searchable encryption system for EHR, which supports patients, healthcare professionals, and researchers alike. Only indexes are applied to the Blockchain in the proposed framework, while real patient information is stored in the cloud in an encrypted format. There are many methods for encrypting data in the cloud and maintaining privacy.

Fu, Junsong, Na Wang, and Yuanyuan Cai suggested a new method for breaking EHR records into sub-messages and then constructing EHR shares to store locally on separate computer nodes and upload the indexes to the healthcare Blockchain (Fu & Na 2020). Using metrics such as disk write-read performance, memory consumption, network data utilization, transaction execution per unit time, and CPU use, Kombe and his fellow researchers evaluated the performance of popular public and private/consortium Blockchain-based healthcare systems, with consortium-based systems delivering the best performance results (Kombe et al., 2018, 2019).

Blockchain-Based Deep-Learning as-a-Service was suggested by Bhattacharya, Pronaya, and colleagues. The system shares EHR records among multiple healthcare users and operates in two phases: authentication and deep learning to prevent collusion attacks and predict potential future conditions for patients (Bhattacharya et al., 2019). A Blockchain-based architecture was proposed by Bhavin, Makwana, et al. that allows access to the database based on user roles and improves the standard encryption mechanism by using a quantum blind signature to secure the system from quantum attacks by using hyperledger fabric (Bhavin et al., 2021).

R. Shanthapriya and V. Vaithianathan proposed a scheme that performs the cryptic operation using AES cryptography and Blockchains using hash keys. Furthermore, their proposed healthcare ecosystem includes a prediction model that uses a deep learning algorithm to diagnose a patient's illness (Shanthapriya et al., 2020). Ekblaw, Ariel, et al. proposed MedRec, an innovative, decentralized record management system designed to handle EHRs using Blockchain. The system allows Patient management of medical records, integrates with existing local databases, includes healthcare participants, and uses Social Security to identify patients. However, cloud storage is not supported (Ekblaw et al., 2016).

Seitz, Juergen, et al. offer a variety of opportunities for automatization and digitalization in their paper. The paper addresses patient identification using German health care and highlights the usage of Blockchain technology for electronic prescriptions. However, integration with existing EHR and healthcare databases and cloud storage are not supported. (Seitz et al., 2017).

Conceicao, Arlindo F. da, et al. proposed implementation of an Electronic Health Records (EHRs) large-scale information architecture based on smart contracts as information mediators, where the patient owns their medical records in the proposed system and integration with cloud storage exists, but it does not propose any solution for data accessibility vs privacy (da et al., 2018).

Rifi, Nabil, et al. illustrate the specific problems and highlight the advantages of Blockchain technology in deploying a secure and scalable medical data exchange solution with the best possible performance. The patient is connected to other participants and is in control of their medical records (Rifi et al., 2017). There is integration with both off-chain data storage and cloud computing. It does not integrate with existing healthcare databases. In 2019, VM, Harshini et al. highlighted the patient-driven standard model framework using Blockchain technology (Harshini et al., 2019). The proposed model provides patients control access over their health records, the ability to share data with required parties, and grant access based on unique ID, but fails to integrate with existing data as well as cloud technology. Similarly, Shahnaz, Ayesha, et al. discussed a framework that could be used for the implementation of Blockchain technology in the healthcare sector for EHR. A framework for secure storage of patient data with role-based access is proposed, highlighting the need for a scalable system (Shahnaz et al., 2019). Off chain storage of data is discussed but there is no integration with the cloud and with existing data and does not provide the patient control over their medical records.

Zghaibeh, Manaf, et al. devised a Smart-Health (SHealth), Blockchain-based health management system where user identity is verified using the national identification provider, integrates different participants (Government, Hospitals, Clinics, etc.) in a layered system, proposed a unified national database to store all data instead of scattered data between various databases and patients control access to their medical reports (Zghaibeh et al., 2020). This is a very detailed paper but misses out on integration with cloud storage. Zhuang, Yan, et al in 2020, proposes a Blockchain model to protect data security and patients' privacy, ensure data provenance, and provide patients full control of their health records where patients have control over their data sharing, allowing clinicians to view the patients' details for the recent visit, links EHR databases by creating touchpoints, and patients have a Blockchain-generated global IDs without revealing their real identities. (Zhuang et al., 2020). This paper is comprehensive but misses out on integration with cloud storage.

Dagher, et al. in their research paper proposes a Blockchain-based platform called Ancile for secure, interoperable, and efficient access to medical records by patients, providers, and third parties while preserving the privacy of patients' sensitive information (Dagher et al., 2018). In the proposed system, various healthcare participants are involved, the patients maintain ownership of their record and manage the access for record sharing, party identification and verification are implemented and are built over existing system. However, the model does not integrate with cloud storage. Sharma, Yogesh & Balamurugan, B presented a system to use Blockchain technology to construct EHRs and make them more secure and private, with increased data access for patients and clinicians, although they only presented a primitive architecture (Sharma et al., 2020).

Cunningham & Ainsworth describe a model that allows individuals to select when and how their electronic health records are accessible for research purposes. In the proposed system, patients control the access to their medical records, and it's inclusive for various other healthcare participants but, the paper does not propose an architecture or detailed implementation (Cunningham et al., 2018).

Ivan, Drew discusses Blockchain as a novel approach to secure health data storage, implementation obstacles, and a plan for transitioning incrementally from current technology to a Blockchain solution (Ivan et al., 2016). The proposed system grants patients access to medical records through EHR clients. The model, however, misses out on features made possible due to new innovations such as integration with existing databases and the cloud. Chen, Yi, et al. proposed a storage system based on Blockchain and cloud storage for managing personal medical data, as well as a service architecture for sharing medical records with cloud data storage and current databases (Chen et al., 2019). The model, however, does not provide patients control over their medical records or involve key participants required in a robust healthcare system.

Alla, Sujatha, et al conducted a methodical literature review to find out the research gaps and future research directions in Blockchain technology in healthcare research which highlights the high-level overview of Blockchain in healthcare regarding people, process, and technology, however, the work does not propose an architecture (Alla et al., 2018). Randall, David, and colleagues suggested that a decentralized benefits administration system can improve enrolment, eligibility, claims payment, and adjudication processes, hence increasing efficiency and minimizing systemic fraud, but they did not suggest a design (Randall et al., 2017).

Yang, G., & Li, C. present a Blockchain-based architecture for electronic health record (EHR) systems. The architecture is built on top of existing databases maintained by health providers and providers take primary responsibilities of maintenance of the Blockchain, including creation, verification, and appending of new blocks (Yang et al., 2018). The proposed system does not provide the patient control over their medical records, or validate their identity; in addition, there is no integration with cloud storage. Vora, Jayneel, and his team presented a Blockchain-based system for EHR storage and management. This also allows patients, providers, and third parties to have secure and efficient access to medical data while maintaining the patient's privacy. The proposed system does not provide the patient control over their medical records or validate their identity in addition there is no integration with cloud storage or existing databases (Vora et al., 2018).

Liu, Jingwei, et al proposed a Blockchain-based privacy preserving data exchange model for EMRs called BPDS. In BPDS, the original EMRs are stored securely in the cloud and the indexes are reserved in a tamper-proof consortium Blockchain. The comprehensive model integrates with existing data and cloud storage, the records and access are controlled by users and are provided with unique identification (Liu et al., 2018).

Carter, Grace, and colleagues propose a novel strategy for a Blockchain and cloud computing network that uses Amazon Web Services and the Ethereum Blockchain to enable semantic level interoperability of Electronic Health Record systems without predefined data types and formatting. The proposed system Integrates cloud (Amazon AWS) to store large data, facilitates interoperability of Electronic Health Records systems via Blockchain, includes multilayer layer encryption security.

However, the system does not validate patient identity through unique identification or provide them control over their records (Carter et al., 2019).

N. Al-Karaki, Jamal, et al present a Blockchain-based framework, called DASS-CARE, that supports decentralized, accessible, scalable, and secure access to healthcare services including medical records. The proposed system provides access across healthcare providers, highlights the importance of interoperability with the existing local system, integrates with cloud storage to share records between providers, discusses tracking of patient identity, and promotes patient control over record sharing (Al-Karaki et al., 2019).

D., Akarca, et al. explored how Blockchain technology may facilitate the handling of health data in the context of regulatory frameworks, patient rights, cybersecurity, and provider-centric perspectives (Akarca et al., 2019). The paper discusses record sharing between patients and other parties, Users are presented as hash values instead of real identities, Patients have read-access and can give read-write permissions to clinicians. However, the proposed system does not integrate with existing EHR and healthcare databases, does not validate patient identity through unique identification, and does not integrate with cloud storage.

To improve the hospital's electronic health system, Liu, Xiaoguang, et al. presented a medical data exchange and protection strategy based on the hospital's private Blockchain. (Liu et al., 2019). The paper proposes a lightweight data sharing scheme using Blockchain, which utilizes the cloud to securely store medical data. Pseudo identity is used for hospitals, doctors, etc. instead of real identification, the medical records from different hospitals and doctors are accessible when required, the patient controls the sharing of their medical data. In their research, Kassab, Mohamad, et al. provide preliminary results of a literature review on the adoption of Blockchain to support the management of EHR in health systems, a detailed analysis of Blockchain implementation for EHR systems, and a realistic challenge, but no architecture is proposed (Kassab et al., 2019).

Niu, Shufen, et al. propose a medical data sharing scheme based on permissioned Blockchains. The proposed system uses ciphertext-based attribute encryption to ensure data confidentiality and access control of medical data and Integration with cloud storage services to verify identity, store indexes, and retrieve keywords, but does not provide the users' control over their medical records (Niu et al., 2019).

Donawa, Alyssa, et al. describe how sidechains might alleviate Blockchain bottlenecks, allowing well-known Blockchains to accommodate even larger medical systems with over 30 million transactions per day. The paper proposes the usage of side chains to facilitate a large volume of transactions, validates identities through public notaries, and requires signoff from participants on record data accuracy (Donawa et al., 2019). However, the proposed system does not provide the patient control over their medical records and does not integrate with cloud storage for the storage of large files. Mahore, Vinay, et al. suggest an approach that focuses on providing researchers with healthcare data for statistical analysis while also maintaining privacy. In the proposed system the patient's identity is created during hospital visitation, encrypted, and stored in the cloud, the patient can directly access their data and provide access to requestors, uses proxy re-encryption technique to share patient's sensitive data, and utilizes Blockchain to connect separate eHealth care systems by resolving issues around trust (Mahore et al., 2019).

BiiMED, a Blockchain framework proposed by Jabbar, Rateb, and colleagues, aims to improve data interoperability and integrity in EHR-sharing. The system allows health record exchange between different participants, cloud storage (AWS) is used for medical data storage, it is scalable for a large population with user identification/validation, it highlights the importance of interoperability with existing databases, and the access management system shares patient data. The comprehensive paper however does not provide patients control over their medical data (Jabbar et al., 2020).

M. M. Madine et al. presented a system that uses decentralized storage of systems (IPFS) and trusted reputation-based re-encryption oracles to securely fetch, store, and distribute medical data from patients. In the proposed system, patients control their medical data, are responsible for registering and sharing their data with requestors, government registered user identification is used for user identification, encrypted medical records are stored on off chain databases, and medical records are transferred to the patients automatically. However, it does not integrate with existing EHR and healthcare databases and does not integrate with cloud storage. (Madine et al., 2020).

The authors conducted literature surveys on the ANN-based text extraction model that could contribute to our work, in addition to the relevant works listed above.

With 98 percent accuracy, Roger Achka, Khodor Ghayad, Rayan Haidar, and colleagues implemented the Artificial Neural Network (ANN) method for text extraction from 64 different types of prescriptions (Achkar et al., 2019). Durjoy Sen Maitra, Ujjwal Bhattacharya, and colleagues devised a CNN-based method for extracting numeric text from handwritten numbers in Indian languages such as Odiya, Telugu, Devnagari, Bangla, and English. Bangla characters were 95 percent correct, Devanagari characters 98.54 percent correct, Odia characters 97.2 percent correct, Telugu characters 96.5 percent correct, and English characters 99.10 percent correct (Maitra et al., 2015).

RESEARCH GAPS

In the previous section, various Blockchain-based EHR system proposals were explored, and their research gaps were briefly discussed. Table 1 provides a bird's eye view of all related work and research gaps. In this section, these common research gaps will be examined. In numerous proposals, the Blockchain-based EHR system is unable to integrate with local EHR systems found in hospitals and other institutions. This is a critical functionality since existing systems contain vast amounts of patient data already. A truly comprehensive Blockchain-based EHR system must include the usage of existing data. The lack of storage for large files is a common research gap seen in many of the proposals, to access large patient related data on the Blockchain-based EHR system, off chain storage options must be utilized and secured. The ability to find patients based on national identity is a functionality missed by many proposals, to implement a nationwide Blockchain-based EHR system, the national government must be involved in identifying and validating patients or institutions. Examples of national identifiers include SSN in the United States or PAN in India. The Blockchain-based EHR system must utilize government resources to streamline the identification of all participants. In multiple proposals, steps on implementing the Blockchain-based EHR system were not provided. Rolling out a nationwide EHR system is complex, a proper Blockchain-based EHR system proposal should include an implementation plan. A common issue, especially in underdeveloped regions, is the dependence on paper records. To implement a successful Blockchain-based EHR system in these regions, the proposed system should facilitate the transfer of written records to the digital space using tools such as Natural Language Processing. Transferring existing written records would greatly reduce dependency on obsolete record keeping practices. The lack of key healthcare participant involvement in numerous proposed systems is the remaining research gap. To effectively set up a successful healthcare system, all participants must be involved. A brief system architecture will be proposed in the next section which resolves various concerns caused by research gaps.

PROPOSED ARCHITECTURE

In this section, a brief system architecture is visualized in Figure 1 to resolve the previously discussed research gaps. In the envisioned Hyperledger Fabric based architecture, the patient will read, write, and control permission to their individual medical records through a web or mobile interface. The interface is the user's gateway to access various member services. The patient can share records with doctors, pharmacies, labs, insurance companies, and government institutions with specified permissions and set access for a limited time. The system will be integrated with government databases for accurate user and institution identification. In case the patient is unable to provide access, the admin user may

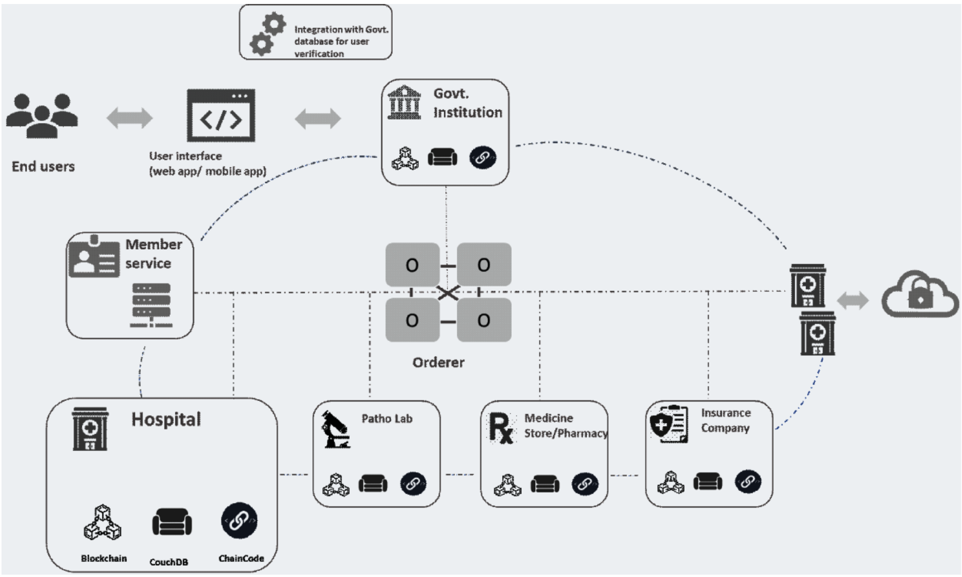
Table 1. Comparison of related works proposing Blockchain-based EHR system

Author	Year	Objective	1	2	3	4	5	Pros	Cons
Tanwar et al.	2020	Proposed a Permission-based EHR sharing system with intention to enhance security and privacy.	✓	✓	✗	✓	✓	• Has access control policy algorithm with smart contract.	• Does not integrate with existing databases.
Dubovitskaya, Alevtina, et al.	2020	Proposed a Blockchain based permissioned EHR system with capability of data integration of local standalone EHR systems that house in different hospitals or clinics.	✓	✗	✓	✓	✗	• Store metadata and access only in Blockchain whereas actual health records in cloud.	• Patient sensitive EHR data resides in cloud and does not enjoy immutability that Blockchain offers.
Singh, Akhilendra Pratap, et al.	2020	Tried to enhance the framework proposed by Tanwar et al. [5]	✓	✓	✗	✓	✓	• Added new modules like chemist, insurance, and doctor's appointment.	• Ignores the scalability of data and interoperability of existing EHR and healthcare databases.
Seitz, Juergen, et al	2017	Offers a variety of opportunities for automatization and digitalization.	✓	✗	✗	✗	✗	• Addresses patient identification using the German health card.	• Does not integrate with existing EHR and healthcare databases. • Does not integrate with cloud storage.
Zhuang, Yan, et al	2020	Proposes a blockchain model to protect data security and patients' privacy, ensure data provenance, and provide patients full control of their health records.	✓	✗	✓	✓	✓	• Patient centric system with patients having control over their data sharing. • Links EHR databases by creating touchpoints. • Patients will have blockchain-generated global IDs without revealing their real identities in the system.	• Does not integrate with cloud storage.
Rifi, Nabil, et al	2017	Illustrates the specific problems and highlights the benefits of Blockchain technology for the deployment of a secure and a scalable solution for medical data exchange with the best possible performance.	✓	✗	✗	✓	✗	• The patent is in control of their medical records. • Integration of off-chain databases for medical data storage. • Provides interface for users to access the Blockchain.	• Does not integrate with existing EHR and healthcare databases.
V M, Harshini, et al	2019	Highlights on the patient-driven model of record maintenance using Blockchain technology.	✓	✗	✗	✗	✗	• Provides patients control access over their health records.	• Does not integrate with existing EHR and healthcare databases. • Does not integrate with cloud storage for storage.
Shahnaz, Ayesha, et al	2019	Presents a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR.	✓	✓	✗	✓	✓	• Usage of off chain database for data storage. • Scalable system.	• Does not integrate with existing EHR and healthcare databases. • Does not provide the patient control over their medical records. • Does not integrate with cloud storage.
Zghaibeh, Manaf, et al	2020	Presents Smart-Health (SHealth), a blockchain-based health management system.	✓	✓	✓	✓	✗	• User identity is verified using the national identification provider. • Integrates different participants (Government, Hospitals, Clinics etc.) in a layered system. • Proposes a unified national database to store all data instead of scattered data between various databases. • Patients provide the providers access to health records through the "wallet" app.	• Does not integrate with cloud storage.
Ekblaw, Ariel, et al	2016	Proposed MedRec, a novel, decentralized record management system to handle EHRs, using blockchain technology.	✓	✗	✓	✗	✗	• Patient management of medical records • Integrates with existing local databases.	• No cloud storage.

1 - Architecture   2 - Algorithm   3 - Data sharing from local EHR   4 - Real life implementation   5 - Performance evaluation

share patient details in case of an emergency. The admin user is provided with unrestricted access to the network. The system will be integrated with existing local EHR systems found in hospitals, allowing patients to import data via pull requests submitted through the mobile or web interface and it will also be integrated with cloud technology for the storage of large, encrypted files. To access a patient's medical records, institutions must have a valid node on the network and request keys from the admin to login. The proposed system allows the transfer of paper-based records to the Blockchain network using Natural Language Processing algorithms, patients can submit paper records for digitalization through the web or mobile interface. Lastly, the implementation plan and result analysis details will be provided for the proposed architecture. The implementation of these key features will ensure an efficient Blockchain-based EHR system. A comprehensive system based on this architecture will be

Figure 1. Proposed Architectural Framework for Blockchain-based Healthcare System



discussed in our future works, however, we have examined a case study with the Indian Subcontinent context in the next section of the paper.

CASE STUDY: INDIAN SUB-CONTINENT

The proposed architecture is more contextualized for the Indian subcontinent due to sizable population of 1.4 billion. Indian health care system has coherent problems like, unavailability of a centralized medical repository, lack of transparency on medical records, frequent data breaches, and frauds. Thousands of patients' COVID-19 test results were exposed on the internet through several government domains, which was one of the most prominent data breaches (Oommen et al., 2021). A similar scam involving a false COVID-19 test report surfaced about a large-scale pilgrimage in north India. This kind of fraud and data breaches, could be avoided with blockchain based EHR system, proposed in this paper.

In the proposed system, the government institution serves as a founding organization or trusted anchor, providing credibility and trusted roles to hospitals, pharmacies, insurance companies, labs, and other institutions. Participants with trusted roles have the ability to generate and distribute credential schema and definitions to the general public or patients. A patient could be authenticated in the system through an Aadhar number whereas participating service providers could be authenticated based on their Tax identification number or PAN.

Patients will be able to choose who has access to their information and who may alter it, although the government reserves the right to give access to an institution in an emergency. Individual hospitals will connect their EHR system to a Blockchain node and a web API with full access to their local EHR to convert any current SQL records to No SQL format for storage on the Blockchain. A hybrid data management approach is used to facilitate EHR data scalability, in which all key patient data, such as demographics, allergies, medications, and access controls, is stored in Blockchain, while sensitive medical files, such as x-ray and scanning reports, are encrypted and stored in private cloud storage.

CONCLUSION

Improved EHR systems will be essential to the advancement of future healthcare systems. Owing to the superiority of Blockchain-based systems over conventional systems, the ability of Blockchain technology to greatly impact the future of EHR systems has been recognized.

Blockchain-based EHR systems not only increase security, performance but help in many ways not limited to the below mentioned advantages:

- The health record is easily accessible and available.
- Reduces human error caused by prescriptions written on paper.
- Brings paper prescriptions into the system, which helps to reduce the influx of counterfeit pharmaceuticals.
- Connects to stand-alone health-care systems.
- Patient-centric: Provides full autonomy to the patients for their own records.

In this survey, the authors have outlined some of the more common problems that have arisen due to the lack of robust communication and monitoring infrastructure, discussed related papers that illustrate these concerns, and the ability of Blockchain-based EHR systems to address them. The authors have also highlighted research gaps and proposed an architecture that can be implemented to address all the research gaps. A detailed architecture and implementation strategy will be part of the Authors' future work.

FUNDING AGENCY

Publisher has waived the Open Access publishing fee.

REFERENCES

Achkar, R., Ghayad, K., Haidar, R., Saleh, S., & Al Hajj, R. (2019). Medical Handwritten Prescription Recognition Using CRNN. In *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 1-5). IEEE.

Akarca, D., Xiu, P. Y., Ebbitt, D., Mustafa, B., Al-Ramadhani, H., & Albeyatti, A. (2019). Blockchain Secured Electronic Health Records: Patient Rights, Privacy and Cybersecurity. In *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 108-111). IEEE.

Al-Karaki, J. N., Gawanmeh, A., Ayache, M., & Mashaleh, A. (2019). DASS-CARE: a decentralized, accessible, scalable, and secure healthcare framework using blockchain. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 330-335). IEEE. doi:10.1109/IWCMC.2019.8766714

Alla, S., Soltanisehat, L., Tatar, U., & Keskin, O. (2018, May). Blockchain technology in electronic healthcare systems. In *Proceedings of the 2018 IISE Annual Conference* (pp. 1-6). IISE.

Bhattacharya, P., Tanwar, S., Bodke, U., Tyagi, S., & Kumar, N. (2019). Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. *IEEE Transactions on Network Science and Engineering*.

Bhavin, M., Tanwar, S., Sharma, N., Tyagi, S., & Kumar, N. (2021). Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. *Journal of Information Security and Applications*, *56*, 102673. doi:10.1016/j.jisa.2020.102673

Carter, G., Shahriar, H., & Sneha, S. (2019). Blockchain-based interoperable electronic health record sharing framework. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (Vol. 2, pp. 452-457). IEEE. doi:10.1109/COMPSAC.2019.10248

Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, *95*, 420–429. doi:10.1016/j.future.2019.01.018

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. *Journal of Medical Systems*, *43*(1), 1–9. doi:10.1007/s10916-018-1121-4 PMID:30467604

Cunningham, J., & Ainsworth, J. (2018). Enabling patient control of personal electronic health records through distributed ledger technology. *Studies in Health Technology and Informatics*, *245*, 45–48. PMID:29295049

da Conceição, A. F., da Silva, F. S. C., Rocha, V., Locoro, A., & Barguil, J. M. (2018). *Electronic health records using blockchain technology.* arXiv preprint arXiv:1804.10078.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. doi:10.1016/j.scs.2018.02.014

Donawa, A., Orukari, I., & Baker, C. E. (2019). *Scaling blockchains to support electronic health records for hospital systems. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 550-556)*. IEEE.

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., Jahangir, M. M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S. D., Ryu, S., & Wang, F. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research*, *22*(8), e13598. doi:10.2196/13598 PMID:32821064

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (*Vol. 13*). Academic Press.

Fu, J., Wang, N., & Cai, Y. (2020). Privacy-preserving in healthcare blockchain systems based on lightweight message sharing. *Sensors (Basel)*, *20*(7), 1898. doi:10.3390/s20071898 PMID:32235389

Harshini, V. M., Danai, S., Usha, H. R., & Kounte, M. R. (2019). Health record management through blockchain technology. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 1411-1415). IEEE. doi:10.1109/ICOEI.2019.8862594

Ivan, D. (2016, August). Moving toward a blockchain-based method for the secure storage of patient records. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST* (pp. 1-11). SN.

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 310-317). IEEE. doi:10.1109/ICIoT48696.2020.9089570

Kassab, M., DeFranco, J., Malas, T., Neto, V. V. G., & Destefanis, G. (2019). Blockchain: a panacea for electronic health records? In *2019 IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH)* (pp. 21-24). IEEE. doi:10.1109/SEH.2019.00011

Kombe, C., Dida, M., & Sam, A. (2018). *A review on healthcare information systems and consensus protocols in blockchain technology*. Academic Press.

Kombe, C., Sam, A., Ally, M., & Finne, A. (2019). Blockchain Technology in Sub-Saharan Africa: Where does it fit in Healthcare Systems: A case of Tanzania. *Journal of Health Informatics in Developing Countries*, *13*(2).

Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018). BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In *2018 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE. doi:10.1109/GLOCOM.2018.8647713

Liu, X., Wang, Z., Jin, C., Li, F., & Li, G. (2019). A blockchain-based medical data sharing and protection scheme. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 118943–118953. doi:10.1109/ACCESS.2019.2937685

Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., & Ellahham, S. (2020). Blockchain for giving patients control over their medical records. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 193102–193115. doi:10.1109/ACCESS.2020.3032553

Mahore, V., Aggarwal, P., Andola, N., & Venkatesan, S. (2019). Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain. In *2019 IEEE Conference on Information and Communication Technology* (pp. 1-6). IEEE. doi:10.1109/CICT48419.2019.9066204

Maitra, D. S., Bhattacharya, U., & Parui, S. K. (2015). CNN based common approach to handwritten character recognition of multiple scripts. In *2015 13th International Conference on Document Analysis and Recognition (ICDAR)* (pp. 1021-1025). IEEE. doi:10.1109/ICDAR.2015.7333916

Niu, S., Chen, L., Wang, J., & Yu, F. (2019). Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 7195–7204. doi:10.1109/ACCESS.2019.2959044

Oommen, C. K. (2021). *Data, Privacy, Pandemic: India just had the Biggest Medical Records Breach Ever*. https://www.orfonline.org/expert-speak/data-privacy-pandemic-india-just-had-the-biggest-medical-records-breach-ever/

Randall, D., Goel, P., & Abujamra, R. (2017). Blockchain applications and use cases in health information technology. *Journal of Health & Medical Informatics*, *8*(3), 8–11. doi:10.4172/2157-7420.1000276

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017). Towards using blockchain technology for eHealth data access management. In *2017 fourth international conference on advances in biomedical engineering (ICABME)* (pp. 1-4). IEEE. doi:10.1109/ICABME.2017.8167555

Seitz, J., & Wickramasinghe, N. (2017). Blockchain technology in e-health: The case of electronic prescriptions in Germany. In *XVII international scientific conference on industrial systems* (pp. 156-159). Academic Press.

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 147782–147795. doi:10.1109/ACCESS.2019.2946373

Shanthapriya, R., & Vaithianathan, V. (2020). Block-healthnet: Security based healthcare system using blockchain technology. *Security Journal*, 1–19.

Sharma, Y., & Balamurugan, B. (2020). Preserving the privacy of electronic health records using blockchain. *Procedia Computer Science*, *173*, 171–180. doi:10.1016/j.procs.2020.06.021

Singh, A. P., Pradhan, N. R., Luhach, A. K., Agnihotri, S., Jhanjhi, N. Z., Verma, S., Kavita, , Ghosh, U., & Roy, D. S. (2020). A novel patient-centric architectural framework for blockchain-enabled healthcare applications. *IEEE Transactions on Industrial Informatics*, *17*(8), 5779–5789. doi:10.1109/TII.2020.3037889

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407. doi:10.1016/j.jisa.2019.102407

Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. (2018). BHEEM: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE. doi:10.1109/GLOCOMW.2018.8644088

Yang, G., & Li, C. (2018). A design of blockchain-based architecture for the security of electronic health record (EHR) systems. In *2018 IEEE International conference on cloud computing technology and science (CloudCom)* (pp. 261-265). IEEE. doi:10.1109/CloudCom2018.2018.00058

Zghaibeh, M., Farooq, U., Hasan, N. U., & Baig, I. (2020). SHealth: A blockchain-based health system with smart contracts capabilities. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 70030–70043. doi:10.1109/ACCESS.2020.2986789

Zhuang, Y., Sheets, L. R., Chen, Y. W., Shae, Z. Y., Tsai, J. J., & Shyu, C. R. (2020). A patient-centric health information exchange framework using blockchain technology. *IEEE Journal of Biomedical and Health Informatics*, *24*(8), 2169–2176. doi:10.1109/JBHI.2020.2993072 PMID:32396110

Hammad S. Choudhury is a driven tech professional with over 2 years of experience working with industry leading companies. He has a bachelors degree in Computer Science from Queens College, The City University of New York. Curranty pursuing his career path as a Business Systems Analyst, he hopes to continue making meaningful contributions to the field of Computer Science and Information Technology.