SURVEY ON BLOCKCHAIN-BASED SECURITY ENHANCEMENT SCHEME FOR HEALTHCARE APPLICATIONS

[1]Mr. K. Britto Alex, [2] Dr.K.Selvan

[1]Research Scholar, P.G. and Research Department of Computer Science, J.J. College of Arts and Science (Autonomous), Affiliated to Bharathidasan University, Pudukkottai. ***britto.alex@gmail.com***

[2]Assistant Professor & Research Advisor,P.G. and Research Department of Computer Science, J.J. College of Arts and Science(Autonomous), Affiliated to Bharathidasan University, Pudukkottai.

ABSTRACT

Considerable interest in Blockchain (BC) technologies may be attributed to the benefits it provides for shared security protocols, stability, and resilience. Banking, satellite data, interpretation of data, and health care system are just a few of the fields that have profited from this technique's development. Medical files, clinical trials, monitoring patients, increased safety, information presentation, and more flexibility can benefit from the usage of BC. It helps hospitals keep track of their finances and reduces the resources spent on data analysis. The use of blockchain-based technology within the healthcare industry allows for the secure transmission of patient's health information, simplifies the distribution of medications, and assists with genetics research. In this article, we investigated the viewpoints and perspectives of healthcare applications based on security enhancement schemes through BC technology. The goal of this review is to contribute to the investigation of blockchain's potential medical-related applications. To begin, it covers topics including medical data administration, data exchange, and data logging. Lastly, we want to investigate blockchain innovations in the healthcare profession by weighing their merits and demerits and providing direction for future research. We also highlight the benefits and drawbacks of the various healthcare procedures employed nowadays.

Keywords: *Blockchain (BC), security protocols, healthcare industry, secure transmission.*

1. INTRODUCTION

Every country's top priority for the world economy is its healthcare system. Healthcare is provided by experts and is defined as the enhancement or preservation of health via detection, therapy, and control of disease, injuries, sickness, as well as other psychologically and physically unwell persons (Raj [1]). The drawback of maintaining patient information traditionally by clinicians in the medical industry leads to record duplication and repetition.A patient's condition can be learned a lot from the available data kept in computerized health services (Tanwar et al. [2]). Additionally, it can be compiled and utilized to examine diseases as well as urban and rural medical centers. Such information is extremely helpful in the development of many different sectors and can help them comprehend events and overcome specific difficulties (Hathaliya et al. [3]). Yet, since it contains specific data regarding patients, this material should be regarded as a secret. Illegal health data exposure could have negative consequences and damage the reputation of medical groups (Sharma et al. [4]). To prevent inappropriate or unpleasant circumstances, it is essential to safeguard individual medical data and prevent unauthorized distribution (Shahnaz et al. [5]).

During the development of blockchain systems, different writers attempted to address the issues of dependability and security within the medical system (Yogeshwar and Kamalakkannan [6]). With this distributed system, it has become feasible to create more dependable platforms that can be controlled by the consumers individually (Zaabar et al. [7]). Due to the robustness, accessibility, durability, and other characteristics of the blockchain, difficulties relating to the security and confidentiality of healthcare data can be reduced (Xi et al. [8]). Another important factor is that blockchain technology helps with database management and information monitoring (Pelekoudas et al. [9]). Blockchain-based medical solutions must still resolve several obstacles, too. Another reason is that the platform's core components are anonymous, which renders it difficult to identify the relationships between nodes and the sources of the data (Alam et al. [10]). Figure 1 represents the role of blockchain in healthcare.

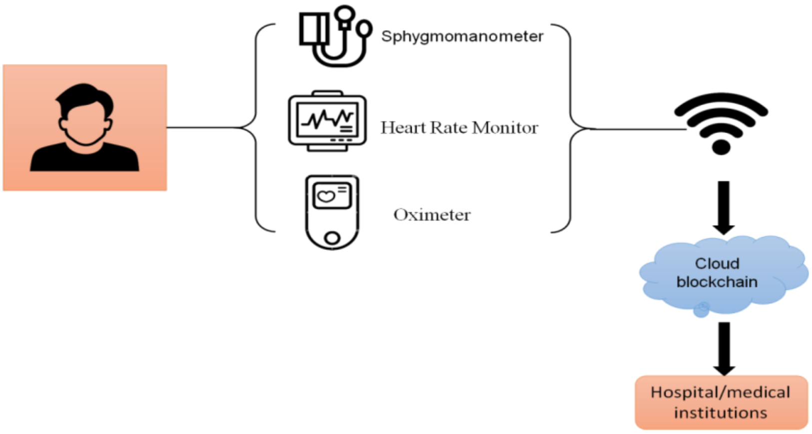

Figure 1: Role ofBlockchain in Healthcare

Based on the mode of involvement, blockchain can be split into three categories: general chain, personal chain, and cooperative chain (Azbeg et al. [11]). As the title suggests, everyone can view and employ a general chain. General chains are regarded as totally randomized since the content of the chain cannot be changed (Zulkifl et al. [12]). Basic learning, writing, and involvement valuation capabilities on the network are created by the group's regulations, and involvement in the cooperative chain is exclusively restricted to approved participants (Liu et al. [13]). Only private organizations have used personal chains, and the reading and writing rights on the network as well as the participation capabilities for billing are established by the regulations of the private entity (Taloba et al. [14]). Table 1 examines several blockchain protocols.

Table 1: Blockchain Protocols

Categories of BC	Federalization	Efficiency	Expensive	Scalability
General chain	Strong	Weak	strong	Bad
Co-operative chain	moderate	moderate	moderate	Good
Personal chain	Weak	Strong	weak	Good
Hybrid chain	-	-	weak	Good

BC is a network of interconnected units which are constantly growing as more transactions are recorded on the units (Gunanidhi and Krishnaveni [15]). This technology employs a randomized methodology that permits the distribution of information and the shared ownership of that scattered data piece (Mondal et al. [16]). Peer-to-peer systems control blockchain, which stores pieces of hashing operations that are secured by the technology. A blockchain offers advantages including safety, autonomy, and integrity of information without outside interference (Azbeg et al. [17]). Due to these advantages, it makes sense to keep patient information on it. Because of the technological advancements in the healthcare field, patient clinical data security has emerged as a significant concern (Purbey et al. [18]). Furthermore, we discussed the uses and difficulties of BC technology in the healthcare industry.

2. SURVEY ON UTILIZATION OF BLOCKCHAIN TECHNOLOGY FOR HEALTHCARE

For different applications, there are currently three main types of uses of blockchain for the transmission of health data. Storage of data and accessibility using a blockchain is the initial step (Hussien et al. [22]). The next is the integration of IoMT with blockchain technology. The final is the employment of blockchain to take the position of the government education system (Agbo and Mahmoud [23]).

2.1 Protection of stored data and its availability

A medical blockchain platform made on blockchain uses the BC as a database to record all of the participant's case details in the unit. To safeguard the information and stop hacking, the information stored is patched to save the calculated hash code, eliminating mistakes in the medical decision (Dwivedi et al. [24]). Information across all sectors is merged into a single hyper field maintained to solve the issue of a broad number of sources and formats of health data. The procedure employs on-chain recording. The BC, meanwhile, becomes less adjustable. On-chain storing costs money as well (Bell et al. [25]). A methodology for access control of personal data in medical practices that prioritizes protecting personal care may be implemented. Next, a personal data-storing framework is constructed using BC innovation, and the process of translation is achieved using conventional cryptographic methods. To further protect against the loss of healthcare private data, the personal data is additionally protected throughout this procedure by a document permission contract (Antwi et al. [26]). The analysis assumes an accessibility control technique with fine-grained data protection that provides constitutional protections for customers based on their kinds.Information is generated as hashing whenever they are stored within the cloud. After that, the hashing is kept on the blockchain (Siyal et al. [27]). By comparing the hash code on the network, it is possible to determine whether online information has been altered. The networks must do a variety of erroneous calculations. a simple blockchain-based system for exchanging and safeguarding patient records. The concept enables data exchange between doctors working in several institutions using proxy re-encryption technologies. The employed hashing is difficult to clash with (Ramzan et al. [28]). As a result, it's nearly difficult to alter recorded health data. Patients with a similar conditions may interact with one another thanks to a process that matches them together. Patients may establish a secret key after verification. Patients may communicate disease-related data with the use of this technique (Ben and Lahami [29]). Even though the personal chain is less decentralized, the transaction happens quickly. Implementations inside businesses or universities are more suited. If clinics and customers are several, it is not relevant. The personal chain of the digital instance was stored in the united network using a hybridized chain-based sharing method, while the non-private portion was stored in the public chain (Katuwal et al. [30]). The personal unit is only accessible to authorized individuals, while the non-private portion may be distributed to academic institutions with the goal of clinical research. To avoid information manipulation, the system primarily employs off-chain storage and only information hashing is saved on the network. Smart contracts may also easily handle the demand, permission, and use processes. No units are given any properties, meanwhile, coarse-grained permissions are employed instead. To get around the forking issue and provide an attack-resistant trust-based consensus method, a new chain structure is created (Kuo et al. [31]). By continual extraction, medical facilities may gain trust ratings. By a significant number of erroneous computations, the reputation program must tally reputation ratings. To have the ability to vote requires a lot of energy. Customers, physicians, caregivers, and executives all have varied authorizations granted to them through blockchain-based fine-grained network systems. This approach guarantees the query's efficiency while preserving the data's security. Role-based user access monitoring is another component of the technique (Hossein et al. [32]).

2.2 Blockchain Integrated with IoMT

The Internet of Medical Things (IoMT) comprises a wide variety of connected medical gadgets that monitor patient vitals utilizing a variety of computer-based sensors. The benefits of IoMT in therapeutic interventions are considerable, and early disease identification by the prediction of clinical indicators is of paramount importance. Despite its promise, IoMT is vulnerable to data leakage because of the proliferation of devices on the market that doesn't adhere to a single set of control rules. Safeguarding healthcare IoMT is a problem, but blockchain technology tries to address it (Khezr et al. [33]).

The safe and reliable transfer of patient information necessitates a data collection system built on the IOMT protocol. To accomplish real-time gathering of the patient's health information throughout surgery, the technology may gather data from several medical equipments concurrently. The technique is intended to function as a proxy re-encryption method for anonymously transmitting patient records over data centers. The confidentiality of sensitive health information is strengthened by this method (Ratta et al. [34]). Blockchains, a permission blockchain framework, form the basis for the platform's implementation; the system's two-channel deployment layout and healthcare chain code are optimized for database management and control. If half of the base stations failed, this scheme will still function, but it will not work if any of the base stations are malevolent. Because of this, the network seems to be more open to assault. To better protect patients' personal health information while in transit between healthcare facilities, a revolutionary blockchain-based secured authentication protocol has been developed. Valuable health records may be sent safely in healthcare IoT networks hosted on data centers owing to its sign creation and verifying capabilities (de et al. [35]). By allowing participants in a transaction to predefine requirements and operate the system via a central server, smart contracts eliminate the need for intermediaries. In addition, smart contracts offerseparate identities and locations on the blockchain, such that one IoT device may access its data and run its code without needing to communicate with the others.

First, information on patients is gathered with the help of IoTs and encoded using the such technique of choice. Moreover, this technique encrypts and compresses the blockchain's hashing. The last step is a categorization procedure. Even though the enhanced encryption technique is safer, it is also more time-consuming to use. Moreover, this design allows extensive utilization of smart contracts to forbid any harmful activity by establishing security rules using smart contracts. Easy identification is all that's used in this procedure. The nodes may be endowed with specific, granular characteristics. The analysis may be improved by doing this. Improper signs need more attention from time to time to lower the probability of a validation loss. IoMT relies heavily on blockchain digital currencies. Smart contracts may execute on their own if certain criteria are satisfied and don't necessitate any outside intervention. Cryptosystem methods are often used in the design for additional safety (Kumar et al. [36]).

2.3 Federated Blockchain for Healthcare and Education

Protecting sensitive information while developing novel algorithms is the goal of a novel process called federalized training. It is possible to effectively protect using federated learning since it allows several units to train a system publicly concurrently, but only the slopes and failures are sent among servers. Nevertheless, a further calculation requires the units to send their information to a central server. The centralized organization's corruption may be avoided with blockchain technology, making it a promising alternative. Utilization blockchain and off-chain methods are used to prevent manipulation of and accessibility to original data. Hazardous networks, which could be introduced by nodes in the network, can induce bias into the training phase. There is now a check and balance system in place to verify the legitimacy of the learning and its documented history (Ismail et al. [37]). It is possible to identify faulty nodes. Reputation scores may be used to filter out fraudulent nodes. The optimal arrangement, in which computational resources and information are shared across nodes, is challenging to establish in practice. Lacking financial incentives, and cooperation across nodes is challenging. Tokens should be distributed more equitably about node burden. The blockchain-based concept is utilized for collaboration amongst government medical facilities. A novel decentralized electronic medical records (EMR) hosting on servers located on the Inter Planetary file system (IPFS) architecture was developed to ease EMR distribution. Specifically, a blockchain-based smart contract was designed as an accessible authenticator to user identity at the platform's periphery without relying on a centralized server. Just a subset of hackers participates in every round of the majority phase's Byzantine algorithm validation. However this method may decrease some of the complexity, but it also makes organizations more vulnerable to attack. The whole training procedure is governed by this framework (Yoon [38]). The authors suggest new data security

International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 03, March 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

and an adaptable privacy protection method. Distortion is adjusted by the system during training to strike a good compromise between confidentiality and prediction precision. In conclusion, a gradient verification-based efficient consensual protocol is created to inspire trustworthy IoT systems and edge nodes to participate in federated learning by contributing information and processing capacity. Blockchain could be used instead of potentially problematic centralized institutions. The possibility of a single rogue node being at the core of the system is eliminated, and the immutable history of all transactions on the blockchain facilitates the prompt identification and removal of any bad actors. Moreover, the token economy enabled by blockchain's special economic qualities might incentivize networks to involve in simulation (Yu et al. [39]). Table 2 summarizes the characteristics of blockchain in the healthcare sector.

Table 2: Characteristics of Blockchain in Healthcare

Characteristics	(McGhin et al. [19])	(Radanović and Likić [20])	(Hölbl et al. [21])	This survey
Provides an overview of healthcare consensus procedures	X			X
Includes introduction of blockchain technology for medical distribution networks	X	X	X	X
Reference works on audits and security logs	X	X	X	X
Details the sources used to compile the study.	X		X	
Discusses the barriers that prevent the widespread use of blockchain technology in healthcare	X		X	X
Offers additional in-depth and recent writings on medical blockchain technology.				X
It provides a survey of the resources used in the business sector for constructing blockchain platforms.				X
Pros and cons of using blockchain technology in healthcare			X	X
Introduces blockchain technology and how it may be used to enhance healthcare privacy practices.				X
It presents how IoT and				X

blockchain work together				
Lists several ideas as to how blockchain may be used to improve healthcare and remote monitoring of patients.				X
Information security in medical records is examined, along with the role that blockchain technology may play in enhancing current systems.				X

3. SURVEY ON BARRIERS TO BLOCKCHAIN'S WIDER USE IN THE HEALTHCARE SYSTEM

Although being a transdisciplinary idea with its own set of issues and limits, blockchain technology has many potential applications. Scientists working in this field are trying to find ways around or mitigate such drawbacks. In this section, we discuss a few of the problems that arise from using blockchain technology in the medical industry (De et al. [40]).

- Efficiency: Higher operations and nodes imply greater verification need to be performed, which might slow things down if the system is already at capacity. With medical technology, high speed is problematic since slow response times would delay a diagnostic that could safeguard a patient's life.
- Delays in the system: the validation of a unit takes approximately ten minutes, which may be harmful to network security forces since assaults may be effective during that period. Although any lag in accessing might negatively impact the interpretation of an assessment, medical technology is continuously evolving and must be available around the clock. With a blockchain network, delay increases since all blocks are taking part in the testing phase. Just allowing a limited number of nodes to interact in the verification process saves resources and boosts processing speed and process efficiency.
- Protection: if a single organization controls 51% of the network's processing capabilities, the whole system is vulnerable. Because a damaged medical system might result in the legitimacy of medical institutions being undermined, this issue warrants significant focus.
- Usage of resources: there is a risk of significant resource depletion associated with the implementation of this technique, mostly due to the high energy costs of the mining operation. Due to the large number of instruments required to keep track of individual customers, the medical industry has increased power expenses. Yet, the deployment of digitalization may potentially result in significant computational and power expenditures. Keeping track of such expenses is a challenge for businesses.
- Accessibility: Usage is a concern with such technologies due to their complexity. Moreover, an API (Application Programming Interface) that is both accessible and intuitive must be developed. Technologies must be user-friendly and straightforward, as medical practitioners often lack the identical level of

technical expertise as computer scientists.To address the issue of scaling, we have implemented several different approaches, including strong forks, softer forks, the Illumination system, and ionized currency.

- Centralized services: While blockchain has a decentralized design, certain implementations concentrate the mining power in a small number of hands, which may lead to decreased system dependability. Data stored at this hub is susceptible to hacking assaults because of its centralized location.
- An emphasis on security: It is generally accepted that the Bitcoins structure makes it possible for blockchain to protect user anonymity. But still, the evidence disproves this theory. Moreover, methods are required to provide this capability to blockchain-based networks. Blockchain-based solutions must respond to the General Data Protection Regulation (GDPR) due to security rules and laws.
- Compatibility: Manufacturers are increasingly concerned about interoperable as they send blockchain designs through their paces for functional testing. The deployment and use of blockchain technology in a real-world medical environment depend on the definition of compatibility for an open system. When it came to compatibility across private blockchains, this ecosystem relied on common guidelines to ensure it.

4. SURVEY ON APPLICATIONS OF BLOCKCHAIN IN HEALTHCARE

Maintaining patient anonymity in the electronic era is of paramount importance. Blockchain technology is necessary for protecting patient information and enhancing the standard of care provided to each individual. Transactions are constructed from information blocks that have already been processed and are then recorded in a distributed ledger. It has found use in safeguarding information in a variety of fields, including the banking, financial, and hospitality sectors. Clinical, genetic, biological, pharmacological, and laboratory purposes are just some of the many areas where blockchain technology has been used (Abdellatif et al. [41]). Blockchain's major applications are illustrated in figure 2.

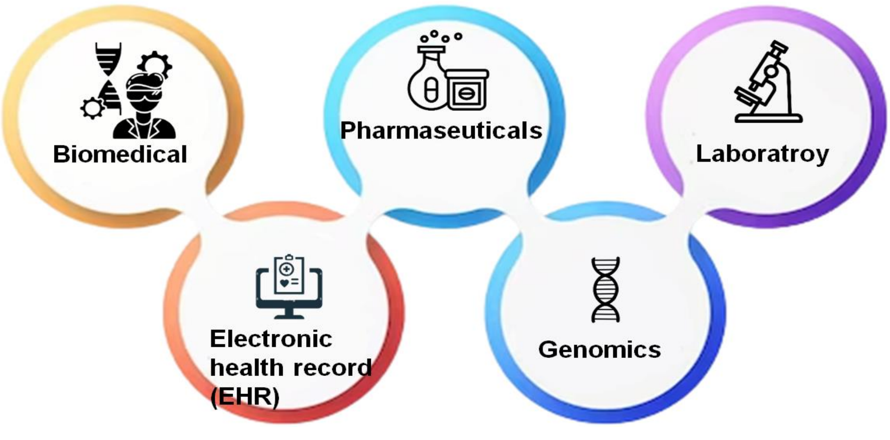

Figure 2: The major applications of BC

HER: The electronic health record (EHR) is a database of patient medical information that is stored in a decentralized ledger, making it impossible for any outside party to access the information. Each node in a blockchain maintains an accurate and verified version of the ledger, making it impossible for a hacker to corrupt the whole record. After receiving consent for treatment, medical institutions like clinics and laboratories may see their data on a blockchain network.

Clinical:When it comes to biomedical transactions, blockchain technology eliminated the possibility of data tampering and duplication. Blockchain alone permits safe and open trade.

Research institute:Blockchain is the only technology capable of creating a protected, decentralized framework for experimental data, and as a result, data may be exchanged safely throughout research teams.

Pharma:Blockchain was used to track drugs in great detail, and it continues to monitor the pharmaceutical distribution network, making sure that medicines and their components are constantly recognized at each stage to prevent any needless product substitutions.

Genetics: Blockchain technology may facilitate a generation of sequencing data revolutions by lowering the price of personal genetic analysis, distributing control of genetic information, and making genetic analysis exchange transparent.

5. CONCLUSION

Blockchain's decentralized, auditable, and tamper-resistant properties have stimulated the attention of the healthcare information industry. The study provides a unique overview and analysis of blockchain-based medical data exchange. This article provides a concise overview of potential use cases for exchanging health information and draws comparisons to more conventional methods of data analysis. Due to the central role played by smart contracts in the blockchain-based paradigm, it is significantly more secure and smarter than the conventional one. Yet, there are problems with the blockchain that limit its usefulness. These factors have slowed the adoption of blockchain for healthcare data exchange. In this article, we explored the potential applications of blockchain in the healthcare industry, namely in the realm of electronic medical records. These problems have persisted regardless of the growth of the medical industry and the introduction of electronic health records systems. Partitioning, cross-chain, and consensus mechanisms are all innovations that will be crucial in the future.

REFERENCE

[1] Raj, J.S., 2021. Security-enhanced Blockchain-based unmanned aerial vehicle health monitoring system. Journal of ISMAC, 3(02), pp.121-131.

[2] Tanwar, S., Parekh, K. and Evans, R., 2020. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, p.102407.

[3] Hathaliya, J., Sharma, P., Tanwar, S. and Gupta, R., 2019, December. Blockchain-based remote patient monitoring in healthcare 4.0. In 2019 IEEE 9th international conference on advanced computing (IACC) (pp. 87-91). IEEE.

[4] Sharma, P., Moparthi, N.R., Namasudra, S., Shanmuganathan, V. and Hsu, C.H., 2022. Blockchain-based IoT architecture to secure healthcare systems using identity-based encryption. Expert Systems, 39(10), p.e12915.

[5] Shahnaz, A., Qamar, U., and Khalid, A., 2019. Using blockchain for electronic health records. IEEE Access, 7, pp.147782-147795.

[6] Yogeshwar, A. and Kamalakkannan, S., 2021, May. Healthcare Domain in IoT with Blockchain-Based Security-A Researcher's Perspectives. In 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1-9). IEEE.

[7] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M. and Abid, M., 2021. HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, p.108500.

[8] Xi, P., Zhang, X., Wang, L., Liu, W., and Peng, S., 2022. A review of Blockchain-based secure sharing of healthcare data. Applied Sciences, 12(15), p.7912.

[9] Pelekoudas-Oikonomou, F., Zachos, G., Papaioannou, M., de Ree, M., Ribeiro, J.C., Mantas, G. and Rodriguez, J., 2022. Blockchain-based security mechanisms for IoMT Edge networks in IoMT-based healthcare monitoring systems. Sensors, 22(7), p.2449.

[10] Alam, S., Shuaib, M., Ahmad, S., Jayakody, D.N.K., Muthanna, A., Bharany, S. and Elgendy, I.A., 2022. Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration. Sustainability, 14(22), p.15312.

[11] Azbeg, K., Ouchetto, O. and Andaloussi, S.J., 2022. BlockMedCare: A healthcare system based on IoT, Blockchain, and IPFS for data management security. Egyptian Informatics Journal, 23(2), pp.329-343.

[12] Zulkifl, Z., Khan, F., Tahir, S., Afzal, M., Iqbal, W., Rehman, A., Saeed, S. and Almuhaideb, A.M., 2022. FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs. IEEE Access, 10, pp.15644-15656.

[13] Liu, Q., Liu, Y., Luo, M., He, D., Wang, H. and Choo, K.K.R., 2022. The security of blockchain-based medical systems: research challenges and opportunities. IEEE Systems Journal, 16(4), pp.5741-5752.

[14] Taloba, A.I., Elhadad, A., Rayan, A., Abd El-Aziz, R.M., Salem, M., Alzahrani, A.A., Alharithi, F.S. and Park, C., 2023. A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. Alexandria Engineering Journal, 65, pp.263-274.

[15] Gunanidhi, G.S. and Krishnaveni, R., 2022, February. Improved security blockchain for IoT-based healthcare monitoring system. In 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS) (pp. 1244-1247). IEEE.

[16] Mondal, S., Shafi, M., Gupta, S. and Gupta, S.K., 2022. Blockchain-based secure architecture for electronic healthcare record management. GMSARN Int J, 16(4), pp.413-26.

[17] Azbeg, K., Ouchetto, O. and Andaloussi, S.J., 2022. Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management. IEEE Transactions on Computational Social Systems.

[18] Purbey, S., Khandelwal, B. and Choudhary, A.K., 2023. Design of a blockchain-based secure and efficient ontology generation model for multiple data genres using augmented stratification in the healthcare industry.

[19] McGhin, T., Choo, K.K.R., Liu, C.Z. and He, D., 2019. Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, pp.62-75.

[20] Radanović, I. and Likić, R., 2018. Opportunities for use of blockchain technology in medicine. Applied health economics and health policy, 16, pp.583-590.

[21] Hölbl, M., Kompara, M., Kamišalić, A. and Nemec Zlatolas, L., 2018. A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), p.470.

[22] Hussien, H.M., Yasin, S.M., Udzir, S.N.I., Zaidan, A.A. and Zaidan, B.B., 2019. A systematic review for enabling of development blockchain technology in healthcare application: taxonomy, substantial analysis, motivations, challenges, recommendations, and future direction. Journal of medical systems, 43, pp.1-35.

[23] Agbo, C.C. and Mahmoud, Q.H., 2019. Comparison of blockchain frameworks for healthcare applications. Internet Technology Letters, 2(5), p.e122.

[24] Dwivedi, A.D., Malina, L., Dzurenda, P. and Srivastava, G., 2019, July. Optimized blockchain model for internet of things-based healthcare applications. In 2019 42nd international conference on telecommunications and signal processing (TSP) (pp. 135-139). IEEE.

[25] Bell, L., Buchanan, W.J., Cameron, J. and Lo, O., 2018. Applications of Blockchain within Healthcare. Blockchain in healthcare today.

[26] Antwi, M., Adnane, A., Ahmad, F., Hussain, R., ur Rehman, M.H. and Kerrache, C.A., 2021. The case of HyperLedger Fabric as a blockchain solution for healthcare applications. Blockchain: Research and Applications, 2(1), p.100012.

[27] Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A. and Soursou, G., 2019. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), p.3.

[28] Ramzan, S., Aqdus, A., Ravi, V., Koundal, D., Amin, R. and Al Ghamdi, M.A., 2022. Healthcare applications using blockchain technology: Motivations and challenges. IEEE Transactions on Engineering Management.

[29] Ben Fekih, R. and Lahami, M., 2020. Application of blockchain technology in healthcare: A comprehensive study. In The Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, June 24–26, 2020, Proceedings 18 (pp. 268-276). Springer International Publishing.

[30] Katuwal, G.J., Pandey, S., Hennessey, M. and Lamichhane, B., 2018. Applications of blockchain in healthcare: current landscape & challenges. arXiv preprint arXiv:1812.02776.

[31] Kuo, T.T., Zavaleta Rojas, H. and Ohno-Machado, L., 2019. Comparison of blockchain platforms: a systematic review and healthcare examples. Journal of the American Medical Informatics Association, 26(5), pp.462-478.

[32] Hossein, K.M., Esmaeili, M.E., Dargahi, T., Khonsari, A. and Conti, M., 2021. BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. Computer Communications, 180, pp.31-47.

[33] Khezr, S., Moniruzzaman, M., Yassine, A. and Benlamri, R., 2019. Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), p.1736.

[34] Ratta, P., Kaur, A., Sharma, S., Shabaz, M. and Dhiman, G., 2021. Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality, 2021, pp.1-20.

[35] de Oliveira, M.T., Reis, L.H., Carrano, R.C., Seixas, F.L., Saade, D.C., Albuquerque, C.V., Fernandes, N.C., Olabarriaga, S.D., Medeiros, D.S. and Mattos, D.M., 2019, May. Towards a blockchain-based secure electronic medical record for healthcare applications. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[36] Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E. and Ylianttila, M., 2018, September. Blockchain utilization in healthcare: Key requirements and challenges. In 2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom) (pp. 1-7). IEEE.

[37] Ismail, L., Materwala, H. and Hennebelle, A., 2021. A scoping review of integrated blockchain-cloud (BcC) architecture for healthcare: applications, challenges, and solutions. Sensors, 21(11), p.3753.

[38] Yoon, H.J., 2019. Blockchain technology and healthcare. Healthcare informatics research, 25(2), pp.59-60.

[39] Yu, H., Sun, H., Wu, D. and Kuo, T.T., 2019. Comparison of smart contract blockchains for healthcare applications. In AMIA Annual Symposium Proceedings (Vol. 2019, p. 1266). American Medical Informatics Association.

[40] De Aguiar, E.J., Faiçal, B.S., Krishnamachari, B. and Ueyama, J., 2020. A survey of Blockchain-based strategies for healthcare. ACM Computing Surveys(CSUR),53(2), pp.1-27.

[41] Abdellatif, A.A., Al-Marridi, A.Z., Mohamed, A., Erbad, A., Chiasserini, C.F. and Refaey, A., 2020. ssHealth: toward secure, blockchain-enabled healthcare systems. IEEE Network, 34(4), pp.312-319.

AUTHOR PROFILE

Mr. K. Britto Alex has a brief experience of 12 years in the field of education and is presently serving as Assistant Professor in the Department of Computer Science, The American College, Madurai and pursuing Ph.D. in J. J. College of Arts and Science (Autonomous),Pudukkottai, Affiliated to Bharathidasan University, Tamilnadu. He acquired his M.Sc., degree from The American College (Autonomous), Madurai. He is specialized in the field of Blockchain, Deep Learning andImage Processing.

Dr. K. Selvan has a rich experience of 24 years in the field of education and is presently serving as Assistant Professor and Research Advisor in the P.G. and Research Department of Computer Science, J.J. College of Arts and Science (Autonomous), Pudukkottai, Affiliated to Bharathidasan University, Tamilnadu. He acquired his M.C.A degree from St. Joseph's College (Autonomous), Tiruchirappalli. He obtained his Ph.D. in Computer Science from Bharathidasan University, Tiruchirappalli in the year 2018. He is specialized in Data mining, Web security and Phishing detection and prevention.