Ingénierie des Systèmes d'Information
Vol. 29, No. 1, February, 2024, pp. 253-260
Journal homepage: http://iieta.org/journals/isi

Role of Blockchain Technology in Data Security for Healthcare

Poonam Sangwan, Banita*

Department of Computer Science and Engineering, Baba Mastnath University, Rohtak 124021, Haryana, India

Corresponding Author Email: banita@bmu.ac.in

https://doi.org/10.18280/isi.290125

Received: 19 July 2023
Revised: 30 November 2023
Accepted: 31 December 2023
Available online: 27 February 2024

Keywords:
healthcare, blockchain, encryption, security, performance, hashing, deep learning

ABSTRACT

Considering growing demand of medical record management it has been considered that there is requirement to keep patient record and identity management in healthcare. To improve the safety and reliability of medical records, the blockchain technology has been determined to be an appropriate tool. The function of blockchain technology in healthcare data security is the focus of this study article. An example of a transaction in this system would be the recording and storage of a patient's medical history in a public ledger known as a block. Two parties are required for a transaction to take place. For every transaction to go through, the system needs the approval of the vast majority of users. Records of transactions kept on a blockchain are immutable and resistant to tampering. Researchers are now encrypting patient data before storing it on blockchain, which adds an extra degree of protection. Additionally, blockchain's security and speed have been enhanced by the use of advanced hashing mechanisms.

1. INTRODUCTION

The need for healthcare-related applications is growing. A safe place to store patient data is still necessary [1]. A number of options exist for preventing unauthorized access to patients' records, including keeping the records in a secure place [2]. On the other hand, these methods have long since become archaic. The use of blockchain-based technologies could ease certain security worries. Block chain, a distributed ledger that encourages decentralization [3, 4], might be used to safeguard individuals' medical records. Medical applications of blockchain research have focused towards developing robust, efficient systems [5].

Over the last decade, several academic institutions and businesses have investigated "block chain" since it is one of the most fascinating new technologies. Blockchain, a distributed, immutable ledger, does away with the need for a reliable third party to confirm and document monetary transactions [6, 7]. Blockchain 3.0 is currently under development, with early adopters hailing from the public sector, the energy industry, and the healthcare sector. Health care providers have embraced these innovations because of the many ways they may improve patient care. Blockchain's decentralised structure [8], along with its in-built privacy precautions and security measures, makes it an attractive technology for usage in the healthcare sector [9]. These options may be used to ensure that only authorised individuals have access to sensitive medical information [10].

Blockchain was proposed as part of the Bitcoin protocol. It may be thought of as a distributed ledger. All network transactions are recorded and verified by a distributed public ledger called a chain of blocks in blockchain. A header and body make up each block [11]. The header of every new block shows the hash of the block before it. In a linked list or chain, each block is linked to the one before it [12]. Merkle trees, timestamps, and nonces in block headers are tools that might potentially reduce the amount of labor necessary in analyzing a block's transactions and speed up the process [13]. Sometimes miners may alter the nonce number in order to solve a mathematical problem.

One little piece of work that is recorded and maintained in a data storage unit called a block is a blockchain transaction. A transaction can only have two participants [14]. For a transaction to go through, the vast majority of users in the system must be in agreement. No one can alter a transaction after it has been recorded on a blockchain, making them completely trustworthy [15]. Due to blockchain's immutability, each participant only needs to keep a single copy of the ledger at all times. To guarantee that transactions can be executed without any interruptions, the business logic of a blockchain is written into computer code known as smart contracts, which runs automatically on the blockchain's underlying architecture [16, 17]. Integrating a smart contract with a blockchain makes it self-verifying when all rules are satisfied and self-enforcing when the blockchain's automated features are used. Blockchain can't be altered or tampered with since it's decentralised, permanent, accessible, and anonymous. Because of this, manipulation is very difficult [18, 19].

1.1 Blockchain use cases in healthcare

One term for the outcome of linking a series of transactions using a cryptographic key is a "blockchain." Connected in a network of nodes or processes, these keys and signatures may be checked [20]. A complete and current copy of the entire chain is maintained by each node in the network. Among the

many benefits of blockchain-based technology, as highlighted by NIST [21], are decentralized digital ledgers, resistance to manipulation, and the difficulty of changing a published transaction later within a user community that shares ledger. It is also known as "digital ledger technology" [22].

1.1.1 Advantages and issues with blockchain in healthcare

There are several obstacles to overcome when using technology based on blockchain in healthcare sector [23].

- Security for whole system
- All individuals must have their identities and participation authenticated.
- Everyone should have consistent access to electronic health records.

DLT has a number of potential uses in the healthcare industry, although it is not widely used. Health records cannot be housed on blockchain because of public nature of the technology [24]. Despite this openness, clinicians have a responsibility to safeguard patient health information (PHI).

Blockchain infrastructures are built with defences meant to lessen the impact of hacking attempts. As a result, ensuring the confidentiality of patient records is crucial [25]. Since information stored on a blockchain cannot be deleted, users should exercise caution when dealing with private health data. It is now safe to remove files that take up a lot of space or are often modified. There should be no record of a person's existence on the web [26]. Due to its decentralised nature, immutable databases, and robust data, blockchain-based healthcare database management solutions, such as patient-based encryption techniques, are gaining popularity.

1.1.2 Applications in healthcare

Technology based on blockchain's distributed ledger architecture may find use in a variety of medical settings [27].

Electronic medical records storage and retrieval.

- Electronic medical records storage and retrieval.
- Healthcare records are protected by several safeguards.
- Treatment of personal health information.
- There is potential for bedside genomics management.
- Responsible for data included in electronic medical records.

1.1.3 Health care applications

Unless two or more hospitals are connected via a private network, there is no way for patients' electronic medical records to be shared or updated between them. If data is organised in this fashion, the initial few blocks of the blockchain might include information that is not protected by PHI or PII [28]. Eventually, millions of people might be available to academics and corporations. Clinical research, the reporting of safety issues and adverse occurrences, and public health reporting might all be hampered by an abundance of data.

1.2 Seamless switching of patients between providers

If patients were willing to provide their secret keys, their medical records may be unlocked and shared with other physicians or organisations. More collaboration and interoperability in the HIT industry may result from this [29].

1.3 Faster, cheaper, better patient care

It's possible that authorised employees may regularly update a central repository containing the medical records of numerous individuals. Many preventable medical errors may be caused by a lack of communication between the various healthcare providers caring for the same patient. These findings may allow for more individualised treatments in the medical field [30].

1.4 Interoperable electronic health records

Blockchain has the ability to function as a single transaction layer provided consensus can be established on a common set of data to be stored on the ledger and encrypted private connections are maintained so that only authorised parties may access supplemental data. Smart contracts might be useful in addition to more conventional authorization schemes for maintaining constant information flow between devices [30].

2. LITERATURE REVIEW

Several of the many blockchain-related healthcare and technology studies are discussed below.

As more individuals use IoT and other forms of remote monitoring, additional flaws in data transmission and recording become apparent, as discussed by Griggs et al. [1]. They propose using smart contracts built on blockchain to evaluate and securely manage PHI from medical sensors. By linking sensors to a private Ethereal-based blockchain, our solution triggers smart contracts and keeps track of all blockchain-related events.

Radanović and Likić [2] presented blockchain, a distributed database composed of blocks of data connected cryptographically, to record the previous dealings of a decentralised network's assets and transactions. This technology has been used in a variety of contexts, including digital contracts, public and financial documents, and property titles.

Calvaresi et al. [3] investigated MAS-based distributed systems that handle sensitive data. Many people think blockchain-based technologies can help rebuild trust in MAS by making the agency more transparent and answerable to its citizens. Despite the fact that most methods have only recently started to investigate this area, the need to define research plan and technological constraints was imperative.

Zhang and Lin [4] discovered that collaborating on medical data online might result in more accurate diagnoses, but cautioned that patients' privacy must be protected. Blockchain has been hailed as an essential component of potential technology for protecting PHI.

Wearable technology, as supplied by Liang et al. [5], has piqued the public's interest in keeping tabs on their health, making them more worried than ever before. This research paper takes a decentralised approach to privacy protection by using the blockchain and the Intel SGX trusted execution platform.

Bitcoin's blockchain technology is being implemented in the present IoT scenario, as first described by Miraz and Ali [6]. Researchers and practitioners in the private sector have recently increased their focus on this area of inquiry.

The authors Firdaus et al. [7] Criminals are creating blockchain-penetrating mobile malware because of the widespread foolishness with which blockchain-based technology is being used in conjunction with Android mobile devices. This research looked at three different types of features-system commands, directory paths, and code-that

might aid machine learning predictions in identifying unanticipated root assaults.

Massive improvements in the amount and quality of medical records, as demonstrated by Li et al. [8], have made it such that no one need ever go without treatment again. This article delves on the development of blockchain-based healthcare DPS. Performance analysis demonstrates the system's usefulness and effectiveness.

In a recent analysis, Epiphaniou et al. [9] predicted that distributed ledger technology will boost various sectors, including the food and pharmaceutical industries, the real estate market, and the financial sector. Several Blockchain healthcare pilot projects are currently underway, and their benefits and drawbacks will be discussed in this article.

Many people, including researchers and medical professionals, are looking forward to the implementation of electronic health records, as discussed by Zhou et al. [10] Using the Med-PPPHIS prototype, they suggest a closed-loop method for dealing with chronic diseases in China's Anhui Province.

An extreme rise in energy consumption threatens both economic and environmental sustainability, as first proposed by Iram et al. [11]. In this research, state-of-the-art techniques and analytics were used to a time series of energy-related variables. Data analysis was shown visually using heat maps.

Rathee et al. [12] examined how use of multimedia techniques have allowed for collection, analysis, and communication of patient data provided in visual, textual, and auditory formats through a number of modern mobile devices. More and more hospitals and clinics throughout the globe are using multimedia approaches to enhance staff efficiency, teamwork, and patient care.

3. PROBLEM STATEMENT

It is critical that these data be kept safe, but there have been many projects in the healthcare industry that have looked at utilizing blockchain to store patient information [13-18]. Traditional approaches to healthcare data security have looked at blockchain technology, but their performance is lacking. Traditional research has really barely scratched the surface of Blockchain's possible use in healthcare.

4. PROPOSED WORK

Research on blockchain security and its health care applications has been the primary emphasis of the proposed study, which has also investigated related security and performance issues. Blockchain security and its potential uses has also been the subject of this investigation. This is done in order to protect the patient's personal information from being stolen.

Recent research has provided a method that, when implemented, may enhance both the safety and the utility of block chains. The reliability of the healthcare system could be improved by enhancing its performance, and the efficiency of applications employed in the healthcare industry could be improved by enhancing their level of security. A comparison is being made between recommended and conventional model in order to evaluate the suggested model's level of performance as well as the classic model's degree of safety for usage in a healthcare context. The health care data set is first compressed in the work that is being suggested, and then it is encrypted using an encryption algorithm. Compression and encryption are applied to the data before it is deposited in the blockchain after the commencement of the block. Accuracy and performance of the work that has traditionally been done is then contrasted with the accuracy and performance of the work that will be suggested. Present research work is considering role of classification techniques in security of health care system. Initially existing research in area of healthcare are considered.

The problem with traditional methods of study is that they are not very accurate or efficient. Because of the problems with conventional research, there is a pressing need to develop advanced mechanisms for deep learning, using which it will be possible to attain greater accuracy parameters than are possible with traditional research. In Figure 1 the security model used for healthcare is defined where compression, encryption and block chain have been used.

Figure 2 presents research methodology of proposed work considering literature review, problem statement, proposed work, and evolution.

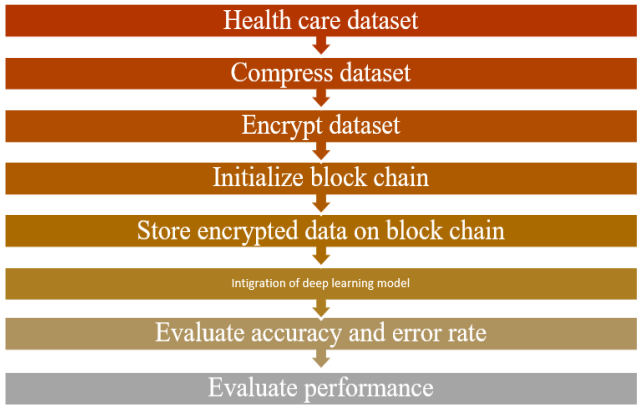

Figure 1. Security model [19]

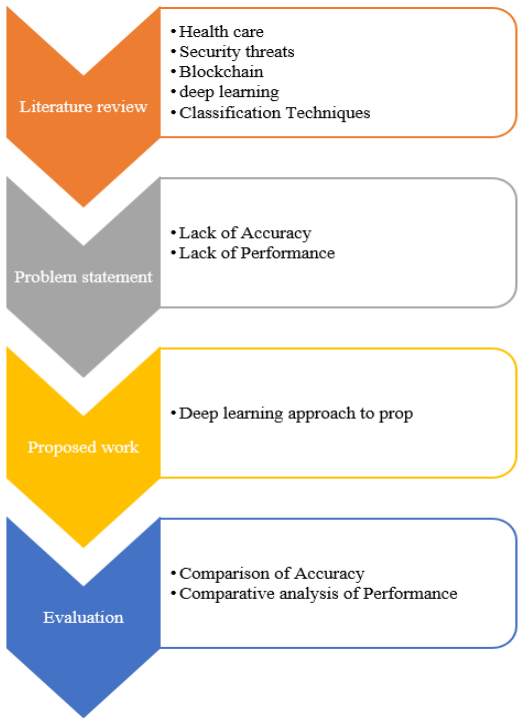

Figure 2. Research methodology [20] of proposed work

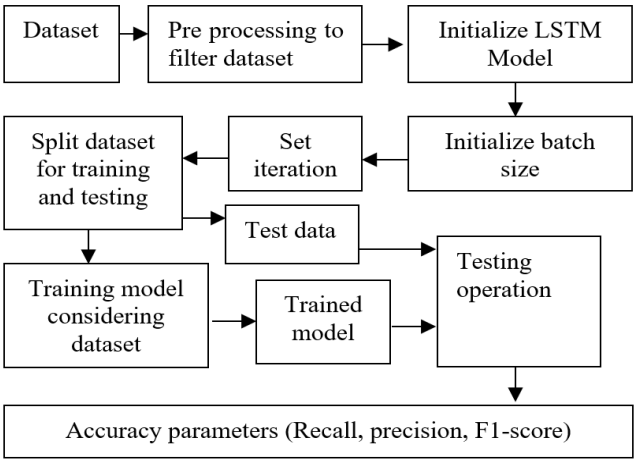

Figure 3. Process flow of training [21] and testing of deep learning model

Process flow of training [21] and testing of deep learning model is shown in Figure 3. In this, intial dataset has processed for filtering and apply initialization LSTM model batch size. It sets iteration and split dataset and perform the opteration for training and testing model. Last, calculate accuracy parameters like recall, precision, and f1score.

5. RESULT AND DISCUSSION

Several deep learning models are compared in this study to determine which provides the best prediction performance. In case of conventional approach, Table 1 displays evaluation of precision, recall, f1 score, and support. With an accuracy of 96 percent, convention deep learning model provide solution for healthcare security. In Table 2, outcome of proposed work are shown with accuracy equal to 98.3%. This it is concluded that proposed approach is providing better accuracy.

Table 1. Accuracy Parameters of Conventional Approach

	Precision	Recall	F1-Score	Support
Redesign	0.91	0.92	0.92	310
Successful	0.96	0.97	0.97	1849
Accuracy	-	-	0.96	2168
Macro avg.	0.94	0.95	0.94	2168
Weighted avg.	0.96	0.95	0.96	2168

Confusion matrix:
[294 25]
[30 1828]
Overall Accuracy: 0.96

Table 2. Accuracy parameters of Proposed work

	Precision	Recall	F1-Score	Support
Redesign	0.92	0.93	0.93	318
Successful	0.98	0.98	0.98	1857
Accuracy			0.98	2176
Macro avg.	0.95	0.96	0.96	2176
Weighted avg.	0.97	0.99	0.97	2176

Confusion matrix:
[301 18]
[22 1836]
Overall Accuracy: 0.98

5.1 Comparison of overall accuracy of traditional and current work

Considering outcome of conventional and proposed accuracy, Table 3 is presenting comparison of both model on the bases of accuracy.

Table 3. Comparison of Overall Accuracy

Conventional Approach	Proposed Work
0.96	0.98

Considering Table 3, comparison of overall accuracy in case of traditional and proposed work is shown.

5.2 Comparison of accuracy parameters of traditional and proposed work

Tables 4-7 are presenting comparative analysis of Precision, recall, F1-score, Support respectively. Figures 4-8 are showing their corresponding graphs.

5.2.1 Precision

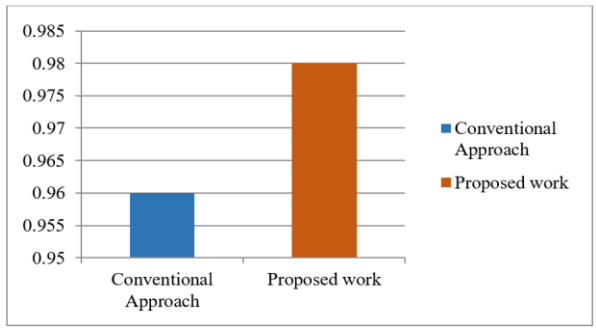

Figure 4. Comparative analysis of Overall Accuracy

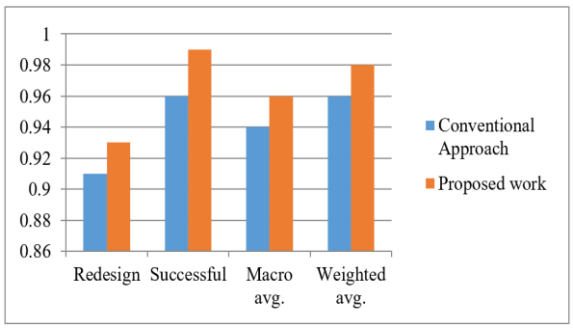

Figure 5. Comparison of Precision

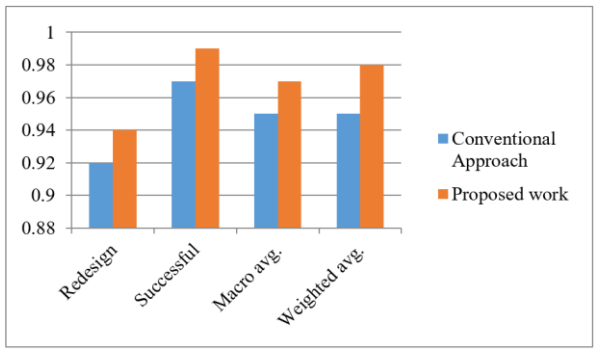

Figure 6. ComparIson of Recall

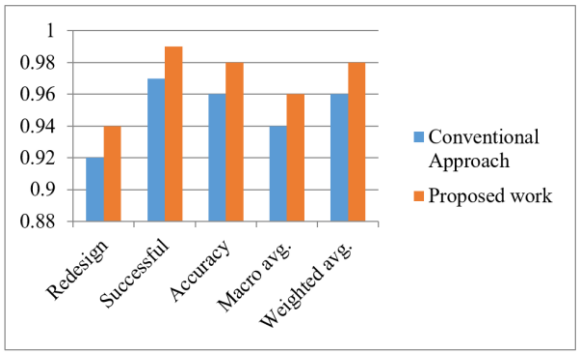

Figure 7. Comparative analysis of F1 score

Table 4. Comparative analysis of Precision

	Conventional Approach	Proposed work
Redesign	0.91	0.92
Successful	0.96	0.98
Macro avg.	0.94	0.95
Weighted avg.	0.96	0.97

5.2.2 Recall

Table 5. Comparison of Recall

	Conventional Approach	Proposed Work
Redesign	0.92	0.93
Successful	0.97	0.98
Macro avg.	0.95	0.96
Weighted avg.	0.95	0.99

5.2.3 F1-score

Table 6. Comparison of F1 score

	Conventional Approach	Proposed Work
Redesign	0.92	0.93
Successful	0.97	0.98
Accuracy	0.96	0.97
Macro avg.	0.94	0.95
Weighted avg.	0.96	0.97

5.2.4 Support

Table 7. Comparative analysis of Support

	Conventional Approach	Proposed Work
Redesign	310	318
Successful	1849	1857
Accuracy	2168	2176
Macro avg.	2168	2176
Weighted avg.	2168	2176

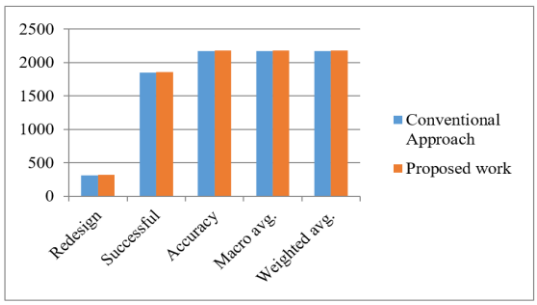

Figure 8. Comparative analysis of support [22]

5.3 Comparison of performance

A simulation of amount of time required to process blocks has been given for your perusal within this section. It has been shown that amount of time necessary to process block is much less than amount of time necessary for conventional processing. This is the case when comparing the two. When counting the number of blocks, divide by ten at each interval. Table 8 displays the findings of a comparative investigation that was carried out between proposed work processing times and the normal approach processing times.

Taking Table 8 into account, the following figure provides comparative analysis of the performance of the recommended design as well as the conventional layout.

Taking Table 8 into account, Figure 9 provides comparative analysis of the performance of the recommended design as well as the conventional layout.

Table 8. Comparison of Performance

Blocks	Conventional Time Taken	Proposed Time Taken
10	1.7171	0.7327
20	3.2190	1.2783
30	5.1681	2.5741
40	5.1681	2.8591
50	5.9259	2.4931
60	6.8624	3.5466
70	8.2142	4.6177
80	8.1148	5.1203
90	9.6872	5.1049
100	11.2424	6.6884

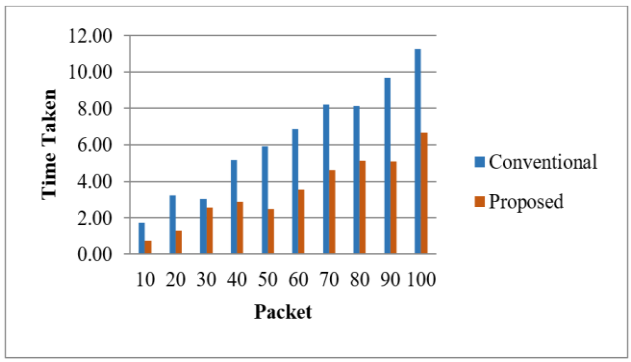

Figure 9. Comparative analysis of performance [23]

5.4 Comparison of error rate

Table 9. Comparison of error rate

Blocks	Conventional	Proposed
10	5	3
20	7	5
30	8	7
40	10	8
50	12	10
60	14	11
70	16	13
80	17	15
90	20	16
100	22	18

This section includes a model that simulates the probability of mistakes happening during the processing of blocks. When compared to the traditional method, it was discovered that the amount of error that takes place when calculating the number

of blocks at intervals of 10 is significantly lower. This was the conclusion reached by the researchers. Table 9 presents the results of an analysis that compares the error rate of the standard task processing time with that of the proposed task processing time.

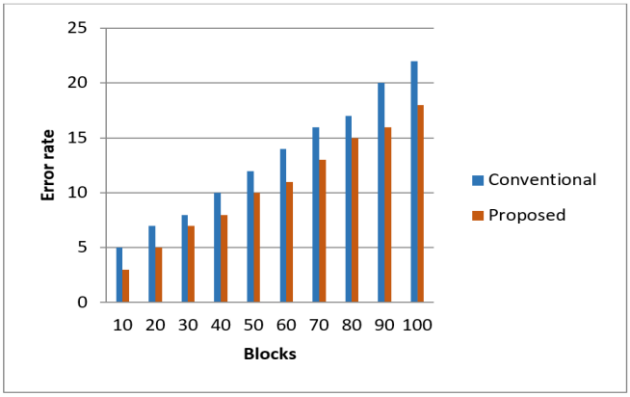

Figure 10. Comparative analysis of error rate [24]

Figure 10 presents a comparative analysis of the error rate for both the old technique and the recommended scheme when Table 9 is taken into account.

5.5 Comparison of blocks affected by external attacks

Impacts of blocks being assaulted from the outside have been modelled in this particular area of the document. When looking at numbers of blocks at intervals of 10, it was discovered that the number of blocks that have been compromised as a result of an external attack is significantly lower than in conventional schemes. This was discovered by comparing the number of blocks that were compromised to the total number of blocks. Table 10 presents the results of a comparison of the Blocks that were affected by external attacks. In this investigation, traditional and proposed work processing times are compared and contrasted [25-29].

When Table 10 is taken into account, the following figure provides a comparative analysis of the Blocks that have been affected by external attacks in circumstances of both existing system and the recommended.

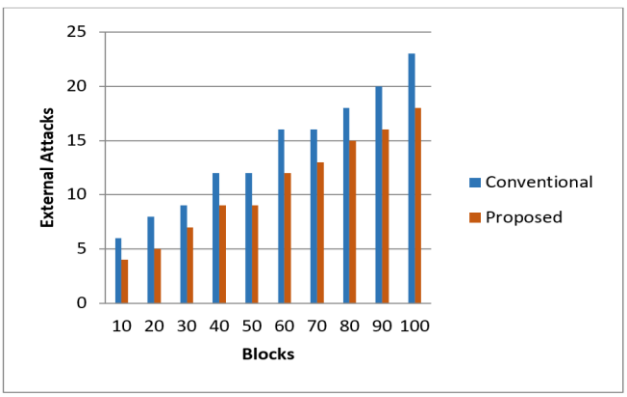

Figure 11. A comparative investigation of the Blocks that have been subjected to external assaults [30]

When Table 10 is taken into account, figure 10 provides a comparative analysis of the Blocks that have been affected by external attacks in circumstances of both existing system and the recommended.

Table 10. Comparison of Blocks affected by external attacks

Blocks	Conventional	Proposed
10	6	4
20	8	5
30	9	7
40	12	9
50	12	9
60	16	12
70	16	13
80	18	15
90	20	16
100	23	18

6. CONCLUSION

Researchers are looking at problems with blockchain security in healthcare apps as a means to avoid the theft of personal patient data. Academics are also thinking about blockchain's potential performance and security issues. With the suggested method, blockchain's security and speed will be greatly improved. Improving the efficiency of the healthcare system and making sure that applications used in the industry are secure are two approaches to make sure that the system is reliable. In order to assess both the performance of the recommended model and the safety of the traditional model for use in a healthcare setting, a comparison between the two models is being conducted. There is ongoing research on both the security and performance issues around blockchain technology. The study focuses heavily on how this innovation might improve healthcare delivery.

7. SCOPE OF RESEARCH

In order to ensure the security of patient information and facilitate its transmission between medical institutions, labs, pharmaceutical companies, and doctors, the healthcare sector has begun using Blockchain networks. This is done to protect the confidentiality of the patient. When used to the medical profession, blockchain-based apps may reliably detect serious, perhaps life-threatening errors. Because of its decentralised nature, blockchain is also great option for companies and groups that deal with sensitive data, protecting its confidentiality. Another major and troublesome security concern for blockchain-based systems is the potential weakness of the technology's endpoints. The conclusion of the blockchain network is accessible from any location where blockchain-related actions are taking place, most notably on computers and mobile phones. Hackers would spy on the user and attack just certain devices to get their key.

REFERENCES

[1] Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems, 42: 1-7. https://doi.org/10.1007/s10916-018-0982-x

[2] Radanović, I., Likić, R. (2018). Opportunities for use of blockchain technology in medicine. Applied Health Economics and Health Policy, 16: 583-590.

https://doi.org/10.1007/s40258-018-0412-8
[3] Calvaresi, D., Dubovitskaya, A., Calbimonte, J.P., Taveter, K., Schumacher, M. (2018). Multi-agent systems and blockchain: Results from a systematic literature review. In Advances in Practical Applications of Agents, Multi-Agent Systems, and Complexity: The PAAMS Collection: 16th International Conference, 16: 110-126. https://doi.org/10.1007/978-3-319-94580-4_9
[4] Zhang, A., Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of Medical Systems, 42(8): 140. https://doi.org/10.1007/s10916-018-0995-5
[5] Liang, X., Shetty, S., Zhao, J., Bowden, D., Li, D., Liu, J. (2018). Towards decentralized accountability and self-sovereignty in healthcare systems. In Information and Communications Security: 19th International Conference, Beijing, China, 19: 387-398. https://doi.org/10.1007/978-3-319-89500-0_34
[6] Miraz, M.H., Ali, M. (2018). Blockchain enabled enhanced IoT ecosystem security. In Emerging Technologies in Computing: First International Conference, iCETiC 2018, London, UK, 1: 38-46. https://doi.org/10.1007/978-3-319-95450-9_3
[7] Firdaus, A., Anuar, N.B., Razak, M.F.A., Hashem, I.A.T., Bachok, S., Sangaiah, A.K. (2018). Root exploit detection and features optimization: Mobile device and blockchain based medical data management. Journal of Medical Systems, 42: 1-23. https://doi.org/10.1007/s10916-018-0966-x
[8] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., Liu, S. (2018). Blockchain-based data preservation system for medical data. Journal of Medical Systems, 42: 1-13. https://doi.org/10.1007/s10916-018-0997-3
[9] Epiphaniou, G., Daly, H., Al-Khateeb, H. (2019). Blockchain and healthcare. In Blockchain and Clinical Trial. Springer International Publishing, Springer, Cham, pp. 1-29. https://doi.org/10.1007/978-3-030-11289-9_1
[10] Zhou, T., Li, X., Zhao, H. (2019). Med-PPPHIS: Blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding. Journal of Medical Systems, 43: 1-23. https://doi.org/10.1007/s10916-019-1430-2
[11] Iram, S., Fernando, T., Hill, R. (2019). Connecting to smart cities: Analyzing energy times series to visualize monthly electricity peak load in residential buildings. In Proceedings of the Future Technologies Conference (FTC) 2018. Springer International Publishing, 1: 333-342. https://doi.org/10.1007/978-3-030-02686-8_26
[12] Rathee, G., Sharma, A., Saini, H., Kumar, R., Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications, 79(15-16): 9711-9733. https://doi.org/10.1007/s11042-019-07835-3
[13] Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., Abd-Alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. International Journal of Medical Informatics, 142: 104246. https://doi.org/10.1016/j.ijmedinf.2020.104246
[14] Munoz, D.J., Constantinescu, D.A., Asenjo, R., Fuentes, L. (2020). Clinicappchain: A low-cost blockchain hyperledger solution for healthcare. In Blockchain and Applications: International Congress. Springer International Publishing, Springer, Cham, pp. 36-44. https://doi.org/10.1007/978-3-030-23813-1_5
[15] Amir Latif, R.M., Hussain, K., Jhanjhi, N.Z., Nayyar, A., Rizwan, O. (2020). A remix IDE: Smart contract-based framework for the healthcare sector by using blockchain technology. Multimedia Tools and Applications, 1-24. https://doi.org/10.1007/s11042-020-10087-1
[16] Mubarakali, A. (2020). Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach. Mobile Networks and Applications, 25: 1330-1337. https://doi.org/10.1007/s11036-020-01551-1
[17] Nagasubramanian, G., Sakthivel, R.K., Patan, R., Gandomi, A.H., Sankayya, M., Balusamy, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications, 32: 639-647. https://doi.org/10.1007/s00521-018-3915-1
[18] Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S.A., Faxvaag, A. (2020). Blockchain in healthcare and health sciences-A scoping review. International Journal of Medical Informatics, 134: 104040. https://doi.org/10.1016/j.ijmedinf.2019.104040
[19] Casado-Vara, R., De la Prieta, F., Rodriguez, S., Prieto, J., Corchado, J.M. (2018). Cooperative algorithm to improve temperature control in recovery unit of healthcare facilities. In International Symposium on Distributed Computing and Artificial Intelligence. Cham: Springer International Publishing, Springer, Cham, pp. 49-62. https://doi.org/10.1007/978-3-030-00524-5_8
[20] McBee, M.P., Wilcox, C. (2020). Blockchain technology: Principles and applications in medical imaging. Journal of Digital Imaging, 33: 726-734. https://doi.org/10.1007/s10278-019-00310-3
[21] Omar, I.A., Jayaraman, R., Salah, K., Yaqoob, I., Ellahham, S. (2021). Applications of blockchain technology in clinical trials: Review and open challenges. Arabian Journal for Science and Engineering, 46: 3001-3015. https://doi.org/10.1007/s13369-020-04989-3
[22] Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P.C., Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. The Journal of Supercomputing, 1-21. https://doi.org/10.1007/s11227-021-03637-3
[23] Santos, J.A., Inacio, P.R., Silva, B.M. (2021). Towards the use of blockchain in mobile health services and applications. Journal of Medical Systems, 45: 1-10. https://doi.org/10.1007/s10916-020-01680-w
[24] Rejeb, A., Treiblmaier, H., Rejeb, K., Zailani, S. (2021). Blockchain research in healthcare: A bibliometric review and current research trends. Journal of Data, Information and Management, 3: 109-124. https://doi.org/10.1007/s42488-021-00046-2
[25] Ratkovic, N. (2022). Improving home security using blockchain. International Journal of Computations, Information and Manufacturing (IJCIM), 2(1): 27-37. https://doi.org/10.54489/ijcim.v2i1.72
[26] Liu, Y., Shan, G., Liu, Y., Alghamdi, A., Alam, I., Biswas, S. (2022). Blockchain bridges critical national infrastructures: E-healthcare data migration perspective. IEEE Access, 10: 28509-28519. https://doi.org/10.1109/ACCESS.2022.3156591
[27] Odeh, A., Keshta, I., Al-Haija, Q.A. (2022). Analysis of blockchain in the healthcare sector: Application and

issues. Symmetry, 14(9): 1760. https://doi.org/10.3390/sym14091760

[28] Mahajan, H.B., Rashid, A.S., Junnarkar, A.A., Uke, N., Deshpande, S.D., Futane, P.R., Alkhayyat, A., Alhayani, B. (2023). Integration of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. Applied Nanoscience, 13(3): 2329-2342. https://doi.org/10.1007%2Fs13204-021-02164-0

[29] Xi, P., Zhang, X., Wang, L., Liu, W., Peng, S. (2022). A review of Blockchain-based secure sharing of healthcare data. Applied Sciences, 12(15): 7912. https://doi.org/10.3390/app12157912

[30] Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15(1): 70-83. https://doi.org/10.1080/20479700.2020.1843887