International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 05, May 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Enhancement of Security and performance of blockchain for healthcare application

Dr. Raghuvinder, Parveen Rani

Assistant Professor, Department of computer Science and Engineering

Abstract

The goal of this study is to prevent the theft of patient information by examining security and performance challenges associated with block chain security in the context of health care applications. The results of this study will provide mechanisms to improve the security and performance of blockchain technology; the former will help guarantee the healthcare system's dependability, while the latter will make healthcare apps more productive. Finally, the suggested model's performance and security will be compared to those of a more traditional approach in the hospital setting. The proposed study has focused on investigating block chain security and its medical applications, and has taken into account the security and performance issues that are intrinsic to the technology. This is done to protect patients' personal data from being stolen. Recent studies have provided a method to enhance the robustness and security of block chains. Enhancing both performance and security would greatly benefit the healthcare industry, with the former ensuring the reliability of the healthcare system and the latter increasing the efficiency of healthcare applications. The proposed model is being compared to the current standard model to see how well it performs and how safe it is to use in a medical context. The suggested technique first compresses the healthcare data collection before encrypting it. Data is protected by compression and encryption before being stored on the blockchain during block initialization. Then, the suggested method's precision and efficiency are measured against those of the standard method.

Keywords: *Blockchain, Healthcare, Data compression, encryption, Performance, Accuracy*

Introduction

There is an increasing need for medical software on a daily basis. The information that pertains to patients still has to be stored in a safe place. The information pertaining to patients need to be kept in a secure area, and there are a variety of various actions that may be done to prevent unauthorized access to this data. These methods, on the other hand, are considered to be out of date at this moment. The use of the blockchain technology ought to allay some of the worries over the state of the security system. There is a possibility that the distributed ledger technology known as block chain, which encourages decentralization, may be used to preserve the medical information of patients. The focus of current efforts in the field of research into the uses of blockchain

technology in the healthcare business is shifting toward the development of solutions that are not only completely risk-free but also highly efficient.

Over the course of the last decade, the concept of "block chain" has been the focus of investigation at a variety of academic institutions as well as commercial businesses. This is due to the fact that "block chain" is now regarded as one of the most exciting newly created technologies. The block chain is a distributed, decentralized, and immutable ledger system that eliminates the need to use a trusted third party to verify and record transactions. This is made possible by the block chain's use of cryptography. The next version of the block chain technology is called Blockchain 3.0, and non-financial businesses such as the government, the energy industry, and the healthcare industry are leading the way in the development of this technology. These technologies have been embraced by hospitals and other institutions that are dedicated to patient care, who have also identified various uses for them as a result of their usage. The decentralized nature of blockchain, together with the privacy precautions and security measures that are already built into it, make it a highly beneficial technology in the healthcare sector. These characteristics provide the potential to be used in a manner that will prevent unauthorized individuals from gaining access to vital medical data.

A blockchain, in its most fundamental manifestation, may be conceptualized as a decentralized ledger that was introduced for the very first time in 2008 as an essential component of the Bitcoin protocol. A public ledger that is referred to as a chain of blocks is used by the blockchain for the goal of recording and validating each and every transaction that takes place throughout the network. Each individual block is composed of two parts: the header and the body. The previous block's hash is shown in the header of each new block, which displays the hash of the block that came before it. A series of linked lists or additional chains is used to establish a connection between each block in a chain and the block that came before it. It is possible to reduce the amount of labor needed to evaluate the transactions included in a block by making use of features like as Merkle trees, timestamps, and nonces in the block headers. This helps to speed up the process. In order to solve a mathematical problem, miners often make adjustments to the nonce number. This is done in an attempt to discover a solution.

A transaction is a little piece of work that is recorded and maintained in a public ledger called a block. Transactions are recorded and saved on a blockchain. It is only possible for there to be two parties involved in a transaction. In order for any transaction to be effectively completed, it is necessary that the vast majority of people participating in the system come to the same conclusion. Transactions that are recorded on a blockchain are unchangeable and cannot be altered by a third party. This makes the blockchain an immutable public ledger. Due to the immutability of the blockchain, it is not necessary for each participant to have several copies of the ledger. It is sufficient for them to keep a single copy. The business logic of a blockchain is referred to as smart contracts, and it is written as computer code that automatically executes itself on the underlying architecture of a blockchain. This ensures that transactions can be performed without any snags occurring along the way. When a smart contract is incorporated into a blockchain, it gains the properties of becoming irreversibly tamper-proof due to the fact that no one can change what has been written, self-verifying due to the automated capabilities of

the blockchain, and self-enforcing when the rules are satisfied at all stages. These properties are in addition to the properties that the smart contract already had before it was incorporated into the blockchain. Blockchain is resistant to censorship and virtually hard to manipulate as a result of its decentralized nature, immutability, availability, and anonymity. This makes it very difficult, if not impossible, to manipulate.

Blockchain Use Cases in Healthcare

When a cryptographic key was used to connect a chain of transactions, the result is called a "blockchain." In order to verify these signatures and keys, they are linked together in a system of nodes or processes. Every node in the network has a fully up-to-date copy of the whole chain. According to NIST, some of the benefits of blockchain technology include the decentralization of digital ledgers, the resistance to tampering, and the difficulty of modifying a published transaction later within a user community that shares the ledger. Digital ledger technology is another name for this method.

People have high hopes for the medicinal applications of blockchain technology. The White Paper Request Ideation Challenge on Blockchain in Healthcare was launched in 2016 by the ONC for Health Information Technology. In 2016, this occurred. As a direct consequence, a variety of blockchain-based healthcare solutions have emerged.

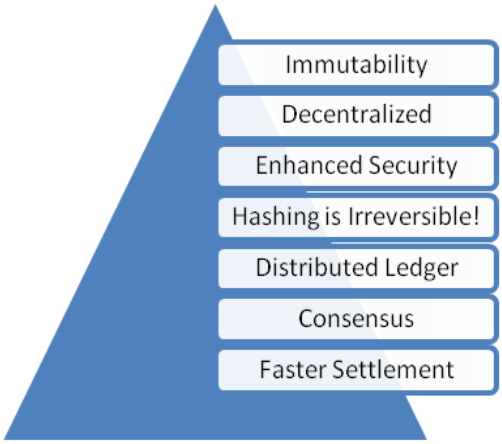

Fig 1 Features of Blockchain

Electronic Medical Records

There is the potential for a revolution in medical treatment if different systems can be brought together and electronic health records are made more accurate. Despite the fact that electronic medical records (EMRs) and electronic health records (EHRs) are not the same thing, some individuals may use these words interchangeably at times. An electronic medical record, often known as an EMR, is a computerised representation of the paper files that are kept on file at a medical institution. Electronic medical records, or EMRs, are computerised records that detail a patient's medical history and treatment. Electronic health records (EHRs) allow for a greater

emphasis on the patient's overall health, and they give more information than is generally accessible from a visit to the doctor's office alone. The mapping analysis came to the conclusion that blockchain technology might be helpful in the administration of EMR systems. Patients have the ability to choose who has access to their medical records because to MedRec's utilisation of the Ethereum network. FHIRChain is another another software that contributes to the process of combining EHRs. The administration of medical records is the primary emphasis of a blockchain programme based on Ethereum.

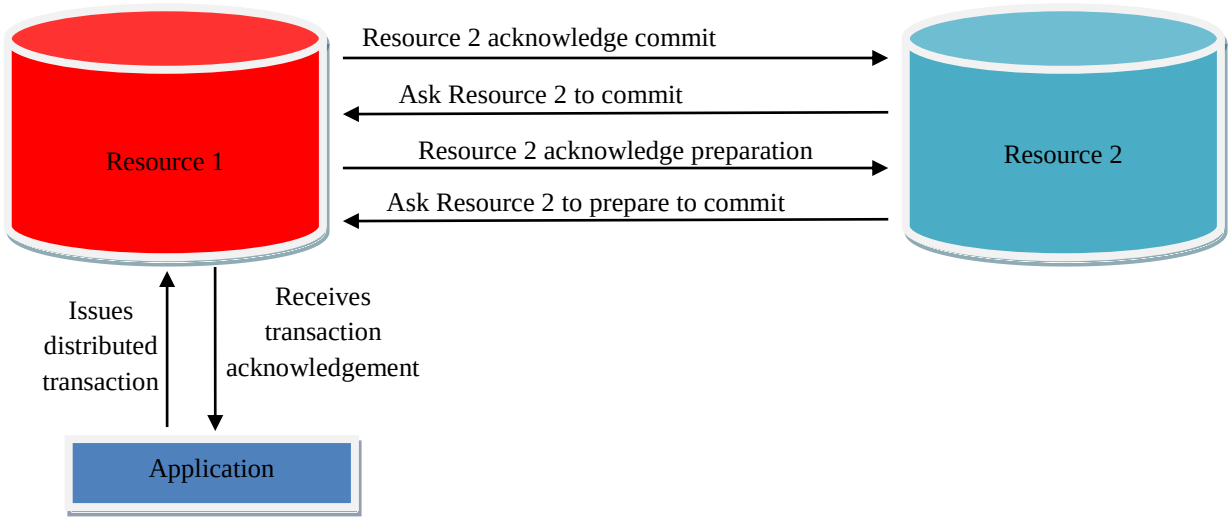

Fig 2 Distributed Transaction Recording Systems

DLT (Distributed Transaction Recording System): In most circumstances, the parties engaged in a transaction will be listed in a public ledger. Everything is in full view, so there's nowhere to hide. For private or federated blockchain, the rationale is slightly different. The ledger can still be seen by many people in these scenarios. Due to the fact that each user contributes are to the network's ledger. This resulted in more expeditious resolution displayed in figure 1.2.

- Consensus: Consensus algorithms ensure that any blockchain is able to exist and grow. At its core is a well-designed system that uses consensus techniques. A consensus mechanism is built into every blockchain to help the network make decisions. Consensus can be blamed for the lack of confidence in the network. Despite the absence of trust between nodes, the underlying algorithms may be trusted. Every action on the network helps the blockchain. Using blockchain technology provides this benefit.
- Expedite the process: While traditional banking techniques take longer to settle transactions, blockchain does it more quickly. The speed of the money transfer greatly reduces the amount of time it takes for users to complete transactions.

International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 05, May 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

- The necessity for blockchain technology: The verification and traceability given by blockchain necessitates the use of multi-step transactions. There are less compliance costs and speedier data transfer processing as well as more secure transactions.
- **1.6 Data Security**
- When it comes to data security, it's all about safeguarding your information against unwanted access and corruption at every stage of its lifespan. Encryption, hashing, tokenization, and key management methods are all part of the data security process.

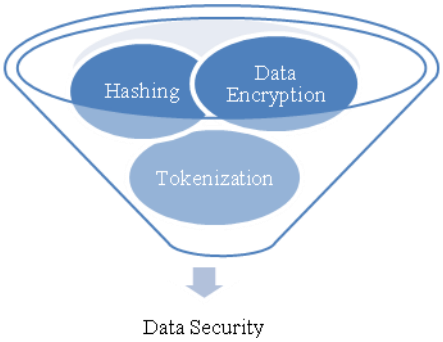

Fig 3 Scope of Data Security

Data encryption

- Because only those who have access to an encrypted data decryption key may read it, data encryption is also known as data decryption. Ciphertext (encrypted data) and plaintext (unencrypted data) are regularly used terms. Encryption is currently one of the most widely utilized and most effective data security solutions in use. It is possible to encode data using asymmetric or public-key encryption (also known as symmetric encryption).
- Messages and files are encrypted and decrypted using the same secret key in symmetric-key cyphers. Asymmetric encryption, on the other hand, requires the sender and recipient to share the encryption key in order to decrypt a message. Most data encryption services have evolved and now employ an asymmetric technique to share the secret key after utilizing a symmetric approach to encrypt data. This allows firms to safely distribute and manage large amounts of keys.
- Asymmetric cryptography, or public-key cryptography, on the other hand, employs two separate keys, one public and one private, to encrypt data. There are two types of keys: the "public key," which may be shared with anybody, and the "private key." For public-key encryption, the Rivest-Sharmir-Adleman (RSA) method is extensively employed, especially when sensitive data is sent across an unsecured network like the internet. In order to ensure the secrecy, integrity, authenticity, and non-repudiability of electronic communications and data, the RSA method relies on the usage of digital signatures, which may be generated using both the public and private keys.

Hashing

- The process of converting a key or a string of characters into a different value is known as hashing. Shorter values or keys are often used to represent the original string and make it easier to discover or use the original string.
- Hash tables are the most common use of hashing. A hash table holds key and value pairs in a list that is accessible by its index. The hash function will map the keys to the table size since key and value pairs are limitless. A hash value then becomes the index for a certain element.
- A hash function creates new values according to a mathematical hashing technique, known as a hash value or simply a hash. To avoid the conversion of hash back into the original key, a good hash always utilizes a one-way hashing method.
- Data indexing and retrieval, digital signatures, cybersecurity, and cryptography all benefit from hashing.
- In addition to facilitating speedy data retrieval, hashing helps encode and decode digital signatures needed to verify message senders and recipients. Using a hash function, the digital signature is transformed into a message digest before being relayed to the receiver in two consecutive transmissions. On reception, a hash function is used to generate the signature's message digest, which is compared to the transmitted message digest. Hash functions index the original value or key and provide access to the data associated with a certain recovered value or key when using a one-way hashing procedure.

Literature review

Conventional research related to research work has been discussed in this section. Here author, objectives, Area of research and limitation of conventional research are discussed.

Sno.	Author/Year	Objective	Area of research	Limitation
1	K. N. Griggs / 2018	To propose Healthcare Blockchain System that should make use of Smart Contracts. Uses for this technology include remote patient monitoring that is both safe and automated.	Healthcare, Blockchain	Lack of technical work
2	I. Radanović / 2018	Use Cases for Blockchain Technology in the Healthcare Industry	Blockchain,Health care	There is no implication in future
3	D. Calvaresi / 2018	Systematic Literature Review on Multi-Agent Systems and Blockchain	Blockchain	There is no security in this system
4	A. Zhang / 2018	Data sharing in e-health systems may be done in a secure and private manner thanks to the Consortium Blockchain.	Secure, Privacy,Healthcare ,Blockchain	Scope of this research is very less

5	X. Liang / 2018	Decentralization of responsibility and self-determination in healthcare systems	Healthcare systems	Performance of this research is very low
6	M. H. Miraz / 2018	Because of blockchain, the Internet of Things (IoT) ecosystem is now more secure.	Blockchain,IOT,Security	There is no work on healthcare
7	A. Firdaus	Management of Medical Data on Mobile Devices: Root Exploit Detection and Functionality Enhancement	Blockchain, Detection	Lack of accuracy
8	H. Li / 2018	A Blockchain-Based Medical Data Archiving System	Blockchain, Data Preservation System	Lack of security
9	G. Epiphaniou / 2019	It's time to talk about blockchain in healthcare.	Blockchain,Healthcare	Lack of accuracy
10	T. Zhou / 2019	The use of a blockchain-based personal healthcare information system for scientific exercise guidance and national physique monitoring	Blockchain, Information System,Healthcare	There is no security in this system
11	S. Iram / 2019	Connecting to smart cities: Visualizing monthly peak power demand in residential structures using energy time series analysis	Smart Cities,Energy Time	There is no work on healthcare
12	G. Rathee / 2020	An IoT-based healthcare system that utilises blockchain technology for multimodal data processing	Hybrid framework, Multimedia	Lack of accuracy
13	I. Abu-elezz / 2020	Scope review: health care applications of blockchain technology and potential drawbacks	Blockchain, Healthcare	Scope of this research is very less
14	D. J. Munoz / 2020	Healthcare blockchain hyperledger solution Clinicappchain: low-cost	Blockchain, Hyperledger, Healthcare	There is no security in this system
15	R. M. Amir Latif / 2020	"A Blockchain-based remix IDE: a smart contract-based healthcare framework"	Blockchain, contract-based Framework, Healthcare	Lack of accuracy

Challenges

There have been a number of studies conducted in the field of healthcare that have examined using blockchain to store patient information; nevertheless, it is essential that these records be kept secure. However, there are traditional methods that have examined blockchain for the purpose of healthcare data security; the problem is that these methods are not very efficient. The potential uses of Blockchain technology in the area of medicine were only partially explored by conventional study.

Proposed work

Proposed work is focusing on the research related to block chain security and health care application and considering the security and performance issues related to block chain security in order to protect patient records from being theft. Then research work has proposed mechanism to enhance the security and performance of block chain. The enhancement of security would assure the reliability in healthcare system where as performance enhancement would increase efficiency of healthcare applications. Evaluation of performance and security has been made in case of proposed to conventional model that would be applied in healthcare environment. Thus, hybrid approach would be proposed in order to improve the security and performance.

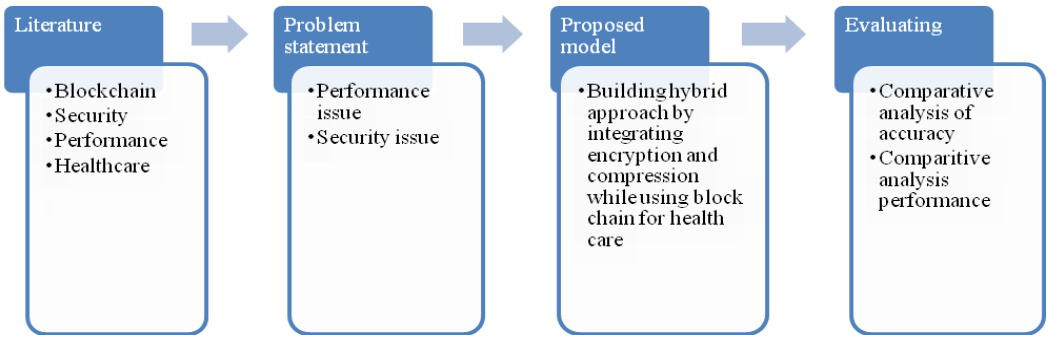

Fig 4 Proposed Research Methodologies

Result and discussion

In this section the time taking during processing of block has been simulated. The numbers of blocks are considered at interval of 10 and it has been observed that processing time of block is less as compared to conventional processing time. Table 1 is presenting comparative analysis of performances between conventional and proposed work processing time.

Table 1 Comparative analysis of performance

Number of blocks	Conventional processing time	Proposed processing time
10	1.23161	0.22511
20	2.33185	0.61771

30	3.01603	1.81461
40	4.40952	2.07098
50	5.85916	2.39535
60	6.19277	3.13437
70	7.47394	4.16924
80	7.76859	4.3766
90	9.24844	4.75727
100	10.5412	6.02997
110	10.2429	6.25872
120	11.9833	7.33292
130	13.6959	7.71301
140	13.6311	8.62271
150	14.6198	9.65163
160	16.434	9.62368
170	15.9666	10.3472
180	18.381	11.3442
190	19.3883	11.8131
200	19.9727	11.981

Considering the table 1, figure 5 is presenting comparative analysis of performance in case of conventional and proposed scheme.

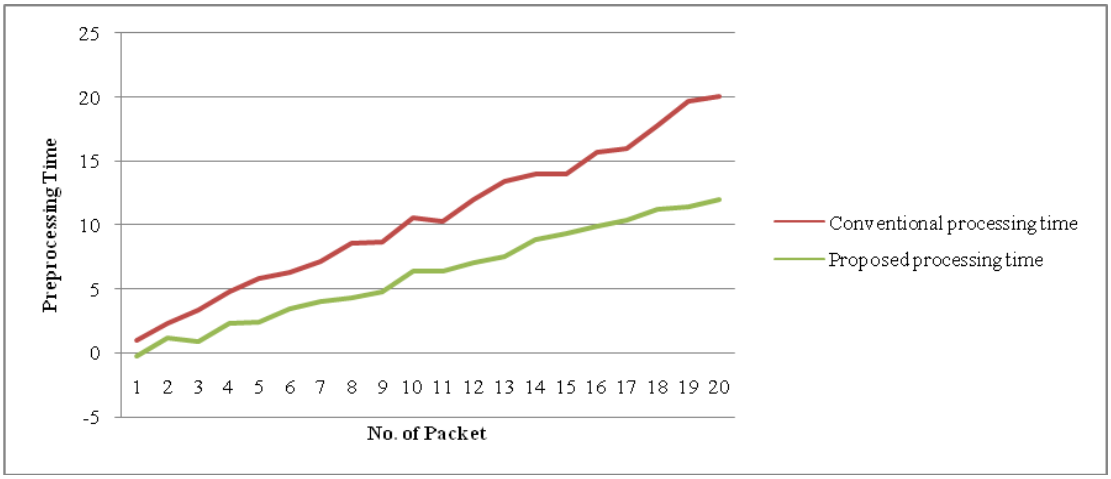

Fig 5 comparative analysis of performance in case of conventional and proposed scheme

Comparative analysis of error rate

In this section the error taking during processing of block has been simulated. The numbers of blocks are considered at interval of 10 and it has been observed that error is less as compared to conventional scheme.

International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 05, May 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Table 2 is presenting comparative analysis of error rate between conventional and proposed work processing time.

Table 2 Comparative analysis of error rate

Number of blocks	Conventional Scheme	Proposed scheme
10	4	2
20	6	4
30	7	6
40	9	7
50	11	9
60	13	10
70	15	12
80	16	14
90	19	15
100	21	17
110	21	18
120	25	18
130	24	21
140	26	22
150	31	25
160	32	25
170	33	25
180	37	28
190	35	29
200	42	34

Considering the table 2, figure 6 is presenting comparative analysis of error rate in case of conventional and proposed scheme.

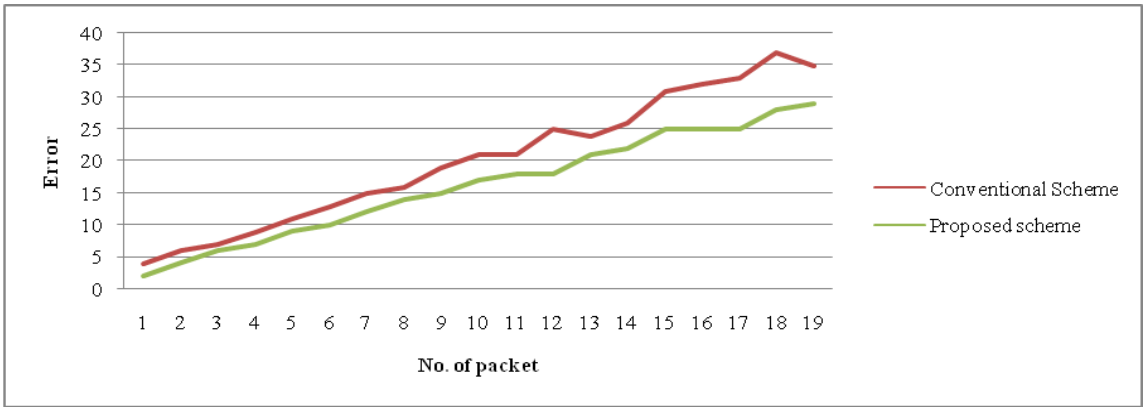

Fig 6 Comparative analysis of error rate

Comparative analysis of Blocks affected by external attacks

In this section the blocks affected by external attack has been simulated. The numbers of blocks are considered at interval of 10 and it has been observed that affected block due to external attack are less as compared to conventional scheme. Table 3 is presenting comparative analysis of Blocks affected by external attacks between conventional and proposed work processing time.

Table 3 Comparative analyses of Blocks affected by external attacks

Number of blocks	Conventional Scheme	Proposed scheme
10	4	3
20	6	4
30	7	6
40	10	8
50	10	8
60	14	11
70	14	12
80	16	14
90	18	15
100	21	17
110	23	17
120	24	19
130	25	21
140	27	24
150	30	26
160	29	25
170	31	27
180	33	27
190	39	31
200	39	31

Considering the table 3, figure 7 is presenting comparative analysis of Blocks affected by external attacks in case of conventional and proposed scheme.

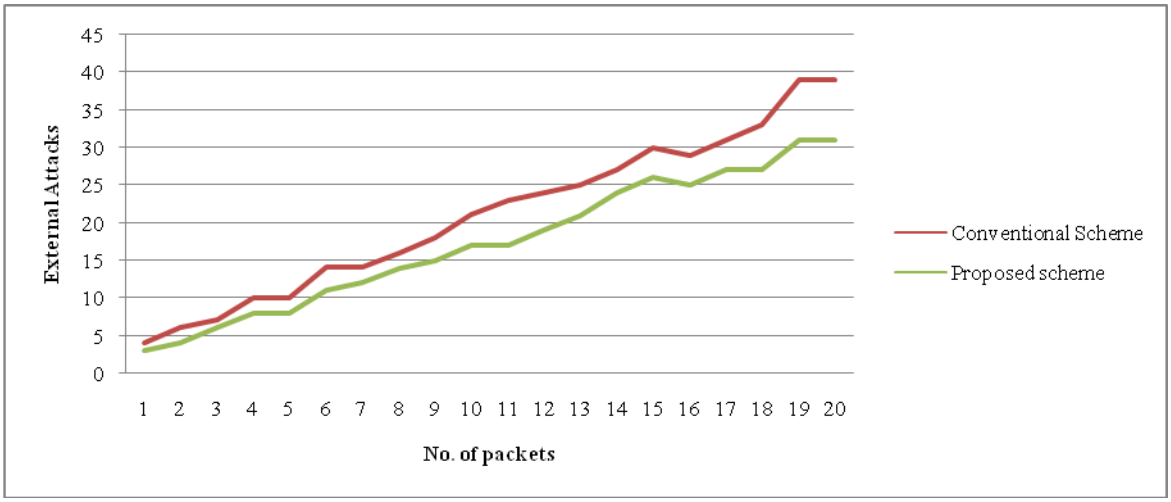

Fig 7 Comparative analysis of Blocks affected by external attacks

Conclusion

There have been a number of studies conducted in the field of healthcare that have examined using blockchain to store patient information; nevertheless, it is essential that these records be kept secure. However, there are traditional methods that have examined blockchain for the purpose of healthcare data security; the problem is that these methods are not very efficient. The potential uses of Blockchain technology in the area of medicine were only partially explored by conventional study. In order to prevent the theft of patient information, research is concentrating on topics linked to block chain security and health care applications. Additionally, researchers are taking into consideration the security and performance challenges associated with block chain security. Block chain would benefit from the proposed technique, which would improve both its safety and its performance. The improvement of performance would ensure the dependability of the healthcare system, whilst the improvement of security would raise the effectiveness of the apps used in healthcare. The suggested model is being compared to the traditional model in order to assess its level of performance as well as its level of security for use in the healthcare setting. Concerns about security and performance are being investigated in the context of block chain security as part of ongoing research, with a particular focus on the use of this technology within the healthcare business. The major objective is to develop methods that will ensure the efficiency and security of blockchain transactions via the use of compression and encryption. The next step would be to evaluate both the usefulness and the security of the proposed system. Therefore, a hybrid strategy is going to be suggested in order to increase both the performance and the security. The findings of the simulation lead one to the conclusion that the performance of the suggested work is superior to that of traditional processing mechanisms. As a result, the likelihood of making a mistake is reduced. In addition, the number of blocks that are vulnerable to assaults from the outside has been decreased as a result of the suggested work. Therefore, the work that has been suggested offers improved performance, accuracy, and security in comparison to the study that has been done traditionally.

Scope of research

A Blockchain network is utilized within the healthcare industry for the aim of safeguarding patient data and enabling data transfer between hospitals, diagnostic laboratories, pharmaceutical firms, and physicians. This is accomplished via the usage of the Blockchain network. Applications based on blockchain technology have the ability to accurately identify major and even harmful mistakes in the field of medicine. Additionally, the fact that blockchain is a decentralized network makes it a great choice for companies and organizations that deal with sensitive information since it ensures that the information will be kept private. The possible vulnerability of blockchain technology's endpoints is yet another significant and problematic security issue for the platform. The conclusion of the blockchain network may be seen anyplace that users participate out actions linked to the blockchain. More particular, it can be found on electronic devices like as computers and mobile phones. In order to get the user's key, hackers will monitor the user's activities and selectively target devices in their attack. The pre-authorization procedure will see a significant decrease in the amount of time it takes if tokenization, smart contracts, and the encryption methods that are used in blockchain network transactions are implemented. Patients will be able to obtain the essential and informed care in a way that is more time and cost efficient as a result of this. A blockchain system employs asymmetric cryptography to ensure the confidentiality of transactions carried out between its users. Every user who logs into one of these systems receives both a public key and a private key to use during their time there. These keys, which are made up of random sequences of numbers, are used in cryptography in some capacity. It is theoretically impossible for one user to deduce the private key of another user based just on that user's public key. In practice, however, this is not an impossibility. It is anticipated that the findings of this sort of research would have far-reaching implications not just for the medical field but also for other commercial applications that are dependent on secure data storage. The reality of the situation is that a wide variety of real-time systems have the potential to tackle the problems that are encountered in the actual world. It is probable that in the not too distant future, additional enhancements to the security of these systems will entail the employment of techniques for the classification of healthcare data that will be applied with blockchain. These ways will be learned via machine learning.

Reference

1. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring,” J. Med. Syst., vol. 42, no. 7, pp. 1–7, 2018, doi: 10.1007/s10916-018-0982-x.
2. Radanović and R. Likić, “Opportunities for Use of Blockchain Technology in Medicine,” Appl. Health Econ. Health Policy, vol. 16, no. 5, pp. 583–590, 2018, doi: 10.1007/s40258-018-0412-8.
3. D. Calvaresi, A. Dubovitskaya, J. P. Calbimonte, K. Taveter, and M. Schumacher, Multi-agent systems and blockchain: Results from a systematic literature review, vol. 10978 LNAI. Springer International Publishing, 2018.
4. Zhang and X. Lin, “Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain,” J. Med. Syst., vol. 42, no. 8, 2018, doi: 10.1007/s10916-018-0995-5.

5. X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, Towards decentralized accountability and self-sovereignty in healthcare systems, vol. 10631 LNCS. Springer International Publishing, 2018.
6. M. H. Miraz and M. Ali, Blockchain enabled enhanced IoT ecosystem security, vol. 200. Springer International Publishing, 2018.
7. Firdaus, N. B. Anuar, M. F. A. Razak, I. A. T. Hashem, S. Bachok, and A. K. Sangaiah, "Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management," J. Med. Syst., vol. 42, no. 6, 2018, doi: 10.1007/s10916-018-0966-x.
8. H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-Based Data Preservation System for Medical Data," J. Med. Syst., vol. 42, no. 8, pp. 1–13, 2018, doi: 10.1007/s10916-018-0997-3.
9. G. Epiphaniou, H. Daly, and H. Al-Khateeb, "Blockchain and healthcare," Adv. Sci. Technol. Secur. Appl., pp. 1–29, 2019, doi: 10.1007/978-3-030-11289-9_1.
10. T. Zhou, X. Li, and H. Zhao, "Med-PPPHIS: Blockchain-Based Personal Healthcare Information System for National Physique Monitoring and Scientific Exercise Guiding," J. Med. Syst., vol. 43, no. 9, 2019, doi: 10.1007/s10916-019-1430-2.
11. S. Iram, T. Fernando, and R. Hill, Connecting to smart cities: Analyzing energy times series to visualize monthly electricity peak load in residential buildings, vol. 880, no. 3. Springer International Publishing, 2019.
12. G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," Multimed. Tools Appl., vol. 79, no. 15–16, pp. 9711–9733, 2020, doi: 10.1007/s11042-019-07835-3.
13. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," Int. J. Med. Inform., vol. 142, no. February, p. 104246, 2020, doi: 10.1016/j.ijmedinf.2020.104246.
14. D. J. Munoz, D. A. Constantinescu, R. Asenjo, and L. Fuentes, Clinicappchain: A low-cost blockchain hyperledger solution for healthcare, vol. 1010. Springer International Publishing, 2020.
15. R. M. Amir Latif, K. Hussain, N. Z. Jhanjhi, A. Nayyar, and O. Rizwan, "A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology," Multimed. Tools Appl., 2020, doi: 10.1007/s11042-020-10087-1.
16. Mubarakali, "Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN(SRHB)Approach," Mob. Networks Appl., vol. 25, no. 4, pp. 1330–1337, 2020, doi: 10.1007/s11036-020-01551-1.
17. G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," Neural Comput. Appl., vol. 32, no. 3, pp. 639–647, 2020, doi: 10.1007/s00521-018-3915-1.
18. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," Int. J. Med. Inform., vol. 134, no. May 2019, p. 104040, 2020, doi: 10.1016/j.ijmedinf.2019.104040.

19. R. Casado-Vara, F. De la Prieta, S. Rodriguez, J. Prieto, and J. M. Corchado, Cooperative algorithm to improve temperature control in recovery unit of healthcare facilities, vol. 802. Springer International Publishing, 2020.
20. M. P. McBee and C. Wilcox, "Blockchain Technology: Principles and Applications in Medical Imaging," J. Digit. Imaging, vol. 33, no. 3, pp. 726–734, 2020, doi: 10.1007/s10278-019-00310-3.
21. Omar, R. Jayaraman, K. Salah, I. Yaqoob, and S. Ellahham, "Applications of Blockchain Technology in Clinical Trials: Review and Open Challenges," Arab. J. Sci. Eng., vol. 46, no. 4, pp. 3001–3015, 2021, doi: 10.1007/s13369-020-04989-3.
22. T. Veeramakali, R. Siva, B. Sivakumar, P. C. Senthil Mahesh, and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," J. Supercomput., vol. 77, no. 9, pp. 9576–9596, 2021, doi: 10.1007/s11227-021-03637-3.
23. Santos, P. R. M. Inácio, and B. M. C. Silva, "Towards the Use of Blockchain in Mobile Health Services and Applications," J. Med. Syst., vol. 45, no. 2, 2021, doi: 10.1007/s10916-020-01680-w.
24. Rejeb, H. Treiblmaier, K. Rejeb, and S. Zailani, "Blockchain research in healthcare: a bibliometric review and current research trends," J. Data, Inf. Manag., vol. 3, no. 2, pp. 109–124, 2021, doi: 10.1007/s42488-021-00046-2.