International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 12 Issue 4, July.-August, 2024, Impact Factor: 8.376

Systematic Review of Healthcare Monitoring System using Blockchain-Based Detection Models

Mr. Vishal R. Shinde[1], Dr. Rahul Thour[2]

[1]Ph.D. (CSE) Scholar, DeshBhagat University, Chandigarh
[2]Department of CSE, DeshBhagat University, Chandigarh

ABSTRACT

The healthcare industry seeks a secure data-sharing technique to protect patient personal information and medical conditions. Therefore security is considered the significant factor in ensuring the patient's medical records. In this instance, Internet of Things (IoT) technology and Blockchain technology play a prominent role in establishing the remote patient monitoring environment and enabling the secure transmission of Electronic Health Records (EHR). From this perspective, the main objective of this study is to explore the possibilities and challenges of IoT and Blockchain technologies in ensuring the transmission of medical Records. Therefore, the review paper explores articles to identify the different blockchain-based detection models and summarize their gaps and benefits. In this review paper, the technologies and their benefits in the healthcare industry are explored and a detailed analysis based on the applications of models, their benefits, and challenges. For this research, designed a taxonomy of methods to frame the challenges and future works along with the description and applications of Blockchain in healthcare systems.

Keywords*: *Blockchain, Security, Privacy, Healthcare system, Internet of Medical Things, Data sharing.

INTRODUCTION

In recent years, the Internet of Things (IoT) has played a major role in top research fields of academics and industry, which include embedded devices, sensors, smartphones, and actuators. These devices are connected through a wireless communication network that collects and shares the garnered information to various smart living application scenarios [15] [16] [1]. The major IoT application is healthcare monitoring whichis achieved by the development of sensors, machine learning, and network technologies [1]. The origin of electronic health records is initialized by various specialized hospitals with numerous patient information, which includes personal information, health status, accounting data, and pharmacy requirements stored in an organized way [7]. The health status information of the patient is transmitted through the wireless communication network to reach the health service provider and physicians for further reference, which is termed remote patient monitoring (RPM) [34] [2].

To securely share healthcare data information, the patient-centric record management system was connected with the peer-to-peer blockchain (BC) communication system with smart contracts [32][7]. Mainly the BC is categorized into three major techniques such as peer to peer-to-peer network with shared ledger, cryptographic keys, and storage transaction block. Every individual block containsa blocknumber, digital signature, message digest, block hash, and so on [31][7]. This IOT-enabled remote monitoring system provides enhanced collection and transmission of healthcare data information [17][1]. This transmission of healthcare analysis deployed various prediction techniques to enhance the accuracy. The collection of obtained data is transmitted to the sensor using a DL-based Convolutional Neural Network (CNN) that automatically extracts large-scale data into informative features [38] [12].

DETECTION MODEL WITH BLOCKCHAIN BASED TECHNIQUES IN HEALTHCARE MONITORING SYSTEM

BC is mainly defined as a peer-to-peer network by combines several nodes that collect all the information and storednetwork block, which perform encryption with the key specification identities to secure the stored information. The BC recognizes a small change in the network and protects the information from malicious attacks.

All the information of the patients is gathered in the form of EHR, which is stored in the BC to preserve the privacy of the medical information. The use of BC eliminates the single-point failure risk and reduces the high computational attributes that maintain the stored data integrity by guaranteeing user security and privacy.

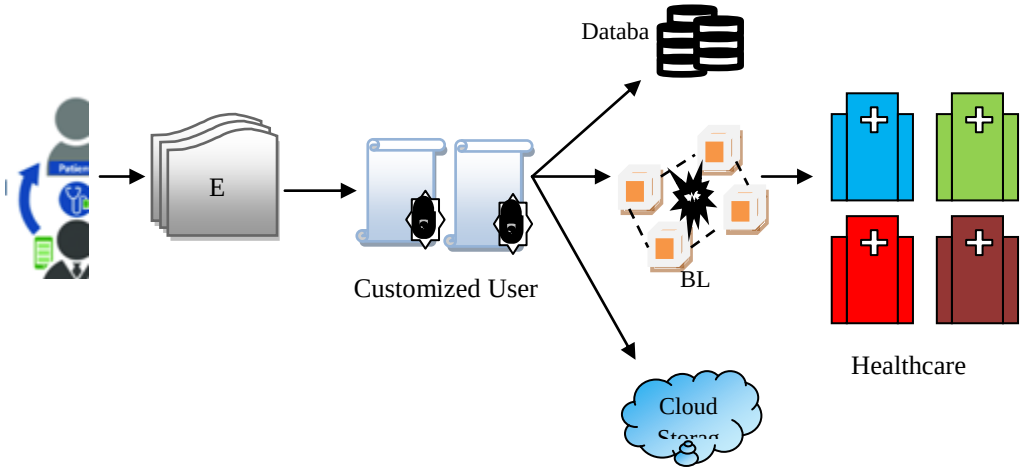

Fig 1: Basic BC-based healthcare monitoring system

Generally, DL-based detection models provide accurate results in prediction, whereas the combined BC-based detection model attains effective data sharing with high-level security purposes that reduce eh response time delay and generate effective outcomes.

Taxonomy: Recent Healthcare monitoring techniques

In the section, the various BC-based schemes, and algorithms along with DL-based detection models are briefly elaborated in the taxonomy diagram, which is depicted in Figure 2.1.

Blockchain-based techniques

a) Blockchain-based schemes and Algorithms

Duc Anh Luong and Jong Hwan Park [2] introduced a healthcare system for preserving the user's private data by zk-SNARK, which emphasized the zero-knowledge succinct non-interactive argument of knowledge in BC that enables third-party collusion with the elimination of anonymous data sharing and ensured secure data transfer. The scheme was not suitable for accessing the health conditions in mobile devices because of the higher computational burden and also suffered of lower performance intimation.

Jingwei Liu, *et al.* [3] employed a secure medical data sharing scheme with a multi-keyword search in inner product searchable encryption (MK-IPSE), which signified the transferred data with effective ciphertext retrieval for entire privacy preservation. In the scheme, the searchable encryption with federated BC was integrated to attain effective multi-keyword search that enhanced the security, with improved performance and resistance to attacks. This BC integrated scheme was affected by certain limitations such as potential complexity and scalability challenges.

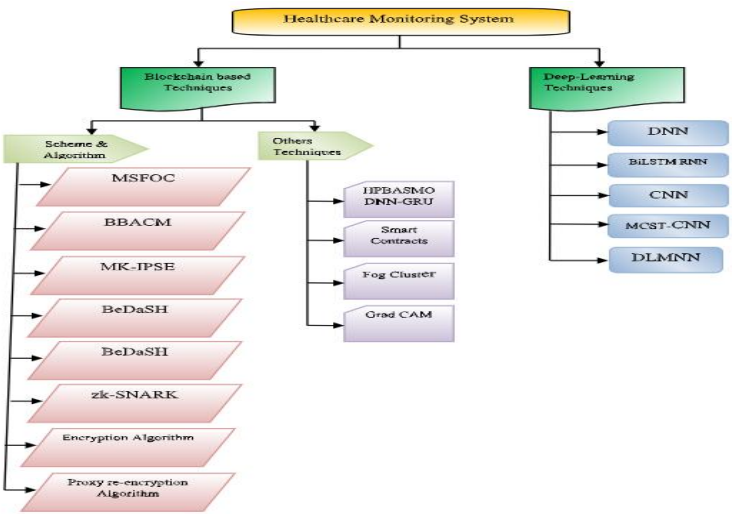

Fig 2: Taxonomy diagram of Healthcare monitoring system

Renpeng Zou, *et al.* [4] implemented a privacy-preserving scheme for secure medical record sharing using SPChain in the BC system, which resisted certain attacks and secured the shared data. The SPChain scheme achieved effective medical sharing repetitively, and because of this reputation, the system suffered from communication overhead problems.

Yingwen Chen, *et al.* [29] proposed a scheme for sharing medical data through medical institutions by K-anonymity and searchable encryption in the BC technique. These smart contracts contained chain code for accessing the control system by implementing additional attributes function, which improves the data sharing techniques without any privacy leakage issues that also attain enhanced scalability and performance. However, the system is affected by computational overhead problems.

Mohamed Younis, *et al.* [30] employed a smart healthcare application with data-driven access control and data management systems enabled with the BC technique (BeDaSH). This scheme performed well in private data preservation without any fraudulent risk factors and identity theft, which improved high-level security verification through AVISPA protocol. The scheme ensured certain limitations such as large storage requirements, computational overhead, limited data encryption, wireless communication leaks, and so on.

Koosha Mohammad Hossein, *et al*.[1] established a health monitoring architecture based on BC using a clustering scheme, which was mainly assessed by two chains such as the access control chain and a data chain that secured the patient's private data and improved confidentiality. The clustering approach improved the scalability, throughput and made a strong resilience against attacks, however, the accessing time of the system was increased and, which did not attain accurate results in real-world applications.

Abir EL Azzaoui, *et al.* [8] established an information-hiding framework for secure data communication in critical scenarios, which secured the data against cyber-attacks and improved the transparency through BC. The smart contracts increased the feasibility of the security level, but the approach was affected by potential complexity and computation overhead problems.

IsmaMassod, *et al*. [21] introduced an Access control model with the integration of BC (BBACM) that effectively accessed the physiological parameters and health information. The proposed system significantly enhanced the fine-grained access control, privacy, and security for cloud computing and wireless body sensor networks. To access a fine-grained system, the framework suffered from scalability and availability challenges under the preservation of a private server and attained loss of data credentials by chain code query.

Eric Appiah Mantey, *et al*. [23] developed a secure medical data transfer with both federated learning and BC technique approaches, which enabled data transmission, and sorting, in a vulnerable training procedure. These federated learning and BC techniques utilized a recommender data management neural architecture (REMANA) for effective data management techniques. Due to this integrated framework (SERTT), the system acquired maximum training time, which resulted in performance accuracy reduction.

Jose Escorcia-Gutierrez, *et al.* [20] established a BC-based healthcare system with an AI technique (AIBS-IoTH) to achieve effective data transmission in IoT networks. The method was also integrated with sunflower-based optimization metaheuristic clustering methods (MSFOC) to attain energy efficiency. In this BC scheme, the communication was carried out by both inter and intra-clustering methods. The MSFOC methods suffered from energy efficiency and security problems in real-time environment scenarios and attained a minimum performance rate.

Ken Miyachi and Tim K. Mackey [5] developed a Hybrid on-chain and off-chain framework with the integration of BC (hoCBS), which enhanced the ability of data privacy, performance, scalability and reduced the storage requirements with vast BC adoption. However, challenges might occur because of the complexity of regulations.

Asad Abbas, *et al*. [6] introduced a framework by implementing secure data management and BC (BSDMF), which improved the system performance with effective data sharing accuracy and security concerns. These framework systems assisted certain benefits such as data integrity, traceability, immutability, and confidentiality without the involvement of third parties, but, the system was affected by potential complexity and scalability issues.

G. Muneeswari, *et al*. [22] established a BC-based platform to ensure patient records from past data without reducing privacy concerns, initially, the data records were obtained from the patient record database, which was encrypted by Edward's Digital Signature Algorithm for secure data transfer finally, the data were retrieved by SDP method. This Algorithmic platform achieved major advantages such as a High-security level, faster verification process, and low space complexity. Because for large-scale evaluation, the framework suffered from certain complexity issues.

N. Balaji, *et al*. [25] introduced a transaction technique by a decentralized digital ledger and BC system that ensured secure data integrity, and privacy preservation-based cryptography technique. In this system, the user identity was encrypted with a specific mask and stored in BC with additional attribute identifiers. Based on these security concerns, additional attribute functions were implemented for large data analysis resulting in increased communication and computation overhead complexity.

Zeng Chen, *et al*. [28] introduced a scheme for sharing medical records by cloud servers and proxy re-encryption algorithm. To attain accurate performance, the system was designed by BC architecture with the combination of hyper ledger fabric, medical chain code, and dual-channelfabric deployment architecture to perform access control and data management. The proposed framework achieved better data transmission security, storage security, and replay to certain attacks. However, the scheme suffered from limitations like potential challenges, availability, and interoperability issues.

b) Other Blockchain-based Techniques

UsharaniChelladurai, *et al*. [7] developed a secure Electronic medical record sharing with the integration of a patient-centric management system and BC system, which enabled a smart contracts processing algorithm that enabled secure data sharing by improving the system throughput and transparency by reducing the network latency. However, the system suffered from computational overhead and interoperability issues.

Ahmed I. Taloba, *et al*. [9] proposed a secure architecture for transferring healthcare multimedia content using the BC technique, which enhanced the patient care performance with minimum cost-effective and storage requirements. However, the operational investigation of the framework accessed based on the illicit act, due to this illegal communication behavior causes falsified assault, over-product drop percentage, intrusion, and so on.

Israr Ahmad, *et al.* [10] introduced a healthcare record-sharing system based on the Fog cluster layer, which was categorized into two systems they are critical fog cluster and non-critical fog cluster. These fog layers handle the patient record securely by BC technology, which reduces the storage requirements and the computation overhead issues. However, the critical fog cluster consumed a large condensed time, and the non-critical fog cluster was affected by delay tolerant issues.

Imran Ahmed, *et al*. [11] established a smart contract BC enabled with AI technique to monitor the health pandemic issues. The method provided an enhanced security solution with a multi-layer sequential deep learning classifier for evaluating radiological images. To achieve a high interpretable, a Gradient-weighted class activation mapping (Grad-CAM) approach was established, these systems acquired a better secure system in data sharing, but the major limitation was that the method did not provide accurate information for classification and segmentation.

Deep Learning-based Techniques

K. Raju, *et al*. [19] introduced a secure scheme with a DL framework for ensuring the preservation of private data. Primarily, the medical data were encrypted by Fully Homomorphic encryption with optical key-based Elliptic Curve Cryptography (OK-HECCFHE), which provides better performance by implementing the optimal key with Hybrid Polar Bear-Ageist Spider Monkey Optimization Algorithm. The encrypted data were decrypted by the optimal key and achieved better performance by compiling with DNN and GRU methods, which secured large amounts of data from malicious attacks. Because of large-scale data, the system was affected by computational complexity and local optima issues.

Aitizaz Ali, *et al*. [14] developed a privacy preservation approach in healthcare applications based on Homomorphic encryption technologies, which was integrated with DL methods. These smart contracts acquire fine-grained entities that were authorized by encrypted data, which enhanced both accountability and transparency. However, the encryption approach suffered from communication overhead, transaction volume, and scalability issues.

Pandian RajanJeyaraj and Edward RAjan Samuel Nadar, [26] implemented an accurate signal prediction algorithm using a deep neural network (DNN), which acquired the physiological signal and predicted accurate outcomes with highly sophisticated data analysis. Based on the performance of DL techniques, the model did not secure the transmitted data and caused overfitting problems.

A Angel Nancy, *et al*. [27] developed a secured healthcare monitoring and accurate heart disease prediction were acquired in a Bi-directional Long short-term memory (BiLSTM) model. The prediction process was done in a recurrent neural network (RNN), which could sequential time-series data. However, the proposed model suffered from certain limitations such as connectivity, bandwidth utilization, and latency that reduced the efficacy of timely predictions.

Md. Reazul Islam, *et al*. [12] introduced an early detection of health problems and a healthcare monitoring system using DL-based techniques, which involved the CNN classifier and the integration of an attention mechanism for classifying potential diseases. The model found any abnormalities in the system and was connected to the nearest

doctor for further reference. However the security access system was very poor, anyone could breach the privacy and security mechanisms of health data reducing the effectiveness of healthcare results.

PriyanMalarvizhi Kumar, *et al*. [13] employed a secureddata storage model using new cryptographic algorithms to attain encryption and decryption process. The method achieved effective security purposes along with prediction accuracythat was achieved by Multi-channel spatiotemporal CNN (MCST-CNN). The model garnered the healthcare data from IoT devices stored the data in the storage model and retrieved the data for further reference. Based on these encryption techniques, the system accurately secured the patient data and suffered from potential scalability issues and computational complexity problems.

SimantaShekharSarmah, [33] established a prediction and monitoring system using a modified deep neural network (DLMNN) classifier. The model achieved the highest level of security system with minimum response time for performing the encryption and decryption process. In this method the secured patient's data were obtained with a vast gamut of sizes, due to this the proposed model faced problems such as interpretability issues, scalability problems, and communication overhead.

ANALYSIS

Blockchain-based Assessment

Table 1: Scheme Concerning Assessment

Technique	Reference	Advantages	Limitations	Attributes	Applications
Clustering	[1]	Enhanced the scalability, throughput, and restricted the malicious attacks.	Access time was increased, due to this, which did not provide accurate results in real-time environments.	With key encryption	Privacy protection
IHT	[8]	Improved data integrity and resisted to cyber attacks	Potential scalability issues and computational overhead problemsoccurred in the model.	With Key	Security Protection
BBACM	[21]	Enhanced the fine-grained access control and acquired better security for cloud computing	Suffered by scalability and availability challenges that resulted in loss of data credentials.	With key	Security Protection
SERTT	[23]	Effective data management and sorting	Maximum training time and reduced performance accuracy	With public key	Privacy protection
MSFOC	[20]	Achieved effective data transmission in intra and inter-clustering methods	Suffered by energy efficiency and security problems in real-time environment	With key	Privacy protection
zk-SNARK	[2]	Enabled anonymous data sharing without the involvement of third-party collusion	Low performance, Computational overhead	With keyGen Algorithm	
MK-IPSE	[3]	Improved performance and resist to attacks	Scalability issues	With cipher text /Key	Security Protection
SPChain	[4]	Enhanced energy efficiency in secure medical data sharing	Communication overhead	With key	Medical protection
K-anonymity	[29]	Improved data sharing without privacy leakage issues	Computational overhead issues	With key/ciphertext	Privacy protection

BeDaSH	[30]	Improved high-level security verification without any fraudulent risk factor and identity theft	Consumed large storage requirements and computational overhead issues.	With key encryption	Security Protection
hoCBS	[5]	Reduced the memory and storage requirements	Regulatory complexities	Cipher or Key	Privacy protection
BSDMF	[6]	Improved High performance and achieved high accuracy	Potential complexities and scalability issues	With key	Security Protection

Table 2: Algorithm Concerning Estimation

Technique	Reference	Advantages	Challenges	Attributes	Applications
SDP	[22]	High-security level, faster verification process, low space complexity	Complexity issues	With key	Security Protection
Encryption Algorithm	[25]	Ensured secure data integrity with specific mask identity	Increased communication and computation overhead issues	With key	Privacy protection
Proxy re-encryption Algorithm	[28]	Achieved accurate performance and secured data transmission	Suffered by potential challenges and interoperability issues	With key/ciphertext	Medical privacy
Smart contracts	[7]	Improved the throughput of the system and reduced the latency of the network	Interoperability challenges	With key	Medical protection
BC Framework	[9]	Minimum cost consumption and storage requirements	Because of illegal communication, intrusion might occur	Cipher or key	Privacy protection
Fog layer clustering	[10]	Reduced storage requirements	Huge time consumption and delay tolerant problem	With key	Medical protection
GradCAM	[11]	Better secure system in data sharing and was highly interpretable	Affected by potential challenges and does not provide accurate outcomes	-	Security Protection

Deep Learning-based Analysis

Technique	Reference	Advantages	Disadvantages	Attributes	Applications
DNN	[26]	An accurate prediction process occurs with highly sophisticated data analysis.	Did not secure the transmitted process and caused an overfitting problem.	-	Accurate prediction
BiLSTM-RNN	[27]	Improved the ability of sequential time-series data	Suffered from connectivity issues, latency problems, and reduced efficiency of prediction.	-	Effective prediction
CNN	[12]	Enhanced the classification of potential diseases.	The security system was very poor.	-	Classification process
MCST-CNN	[13]	Accurate disease prediction	Suffered from potential and scalability issues.	With Key	Security Protection

DLMNN	[33]	Achieved the highest level of security system with minimum response time.	The secured patient data were huge, due to this issue the model was affected by interpretability issues and communication overhead problems	With key	Security Protection
HE	[14]	Improved the fine-grained entities with fair accountability and transparency.	Affected by communication overhead, scalability issues, and transaction volume.	Cipher text, Key	Medical protection
HPB-ASMO-DNN-GRU	[19]	Provided better performance and secure data from malicious attack	Computational complexity and local optima issues.	Cipher text /optimal key	Medical security

RESEARCH GAP AND FUTURE WORK

Blockchain-based Evaluation

a) Shortcoming

1. The model increased the computational burden of the users with high computation power, which reduced the performance and led to high computation costs that were also affected by huge storage requirements [2].
2. Quick patient data retrieval leads to high communication overhead by reducing the effective throughput of the network [4].
3. BeDaSH method suffered from large storage requirements, limited data encryption, computational overhead, and communication leakage issues [30].
4. Increased the accessing time of the cluster-based approach and did not provide accurate performance results in real-world environments [1].
5. In real-time applications, the integrated model (smart contracts and BC-based techniques) did not evaluate the encryption and decryption technique to obtain secure data. Additionally, it consumeda larger execution time [8].
6. The BBACM method suffered from scalability and availability challenges, together with these issues, loss of data credentials also occurred in on-chain and off-chain code systems [21].
7. The major limitations of IoT-based healthcare systems were energy efficiency and security problems, which reduced the performance rate and increased the complexity issues [20].

b) Future work

1 .In the future scope, decrease the computation burden and increase the cryptography technique to achieve high-performance accuracy with fast authentication and effective verification [2].
2. In the future, communication overhead could be reduced while retrieving the patient's data and could improve the throughput of the system, which resulted in better accuracy and performance in the real-time environment [4].
3. The performance of healthcare would be improved to attain a secured timestamped mechanism with the enhanced regulatory framework to preserve private data in future directions [5].
4. In the cluster-based approach, the evaluation of cluster management and optimization would be very difficult to identify the best cluster to attain the user location and network load for stored the archive data in the future [1].
5. In future directions, the integrated method achieve lower execution time by performing encryption and decryption to attain highly secure data in real-world scenarios [8].
6. The versatility and applicability of the data would be improved to explore more complex healthcare domains by providing advanced effective secure data protection schemes in the future [21].
7. Improved the efficiency and accuracy performance of the model by reduced the training time of the gradient distribution algorithm in federated learning technique, which provided a better verification approach along with high-level privacy preservation methods in future scope [23].
8. In future studies, the MSFOC model techniques would be extended to perform well in real-world scenarios [20].

Other BC-based Techniques Evaluation

a) Shortcoming

1. In BC-based hybrid framework that acquired illegal communication behavior, which faced interoperability issues with falsified assault, intrusion, and so on [9].
2. The Fog cluster method suffered from software simulation impact that reduced the accurate performance with increased time consumption and caused delay tolerant problems [10].
3. In Grad-CAM methods, potential challenges might occur and might not provide accurate results [11].

b) Future work

1. In the future scope, ensure the data integrity content and achieve better transparency and privacy concerns by increasing the performance and throughput of the system and reduced the latency with minimum resource requirements [7].
2. Improved the potential challenges by increasing the quality of the eHealth data system, which would be integrated with BC to perform effective secure data integrity in future research [11].
3. In future directions, additional sensors would beimplemented, to calculate the actual position of patients with accurate feature information to obtain effective results [10].
4. In healthcare investigation of multimedia information, the transaction time and estimated cost would be measured in future studies to achieve effective outcome results [9].

Deep Learning-based Assessment

a) Shortcoming

1. In the model, the Sequence data prediction may led to difficult challenges in the data science environment and consume a huge time to tackle the data [27].
2. The security system of the model was very poor in which anyone could breach the model to pirate the obtained healthcare data [12].
3. The proposed DLMNN model attained certain challenges such as higher interpretability issues, scalability problems, communication overhead, and so on [33].

b) Future Work

1. The proposed BiLSTM-RNN-based prediction technique could integrated with a hierarchical fog-cloud model to reduce the delay constraints in future scope, which also addressed the limitations such as increased latency, intrinsic constraints, and bandwidth utilization [27].
2. In future scope, the security and private mechanisms were enhanced for better security protection of achieved healthcare data that resulted in increased efficiency and accuracy of the model [12].
3. The DLMNN model centeredonIoT-based techniques would achieve effective monitoring of patient health by identifying the normal and abnormal conditions of the patients in future directions [33].
4. Improved real-world implementation in the future with the involvement of better scalability and performance optimization, security and threat analysis methods, usability, and user experience methods [14].

CONCLUSION

Privacy preservation is a most essential task in healthcare applications, which garnered better security and protects private data from malicious attacks. The study provides various existing methods for preserving the patient's privacy in healthcare applications, which are enabled with BC-based detection models techniques, schemes, and algorithms to share the healthcare details securely with the medical staff by having access control, which is briefly elaborated in this study. The study provides a detailed explanation of existing literary articles with various schemes along with the utilization of distinct datasets along with the achieved performance metrics. In this perspective, the utility of BC is essential for collecting the health record data and transferring particular data through IOT sensors from one location to another, which also suffer from several challenges such as decreased throughput, Scalability issues, computational problems, lower performance, communication problems, and so on. This problem was obtained while the model was implemented in a real-time environment, to overcome this limitation, explore more BC-based detection methods in future studies.

REFERENCES

[1]. Hossein, Koosha Mohammad, Mohammad EsmaeilEsmaeili, TooskaDargahi, Ahmad Khonsari, and Mauro Conti. "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications." Computer Communications 180 (2021): 31-47.
[2]. Luong, Duc Anh, and Jong Hwan Park. "Privacy-preserving blockchain-based healthcare system for IoT devices using zk-SNARK." IEEE Access 10 (2022): 55739-55752.
[3]. Liu, Jingwei, Yue Fan, Rong Sun, Lei Liu, Celimuge Wu, and ShahidMumtaz. "Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System." IEEE Internet of Things Journal (2023).
[4]. Zou, Renpeng, XixiangLv, and Jingsong Zhao. "SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system." Information Processing & Management 58, no. 4 (2021): 102604.
[5]. Miyachi, Ken, and Tim K. Mackey. "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design." Information Processing & Management 58, no. 3 (2021): 102535.
[6]. Abbas, Asad, RoobaeaAlroobaea, MoezKrichen, Saeed Rubaiee, S. Vimal, and Fahad M. Almansour. "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things." Personal and ubiquitous computing (2021): 1-14.

[7]. CHELLADURAI, Mrs USHARANI, Seethalakshmi Pandian, and KrishnamoorthyRamasamy. "A blockchain-based patient-centric electronic health record storage and integrity management for e-Health systems." Health Policy and Technology 10, no. 4 (2021): 100513.
[8]. El Azzaoui, Abir, Haotian Chen, So Hyeon Kim, Yi Pan, and Jong Hyuk Park. "Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems." Sensors 22, no. 4 (2022): 1371.
[9]. Taloba AI, Elhadad A, Rayan A, Abd El-Aziz RM, Salem M, Alzahrani AA, Alharithi FS, Park C. A blockchain-based hybrid platform for multimedia data processing in IoT healthcare. Alexandria Engineering Journal. 2023 Feb 15;65:263-74.
[10]. Ahmad I, Abdullah S, Ahmed A. IoT-fog-based healthcare 4.0 system using blockchain technology. The Journal of Supercomputing. 2023 Mar;79(4):3999-4020.
[11]. Ahmed I, Chehri A, Jeon G. Artificial intelligence and blockchain-enabled smart healthcare system for monitoring and detection of COVID-19 in biomedical images. IEEE/ACM Transactions on Computational Biology and Bioinformatics. 2023 Jul 12.
[12]. Islam, M.R., Kabir, M.M., Mridha, M.F., Alfarhood, S., Safran, M. and Che, D., 2023. Deep learning-based IoT system for remote monitoring and early detection of health issues in realtime. Sensors, 23(11), p.5204.
[13]. Malarvizhi Kumar, P., Hong, C.S., Chandra Babu, G., Selvaraj, J. and Gandhi, U.D., 2021. Cloud-and IoT-based deep learning technique-incorporated secured health monitoring systems for dead diseases. Soft Computing, 25(18), pp.12159-12174.
[14]. Ali A, Al-Rimy BA, Alsubaei FS, Almazroi AA, Almazroi AA. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors. 2023 Jul 28;23(15):6762.
[15]. T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the Internet of things, IEEE Access 6 (2018) 32979–33001.
[16]. M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the Internet of Things: A comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1676–1717.
[17]. E. Petelko, IoT in healthcare: Use cases, trends, advantages and disadvantages, 2019, https://medium.com/existek/iot-in-healthcare-use-cases-trendsadvantages-and-disadvantages-8213e738e03.
[18]. Karim Abouelmehdi, AbderrahimBeni-Hessane, and Hayat Khaloufi "Big healthcare data: preserving security and privacy" Journal of Big Data, 2018, pp. 438-458.
[19]. Raju K, Ramshankar N, Shathik JA, Lavanya R. Blockchain Assisted Cloud Security and Privacy Preservation using Hybridized Encryption and Deep Learning Mechanism in IoT-Healthcare Application. Journal of Grid Computing. 2023 Sep;21(3):45.
[20]. Escorcia-Gutierrez J, Mansour RF, Leal E, Villanueva J, Jimenez-Cabas J, Soto C, Soto-Díaz R. Privacy Preserving blockchain with energy-aware clustering scheme for IoT healthcare systems. Mobile Networks and Applications. 2023 Mar 3:1-2.
[21]. Masood I, Daud A, Wang Y, Banjar A, Alharbey R. A blockchain-based system for patient data privacy and security. Multimedia Tools and Applications. 2024 Jan 5:1-25.
[22]. Muneeswari G, Varun SS, Hegde R, Priya SS, Shermila PJ, Prasanth A. Self-diagnosis platform via IOT-based privacy preserving medical data. Measurement: Sensors. 2023 Feb 1;25:100636.
[23]. Mantey, E.A., Zhou, C., Anajemba, J.H., Hamid, Y. and Arthur, J.K., 2023. Blockchain-enabled technique for privacy-preserved medical recommender system. IEEE Access, 11, pp.40944-40953.
[24]. Dimiter V. Dimitrov, "Blockchain Applications for Healthcare Data Management ", Healthcare Informatics Research, A case Report, 2019, pp 51-56.
[25]. Bhalaji, N., Abilashkumar, P.C. and Aboorva, S., 2020. A blockchain-based approach for privacy preservation in healthcare IoT. In ICICCT 2019–System Reliability, Quality Control, Safety, Maintenance, and Management: Applications to Electrical, Electronics and Computer Science and Engineering (pp. 465-473). Springer Singapore.
[26]. RajanJeyaraj, P. and Nadar, E.R.S., 2022. Smart-monitor: Patient monitoring system for IoT-based healthcare system using deep learning. IETE Journal of Research, 68(2), pp.1435-1442.
[27]. Nancy, A.A., Ravindran, D., Raj Vincent, P.D., Srinivasan, K. and Gutierrez Reina, D., 2022. Iot-cloud-based smart healthcare monitoring system for heart disease prediction via deep learning. Electronics, 11(15), p.2292.
[28]. Chen Z, Xu W, Wang B, Yu H. A blockchain-based preserving and sharing system for medical data privacy. Future Generation Computer Systems. 2021 Nov 1;124:338-50.
[29]. Chen Y, Meng L, Zhou H, Xue G. A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. Wireless Communications and Mobile Computing. 2021;2021(1):6685762.
[30]. Younis M, Lalouani W, Lasla N, Emokpae L, Abdallah M. Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access. IEEE Systems Journal. 2021 Jul 12;16(3):3746
[31]. CongYue, ZhongleXie, MeihuiZhang, GangChen, BengChinOoi, ShengWang, XiaokuiXiao, Analysis of Indexing Structures for Immutable Data, arXiv:2003.02090v2 [cs.DB], 2020, Pp 1-17.
[32]. VitalikButerin, "A next-generation smart contract and decentralized application platform", White Paper, 2014.

[33]. Sarmah, S.S., 2020. An efficient IoT-based patient monitoring and heart disease prediction system using deep learning modified neural network. Ieee access, 8, pp.135784-135797.
[34]. L. P. Malasinghe, N. Ramzan, and K. Dahal, ''Remote patient monitoring:A comprehensive study,'' J. Ambient Intell. Hum. Comput., vol. 10, no. 1,pp. 57–76, Jan. 2019
[35]. Miotto, R.; Wang, F.; Wang, S.; Jiang, X.; Dudley, J.T. Deep Learning for Healthcare: Review, Opportunities and Challenges. Brief. Bioinform. 2018, 19, 1236–1246.
[36]. Pandey, S.; Janghel, R. Recent Deep Learning Techniques, Challenges and Its Applications for Medical Healthcare System: A Review. Neural Process. Lett. 2019, 50, 1907–1935.
[37]. Chuah, M.C.; Fu, F. ECG anomaly detection via time series analysis. In Proceedings of the Frontiers of High Performance Computing and Networking ISPA 2007 Workshops: ISPA 2007 International Workshops SSDSN, UPWN, WISH, SGC, ParDMCom, HiPCoMB, and IST-AWSN Niagara Falls, Canada, 28 August–1 September 2007 Proceedings 5; Springer: Berlin/Heidelberg, Germany, 2007;pp. 123–135
[38]. Razzak, M.I.; Naz, S.; Zaib, A. Deep learning for medical image processing: Overview, challenges, and the future. In Classification BioApps: Automation of Decision Making; Springer: Berlin/Heidelberg, Germany, 2018; pp. 323–350
[39]. Brauwers, G.; Frasincar, F. A general survey on attention mechanisms in deep learning. IEEE Trans. Knowl. Data Eng. 2021, 35,3279–3298.