Analysis Of Blockchain Technology To Protect Data Access Using Intelligent Contract Mechanism For 5G Networks

P. William
Department of Information Technology
Sanjivani College of Engineering
Savitribai Phule Pune University
Pune, Maharashtra, India.
william160891@gmail.com

Anjani Kumar Rai
Institute of Engineering & Technology
GLA University
Mathura, Uttar Pradesh, India.
anuragshri76@gmail.com

Parul Madan
Assistant Professor
Department of Computer Science & Engineering
Graphic Era Deemed to be University
Dehradun, Uttarakhand, India.
parulmadan@geu.ac.in

C Praveen Kumar
Department of Computer Science and Engineering
Institute of Aeronautical Engineering
Hyderabad, Telangana, India.
praveenchatakunt@gmail.com

Dr. Anurag Shrivastava
Saveetha School of Engineering
Saveetha Institute of Medical and Technical Sciences
Chennai, Tamilnadu, India.
anuragshri76@gmail.com

Ajay Rana
Amity University
Greater Noida
Uttar Pradesh, India.
ajay_rana@amity.edu

2023 6th International Conference on Contemporary Computing and Informatics (IC3I) | 979-8-3503-0448-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/IC3I59117.2023.10397700

***Absract* - With constantly changing internet models automating and digitising countless residential and industrial applications, the world of today has made significant progress in the sharing of healthcare data and the implementation of crucial actions. The two most crucial factors in the setting of healthcare data exchange today are privacy and data integrity. In order to prevent unauthorised individuals from viewing or accessing sensitive data, such as medical information, encryption is essential. The intermediary nodes shouldn't be given too much weight because conventional encryption techniques could not be deployable through them. The current security alternatives for IoT-driven healthcare monitoring frameworks are discussed in this article along with the numerous security challenges that exist in the current 5G network design and how blockchain technology may be used to encrypt data between nodes. The suggested approach outperformed the alternatives and the present strategies for IoT-driven healthcare monitoring frameworks' security solutions, according to a variety of performance factors utilised to test it. A number of performance parameters were used to test the suggested technique, and the results showed that it performed better than the alternatives.**

Keywords - Block chain, IoT, Security, Healthcare, Data Integrity, and Encryption.

I. INTRODUCTION

The use of block chain technology to improve the efficiency with which healthcare data records are transmitted, as well as transparency, privacy, confidentiality, and traceability. The healthcare sector is about to undergo a revolution because to block chain technology, machine learning, and artificial intelligence (AI).

Technology, such as Healthcare Information Sharing [1-4], has shown to accelerate the transfer of healthcare data across an unsecured route. The usage of HIE technology has expanded, the cost of data interchange has lowered, and patient care and monitoring has been strengthened by improvised surveillance as a result of this technology.

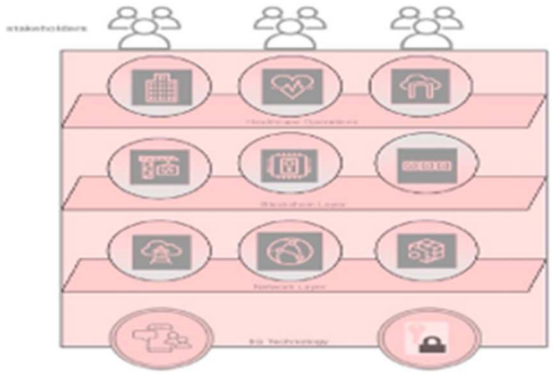

Figure 1. Health care operations based on layer dependency

Improved analysis and interpretation of clinical research results may be achieved via the application of BlocHIE technology [5]. The EMR-chain and PHD-chain frameworks for storing and distributing huge quantities of data may be handled effectively by HIE technology by storing and distributing storage models such as EMRs and PHDs. Figure 1 depicts a blockchain's tier-based architecture, which may be used in many healthcare applications. Healthcare monitoring service providers (HMS), patients, and medical professionals—including radiologists—all constitute stakeholders.

A variety of vertical applications may be supported by connecting a wide range of heterogeneous hardware and software, resulting in significant increases in network node service quality as well as overall architecture throughput. 5G healthcare frameworks and beyond have been significantly impacted by issues including decentralised openness, data interoperability hazards, and network privacy [6]. Security

management in 5G is complex owing to the network's diversity of devices, and establishing immutability and transparency is critical [7].

It is the major goal of this project to use Internet of Things (IoT)-connected devices to enhance remote patient surveillance and tele-guidance. Internet-enabled health care models have the potential to enhance patient safety and healthcare outcomes. There are several benefits to using IoT-enabled healthcare systems, including reduced costs and improved patient outcomes [8]. IoT devices in the future will be connected to a 10x faster, more reliable, and lower-latency 5G wireless network than is now available. Network slicing and distributed architecture will be key features of 5G technology, which will be used in the future. Networking equipment from many manufacturers may be seamlessly integrated into a single network.

Current research, applications, and 5G technological aspects are all covered in this article here. In order to ensure the integrity and immutability of data sent over the 5G network's diverse devices, security mechanisms such as blockchain technology are used. 5G blockchain is explained in detail, as is the concept of sensor clustering and a way to identify a Cluster Head (CH), which is responsible for exchanging data with the base station or sink. The present study offers a layered model that includes all of these concepts. To demonstrate how a distributed system's ledger may be updated, pseudocodes are used. We're going to look at the performance of a SHA-256-based security system, model it mathematically, and then do a static analysis of it here. There is an introduction to the topic and a discussion of the work's significance at the beginning, followed by a look at how the piece is structured [10]. An overview of similar studies and the research's historical background is included in the second section of the paper. There will be a blockchain-based mechanism for secure data transmission over 5G networking components, including the blockchain's layered structure and node clustering and head selection processes. The suggested blockchain-based data encryption between networking nodes comes to an end, and its implications and possible ramifications are then examined.

II. Background And Relative Work

A. Existing Research on Security Mechanisms

Long-standing cryptographic standard, the Data Encryption Standard (DES), is now considered the least safe way to encode information. Using a 56-bit key has had an influence on current encryption methods. As a result of its inability to resist modern-day security concerns, the method developed in the early 1970s was rendered obsolete. The DES method is based on the idea of substitution and permutation, which is repeated 16 times via eight S-boxes on the sender's side and in reverse order on the receiver's side.method is based on the idea of substitution and permutation, which is repeated 16 times via eight S-boxes on the sender's side and in reverse order on the receiver's side. Due to the vulnerability of the DES process to Brute force attacks and the ability of cryptanalysis to decipher the ciphertext, Surendran et al. [11] concluded that the technique is inadequate for handling sensitive data. Data may be encrypted simultaneously using 112 and 168-bit keys in 3DES, an enhanced version of the DES algorithm. When it comes to collision attacks, however, the authors of 3DES [12] emphasise that it has a higher resistance than ordinary DES.

When it comes to RSA, the public key cryptosystem provides the basis for the cypher. Because of the network's two nodes employing both public and private keys to encrypt data, asymmetric key logic is used. Public and private keys of 1024, 2048, or 4096 may be generated using the RSA algorithm, which employs two prime numbers to produce the keys. Despite the fact that the RSA technique requires a slightly bigger key size, it is seldom employed in the modern period. Nevertheless, the RSA method is susceptible to side-channel attacks and approximation of random probabilities. The resilience of the RSA technique is determined by the magnitude of the prime numbers used to generate the keys. The higher the prime numbers, the more secure they are, but this requires an extraordinary amount of processing work.

In contrast to the DES algorithm's eight replacement boxes, DESL utilises a single substitution box for maximum memory and computation efficiency. However, Surendran et al. [13] note that the DESL-based encryption becomes less secure as the number of S-Boxes decreases. For several rounds, up to 64 times, the Tiny Encryption Algorithm (TEA) employs mathematical operations such as shift, XOR, and addition to create an encryption key of 128 bits. This method was developed by S. A. Yee Hunn et al.

A well-liked linear hybrid encryption method called Hummingbird uses both block and stream cyphers. The entropy transmission from specified to permutation function is affected by the encryption of 16-bit blocks with an internal state of 80 bits using a 256-bit key. It is the most popular and effective computational method for encrypting data on embedded devices [14]. The hummingbird technique requires specific hardware, which makes it challenging to deploy. Kobayashi et al. refer to Tomoyasu's TWINE encryption as a Feistel-based model, and it was developed for usage on less capable hardware implementable with strong encryption rounds.

Based on the user's access, location, account type, and more, ABE uses asymmetric key encryption to decode data. There would be tremendous pressure on the nodes and handling servers since the ABE found design required private key updates for each node. Staar et al. [15] noted that key management difficulties.

There are other more techniques for data encryption that are frequently utilised. Numerous them are optimised for use with low-power computing devices such as nodes and sensors in a 5G network based on the Internet of Things. Due to the difficulties and security concerns, a security model for data transfers in 5G nodes is required [16].

TABLE I. SECURITY MECHANISM COMPARATIVE ANALYSIS

Encryption Algorithm	Reference Citation	Block Size	Key Size (bits)	The Approximate Number of Rounds	Challenges/Attacks
DES	Surendran et al. [28]	64	56	16	Brute force attack, cryptanalysis
AES	Li, R., Jin, C. [30]; Roche T et al. [31]	128	128/192/256	10/12/14	meet in the middle, Side-channel
3DES	Choi J et al. [29]	64	56/112/168	48	collision attack
RSA	Mahanta, H.J. et al. [32]	-	1024/2048 /4096	1	High order DPA attacks
DESL	Surendran et al. [28]	64	54	16	Chosen Plain-text/Chosen-cypher text attack
TEA	S. A. Yoe Hunn et al. [33]; Roche T et al. [31]	64	128	64	Side-Channel Attack
HUMMINGBIRD	Salehani, Yaser, and Youssef, Amr. [35];	16	256	4	Differential Fault Analysis, cryptanalysis
TWINE	Kobayashi et al. [36],	64	80/128	36	A man-In-The-Middle attack,
SPECK	Biryukov A et al. [37] R. Beaulieu et al. [38]	96	96	28	Differential Cryptanalysis Chosen
SIMON	R. Beaulieu et al. [38]	96	96	52	Plain-text/Chosen-cypher text attack, Differential Cryptanalysis

The algorithm is lighter as a result of the technological trade-off. The number of encryption or arithmetic rounds is lowered, jeopardising the security of the data. Cryptanalysis is the most often seen sort of attack on many of the lightweight cryptographic techniques listed above. The following table summarises the many encryption techniques that are prevalent in IoT-based architectures.

B. Network Model Aspects of Evaluation

Numerous assessment factors are taken into account while determining the network's resilience. It is desirable to have a scalable network with a long lifespan, and this section discusses numerous essential evaluation aspects.

Scalability: Distributed ledger technology (DLT) may link a blockchain network powered by data from many 5G devices, which in turn send data to a gateway. The 5G gateway may be utilised to manage this large amount of data, and many gateways may be used to feed the data into the blockchain network. In today's network, the Chain of Survival is a high-performance structure capable of transporting massive amounts of data. Several large-scale data volume control organisations are encouraging the use of a modular approach to Internet of Things architecture.

Reliability: Gartner expects that 200 billion internet-connected items will be sold by 2020. IoT devices may be used to access many of these Internet-enabled gadgets. To support data transmissions over short to long distances while using little power and latency, 5G devices were created. Research is now being conducted to determine the best methods for minimising data leakage, lock-in, data manipulation, and communication problems. Chipsets and architectures are becoming more advanced in order to enhance standards. Increased endurance is achieved by the use of technologies such as WiFi, ZigBee.

Security: In this 5G network-Blockchain system, the data security risk is borne by the Internet of Things computer and its network. During its storage period, data stored in the blockchain network is tamper-proof, immutable, and hence secure. WiFi and other WiFi connections used by IoT devices and gateways put IoT data at risk. It is impossible to have a secure IoT network without a stable IoT network. Research and development in the field of 5G network security is taking place in order to ensure that this technological combination is effective.

Standardization and Interoperability: With increasing exposure to block chain technology, numerous businesses, entrepreneurs, organisations, and academics build diverse block chain networks. Numerous architectural and programming languages are used in the systems, as well as consensus protocols and transaction flow. As a result, applications developed for several platforms are incompatible with one another. Standardization may enable enterprises to establish channels that facilitate communication across disparate networks. [17] The Seele cooperative network is a cross-blockchain one. Block chains are a kind of distributed ledger technology, and they are becoming more popular. Additional effort must be done to define fundamental platform architectural standards and consensus protocols that allow the interoperability of blockchain applications [18].

Cost Effective: There are a plethora of Block chain options available, each with a fee per unit of transaction data. For instance, the Oracle Blockchain Platform offers cloud services on a per-transaction basis. Free sample models are often provided by organisations in order to increase adoption. The 5G network will need a considerable investment in sensors, and firms such as Oracle provide connection. In general, the number of sensors and the volume of data collected define the majority of the ownership expenses. But because of the value they will bring the firm, the acquisitions are relatively reasonable, since they will not need any upfront fees and will result in considerable reductions in ownership expenses over time [19-20].

III. BLOCKCHAIN LAYERED MODEL

The proposed blockchain network design is comprised of four levels. The layers are classified according to their respective tasks. Fig.3 illustrates the suggested model's layered construction. Each layer is assigned a certain task, as shown below. Unless a certain paradigm is followed, it is impossible to get safe. IoT powered by 5G has the ability to significantly increase this potential. In the absence of such a paradigm change, infrastructures, operators, and smaller apps can only create and execute particular blockchain solutions for the agricultural, medical, automotive, and logistics industries [21]. A 5G-enabled Internet of Things (IoT) presents both obstacles and opportunities for Blockchain technology.

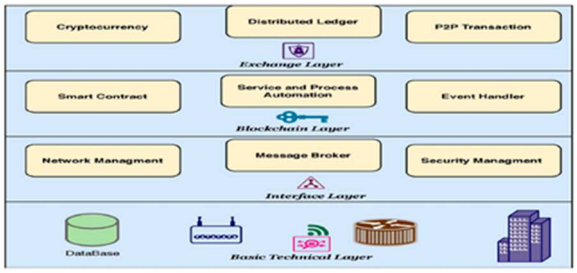

Figure 2. 5G network based Blockchain Layered Model

Blockchain technology, in particular, has the potential to serve as both a method of logging data that is extremely resistant to integrity attacks and a means for preventing malevolent devices from gaining access to our networks. Millions of inexpensive networked PCs exacerbate network hazards due to a lack of native protective measures [20].

The proliferation of such devices has facilitated enormous DDoS assaults on large swaths of the Internet. Increasing reliance on integrated networking infrastructure for normal operations exposes us to these vulnerabilities in our homes (e.g. the Nest) and autos (e.g. autonomous vehicles). 5G IoT-based blockchain technology is being used by a slew of new start-ups [21]. The 5G IoT will be bolstered by blockchain-based technologies as a result. Figure 4 depicts the proposed model's design.

It is possible to save an enormous amount of information on a big number of people using this method. These connections are identifiable because their information is recorded in a block chain.

Commercial IoT applications, such as slock, will make advantage of this approach in order to deliver their services. As a result, Blockchain's most prevalent difficulty - improving bandwidth and records - might be addressed by recording all transactions on its network [22].

The encryption format of one technology is used to transmit healthcare information. Each cluster head node updates the ledger using a public key, which is also used to encrypt and decrypt the data. It is crucial to identify the cluster-head since the remaining network nodes will communicate with the intermediary networking nodes of the Internet of Things.

A. Clustering of Intermediate Networking Components (Routers)

In an IoT ecosystem, nodes come in a variety of forms and are not just restricted to simple sensors with their basic functionality. Regarding connection, frequency spectrum, and power consumption, all of these devices differ significantly from one another. Any IoT system periodically broadcasts its status to the relevant Base Station; as a result, the BS possesses extensive topological data. The IoT model is divided into present duration zones at first, where several sensors are grouped together and equipment is provided with local knowledge. Nodes keep track of the identities, locations, and separations of every neighbour just before the coherent area leaves the clustering process.

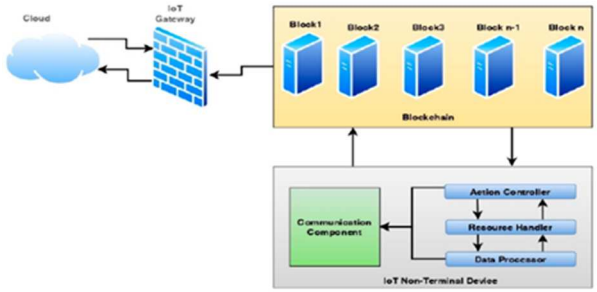

Figure 3. Blockchain model Architecture

Nodes first try to group together with other nodes that share a social pattern. On the list of closest nodes, participants in the cluster become the node with the most significant optimistic mark and a node belonging to the same social trend. In accordance with its social pattern, the node joins and leaves the cluster. at assume control of the network's communications, look at the clusters of intermediary networking nodes in Fig. 5. One of the intermediate networking nodes in the IoT architecture—designated by the variable Nt=N1, N2, N3,…..Nn)—will be referred to as the cluster-head. Numerous factors are used to perform clustering. Connection, node distance, and node residual energy are examples of these measures. The suggested model for clustering the intermediate networking nodes takes into account two parameters. The distances between nearby nodes and the residual energy of each node are the variables that are examined [23]. When determining the number of surrounding intermediate networking nodes to utilise, it is important to remember that the cluster may only be constructed with the usage of neighbouring nodes. In order to determine whether or not a particular node is a neighbourhood member, the radius of the propagation spectrum and the number of nearby nodes whose beacons fulfil the requisite SNRs for deciding whether or not the given node is a neighbourhood member will be considered. As a cluster head, the residual energy parameter is critical, and the node with the highest residual energy should be chosen.

B. Implementation Environment

It is being developed using the Docker container environment to implement the planned 5G architecture concept, which is based on blockchain technology and allows for data transmission between non-terminal nodes. The blockchain framework is being deployed using Hyperledger Fabric [24-25]. The ledger states are maintained using CouchDB. The command-line interface is used to deploy and manage the smart ledgers. The table below summarises the context in which the suggested model Blockchain for 5G

architecture would be implemented. Table 2 outlines the suggested model's implementation

TABLE II. IMPLEMENTATION ENVIRONMENT INFORMATION

Environment Specifications	
Operating System:	Version 11.0.1 Big Sur
Processor:	2.7 GHz Quad-Core i7 processor
RAM:	8GB
IDE:	Composer Playground
Docker Version:	Version 2.5.0.1
HyperLedger Fabric:	Version 2.0
Database:	Couch DB
Platform:	Node.js

IV. DELIBERATIONS OF PERFORMANCE ANALYSIS

The effectiveness of the suggested model is compared to other existing strategies, which are assessed based on a variety of factors. A cluster of intermediate networking nodes made up of 50, 150, 250, and 350 nodes is used to assess the validity of the proposed method. In this part of the study project, performance parameters like execution time, network latency, and process overhead are examined and assessed. This was done by utilising the Hyperledger Calliper modelling framework, which enables users to adapt the use case script to their own blockchain architecture, which consists of a number of intermediate networking nodes, as necessary. The minimum, average, and maximum durations of the proposed blockchain network's execution were stated in order to establish a timestamp for the network's operation . The time needed for device registration in the network for clusters with various numbers of intermediate networking nodes is shown in Fig.7 using data from Table 3 (intermediate networking nodes are shown in red). For performance analysis, the network model's lowest, average, and maximum values are computed from various network model executions and added.

In order to ease path estimations and data transfer, these nodes are responsible for maintaining the routing table Multiple times, techniques for gathering statistical data have been rehearsed to identify and save the node's information in the database. Table 4 displays the transaction's execution time for node reading, and Fig 5 displays a corresponding graph. The lowest, average, and maximum values provided in this research are those obtained after repeatedly running the model for the purpose of assessing peak performance.

TABLE III.. INDICATED BY THE TIME IT TAKES TO REGISTER A NEW NODE.

No. of Devices	Minimum Time (ms)	Average Time (ms)	Maximum Time (ms)
50	2109	2179	2211
150	2148	2208	2282
250	2221	2289	2325
350	2274	2335	2397

In order to ease path estimations and data transfer, these nodes are responsible for maintaining the routing table Multiple times, techniques for gathering statistical data have been rehearsed to identify and save the node's information in the database. Table 4 displays the transaction's execution time for node reading, and Fig 5 displays a corresponding graph. The lowest, average, and maximum values provided in this research are those obtained after repeatedly running the model for the purpose of assessing peak performance.

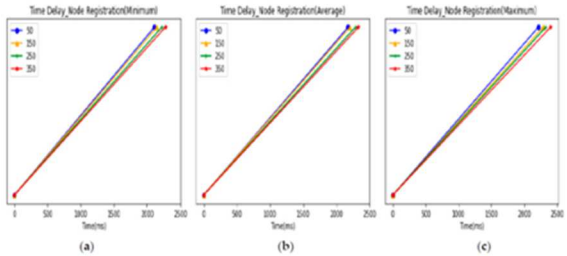

Figure 4: This graph represents the time required for node registration execution, including (a) the time spent in the best case, (b) the time used in the average scenario, and (c) the time wasted in the worst case (if applicable).

TABLE IV. THE EXECUTION OF NODE READING TRANSACTIONS IS REPRESENTED BY THIS OBJECT

No. of Devices	Minimum Time (ms)	Average Time (ms)	Maximum Time (ms)
50	1875	1952	2014
150	1912	1979	2081
250	1986	2074	2115
350	2103	2198	2278

TABLE V SHARING THE RECORDS FOR TIME DELAY

Number_of_Records	Time Delay (ms)
50	79
150	214
250	356
350	597
550	707
750	924

Graph 9. You could see the delay visually by using record sharing. The results of calculating the time for each non-terminal node in the IoT design of the 5G network to update the digital ledger are updated in Table 6. Fig 7 displays the produced graph.

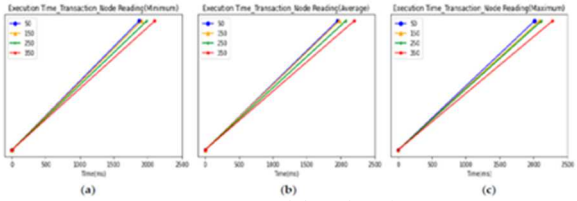

Figure 5. Graph based on time

Node reading execution time is shown in Figure 5 with (a) the best case quickest, (b) the average case quickest, and (c) worst scenario using the largest amount of time.

The performance of the suggested architecture is compared to the time required to exchange ledger records across networking nodes in a 5G network [26-29]. The time delay includes the time required to encrypt data between networking nodes using Blockchain technology. Table 5 shows the delay as a function of the variable number of records, and Figure 6 shows the related chart

The statistical study of node registration reading across a variety of non-terminal nodes described in Tables 2 and 3 demonstrates that the proposed model's execution time in the 5G network is rather consistent [30]. The delay in record-sharing is to be expected. Table 6 demonstrates that it has no adverse financial effects on the network.

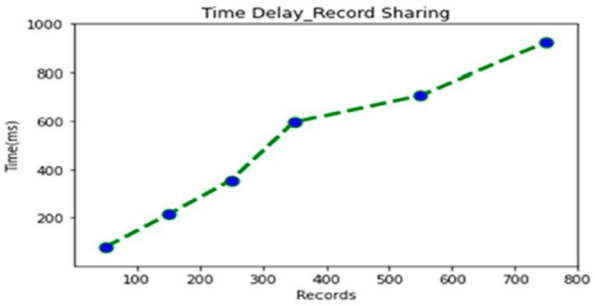

Figure 6. Graphs represent time delay in record sharing

When it comes to computing power, SHA-256 is about as expensive as adding all all the hash functions of a stream cypher together. The complexity of an algorithm may be expressed using the Big O notation. SHA-256's O(c + pn1 + qn2) complexity is roughly identical to that of O(c + pn1 + qn2). n1 0 and n2 0 represent the input and output sizes, respectively, while the constant "c" indicates the size of the key. For each input block, there's a cost connected with overhead; for each output block, there's a cost associated with bitstream. An O(n) model's complexity is defined as the total of the input and output bits, which are n = n + n2.

TABLE VI. REPRESENTS THE TIME DELAY FOR UPDATING THE DIGITAL LEDGER

Number_of_Records	Time Delay (ms)
50	59
150	168
250	291
350	410
550	577
750	722

V. CONCLUSIONS

The goal of this article was to conduct a review of the existing state-of-the-art literature on Blockchain in order to determine how it may be used to a variety of significant difficulties associated with the exchange of sensitive data, such as healthcare data, over the 5G network. We believe that 5G and other future networks have enormous potential and should be further investigated. When completely deployed, 5G networking will be reliable, inexpensive, and productive on a global scale. Along with the many advantages, certain challenges such as managing a larger number of devices will be a key problem; managing 350 devices in simulation settings may not be the same as managing 350 devices in a real-time implementation environment. While utilising 5G-based blockchain technology to handle healthcare-related data, real-time issues such as scalability, interoperability, and regulatory requirements may arise.

VI. FUTURE SCOPE

When it comes to safeguarding the integrity of healthcare data, the experimental examination of the suggested security mechanism model using blockchain technology reveals that it is quite reliable. A further advantage of blockchain technology is that it is successful when used in a distributed situation since it makes use of digital ledgers. Because the suggested model consumes a significant amount of storage space over time, it is recommended that the storage capacity of the proposed model be improved. Non-terminal nodes must expend a large amount of effort in order to produce records and share them with the next node. Since the data posted to the network cannot currently be modified, a mechanism for tracking the changes made to the blockchain network must be created. By managing storage at each administrative node in the mobile network and using distributed processes, the quantum Blockchain concept may efficiently share the responsibility of managing the ledger.

REFERENCES

[1] Kim, S.; Lee, I. IoT device security based on proxy re-encryption. J. Ambient. Intell. Humaniz. Comput. 2017, 9, 1267–1273. [CrossRef]

[2] Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT privacy and security: Challenges and solutions. Appl. Sci. 2020, 10, 4102. [CrossRef]

[3] Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-based packing of industrial iot data in permissioned blockchains. IEEE Trans. Ind. Informatics 2020, PP, 1. [CrossRef]

[4] P. William, A. Shrivastava, H. Chauhan, P Rawat, R., Rimal, Y. N., William, P., Dahima, S., Gupta, S., & Sankaran, K. S. (2022). Malware Threat Affecting Financial Organization Analysis Using Machine Learning Approach. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-20. http://doi.org/10.4018/IJITWE.304051

[5] William, P., Shrivastava, A., Shunmuga Karpagam, N., Mohanaprakash, T.A., Tongkachok, K., Kumar, K. (2023). Crime Analysis Using Computer Vision Approach with Machine Learning. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_25

[6] William, P., Shrivastava, A., Chauhan, P.S., Raja, M., Ojha, S.B., Kumar, K. (2023). Natural Language Processing Implementation for Sentiment Analysis on Tweets. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_26

[7] P. William, G. R. Lanke, D. Bordoloi, A. Shrivastava, A. P. Srivastavaa and S. V. Deshmukh, "Assessment of Human Activity Recognition based on Impact of Feature Extraction Prediction Accuracy," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-6, doi: 10.1109/ICIEM59379.2023.10166247.

[8] P. William, G. R. Lanke, V. N. R. Inukollu, P. Singh, A. Shrivastava and R. Kumar, "Framework for Design and Implementation of Chat Support System using Natural Language Processing," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-7, doi: 10.1109/ICIEM59379.2023.10166939.

[9] P. William, A. Shrivastava, U. S. Aswal, I. Kumar, M. Gupta and A. K. Rao, "Framework for Implementation of Android Automation Tool in Agro Business Sector," 2023 4th International Conference on

Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-6, doi: 10.1109/ICIEM59379.2023.10167328.

[10] P. William, V. N. R. Inukollu, V. Ramasamy, P. Madan, A. Shrivastava and A. Srivastava, "Implementation of Machine Learning Classification Techniques for Intrusion Detection System," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-7, doi: 10.1109/ICIEM59379.2023.10167390.

[11] Neha Sharma, P. William, Kushagra Kulshreshtha, Gunjan Sharma, Bhadrappa Haralayya, Yogesh Chauhan, Anurag Shrivastava, "Human Resource Management Model with ICT Architecture: Solution of Management & Understanding of Psychology of Human Resources and Corporate Social Responsibility", JRTDD, vol. 6, no. 9s(2), pp. 219–230, Aug. 2023.

[12] K. Maheswari, P. William, Gunjan Sharma, Firas Tayseer Mohammad Ayasrah, Ahmad Y. A. Bani Ahmad, Gowtham Ramkumar, Anurag Shrivastava, "Enterprise Human Resource Management Model by Artificial Intelligence to Get Befitted in Psychology of Consumers Towards Digital Technology", JRTDD, vol. 6, no. 10s(2), pp. 209–220, Sep. 2023.

[13] P. William, A. Chaturvedi, M. G. Yadav, S. Lakhanpal, N. Garg and A. Shrivastava, "Artificial Intelligence Based Models to Support Water Quality Prediction using Machine Learning Approach," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-6, doi: 10.1109/WCONF58270.2023.10235121.

[14] P. William, M. Gupta, N. Chinthamu, A. Shrivastava, I. Kumar and A. K. Rao, "Novel Approach for Software Reliability Analysis Controlled with Multifunctional Machine Learning Approach," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 1445-1450, doi: 10.1109/ICESC57686.2023.10193348.

[15] Kumar, A., More, C., Shinde, N. K., Muralidhar, N. V., Shrivastava, A., Reddy, C. V. K., & William, P. (2023). Distributed Electromagnetic Radiation Based Renewable Energy Assessment Using Novel Ensembling Approach. Journal of Nano-and Electronic Physics, 15(4).

[16] P. William, S. Choubey, M. Ramkumar, A. Verma, K. Vengatesan and A. Choubey, "Implementation of 5G Network Architecture with Interoperability in Heterogeneous Wireless Environment using Radio Spectrum," 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022, pp. 786-791, doi: 10.1109/ICEARS53579.2022.9752267.

[17] P. William, D. Jadhav, P. Cholke, M. A. Jawale and A. B. Pawar, "Framework for Product Anti-Counterfeiting using Blockchain Technology," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), 2022, pp. 1254-1258, doi: 10.1109/ICSCDS53736.2022.9760916.

[18] P. William, A. Badholia, B. Patel and M. Nigam, "Hybrid Machine Learning Technique for Personality Classification from Online Text using HEXACO Model," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), 2022, pp. 253-259, doi: 10.1109/ICSCDS53736.2022.9760970.

[19] Wakchaure, P. Kanawade, M. A. Jawale, P. William and A. B. Pawar, "Face Mask Detection in Realtime Environment using Machine Learning based Google Cloud," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 557-561, doi: 10.1109/ICAAIC53929.2022.9793201.

[20] William, P.,et al. "Darknet Traffic Analysis and Network Management for Malicious Intent Detection by Neural Network Frameworks." Using Computational Intelligence for the Dark Web and Illicit Behavior Detection, edited by Romil Rawat, et al., IGI Global, 2022, pp. 1-19. https://doi.org/10.4018/978-1-6684-6444-1.ch001

[21] William, P.,et al. "Systematic Approach for Detection and Assessment of Dark Web Threat Evolution." Using Computational Intelligence for the Dark Web and Illicit Behavior Detection, edited by Romil Rawat, et al., IGI Global, 2022, pp. 230-256. https://doi.org/10.4018/978-1-6684-6444-1.ch013.

[22] R. Jadhav, A. Shaikh, M. A. Jawale, A. B. Pawar and P. William, "System for Identifying Fake Product using Blockchain Technology," 2022 7th International Conference on Communication and Electronics Systems (ICCES), 2022, pp. 851-854, doi: 10.1109/ICCES54183.2022.9835866.

[23] Rawat, R., Rimal, Y. N., William, P., Dahima, S., Gupta, S., & Sankaran, K. S. (2022). Malware Threat Affecting Financial Organization Analysis Using Machine Learning Approach. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-20. http://doi.org/10.4018/IJITWE.304051

[24] P. William, A. Shrivastava, H. Chauhan, P. Nagpal, V. K. T. N and P. Singh, "Framework for Intelligent Smart City Deployment via Artificial Intelligence Software Networking," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), 2022, pp. 455-460, doi: 10.1109/ICIEM54221.2022.9853119.

[25] P. William, Y. N., S. Vimala, P. Gite and S. K. S, "Blockchain Technology for Data Privacy using Contract Mechanism for 5G Networks," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), 2022, pp. 461-465, doi: 10.1109/ICIEM54221.2022.9853118.

[26] William, P., Shrivastava, A., Shunmuga Karpagam, N., Mohanaprakash, T.A., Tongkachok, K., Kumar, K. (2023). Crime Analysis Using Computer Vision Approach with Machine Learning. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_25

[27] William, P., Shrivastava, A., Chauhan, P.S., Raja, M., Ojha, S.B., Kumar, K. (2023). Natural Language Processing Implementation for Sentiment Analysis on Tweets. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_26

[28] P. William, G. R. Lanke, D. Bordoloi, A. Shrivastava, A. P. Srivastavaa and S. V. Deshmukh, "Assessment of Human Activity Recognition based on Impact of Feature Extraction Prediction Accuracy," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-6, doi: 10.1109/ICIEM59379.2023.10166247.

[29] P. William, G. R. Lanke, V. N. R. Inukollu, P. Singh, A. Shrivastava and R. Kumar, "Framework for Design and Implementation of Chat Support System using Natural Language Processing," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-7, doi: 10.1109/ICIEM59379.2023.10166939.

[30] Mall, S., Srivastava, A., Mazumdar, B.D., Bangare, S.L., Deepak, A., Implementation of machine learning techniques for disease diagnosis, Materials Today: Proceedings, 2022, 51, pp. 2198–2201.