International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 09 | September - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Review Paper on Secure Cloud-based Electronic Health Records Systems using Blockchain

Sonal Shakya (0225CS20MT18, sonalshakya97@gmail.com)*

*[1](Department of CSE, Global Nature Care Sangathan's Group of Institutions, Jabalpur)

Abstract

Cloud-based electronic health records (EHRs) have gained significant attention to enable remote patient monitoring. The recent development of Healthcare 4.0 using the Internet of Things (IoT) components and cloud computingto access medical operations remotely has gained the researcher's attention from a smart city perspective. Healthcare 4.0 mainly consisted of periodic medical data sensing, aggregation, data transmission, data sharing, and data storage. The sensitive and personal data of patients lead to several challenges while protecting it from hackers. Therefore storing, accessing, and sharing the patient medical information on the cloud needs security attention that data should not be compromised by the authorized user's components of E-healthcare systems. To achieve secure medical data storage, sharing, and accessing in cloud service provider, several cryptography algorithms are designed so far. However, such conventional solutions failed to achieve the trade-off between the requirements of EHR security solutions such as computational efficiency, service side verification, user side verifications, without the trusted third party, and strong security. Blockchain-based security solutionsgained significant attention in the recent past due to the ability to provide strong security for data storage and sharing with the minimum computation efforts. Utilizing the blockchain which secure healthcare records management has been of recent interest. This review paper presents the systematic study of modern blockchain-based solutions for securing medical data with or without cloud computing.

Keywords Bitcoin · Blockchain · Cloud service provider · Electronic heath records · Healthcare 4.0 · Medical data · Datastorage · Data sharing · Security

Introduction

Healthcare 4.0 is a phrase that has developed lately and received from Industry. Nowadays, the healthcare area is more digital than earlier days; for instance, growing from Magnetic Resonance Imaging (MRI) and X-rays to Computed Tomography (CT) and ultrasound scans to electronic medical documents. Medical data

processing is an important task of the Healthcare 4.0 standard. Since from the 10 year, it observed that healthcare is data- intensive technology in which a huge amount of data introduced , disseminated, saved, and fetched frequently. When the patient undergoes any tests, for example, its data are created that further needs to disseminate to the medical experts like radiographer and physician. In smart health- care systems, the medical data stored in the hospital servers by considering the future requirements of accessing by the authorized physician from the hospital located within their networks. A significant role can play by technology while improving the quality of service for the patients. It allows data analytics to take appropriate medical decisions.

Healthcare 4.0

For healthcare 4.0, several components considered to estab-lish the remote health monitoring and emergency control. This section presents the design of cloud-based healthcare data processing, security requirements, and emergence of blockhain technology.

Cloud-based healthcare system

In general, *Electronic Medical Records (EMRs)* contain ther-apeutic and clinical data identified with a given patient andput away by the dependable healthcare supplier. It encour- ages the recovery and examination of healthcare data. To more readily bolster the administration of EMRs, early agesof *Healthcare Information System* (HIS) planned with the ability to make new EMR examples, store them, and ques- tion and recover put away EMRs of interest. HIS can be moderately straightforward solutions and schematically depicted as a graphical user interface or a web administra- tion. These are commonly the front-end with a database at the back-end, in concentrated or disseminated implementa- tion. With patient portability (both inside and remotely toa given nation) being progressively the standard in the pre- sent society, it wound up evident that numerous independent EMR solutions must make interoperable to encourage the sharing of healthcare data among various suppliers. Even crosswise over national fringes, as required.

To encourage data distribution and patient data dispatch capability, there is a demand for EMRs to formalize their data composition and the design of HIS. The EHRs are designed to facilitate patient therapeutic records to proceedwith the victim or be made available to diverse healthcare suppliers. EHRs have an improvident data structure com- pared to EMRs. There are supplementary actions to developup HIS and foundations to balance and sustain future demands, as approved by the various national and global enterprises. For example, the Fascicolo Sanitario Elettronico (FSE) venture in Italy, the epSOS venture in Europe, and a continuous task to institutionalize the sharing of EHRs. As of late, the inescapability of savvy devices (Android and iOS devices and wearable devices) has likewise brought about a change in perspective inside the healthcare busi-

ness. Such devices can be client possessed or introduced bythe healthcare supplier to gauge the prosperity of the clients(for example, patients) and educate/encourage treatment andobserving of patients. For instance, there is a wide scope ofportable (applications) in wellbeing, wellness, weight reduc-tion, and other healthcare-related classes. These applicationspredominantly work as the following apparatus, for exam- ple, enlisting client exercises/exercises, keeping the check of devoured calories, and different insights (for example, number of steps taken, etc.

There are likewise devices with implanted sensors for further developed therapeutic errands, for example, brace- lets to quantify heartbeat during exercises, or devices for self-testing of glucose. The data (for example, the client's crucial signs) can be consistently accumulated and sent pro-gressively to a brilliant gadget, before being sent to a remote healthcare cloud for further analysis. The ongoing improve- ments made ready for *Personal Health Records* (PHR), where patients progressively engaged with their data col- lection, observing their wellbeing conditions, and so on, utilizing their advanced mobile phones or wearable devices (for example, shrewd shirts and brilliant socks). With such systems, several challenges associated such as related to theprocess of medical data collection and its processing:

- Should we depend on medical data gathered by end-usersthemselves?
- Should the appropriate healthcare providers approved data gathered by the subjects, and if consequently, whence can that be achieved?
- Who should be professionally responsible for misdiagnsis or late diagnosis, because of judgments being made on the data transmitted from the device of the patient thatis afterward confirmed to be inaccurate or flawed?

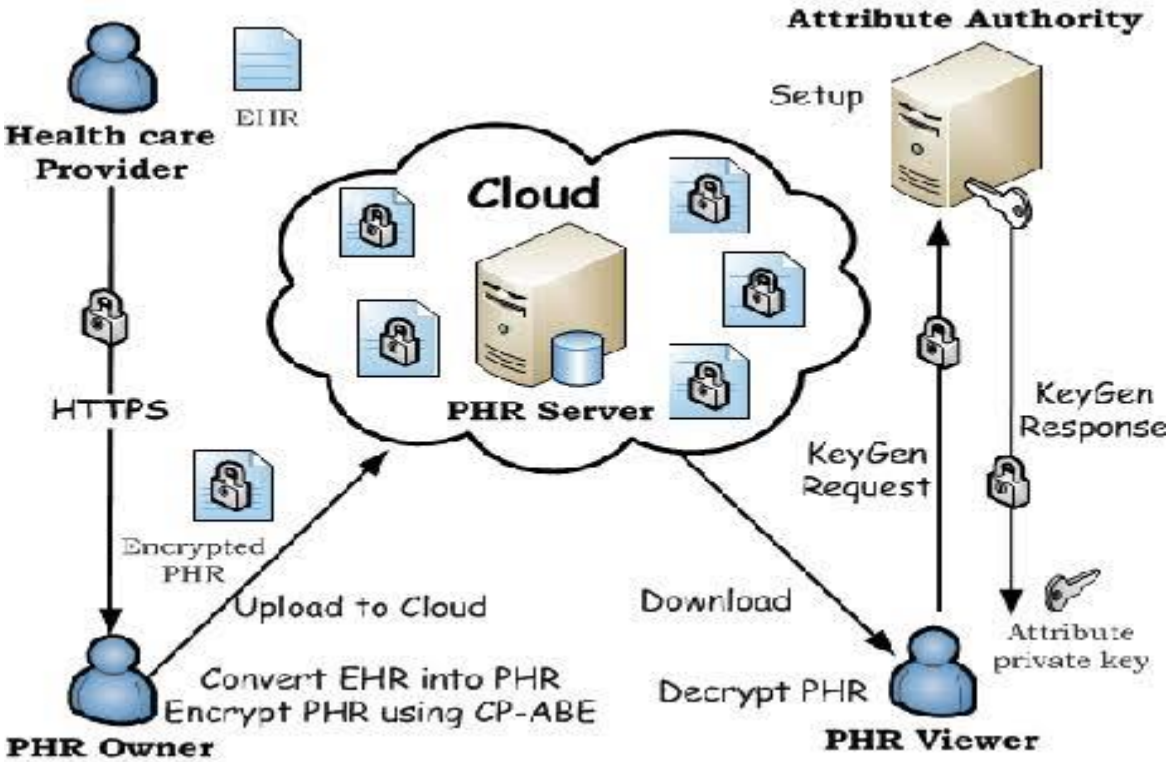
Despite the above-listed challenges of healthcare systems, the presence of such a system can provide seamless data sharing among hospitals, and patients who provide theabstraction of single wellbeing data stockpiling for some random patient will profit all clients, going from patients tosocial insurance suppliers to governments. The well-knownframework called cloud computing is an appropriate solution as it supports the real-time data sharing all over the world, supports resource elasticity, and handling the big data to fetch the important information from the enormous medicinal services data for research and strategy basic leadership. General cloud-based system of storing and sharing the medical data among the different providers which sup- porting every supplier in dealing with their data, giving a consistent method for trading and possibly ensuring data among EHR and PHR, and giving a bound together perspective on human services records for every patient. As showingin Fig. 1, all key terms of healthcare systems demonstrated such as PHR in which the patients collect their data and storein the cloud, EMR at every healthcare provider which can access the reports of the individual patient from the cloud storage, and EHR, a cloud storage system from which the user or hospitals

can access the medical history of the patientwhen it's required from any geographical location.

security and privacy in Healthcare

As the medical reports containing the sensitive data of individuals , it may get attention from hackers. The attackers looking to profit monetarily from the hacking of individual medicinal data as it would hold any importance with specific associations or industries. Thus it becomes essential to provide security for systems like EHR, PHR, and EMR. Moreover, the privacy and integrity of healthcare attacks can be purposeful and unintentional, and associations might be punished or held criminally obligated for such episodes, for instance, under the Medical coverage Compactness and Accountability Act. Since from the last two decades, how to secure such a system that ensures the protection and integrity of the data is increasingly critical considerations. Strategies incorporate utilizing cryptographic natives, for example,
those dependent on an open key foundation and open mists to guarantee data secrecy and protection.

But such methods having the limitation of data searching as in medicinal services suppliers need to unscramble the data preceding looking at the decoded data, bringing about increments in time and expenses for the data recovery and (Poh et al. 2017). Access control models have additionally been utilized to direct and restrict access to the data, in light of predefined get to policies. Such models can be especially successful for outside assaults, however, commonly ineffectual against inside attackers as they are probably going to be approved to get to the data (Alam et al. 2017; Li et al.2013).



Emergence of blockchain

The blockchain is an answer to all the challenges of other centralized security solutions of data storage and sharing in cloud computing (Knirsch et al. 2019; Pirtle and Ehrenfeld 2018). It is a new paradigm of data documentation on the internet. The blockchain can be used in applications such as voting systems, online shopping, social networks, games (Scriber 2018; Esposito et al. 2018), storage platforms (like cloud computing), messengers, prediction markets, and online education (Kshetri 2018; Alhayani and Abdallah 2020). The data considered in blockchain can be of any form such as medical reports sharing, money transfer, individual's identity, ownership (Alhayani and llhan 2021; Alhayani et al. 2021a), sensitive information. Figure 2 illustrates the step by step working of blockchain technology, and Fig. 3 shows the same technology using the cryptography structure (Al-Hayani and Ilhan 2020; Kwekha-Rashid et al. 2021).

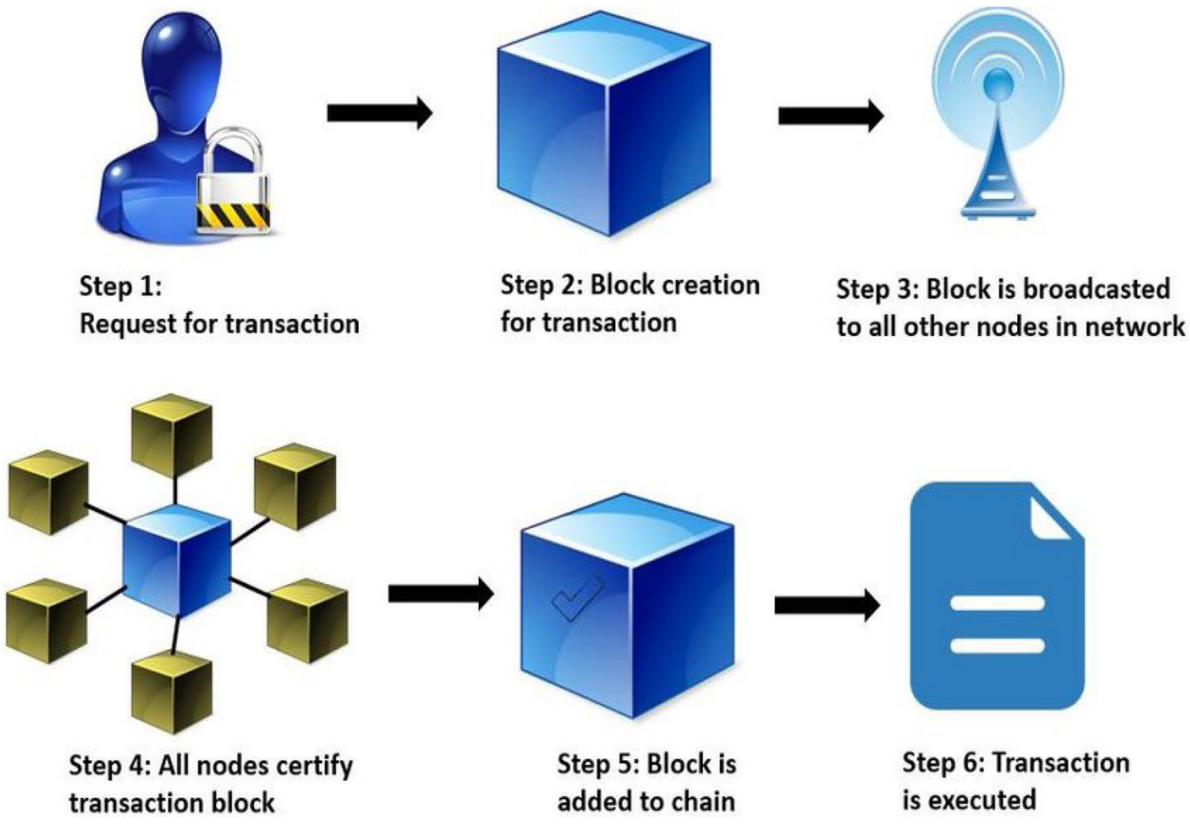


Fig. 2 step by step working of block chain

Literature Review

Hence medical data dissemination has received the researcher's attention for novel approaches for patient treatment. The digitization, electronic storage, and medical data remote access by the medical experts are a key base for an above-said statement (Costa 2014). The electronic information about the patients created by the hospitals since after their visit and making them individual owners of such electronic data (Huang et al. 2014).

The significance of medical data and the integration with its distribution has given origin to enterprise substances that consolidate, process, interpret, store, and presented the appropriate incentive distribution of data with other connected individuals (Huang et al. 2018; Aceto et al. 2013; Assis et al. 2014; O'Driscoll et al. 2013).

Due to the industrial nature, assuring the integrity, security, privacy of medical data is essential. Thus it required the efficient and secure framework of data management (Grozev and Buyya 2012). The CSP contested with a necessity of collaboration for medical data sharing because of unfavorable hazards acted on exhibiting the details on their data (Fazio et al. 2015). For data masters and managers, it is the actual danger of received data revealed in the controls of attacker data users (Kuo 2011; Weber et al. 2014; Shao et al. 2015).

To address such challenges many cryptographic techniques have been introduced for secure healthcare data storage and sharing, however, they have still been inadequate (Thilakanathan et al. 2014; Khan et al. 2014; Dong et al. 2014; Yang et al. 2015). The cryptography techniques are proposed by considering the cloud server's untrustworthiness and the user's data privacy. It's important to perform data encryption before outsourcing it to the cloud server.

The recent works introduced the blockchain for secure data processing (Tschorsch and Scheuermann 2016; Azaria et al. 2016; Zhang et al. 2016). The blockchain is a technology ready to assemble an open and circulated online database comprises a rundown of data structures called obstructs that are connected to fabricate the chain. These blocks are conveyed among numerous hubs of a foundation and not halfway put away.

The attributed based encryption is another solution that integrates access control with some cryptographic primitives (Xu 2016; Niranjanamurthy et al. 2018). However, such a method does not achieve all concerns of security with acceptable (Dinh et al. 2018; Ocheja et al. 2019; Shahzad and Crowcroft 2019; Turkanovic et al. 2018) computational efforts. The conventional centralized solutions may get compromised during the online

data processing systems (Kshetri and Voas 2018; Chen et al. 2018a), thus the recent decentralized approach called blockchain gains significant interests since from last five years.

The data considered in blockchain can be of any form such as medical reports sharing, money transfer, individual's identity, ownership (Alhayani and llhan 2021; Alhayani et al. 2021a), sensitive information.

it noticed that in blockchain the information does not keep at a central point like the conventional security methods (Hasan and Alhayani 2021; Yahya et al. 2021; Abu-Rumman 2021; Abu-Rumman et al. 2021). The multiple copies of similar data are stored in various locations and on various devices, and hence it is called distributed technology (Aldiabat et al. 2018, 2019). As the multiple copies of the same data available, the loss of any single point of storage does not affect the security of the original data (Rashid et al. 2021; Chen et al. 2019).

In short, the data packaged into different a block that links to build the chain with other blocks of the same information (Kamel Boulos et al. 2018; Zhou et al.2018).

Once the chain of block build (Xia et al. 2017a, 2017b), it is not possible to alter any single block without altering all other blocks, hence it becomes very difficult to compromise the security using blockchain.

The public blockchain technology is available for everyone publically as the name indicates.
In the public blockchain, there is no need for taking permission to become part of the public blockchain (Xia et al. 2017b; Gao et al. 2018). In a public blockchain, any kind of transaction is valid for all the end-users (Zhang et al. 2018b; Chen et al. 2018b).

This type of blockchain exactly opposite to the public blockchain as it is a centralized system. However, the security threat risk higher in this blockchain technology (Tian et al. 2019; Rathee et al. 2020). The cost of transactions is less as well as the process of document handling is easier using a private blockchain. The well-known private blockchain technologies are MONAX and Multichain.

Initially, several malicious activities and frauds that can be tackled using the blockchain method presented in Mikhail et al. (2017a). They presented the suggestions for future research into the methods of protecting the malicious activities related to the blockchains.

Alhayani et al. (2021b) in which the definition of blockchain presented, types of blockchain, working of blockchain, and SWOT analysis of blockchain introduced. They also presented the advantages and challenges of using blockchain based on the SWOT analysis. In (Dinh et al. 2018), the author presented the study to understand and estimate the future directions of using the blockchain. They designed the
block bench framework to understand the performance of the private blockchain against the workloads of data processing. They evaluated three different blockchains such as Parity, Ethereum, and Hyper ledger Fabric on block bench.

The study presented in Xu (2016), Niranjanamurthy et al. (2018), and Dinh et al. (2018) is more on the functionality understanding of blockchain and future directions without actual implantation by considering the applications.

In Ocheja et al. (2019), the author presented the framework called blockchain of learning logs (BOLL) to move the students their study records starting with one organization, then onto the next in a verifiable and secure manner to address the cool beginning issue in learning frameworks. The BOLL framework allowed access to learning logs from other institutions to the existing learning data analytic stages
according to the learners and/or institution permission. However, BOLL was introduced at the initial level without considering the challenges of scalability and reliability.

In Shahzad and Crowcroft (2019), another recent blockchain- based framework was introduced to secure the electronic voting system. They presented a framework based on successful hashing techniques to guarantee data security.

In Turkanovic et al. (2018), the blockchain-based education system introduced called EduCTX. The EduCTX in light of the idea of the European Credit Move and Aggregation Framework (ECTS). They presented the environment prototype implementation using the Ark Blockchain platform. They mentioned that EduCTX will process, oversee, and control the ECTX tokens that demonstrate the student
credits gained from course completion. Similar to the limitations of Shahzad and Crowcroft (2019), this approach also suffered from those issues.

Similar to Shahzad and Crowcroft (2019), another blockchain- based E-voting system introduced in Kshetri and Voas (2018) called Blockchain-enabled e-voting (BEV). They presented the study of various BEV implementations and their challenges. They summarized their study with the advantages

of BEV over the conventional voting process without actually any design and implementations for it.

In Chen et al. (2018a), the author presented various applications of education and the use of a blockchain framework to address some problems of such applications. They presented the advantages and working of blockchain technology. They reviewed some blockchain-based applications with their advantages for education.

In Bistarelli et al. (2019), the author proposed the decentralized start to finish casting a ballot stage dependent on the blockchain innovation. They designed the e-voting system using the Bitcoin and Multi Chain systems with a similar underlying concept as a transaction among the voter and competitor speak to a vote, which is communicated to the distributed network and confirmed by diggers.

In Alhayani and Abdallah (2020), the first proper methodology presented in which the design and analysis of blockchain-based securing healthcare data in cloud servers are presented. They designed a blockchain-based accessible encryption method for the EHRs. The EHRs file constructed using the mind-boggling rationale articulations and afterward put away in blockchain such a way that users can exploit the expressions to index searching.

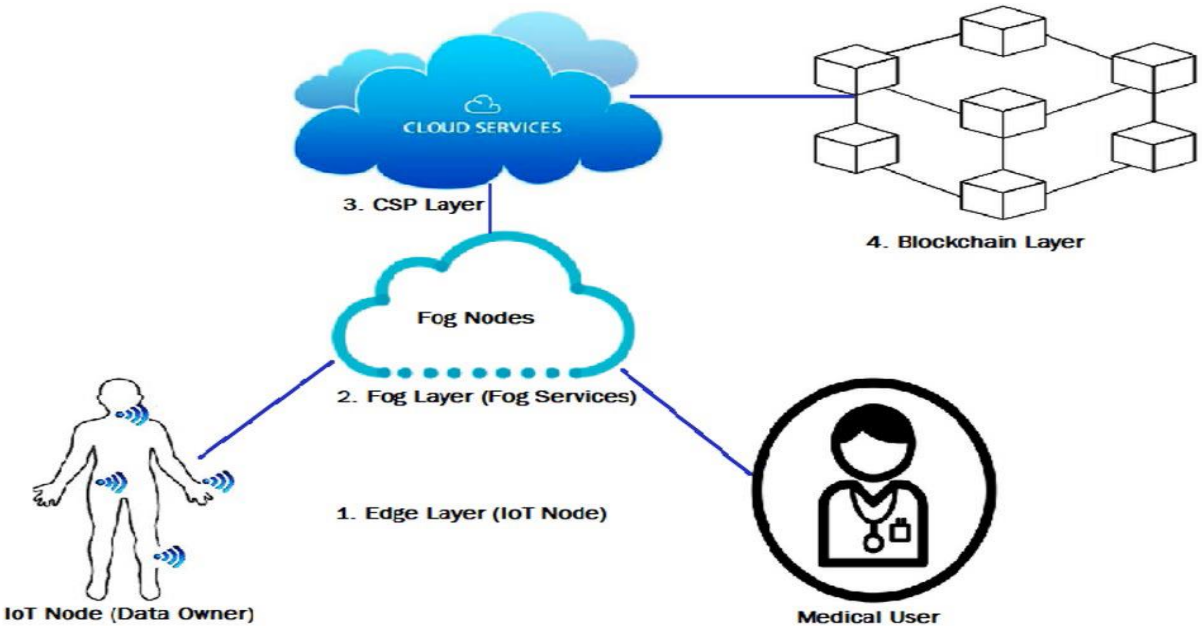
In Alhayani and llhan (2021), another approach of parallel PHSs utilizing the Fake frameworks, Computational analyses, Parallel execution called ACP proposed. The artificial intelligence was used for the decision-making process in patients' diagnosis and treatment process. They additionally used the blockchain methodology using constructing a consortium blockchain connecting patients, wellbeing
authorities, hospitals, and the medicinal services networks for secure medical data storage and sharing.

In Kwekha-Rashid et al. (2021), another study-based invention presented over the blockchain system for the healthcare systems. They presented the promises, challenges, and scenarios in healthcare systems using the geospatial blockchain along with the future directions. In Hasan and Alhayani (2021), the author proposed a blockchain based medical insurance storage framework called MI Store. They designed the MI Store framework with key features such as decentralization, secure data storage, threshold,
verifiable, efficient verification, and efficient homomorphic computation.

The MeD Share proposed in Abu-Rumman (2021) to tackle the problem of healthcare data sharing between pharmaceutical big data escorts in trust-less conditions. The blockchain technology applied to achieve the data auditing, data provenance, and control for shared data in cloud containers among big data substances.

Proposed Model

This section presents the proposed system model for healthcare monitoring using blockchain and cloud computing.



Conclusion

Nowadays, most healthcare organizations do not have the facility to protect the patient's data from unauthorized access, and hence present EHRs may fail to meet the privacy requirements of patients. The emergence of Healthcare 4.0 using the technologies Internet of Things (IoT), Cloud computing, Big data, and blockchain has required to deal with security challenges for medical data processing. Various centralized cryptography solutions were introduced to secure such data, however, they failed to address the problems completely. In this paper, we introduced blockchain technology that may overcome the challenges of providing EHRs security based on the review of recent works. We presented the model of EHRs first, then the applicability of blockchain in EHRs along with its benefits.

References

1.Abu-Rumman A, Al Shraah A, Al-Madi F et al (2021) Entrepreneurial networks, entrepreneurial orientation, and performance of small and medium enterprises: are dynamic capabilities the missing link? J Innov Entrep 10:29.

2. Aceto G, Botta A, de Donato W, Pescapè A (2013) Cloud monitoring: a survey. Comput Netw 57(9):2093–2115.

3. Alam Q, Malik SUR, Akhunzada A, Choo K-KR, Tabbasum S, Alam M (2017) A cross tenant access control (CTAC) model for cloud computing: formal specification and verification. IEEE Trans Inf Forensics Secur 12(6):1259–1268.

4. Aldiabat K, Kwekha Rashid AS, Talafha H, Karajeh A (2018) The extent of smartphones users to adopt the use of cloud storage. J Comput Sci 14(12):1588–1598.

5. Aldiabat K, Al-Gasaymeh A, Rashid AK (2019) The Effect of Mobile Banking Application on Customer Interaction in the Jordanian Banking Industry 13(2):37–49.

6. Alhayani B, Abdallah AA (2020) Manufacturing intelligent Corvus corone module for a secured two way image transmission under WSN. Eng Comput.

7. Alhayani B, Ilhan H (2020) Efficient cooperative image transmission in one-way multi-hop sensor network. Int J Electr Eng Educ 57(4):321–339

8. Alhayani BSA, llhan H (2021) Visual sensor intelligent module based image transmission in industrial manufacturing for monitoring and manipulation problems. J Intell Manuf 32(2):597–610

9. Alhayani B, Abbas ST, Mohammed HJ et al (2021a) Intelligent secured two-way image transmission using corvus corone module over WSN. Wirel Pers Commun.

10. Alhayani B, Abbas ST, Mohammed HJ, Mahajan HB (2021b) Intelligent secured two-way image transmission using corvus corone module over WSN. Wirel Pers Commun.

11. Assis MRM, Bittencourt LF, Tolosana-Calasanz R (2014) Cloud federation: characterisation and conceptual model. In: 2014 IEEE/ ACM 7th ınternational conference on utility and cloud computing.

12. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: using blockchain for medical data access and permission management. In: 2016 2nd ınternational conference on open and big data.

13. Bistarelli S, Mercanti I, Santancini P, Santini F (2019) End-to-end voting with non-permissioned and permissioned ledgers. J Grid Comput.

14. Borgman CL (2011) The conundrum of sharing research data. SSRN Electron J.

15. Chen M, Mao S, Liu Y (2014) Big data: a survey. Mobile Netw Appl 19(2):171–209.

16. Chen G, Xu B, Lu M, Chen N-S (2018a) Exploring blockchain technology and its potential applications for education. Smart Learn Environ.

17. Chen L, Lee W-K, Chang C-C, Choo K-KR, Zhang N (2019) Blockchain based searchable encryption for electronic health record sharing. Futur Gener Comput Syst.

18. Kwekha-Rashid AS, Abduljabbar HN, Alhayani B (2021) Coronavirus disease (COVID-19) cases analysis using machine learning applications. Appl Nanosci.

19. Mahajan HB, Badarla A (2020) Detecting HTTP vulnerabilities in IoT-based precision farming connected with cloud environment using artificial intelligence. Int J Adv Sci Technol 29(3):214–226.

20. Mahajan HB, Badarla A (2021) Cross-layer protocol for WSN-assisted IoT smart farming applications using nature inspired algorithm. Wirel Pers Commun.

21. Mahajan HB, Badarla A, Junnarkar AA (2021) CL-IoT: cross-layer internet of things protocol for intelligent manufacturing of smart farming. J Ambient Intell Human Comput 12:7777–7791.

22. Rocha Á, Adeli H, Reis LP, Costanzo S, Orovic I, Moreira F (eds) (2020) Trends and ınnovations in ınformation systems and technologies. Adv Intell Syst Comput.

23. Tian H, He J, Ding Y (2019) Medical data management on blockchain with privacy. J Med Syst.

24. Pournaghi SM, Bayat M, Farjami Y (2020) MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. J Ambient Intell Humaniz Comput.

25. Nepal S, Ranjan R, Choo K-KR (2015) Trustworthy processing of healthcare big data in hybrid clouds. IEEE Cloud Comput
2(2):78–84.

26. Mahajan HB, Badarla A (2021) Cross-layer protocol for WSN-assisted IoT smart farming applications using nature inspired algorithm. Wirel Pers Commun.

27. Tian H, He J, Ding Y (2019) Medical data management on blockchain with privacy. J Med Syst.

28. Shahzad B, Crowcroft J (2019) Fast iterative semi-blind receiver for URLLC in short-frame full-duplex systems with CFO. IEEE Access.

29. Rashid AS, Tout K, Yakan A (2021) The critical human behavior factors and their impact on knowledge management system– cycles. Bus Process Manag J.

30. Rathee G, Sharma A, Saini H, Kumar R, Iqbal R (2020) A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimed Tools Appl.