Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network

Parvathaneni Naga Srinivasu 1,*, Akash Kumar Bhoi 2,*, Soumya Ranjan Nayak 3, Muhammad Raheel Bhutta 4 and Marcin Woźniak 5

1 Department of Computer Science and Engineering, Gitam Institute of Technology, GITAM Deemed to be University, Rushikonda, Visakhapatnam 530045, India
2 Department of Electrical and Electronics Engineering, Sikkim Manipal Institute of Technology, Sikkim Manipal University, Majitar 737136, India
3 Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida 201301, India; srnayak@amity.edu
4 Department of Computer Science and Engineering, Sejong University, Seoul 05006, Korea; raheel.bhutta@sejong.ac.kr
5 Faculty of Applied Mathematics, Silesian University of Technology, 44-100 Gliwice, Poland; marcin.wozniak@polsl.pl
* Correspondence: parvathanenis@gmail.com (P.N.S.); akashkrbhoi@gmail.com (A.K.B.)

Abstract: In the contemporary world, with ever-evolving internet models in the process of automating and digitalizing various industrial and domestic implementations, the Internet of Things (IoT) has made remarkable advancements in sharing the healthcare data and triggering the associated necessary actions. Healthcare-related data sharing among the intermediate nodes, privacy, and data integrity are the two critical challenges in the present-day scenario. Data needs to be encrypted to ensure the confidentiality of the sensitive information shared among the nodes, especially in the case of healthcare-related data records. Implementing the conventional encryption algorithms over the intermediate node may not be technically feasible, and too much burden on the intermediate nodes is not advisable. This article has focused on various security challenges in the existing mechanism, existing strategies in security solutions for IoT driven healthcare monitoring frameworks and proposes a context-aware state of art model based on Blockchain technology that has been deployed for encrypting the data among the nodes in the architecture of a 5G network. The proposed strategy was examined through various performance evaluation metrics, and the proposed approach had outperformed compared to its counterparts.

Keywords: blockchain; Internet of Things; 5G network; network security; cluster head; distributed ledger

1. Introduction

In the recent advancement that has taken place in the field of computer network and sensor networks for distributed architecture models that are responsible for maintaining and monitoring the smart environments like smart grids, smart cities, smart homes, smart retail, wearable healthcare devices, intelligent agricultural implementation, smart industrial internet that are operated remotely through the Internet of Things (IoT) technology. The IoT is an interconnection of various devious for data acquisition remotely, processing the data, and analyzing the appropriate action data. In automation, the IoT technology has incorporated hyper-communication technology among the individuals, and the automation equipment collaborated with different fields of technology remotely. In such a context, the shared data’s security among the individuals and the terminal devices like storage devices, processing units, embedded sensors, and actuators is a significant concern. The sensors and the terminal devices do share sensitive data related to individuals, organizations, and
The exposed data associated with the individual, like data from wearable devices, can give insight into their medical status. The data from the smart meters of electrical consumption related to the individual can help analyze the individuals’ lifestyle through data integrity breaches, as discussed by Kim, S., Lee, I. [1] in the article proxy re-encryption.

Kevin Ashton first coined the IoT technology in 1999 to incorporate ubiquitous sensors promoting the Radio Frequency Identification technology to work with embedded Internet. As per the statistics, in 2020, approximately 127 new IoT-based devices are being deployed with the web for performing network and cloud-based operations. It is estimated that around 31 billion IoT-based devices are in use, and it is anticipated to have 35 billion IoT devices to be installed by the end of 2021, as per the view of experts. The wake of the digital revolution has resulted in an enormous increase in the new IoT devices, evolving more than 75 billion new devices by the end of 2025. The IoT technology has drastically improved over time and has redefined the communication among the nodes in the networks that has extemporize the scope of IoT industrially and automated services. The massive number of users and nodes in the networks and the transferring of data have critical issues related to the data’s security and privacy, as discussed in Tawalbeh, L. et al. [2], Srinivasu, P.N. et al. [3]; Naga Srinivasu et al. [4].

In the process of acquiring the new devices as part of the IoT architecture, various new devices have been added to the network, and each of those standalone devices works independently with the pre-determined protocol. The technology gap among the network devices leads to security breaches that had led to network attacks that include physical attacks that include node tampering, as stated by Burhan et al. [5]; Smaila et al. [6], malicious injection, as stated by Ray D. and Ligatti J. [7]; Chen, J. et al. [8], software attacks, as mention by Mahmudul Hasan et al. [9]; Oza A.D. et al. [10] in their papers, privacy, and integrity attacks, as mention by Sumra I.A. et al. [11]; Chenthara S et al. [12].

There is a significant growth in the nodes in the IoT architecture that has led to attacks on the nodes in the network for taking control of the network and the individuals’ sensitive data. There are different attacks on the network devices, as discussed earlier. Many robust technologies are put forward to tackle such attacks. However, there is a tremendous demand for robust approaches for handling the data sensed by the nodes in the IoT architecture and the information shared among the network devices. The attacks are so severe in many cases that the denial of service impacts the network’s availability in the network, which results in the collapse of the network.

Blockchain technology is evincing to be robust in ensuring the security of the data exchanged over the IoT architecture [13,14]. Thus, the patient monitoring models and the healthcare management framework that relies on the IoT architecture for monitoring are driven by blockchain technology, which can operate over a distributed network models with broader security attributes over advanced cryptographic primitive. The healthcare management models like Remote patient monitoring frames works [15,16] are driven by the blockchain technology that ensures data privacy by preserving the transaction history of the nodes in the architecture. Blockchain architecture is built upon on proof of work principle. A transaction is deemed legitimate only if the network validates that authorized nodes have performed sufficient computational effort. Therefore, the technology based on the Blockchain model is being developed to ensure authorized access and privacy to patients’ medical records in such a context.

Blockchain technology has the potential to significantly enhance the security of healthcare and medical information systems that deal with the data like the electronic healthcare records of the patients, personal health record, individual diagnosis reports, data from wearable devices, records of post-operative assessments, records of the hospital management system, clinical consents, supply chain in the pharmaceutical domain, blockchain-based telemonitoring data, genomic data, data for insurance companies, and other sensitive data related to the clinical trials. Utilization of blockchain technology that can improve transparency, privacy, confidentiality and traceability, and effectiveness in exchanging healthcare data records. The healthcare sector is about to be transformed by blockchain applications.
combined with artificial intelligence (AI) and machine learning. The blockchain technology is being integrated with the storage technology for ensuring the privacy of the data through the decentralized architecture for the stockholders using the public ledger mechanism as presented by Yue, X. et al. [17] and a mobile application named Healthcare Data Gateway (HDG) is presented in upholding the healthcare-related data. Guo, R. et al. [18], and Li, H. et al. [19] have presented the blockchain-based platform in effectively handling electronic health care records and medical data.

The key technologies like Healthcare Information Exchange (HIE) [20] are proven to accelerate healthcare data privacy to exchange over the unsecured channel. The HIE technology has extensively enhanced the utilization, reduced the cost of exchanging the data, and improved patient care and monitoring for improvised surveillance. BlocHIE technology [21] is used to deal with clinical trials related data that yield better analysis and comprehensibility of the outcome of the clinical studies. Through the involvement of HIE technology, the storage models like Electronic Medical Records (EMR) and Personal Healthcare Data (PHD) are effectively managed to handle and share the huge amount of data using the EMR-chain and the PHD-chain frameworks. The results of the HIE are efficient compared to conventional approaches, despite which there is the architectural change in the IoT model in 5G environment that has necessitated the energy-efficient use of distributed ledger architecture presented in the current study. There are various other mobile-based healthcare monitoring models in healthcare domain. Figure 1 presents the layered model of the blockchain over the 5G network and the divergent healthcare-related applications. The stakeholders will be the practitioners, radiologists, patients, and healthcare monitoring service agencies.

In the recent advancements in cellular technology, the fifth-generation (5G) wireless networks are underway across the globe. It is intended to serve various vertical applications by linking heterogeneous devices and machines, with significant increases in service quality of the nodes in the network, infrastructure capacity, interpretability, and overall architecture throughput. Despite these advancements mentioned above, the security of the data exchanged over the 5G networks has become a major concern. The limitations like decentralization transparency, hazards of data interoperability, and network privacy have largely impacted the healthcare frameworks that operate on the 5G technology and beyond [22]. Integration of blockchain over the 5G network architecture will improvise the security standards of the network. The management of the security in the 5G is challenging...
due to the involvement of diverse devices in the network, and achieving immutability and transparency is crucial [23].

The main object of the present study is to enhance the remote surveillance of the patient and tele-guidance through consistent monitoring of patients that have been enabled by the Internet of Things (IoT)-connected devices. The IoT-driven healthcare models can maintain patients’ health and safety, allowing the medical practitioners to give superior treatment. Additionally, IoT-driven healthcare frameworks significantly influence lowering healthcare expenses and greatly enhance the performance outcome. The future IoT technology over the 5G based wireless network which is comparatively ten times faster than the current LTE technology, reliable, and has lower latency. The future technology will rely on the 5G technology with advanced features like distributed architecture through network slicing. It can accommodate the numerous divergent networking devices in forming a reliable network. The security and privacy limitations of 5G technology have a great demand for incorporating lightweight and robust security frameworks like blockchain technology to ensure the privacy and confidentiality of the model.

In this paper, the fundamental topics like the existing studies, applications, and properties of the 5G technology are presented. To ensure the confidentiality of the data being exchanged over the 5G network that operates over numerous heterogeneous devices, the security mechanisms like blockchain technology are incorporated to ensure the immutability and transparency of the data. The layered model with a detailed description of blockchain in 5G is proposed in the current study, and the concept of clustering the sensor network and the algorithm for recognizing the Cluster Head (CH), which is responsible for exchanging the data with the base station or the sink, is presented. The process of updating the ledger in the distributed environment is discussed with pseudocodes. The SHA-256 based security scheme with mathematical modeling and the statical analysis of the performance is discussed in the current study.

The entire paper is organized as follows; initially, the introduction to the domain and the significance of the work are discussed. In the section two, the background of the current study and the relevant work is presented. In the proposed section, a blockchain-based mechanism for secured communication of the data over the networking components in 5G is discussed alongside the layered architecture of blockchain, the process of node Clustering and cluster head selection, assessing the degree of centrality, SHA-256 security scheme, and Implementation Environment are discussed. The next section is about the performance analysis and deliberations about the proposed model. Then, the conclusion and the future scope of the proposed Blockchain-based data encryption among the networking nodes are presented.

2. Background and Relative Work

There are divergent categories of networking components that are used in the 5G network settings, and the nodes will communicate to each other about their availability and the residual energy in a context specific manner. It updates the centralized server and simultaneously the neighboring nodes about the sensed data and monitoring information. The data can be intruded on to take over the sensitive data and control the smart environment in sharing the data. The data must be encrypted before transmitted over the unsecured channel to make the data more robust over such unwanted access. In sharing the data among the intermediate nodes, the data can be shared among the node over a virtual private channel in many industrial implementations for ensuring data confidentiality and integrity. Nevertheless, the VPN has limitations in security breaches and protocol flaws, as Rahimi S. and Zargham M [24] stated in the paper VPN Configurations in Industrial Control Environments. The cost of employing a virtual private channel/network is not economically feasible and reserves the resources in advance, irrespective of the utilization of the resources. In such cases, the cryptographic approaches are more efficient in securing the sensor data among the intermediate networking nodes in the 5G-based network architecture.
In the proposed model, for ease of implementation, data is encrypted only at the 
cluster heads to avoid unnecessary overheads at each intermediate node in the network. 
That would result in the effective management of the network with considerably lighter 
transactions in sharing the data. There are significant challenges that are to be addressed 
in the 5G network for the IoT architecture. The challenges include the scalability issue 
that results in plenty of the current Blockchain implementations result in a low transaction 
rate that is caused due to the inappropriate evaluation about how block can be applied to 
a transaction. Operability in the 3G and 4G network are the other aspects that severely 
impact Blockchain’s performance because of lower network speed and higher latency. 
Blockchain-based options would add an extra delay in 3G and 4G architectures, making it 
difficult to operate. The intermediate nodes in the 5G network are considered efficient in 
processing the data with lesser energy consumption.

The non-terminal nodes in the 5G architecture are deployed to sense the real-time 
healthcare data with limited computational capability; in such a scenario, the encryption 
algorithm must consume negligible computational efforts. The non-terminal here is 
concerning to the networking nodes that are responsible for analyzing, processing, and 
exchanging the data in the 5G architecture, which includes the distributed units, central-
ized units, data centers, mergers, routers, and the switches. Blockchain has a few of the 
properties that are advent in the IoT nodes in the network, as Mistry, I. et al. [25] stated. A 
few of the properties of the blockchain-based network are as follows:

- **Trust-free**: The nodes that participate in the network are invisible to each other, and the 
  node does exchange the services and collaborate each other for the sake of information 
  exchange with knowing much about the node with which it is communicating, this 
  implies that there is no prerequisite for licensed public signatures to carry out any 
  interaction between nodes in the network.

- **Permission-free**: The nodes in the network can work without procuring the adminis-
  trator’s permission. There is no restriction on who can utilize the network resources 
  for communication.

- **Censorship Resistant**: The nodes in the network does not have the controller to restrict 
  the communication and performing the transactions among the nodes in the blockchain 
  technology. However, it is not possible to alter or censor any verified transactions.

- **Distributed Ledger**: The distributed ledger mechanism is considered to be the pivotal 
  feature of blockchain technology. The ledger included all data related to a transaction 
  and its client’s information. Every user in the sensor network will maintain the ledger, 
  and the distributed model will enhance the network’s performance and effectively 
  utilize the computational recourses.

- **Faster resolution**: The conventional encryption models are comparatively slow and 
  need more computational efforts. The transactions related to data exchange are fasters 
  and relatively more secure.

### 2.1. Existing Studies on the Security Mechanism

In the 5G network-based architecture, apart from the network establishment, the secur-
ity of the healthcare data is held by the sensor nodes and the privacy of the terminal nodes’ 
information. Different crypto techniques are being used to encrypt the data distributed 
between the nodes in the network. Various approaches are mechanized in the secured 
communication of the healthcare-related data among the devices, Virtual (private VPN), 
that shields the data transferred over the channels by anonymizing the metadata associated 
with the information exchanged among the nodes through anonymous tunneling. Many 
standardized approaches are using the symmetric key and asymmetric vital cryptosystems, 
and a majority of those algorithms would replace the plain text into ciphertext data that 
is not understandable that is done by performing substitution and arithmetic operations
over the plain text, and different mechanisms are used in identifying such anomalous activities [26,27].

Data Encryption Standard (DES), considered a very long-established cryptographic model, has now been considered the most insecure way of data encryption using a key of size 56-bit has influenced the present-day encryption algorithms. The algorithm developed in the early 1970 has failed to sustain the present-day security challenges due to the comparatively smaller key size used in the encryption process. The DES algorithm works on the principle of substitution and permutation performed for 16 rounds through 8 S-boxes, and on the receiver side, the same thing is performed in the reverse order. DES mechanism is susceptible to Brute force attack, and cryptanalysis can decrypt the ciphertext, which has made the approach unsuitable for handling sensitive data, as stated by Surendran et al. [28]. Triple Data Encryption standards (3DES) are the enhanced version of the DES algorithm that uses the keys of sizes 112-bit and 168-bit simultaneously to encrypt the data. 3DES is comparatively more robust than the traditional DES; however, 3DES is vulnerable to collision attacks as mentioned by Choi, J. et al. [29].

Advanced Encryption Standard (AES) is the advanced version of the DES standard, that is developed in 1998, that is comparatively efficient in encrypting the data when compared to the conventional DES algorithm with an enhanced key length of variable size keys of sizes 128-bit, 192-bit, and 256-bits that are comparatively better than the standard 56-bit key that is susceptible to brute force attacks and cryptanalysis. The number of rounds of encryption is proportional to the key size that varies from 10 to 14 rounds, and each of these rounds performs the transforms like Sub-bytes, Shift-rows, Mix-columns, and add round-key. The AES-based encryption approach is vulnerable to known attacks, as stated, R. and Jin, C. [30] in the article meet in the middle and Side-channel attacks as presented by Roche T et al. [31] in their paper.

Rivest-Shamir-Adleman (RSA) based encryption technology works on the principle of the public key cryptosystem. It works on the asymmetric key logic that uses both public and private keys to encrypt the data among the two nodes in the network. RSA algorithm employs two prime numbers for generating the public and private of sizes 1024, 2048, and 4096 depending on the application for the encryption process that is being used. RSA algorithm is not significantly used in the present-day scenario despite a considerably larger size key. Still, the RSA algorithm is vulnerable to side-channel attack and random probability approximation. The RSA algorithm’s robustness relies on the size of the prime numbers considered for the key generation. The larger the size of prime numbers, the better the security, but it needs an outstanding computational effort. Moreover, RSA-based encryption is vulnerable to attacks like high order DPA attacks, as Mahanta, H.J. et al. [32] examine in their paper.

Data Encryption Standard lightweight (DESL) is the enhanced and computationally efficient version of the traditional DES approach. DESL employs a single substitution box, unlike the 8-substitution box conventional DES algorithm that results in optimal memory and computationally efficient use. However, as the number of S-Boxes is reduced, the DESL based encryption results in a compromised level of robustness over the attacks, as mentioned by Surendran et al. [28]. Tiny Encryption Algorithm (TEA) is designed for the lighter nodes in the IoT architecture that works on the principle of block cipher mechanism using mathematical operations like shift, XOR, and addition operation using a 128-bit key for multiple rounds up to 64 times as stated in the paper by S. A. Yee Hunn et al. [33]. However, TEA-based encryption is vulnerable to cryptanalysis, as Hong S. et al. [34] stated in the paper.

Hummingbird is another most predominantly used linear type of hybrid encryption technique that relies on both block and stream cipher principles. It divides the data into 16-bit blocks with an 80-bit internal state and encrypted through a 256-bit key that had impacted the pass of the entropy from stated to the permutation function. It is a computationally efficient algorithm most widely used in embedded applications for securing data. The challenging aspect of the hummingbird approach is hardware-dependent that
makes the implementation a challenging task. The hummingbird encryption algorithm is vulnerable to Differential Fault analysis attacks and cryptanalysis, as mentioned by Salehani, Y. and Youssef, A. [35] in their papers, respectively. TWINE encryption, as proposed by Tomoyasu, as stated by Kobayashi et al. [36] for lightweight encryption that relies on a Feistel-based encryption model designed to work effectively over lighter hardware implementable that needs severe rounds for encryption. TWINE encryption is of two flavors, i.e., TWINE80, for which the key size is 80-bit over 64-bit block size, and TWINE128 works with a 128-bit key over a block size of 64-bit for 36 rounds in either of the cases as stated by Biryukov, A. et al. [37]. TWINE is vulnerable to man-in-the-middle attack, differential crytpanalysis.

SPECK is among the most predominantly used computationally efficient and lightweight block cipher technology that works on the principle of Add-Rotate-XOR operated cipher technology, as stated by Beaulieu R. et al. [38] in their paper. The SPECK based encryption is vulnerable to differential cryptanalysis and side-channel attack, as stated by Dwivedi et al. [39]. Simon is the other improvised version of SPECK that works almost the same way to work with hardware implementation. However, Simon-based encryption is also vulnerable to differential power analysis attacks, as Shanmugam D. et al. [40] stated in their paper.

Attribute-Based Encryption (ABE) is widely used for distributed storage architectures, as Sahai A. and Brent W. [41] stated in their paper. The ABE technology is an asymmetric key technology that uses the receiver’s private key to decrypt the data based on the parameters like access, position, account type, and many other things. In ABE found architecture, each node would be updated with a private key from Time to Time that would incur considerable load on the nodes and the handling server. The key management like key coordination, revocation, and escrow are the main challenges of the ABE-based security architecture in the IoT network, as Staar et al. [42] stated in their paper.

There are various other approaches that are widely used with the encryption of data. Many of them are designed to work with lighter computational devices like nodes and sensors in the IoT-based 5G network. The challenges and the security issued related has mandated the necessity of security model to the data exchanges in the 5G nodes [43,44]. However, the technical trade-off makes the algorithm lighter. The number of rounds of encryption or arithmetic operations is reduced, compromising the data’s security. Cryptanalysis is the most common type of attack observed in many of those mentioned above lightweight cryptographic algorithms. Table 1 which is stated below depicts various encryption algorithms that are being widely used in the IoT based architecture.

| 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 collision attack |
| 3DES                 | Choi J et al. [29] | 64         | 56/112/168     | 48                              |                  |
| RSA                  | Mahanta, H.J. et al. [32] | -           | 1024/2048/4096 | 1                               | High order DPA attacks, Chosen Plain-text/Chosen-cypher text attack |
| DESL                | Surendran et al. [28] | 64         | 54             | 16                              |                  |
| TEA                  | S. A. Yee Hunn et al. [33]; Roche T et al. [31] | 64         | 128            | 64                              | Side-Channel Attack |
| HUMMINGBIRD         | Salehani, Yaser, and Youssef, Armr. [35], Kobayashi et al. [36], Biryukov, A et al. [37] | 16         | 256            | 4                               | Differential Fault Analysis, cryptanalysis |
| TWINE               | 64         | 80/128     | 36             | A man-In-The-Middle attack, Differential Cryptanalysis |
| SPECK               | 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 |

Table 1. Comparative analysis chart of various existing security mechanisms.
2.2. Evaluation Aspects in the Network Model

Various evaluation aspects are being considered in evaluating the robustness of the network. It is desired to have a scalable network with extended lifetime, and various significant evaluation features are presented in this section.

**Scalability**: Several 5G devices may supply data to a gateway, which leads to a blockchain network that runs on the technology of distributed ledger. The 5G gateway is built for this massive number, and several gateways can feed the data through the blockchain network. The Chain of Survival in today’s network is a business-grade structure that carries vast data volumes. This is also a modular method for the IoT architecture powered by wide-scale data volume control organizations.

**Reliability**: By 2020, Gartner anticipates 200 billion internet stuff. Many of these Internet-linked items would take advantage of IoT devices to use them. Fast speed, high frequency, low power, low latency data transfers, and short to long-range data transfers are built and tuned for 5G devices. A study to reduce data leakage, lock-in, data manipulation, and communication challenges is being carried out. Increasingly sophisticated chipsets and architectures are built to raise standards. Increased durability is accomplished through innovations like ZigBee, WiFi, WiMax, Z-Wave, and LPwAN.

**Security**: In this 5G network-Blockchain scheme, the data protection threat resides with the IoT computer and its network. The information is tamper-proof, unchangeable, and thus safe while data is in the blockchain network. Different device types and their integration with gateway connections through WiFi and other WiFi communications endanger IoT info. The stability and protection of the IoT network are the same as the network’s safety and security. The 5G network security research and development progress are ongoing to ensure this technological mix’s effectiveness.

**Transparency and Accessibility**: Both blockchain data services (including company quality technologies such as Oracle Blockchain services located in Hyperledger) offer smartphone application-based data connectivity with maximum protection and usability via the data held in a blockchain network. Blockchain’s smart contracts render data seamlessly and transparently available to collaborators with Blockchain as the cardinal data management mechanism from the 5G network.

**Standardization and Interoperability**: Different firms, entrepreneurs, organizations, and academics create various blockchain networks with growing exposure to blockchains technologies. The systems include numerous architectures and languages of programming, consensus protocols, and flow of transactions. Applications constructed for multiple platforms are thus not capable of operating together. Standardization could allow organizations to create channels that will encourage contact between heterogeneous networks. Seele is a cross-blockchain network for collaboration [45]. Blockchain networks Open chain and Components provide this data sharing through a sidechain that communicates with the main Blockchain. Further work must be done to establish basic platform architecture specifications and consensus protocols that enable blockchain apps to be interoperable.

**Cost Efficient**: Many Blockchain solutions are available, costing per unit of transaction data as a process. For example, cloud service is available per transaction from the Oracle Blockchain Platform. Cost ownership of Blockchain is then driven by evidence. The technology is inexpensive, and several businesses evaluate it on a trial basis since Blockchain comes on a cloud network, and no fixed implementation costs are available. Organizations often sell free sample models to encourage acceptance. Investment in sensors is needed for the 5G network, and companies like Oracle give connectors. Overall, ownership costs are primarily driven by the number of sensors and the data volume. However, the acquisitions are very inexpensive because of the value they will provide to the company without any upfront expenses and decreasing ownership costs.

3. Blockchain for 5G Network

The Blockchain has the primary components discussed below. The proposed model’s target is to ensure the secure sharing of the healthcare data among the non-terminal nodes
as shown in Figure 2 with a real-time secured network model that consist of various components like the local data center, service access points, macro base stations, Blockchain application server, distributed unit (DU), and centralized unit (CU) of 5G. It is quite essential to make the healthcare records more secure to ensure the individuals’ privacy and avoid tampering of the data that may impact in different ways, like allowing abuse of identities and fraudulent insurance claims or disclosing public–private records, impacting the individual’s public reputation.

Figure 2. Represents the various components in the real-time secured network model.

The blockchain technology is maintained and monitored through the transactions and the information related to the transactions are maintained through the distributed ledgers. The following are the key components of the blockchain technology.

**Consensus:** The PoW Protocol checks any behavior in the network necessary to avoid the whole blockchain network from being owned by a single miner node and exploiting its history.

**Ledger:** It is a collaborative and decentralized archive of healthcare data about certain network transactions. It is, by its essence, permanent where once processed, knowledge cannot be erased. It means that each transaction is checked and acknowledged by most clients at a certain period as a legitimate transaction.

**Cryptography:** It guarantees that all network data are protected through strong encryption. It only enables approved users to decrypt files.

**Smart Contract:** It is used to verify and review the network members.

**Decentralized Architecture:** The blockchain technology is a distributed model, where the monitoring and maintenance of the transactions and ledgers are done among the cluster of nodes, that assist in faster settlement and the resource efficient with a lesser burden to any of the devices in the network.

### 3.1. Proposed Blockchain Layered Model

The blockchain network model consists of four layers in the proposed model. The layers are identified based on the responsibilities of each of the layers. The layered build of the proposed model is presented in Figure 3. Each of the layers has the designated responsibility as presented below.
Electronics 2021, 10, x FOR PEER REVIEW 11 of 27

Figure 3. Layered model of the proposed Blockchain-based 5G network.

**Basic Technical Layer:** The primary technical layer is the bottom-most layer of the proposed model with various physical components of the network model with a cluster of sensors for communication in a real-time scenario with switches, routers, and hubs for communication in a 5G environment. This is analogous to the sensor layer of the IoT layered architecture, as Shuaib, K. et al. [46]; Honar Pajooh, H. et al. [47], which looks after the communication’s physical media. Various communication protocols, like Zigbee, Z-wave, LoRa, WiFi, and Bluetooth, are extensively used in communication. The healthcare data is being encrypted by the Time the information reaches the bottom-most layer of the proposed model.

**Interface Layer:** The Interface layer comprises many connected components like connectivity, machine, and data storage capacities for the blockchain management. The network management is a primary feature of the interface layer alongside the other responsibilities like Route Management, and Security management. Networking nodes need to be self-sufficient in the routing because there are no global internet protocols on physical devices themselves. Message brokers, which is part of the inference layer, will look into the message validation, transformation, and routing procedure.

**Blockchain Layer:** The blockchain layer does have the pivotal authorities of the model that include Smart Contract, Services, and process automation, an event handler that is essential ineffective handling of the data. The smart contact component of the network may allow the appropriating allotment of the resource for utilization. A smart contract is a script triggered in the ledger by an internal and external networking nodes in the network. Event handlers include modules designed to adhere to updates to the Blockchain or related nodes and automatically invoke relevant business logic to react to them. Services and process management technologies can reach the blockchain layer of a corporate network or other blockchain-related capabilities used in given business logic.

**Exchange Layer:** The Exchange layer is the topmost layer of the proposed model, which is almost analogs to the application sub-layer of the blockchain layer of the conventional models presented by Hang, L. and Kim, D. [48] in their paper on Integrated IoT Blockchain Platform. The distributed ledger model collects mirrored, exchanged, and synchronized digital information across the whole blockchain network, where anyone on the network will own a copy of the directory. Eventually, every operation over the leader is mirrored in each distributed copy. The ledger may be either licensed or unauthorized for the peer over
the network if anyone may run an authorized peer to verify the transactions or mechanize to allow any peer in the network. P2P transaction components enable transferring funds from their respective bank accounts between two parties through a third-party assistant. Cryptocurrency is a digital resource intended to function as a trading method where individual coin ownership documents are maintained in a computerized archive of the transaction record.

3.2. Proposed Model of Blockchain for IoT in 5G architecture

The expectation of secure, real-time healthcare data on service production processes that a specific developed model requires bandwidth capability does not exist. 5G-enabled IoT would significantly improve this capability. Without that kind of change towards the Network Infrastructures, operators and other small-scale applications are restricted to designing and applying certain blockchain technologies involving agriculture, medical, automobile, and logistic industries. In specific Blockchain, technology is suitable to overcome both the obstacles and opportunities of a 5G-enabled IoT. Probability sampling technology is more likely to promote greater acceptance by the industry, as stated by Zhang, Y. et al. [49] as mentioned in the paper using blockchain technology for the internet of things.

In particular, Blockchain may function as both a way to log data in a way that is highly immune to integrity attack and as a mechanism to counteract the entry to our networks of malicious devices. Millions of cheap networked computers compound network risks with little to no native protection features. The spread of such devices has contributed to massive attacks by DDoS on wide parts of the Internet. The protection in our homes (e.g., the Nest) and cars (e.g., automated vehicles) that are progressively reliant on embedded networking infrastructure in regular business often constitutes a danger to these shortcomings. Therefore, it is necessary to protect this device network, maintain regard for privacy rights, and keep confidential information at the hands of bad actors. Through registration of an IoT computer on a blockchain, other devices on the network may be assured that a device is as it claims, without depending on a centralized servant, who in some cases may be more readily manipulated. Many start-ups operate on 5G IoT-based blockchain technologies. This will continue to boost the 5G IoT through blockchain approaches. Figure 4 represents the design of the proposed model.

![Figure 4. Represents the architecture of the Blockchain model.](image-url)

Many of the interactions go into Blockchain with this approach, allowing a permanent record of interactions. This method makes sure that all the connections selected can be traceable because their information can be verified in a blockchain. IoT apps meant to commercialize or sell, like Slock, will use this method to provide their services. Neverthe-
less, tracking all blockchain transactions would improve bandwidth and records, one of Blockchain’s most popular challenges. All IoT data related to such purchases, on the other side, should also be held in Blockchain, as stated by Reyna, A. et al. [50].

In the proposed model, the healthcare data in the IoT nodes shared from a sensor to the database server or the cloud server to process the data. The healthcare data is exchanged in an encrypted format like in 1 technology. The information is being encrypted through blockchain technology, and the corresponding ledger at each of the cluster-head node is being updated through the public_key of the node. It is significant in identifying the cluster-head, as the rest of the nodes in the network will work in conjunction with the other intermediate networking nodes in the IoT architecture. The cluster heads are identified through the degree centrality, and the particular corresponding node does share the healthcare data that it has received from the nodes in its cluster, which would reduce the overhead at various other nodes in the network as stated by Z. Niu et al. [51] in the paper on the identification of critical nodes.

3.3. Clustering of Intermediate Networking Components (Routers)

In the IoT environment, the nodes are diverse and do not restrict themselves to simple sensors with their framework functions. The connectivity, frequency band, and power usage differ significantly in all these units. Any IoT system periodically reports its status to the corresponding Base Station; hence the BS has the complete topological information. At first, the IoT model is separated into regions of defined duration, in each of which several instruments are clustered, and community details returned to equipment. Just before the clustering does coherent region depart, nodes watch the identity, position, and distances of all neighbors. Initially, nodes attempt to create clusters with nodes with the same social template. Cluster participants become the node with the most considerable optimistic mark and a node of the same social trend on the closest nodes list. The node enters and disassociates the cluster based on its social pattern. Figure 5 represents the clusters of intermediate networking nodes, and the cluster head is responsible for taking over the communications in the network [52].

Figure 5. Graphs representing the fully connected network to clustered network.

The IoT architecture consists of several intermediate networking nodes designated by the variable \( N_t = \{N_1, N_2, N_3, \ldots, N_t\} \), and one among the nodes will be considered as the cluster-head. A variety of parameters are utilized to conduct the clustering. These parameters are usually connectivity, node distance, node residual energy, and so on. In the proposed model, two parameters are considered for clustering the intermediate networking nodes. The parameters considered include the distance measures among the adjacent nodes and the node’s residual energy. The significance of choosing the number of adjacent intermediate networking nodes is that the cluster can only be created utilizing the adjacent nodes. The adjacent node to be the part of the cluster will be determined based on the
propagation spectrum radius and the nodes whose beacon fulfills those legitimate SNRs for deciding whether or not the provided node is a neighborhood member. The residual energy parameter is incredibly significant as a cluster head and should be selected as the node with more residual energy.

Suppose any of the intermediate networking nodes have more residual resources. In that case, its range of propagation and SNR are more extensive and more likely to involve certain non-terminal nodes than concerning other nodes in the cluster. This refers to the choosing of the amount of adjacent intermediate networking nodes for residual energy. In comparison, the more neighboring nodes in the cluster are available, the greater the network coverage in the field of concern. As the computing overhead is reduced due to the minimal number of cluster heads, the minimum number of cluster heads interact with the upper layer IoT terminal nodes.

\[ A_N = \sum_{j=1}^{n} X_j \]  

(1)

From Equation (1), the value of \( X_j \) is set to 1, if the node \( j \) is in the range of transmission ranges of the cluster head and within in the limits of SNR and the value of the variable \( X_j \) is set to 0 otherwise. The residual energy \( R_e \) of the intermediate networking node \( i \) in the network is approximated through the Equation (2) stated below

\[ R_e = e_{initial}(i) - \{ e_t(i) + e_r(i) + e_{com}(i) \} \]  

(2)

From Equation (2), the variable \( e_{initial}(i) \) represents the initial energy of the intermediate networking node, the variable \( e_t(i) \) represents the energy spent on transmitting the data. The variable \( e_r(i) \), is the energy spent for the radially active network by the non-terminal node \( i \) and the variable \( e_{com}(i) \) is the energy spent by the intermediate networking node \( i \) on performing the computations. The energy consumed for radially active is assessed through the Equation (3) stated below

\[ e_r(i) = b \times R_{net} \]  

(3)

The variable \( R_{net} \) is the residual energy of the IoT network, and the variable \( b \) represents the number of bits received by the corresponding intermediate networking node \( i \). The energy spent on the transmission of the data is presented in Equation (4), which is stated below

\[ e_t(i) = b \times \left( R_{net} + \varepsilon \times dist^2 \right) \]  

(4)

From Equation (4), the variable \( \varepsilon \) denotes the energy utilized to propagate the data. The variable \( dist \) represents the distance of the propagation.

### 3.4. Assessing the Degree Centrality

The logic of the degree centrality work based on several nodes connected to the corresponding node is considered. In the undirected graph-based network model, the adjacent node makes the node’s degree in the network. For any network \( N \), the network is assumed to have \( n \) numbers. The adjacency matrix of the model is identified as \( A_m = [a_{ij}] \in \mathbb{R}^{n \times n} \) and the degree centrality of the node in the model is determined by \( D_c = \{ D_{c_1}, D_{c_2}, D_{c_3}, D_{c_4}, D_{c_5}, \ldots D_{c_i}, \ldots D_{c_n} \} \), wherein \( D_{c_i} \) is the degree of centrality of a node \( n_i \). The value of the variable \( D_{c_i} \) is determined through the Equation (5) as shown below

\[ D_{c_i} = \frac{\sum_{j=1}^{n} a_{ij}}{n - 1} \]  

(5)
The variable \( D_c \) is being further normalized as \( D = \{ D_1, D_2, \ldots D_i, \ldots D_n \} \), where the variable \( D_i \) is the normalized degree centrality of the node \( v_i \) and the value of the \( D_i \) is determined through Equation (6), which is shown below

\[
D_i = \frac{D_c - \min(D_c)}{\max(D_c) - \min(D_c)}
\]

(6)

The significance of the degree centrality approximates the correlation between the cluster head and the adjacent nodes in the network. The node with an optimal degree is considered the point of access to the external intermediate networking node that collects the data from its neighboring nodes and updates the ledger. It sends the data to the other intermediate networking node. By doing so, every intermediate networking device in the network need not have computational capabilities.

3.5. The Conceptualized Policy of Communication Exchange

The data is encrypted to maintain its integrity in the healthcare data exchange process among the intermediate networking nodes in the 5G network. There are a few things that each non-terminal network node must perform before it exchanges the network’s data. The conceptualized policy of data exchange does have the responsibilities that are performed on establishment and communication. The nodes in the network will undergo a contact as a part of the healthcare data exchange using the tokens. The healthcare data that is being exchanged among the parties are considered transactions. The information pertaining to the transactions that are performed will be maintained through the ledgers. The ledgers are being distributed among the parties, and they are simultaneously updated. The devices that wish to exchange the healthcare information must be authenticated by themselves on then they are eligible for exchanging the data. In case the node wishes to leave the network, they have to synchronize with the authoritative node. The Algorithm 1 presents the algorithm followed for adding the node to the network.

**Algorithm 1: Adding a Networking Node**

**Input:** new_Networking-Node_Address // MAC address of the node.
**Output:** Boolean Value (True/False) // True if Accepted else false.

**Begin**

if (req.sender is not_Auth), then
    throw;
else if (new_Non-Terminal-Node already exists), then
    return false;
else
    authorised_node[add_new_Networking-Node];
    return true;
end if

**End**

The function authorised_node() function stated in the above algorithm can be used to authorize the non-terminal nodes to join the network by validating the device’s MAC address. They exchange the certificate upon successful linking to the network for further communication among the nodes. If the Non-Terminal-Node is already existing, then the request is ignored by the administrator of the network. Algorithm 2 presents the algorithm for adding the token.

**Algorithm 2: Adding a token**

**Input:** key, trans_id, token
**Output:** Boolean Value (True/False) // True if Accepted else false.

**Begin**

if (req.sender is not_Auth), then
    throw;
else
    Perform mapping token to Non_Terminal(tran_id, key) to the token collection
    return true;
end if

**End**
The number of networking components that are to be attached to the cluster head, the corresponding cluster head is being identified, and all the adjacent nodes are linked to the cluster head. The cluster heads are responsible for exchanging the data in the network because low-energy devices are part of the network. The data exchange needs a considerable computational capability for data processing and transmission to the base station, farther from the corresponding node. In such a situation, the nodes will forward the data to the neat cluster head, and in turn, the cluster heads will exchange the data with the base station or sink. On exchanging the data with the cluster head, the ledger is being updated with the transaction that is being performed. The hashing is being performed on the data being exchanged over the network to ensure the privacy of the healthcare data being transmitted. The below is the pseudocode for clustering the sensor network and identifying the cluster head in the network. The clustering and cluster heads are identified at regular intervals in a dynamically changing network. Algorithm 3 presents the procedure for clustering and Cluster-Head selection.

**Algorithm 3: Clustering and Cluster-Head selection**

| Input: | n that represents the number of nodes, time interval |
| Output: | Cluster with non-terminal nodes and Corresponding Cluster |
| Begin | Select random(cluster_head); |
| | Set the residual energy parameters; |
| | while (time_interval) do |
| | for (every node i to n) do |
| | perform flooding; |
| | Broadcast adjacent_node_count, ReResidualenergy; |
| | Assess Cluster_head from max(adjacent_node_count, Resedualenergy) |
| | Create a cluster concerning the identified Cluster_head |
| | end of for |
| | update the cluster_data; |
| End |

The ledger at the intermediate networking nodes is updated on performing the transaction, which would help ease the ease of tracking the data exchanged among the nodes in the network. The algorithm below represents the updating procedure of the digital ledger in the proposed model. In data exchange among the nodes, either the nodes, i.e., sender and the receiver, are authenticated before exchanging the data. Send_data() is the function used in sending the data the entities like a key, token, and transaction_id is being used in sending the payload among the nodes in the network. Algorithm 4 presents the procedure for ledger updating process.

**Algorithm 4: Ledger Updating Process**

| Input: | Public_key, trans_id, attribute, value |
| Output: | Boolean Value (Successful/unsuccesful)/1 if updated successfully else 0; |
| Begin | if (req.node is not Auth), then |
| | throw; |
| end if |
| if (public key is valid), then |
| update_ledger{attribute, value}; |
| return 1; //on successful updating of the ledger; |
| else |
| return 0; //on unsuccessful updating of ledger; |
| end if else |
| End |

In Blockchain-based encryption technology for the data exchange, the token is the digital unit that provides access privileges. If the request comes from the valid node, the token is assigned, and the token list of the respective node is being updated accordingly. In every data exchange among the peers, the tokens are used while transferring. Algorithm 5 represents the data exchange process.
Algorithm 5: Data Exchange

Input: key, trans_id, token, data
Output: Boolean Value (True/False) // True if Accepted else false.

Begin
  if (req. sender is not_Auth) then
    throw;
  end if
  if (req.receiver is not_Auth) then
    throw;
  end if
  if (data_Non-Terminal-Node is available) then
    Send_data[key,trans_id,token,payload_data];
    return true;
  else
    return false;
  end if
End

The ledger at the intermediate networking nodes is updated on performing the trans-
action, which would help ease the ease of tracking the data exchanged among the nodes in
the network. The algorithm below represents the updating procedure of the digital ledger
in the proposed model. In data exchange among the nodes, either the nodes, i.e., sender
and the receiver, are authenticated before exchanging the data. Send_data() is the function
used in sending the data the entities like a key, token, and transaction_id is being used in
sending the payload among the nodes in the network. Algorithm 6 presents the procedure
for deleting the non-terminal node in the network.

Algorithm 6: Deleting a Non-Terminal Node

Input: existing_Non_Terminal-Node_Address//MAC address of the node;
Output: Boolean Value (True/False) // True if Accepted else false;

Begin
  if(req.sender is not_Auth) then
    throw;
  end if
  if existing_Non-Terminal-Node is already exited, then
    return false;
  else
    authorised_node[remove_existing_Non-Terminal-Node];
    return true;
  end if
End

The administrator node can either add a new-Networking-Node or remove an existing-
Networking_Node from the architecture. The MAC address of the corresponding node is
deleted from the node_list. Resultantly, the node is not able to exchange the data with any
other node in the network.

3.6. Security Scheme for 5G based Blockchain Model

The Secure Hash Algorithm (SHA) is indeed a hash function-based cryptographic
algorithm utilized across several blockchain networks. It has an output size of 256 bits
(SHA-256) and SHA-256 is one of the predominantly used lightweight encryption technique.
The specific category of the encryption model will yield a 32 byte result often represented
by hexadecimal string data. Blockchain technology is comprised of blocks. Every block is
composed of data and the preceding block’s hash, except for the origin block, which has no
prior hashing. Blockchain technology operations are suitable for use with a hashing crypto
technique, enabling the generation of a robust and secure hashing code and its conversion
from bits of fixed-sized data to strings of characters. Every transaction in a blockchain
gets hashed before moving it into a block, and hash pointers link each block to the next
block to retain the preceding block’s hash data, which is irreversible. Consequently, any
modifications to the blockchain’s hashing method will result in a new hash string for each
character and, therefore, will influence all the blocks concerned. The hash that is assessed
in the current cycle is dependent on the previous hash value. The entire procedure of
hashing is classified into five phases, which are presented as follows
1. **Stage 1:**
   The padding is performed on the data by adding additional bits to the original to attain the minimum input block size. The value 0 is added to the input until it reaches 448-bits. Followed by 64-bit length is appended to the input data until it reaches 512-bits.

2. **Stage 2:**
   The data is divided into 16 groups of 512-bit each. The groups are recognized as G1–G16.

3. **Stage 3:**
   The vectors that are needed at the time of data are recognized as a0–a63 and b0–b7. The variables I, J, K, L, M, N, O, and P are assigned with b0–b7, respectively.

4. **Stage 4:**
   There are various mathematical operations over 64 iterations at this stage. The values associated with the design variables I–P are updated depending on the hash value of the primary variable. The looping variable l is initialized to 0, and it will iterate until the value is less than 63.

   Set, \( I_{l+1} = I_l; \ K_{l+1} = K_l; \ L_{l+1} = L_l; \ M_{l+1} = M_l; \ O_{l+1} = O_l; \)

   Evaluate, \( I_{l+1} = P_l + \sum_i (M_i) + ch(M_i, N_i, O_i) + a_l + w_l + \sum_o (I_l) + M(I_l, J_l, K_l)M_{l+1} = P_l + \sum_i (M_i) + ch(M_i, N_i, O_i) + a_l + w_l + L_l \)

5. **Stage 5:**
   In this stage the values of output variables are determined as shown below
   
   \[ b_0 = b_0 + l_{63}; \ b_1 = b_1 + I_{63}; \ b_2 = b_2 + K_{63}; \ b_3 = b_3 + L_{63}; \ b_4 = b_4 + M_{63}; \ b_5 = b_5 + N_{63}; \ b_6 = b_6 + O_{63}; \ b_7 = b_7 + P_{63} \]

   In the above evolutions, \( ch(M_i, N_i, O_i), \sum_i (M_i), \sum_o (I_l), M(I_l, J_l, K_l) \) are the logical functions and the value of \( w_l \) is determined as follows

   \( w_l \) is set to a if \( 0 \leq l \leq 15 \)
   
   \( w_l \) is set to \( b \) if \( 16 \leq l \leq 63 \)

   Where \( b = \sigma_1(w_{l-2}) + w_{l-7} + \sigma_0(w_{l-15}) + w_{l-16} \)

   I and M’s values are re-evaluated to optimize the time consumed for performing the hashing on the input data. Figure 6, which is stated below, represents the block diagram of the SHA-256 algorithm, which contains an array of registers of sizes 16 × 32 and 8 × 32. The implementation specification of the SHA-256 is presented in Table 2. The below is the example for input and output hash values through the SHA-256 algorithm.

---

**Figure 6.** Image representing the block diagram of SHA-256.
Table 2. SHA-256 Implementation specifications.

| SHA-256 Security Scheme Specifications |
|----------------------------------------|
| Hash value size                         | 256-bits                      |
| The complexity of the attack            | $2^{128}$                     |
| Message Size                            | Below $2^{64}$                |
| Block size                              | 512                           |
| Word size                               | 32                            |
| Number of Words                         | 8                             |
| Number of rounds                        | 64                            |

Input: Blockchain  
Output: 625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1

The algorithm pertaining the procedure for the block updating as presented in Algorithm 7 and the block verification is presented in Algorithm 8 that is the part of the SHA-256 cryptographic hash mechanism. The distributed ledger is being updated with every transaction that is being performed in exchanging the data among the networking nodes. The hash value of the previous block is considered in evaluating the current hash value of the block.

**Algorithm 7: Block Updating**

Input: valid Block$_i$  
Output: Updated Distributed Ledger(DL)  
Begin  
if (w<max_capacity), then  
// $w$ = sizeof(Block$_i$ + DL)  
Update DL from Block$_i$ and DL  
DL = DL | Block$_i$;  
return DL;  
else  
Update DL by deleting old_DL value  
set DL = DL | Block$_i$;  
return DL;  
end if  
End

**Algorithm 8: Hash Block Verification**

Input: Block$_i$ for verification  
Output: Status of verification  
Begin  
if(transaction is valid), then  
if (Block$_i$.prev_block_hash! = prev_Block_Hash), then  
return false;  
else  
return true;  
Prev_Block_Hash = Block$_i$.Prev_Block_Hash  
Update Block$_i$.Hash;  
end if  
else  
return false;  
End

Hashing technique is extensively used in blockchains technology to create new transactions, timestamping the transactions, and eventually include a reference to them in the previous block [53,54]. Whenever a new block of transactions is being appended to the blockchain as well as consensus has been updated among different connected nodes ensuring the valid and relevant version of ledger, it will be harder to alter or reverse a transaction with one directional way of hashing and it needs massive computing resources to alter the
blockchain. Thus, hashing is essential for ensuring the blockchain’s cryptographic integrity in the 5G network [55,56].

3.7. Implementation Environment

The proposed Blockchain-based 5G architecture model for data exchange among the non-terminal nodes is being implemented over the docker environment. The model is implemented in the personal computer runs on top of the Mac OS (Version 11.0.1 Big Sur) over a 2.7 GHz Quad-Core i7 processor with 8GB 2133MHz LPDDR3 RAM. Docker Desktop Community 2.5.0.1 creates the runtime environment for carrying the execution procedures. Hyperledger Fabric is being used in deploying the blockchain framework. CouchDB is being used in maintaining the ledger states. Deployment and managing the smart ledgers are done through the command-line interface. The table below presents the implementation environment of the proposed model Blockchain for the 5G architecture. The implementation details of the proposed model are presented in Table 3.

| Environment Specifications | Version 11.0.1 Big Sur |
|---------------------------|------------------------|
| 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                |

4. Performance Analysis and Deliberations

The proposed model’s performance is being evaluated against the various existing approaches by considering different parameters. The integrity of the proposed method is being assessed through a cluster of 50, 150, 250, and 350 intermediate networking nodes. The performance metrics are being assessed in the paper’s current section like the execution time, network delay, and process overhead of the proposed model. This has been accomplished by utilizing the modeling framework named Hyperledger Caliper [57], enabling users to customize the use case script of a particular blockchain architecture with a collection of intermediate networking nodes. The execution timestamp taken by the proposed blockchain network to execute the transaction was reported in terms of minimum, average, and maximum time. The time taken for the device registration in the network with the various number of intermediate networking nodes in each cluster is presented in Table 4 and Figure 7. The minimum, average, and maximum are the values that are obtained on the repeated execution for network model and the obtained values are being tabulated for the performance analysis.

| 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              |

It can be observed from the Table 2 that there is a slight increase in the network delay due to increase in the networking devices, as the data that is being exchanged needs to be analyzed, processed, and forwarded by each intermediate node that consumes additional time for processing each data packet received and the transaction information. The information of the neighboring intermediate nodes in the network is shared among the adjacent
nodes for updating the routing table for easy path estimation and faster data exchange. The node’s information is sensed and maintained in the database, and the procedures have been practiced several times for recording the statistical data. The execution time for the transaction for node reading is presented in Table 5, and the corresponding graph is shown in Figure 8. The minimum, average, and maximum that are presented in the current study are the values obtained on repeated execution of the model for analyzing the peak performance.

![Graph](image)

**Figure 7.** Represents the graph for execution-time for node registration, (a) Time consumed in best case representing the minimum time, (b) Time consumed in average case representing the average time and, (c) Time consumed in worst case representing the maximum time.

**Table 5.** Represents the execution of the transactions for node reading.

| 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             |

![Graph](image)

**Figure 8.** Represents the graph for execution-time for node reading, (a) Execution time in best case representing the minimum time, (b) Execution time in average case representing the average time and, (c) Execution time in worst case representing the maximum time.
The proposed model’s performance is evaluated against the delay in exchanging the ledger records among the networking nodes in the 5G network. The time delay includes the delay incurred due to Blockchain-based encryption of the data among the networking nodes. The delay against the variable number of records is presented in Table 6, and the corresponding chart is shown in Figure 9.

Table 6. Represents the time delay for sharing the records.

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

Figure 9. Graphs represent Time Delay in record sharing.

The delay in updating the digital ledger at each of the non-terminal nodes in IoT architecture in the 5G network is evaluated for the varied number of records, and the obtained time delays are updated in Table 7. The graph that is generated is being presented in Figure 10.

Table 7. 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            |

It can be observed in the practical implementation of the proposed model that the execution time of the Blockchain-based model in the 5G network is reasonably fair, which can be observed in the statistical analysis presented in Tables 2 and 3 for node registration reading over a range of non-terminal nodes. The time delay for the record share is reasonably fair. It does not incur too much of a burden over the network, which can be observed from Table 7.
The computational complexity of the SHA-256 is almost equivalent to the sum of hash functions of a stream cipher. The complexity of the algorithm is assessed through the Big O notation. Similarly, the complexity of the SHA-256 is approximately equivalent to $O(c + p n_1 + q n_2)$ by using an extensible output function. The variable ‘$c$’ is the constant value dependent on the size of the key, variables ‘$n_1$’ and ‘$n_2$’ represent the input and output size, respectively. The variable ‘$p$’ denotes the overhead associated with each input block, and the ‘$q$’ denotes the overhead associated with the bitstream corresponding to the output block. In a much simpler way, the complexity of the model is determined as $O(n)$, where $n = n_1 + n_2$ is the combination of input and output bits.

![Time Delay Updating Ledger](image)

Figure 10. Graphs represent Time Delay in updating the digital ledger.

The performance of the proposed model is being analyzed concerning the processing delay, hash rate, and throughput of the network on implementing the security scheme in the dynamic environment concerning the fixed-size hash function. Table 8 represents the evaluated value of implementing the proposed SHA-256 scheme for the blockchain in the 5G environment. Figure 11 represents the associated graphs that are obtained for experimental study. The performance is evaluated against the string of 128 bits in length for variable number of networking devices in the network. The throughput is approximated by incorporating the blockchain based encryption. The crucial task of encryption and updating the ledger will be taken care of by the cluster heads.

| Number of Nodes | Processing Delay (ms) | Hash Rate (Mhash/s) | Throughput (Mbps) |
|-----------------|-----------------------|---------------------|------------------|
| 50              | 63.98                 | 15.23               | 1974             |
| 150             | 64.50                 | 15.18               | 1938             |
| 250             | 65.48                 | 15.17               | 1894             |
| 350             | 66.12                 | 15.10               | 1843             |

The obtained values in the Table 5 makes it clear that the SHA-256 based encryption scheme is lightweight, and the network has performed almost the same performance concerning to operational delay and the hash rate irrespective of number of nodes in the network.
Figure 11. Graphs representing the performance analysis of SHA-256 security scheme on experimenting over variable number of nodes, (a) Represents the processing delay (b) Represents the hash rate and, (c) Represents the throughput.

5. Conclusions

Blockchain has gone past crypto-monetary legislation and is now revolutionizing numerous sectors. The excitement extends beyond the speculation as many companies are embarking on a technology focused Blockchain to boost business requirements. Similarly, this applies to the 5G network and beyond the 5G network, since numerous experiments have been carried out to promote Blockchain’s 5G network. The possibility that upcoming 5G networks will be widely dispersed and autonomous means network control and protection challenges are more prominent and challenging than highly centralized previous generations. Blockchain deals with crucial safety concerns such as honesty, authentication, faith, and distributional availability due to its stable architecture principles. Besides, smart contracts will enable the distribution/sharing of end-to-end capital, network management, and organization of the expected 5G services. Similarly, Blockchain allows many new market structures, reduces network provider collaboration challenges, and seamlessly manages numerous processes.

This paper analyzed Blockchain’s state-of-the-art literature to cope with various primary problems in the 5G network in sharing sensitive data like healthcare records. The current study offered taxonomy in network administration, device management, contact management, and services for the 5G network framework in Blockchain. We assume that the 5G and future networks have tremendous promise. When fully introduced, 5G networking will be implemented worldwide in a stable, economical, and productive manner. In addition to multiple benefits, various obstacles like handling the wider number of devices will be a major concern, dealing with 350 devices in the simulation environments may not be the same way in real-time implementation environment. The real-time challenges like the scalability, interoperability, and standardization regulatory might be challenging in the 5G based blockchain technology for handling the healthcare related data.

6. Future Scope

The experimental study of the proposed security mechanism model through blockchain models seems to be robust in maintaining the integrity of the healthcare data. Blockchain is efficient in working in a distributed environment through digital ledgers. The proposed model needs to be improved in storage competence, as the proposed model needs considerable storage space over time. The non-terminal nodes need tremendous efforts in creating a record and sharing the records with the adjacent node. An efficient model needs to be identified in monitoring the changes added to the blockchain network as the data added to the network cannot be modified in the current scenario. The quantum Blockchain model can efficiently distribute the load of the ledger management effectively through distributed
operations and effectively manage the storage management at each of the administrative nodes in the mobile network.

**Author Contributions:** Conceptualization, P.N.S., A.K.B., M.R.B. and M.W.; data curation, P.N.S., M.R.B. and S.R.N.; formal analysis, A.K.B. and M.R.B.; funding acquisition, M.R.B., M.W. and A.K.B.; investigation; M.R.B. and P.N.S.; methodology, P.N.S. and S.R.N.; project administration, M.W. and A.K.B.; resources, P.N.S. and A.K.B.; software, P.N.S., M.R.B. and S.R.N.; supervision, M.R.B., A.K.B. and M.W.; validation, A.K.B. and M.R.B.; visualization, P.N.S. and M.R.B.; writing—review and editing, P.N.S., A.K.B., M.R.B. and S.R.N. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the National Research Foundation (NRF) of Korea under the Ministry of Science and ICT, Republic of Korea (grant no. NRF-2020R1G1A1012741).

**Acknowledgments:** Authors acknowledge contribution from the National Agency for Academic Ex-change of Poland under the Academic International Partnerships program, grant agreement no. PPI/APM/2018/1/00004/U/001.

**Conflicts of Interest:** The authors declare no conflict of interest.

**References**

1. Kim, S.; Lee, I. IoT device security based on proxy re-encryption. *J. Ambient. Intell. Humiz. 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. Srinivasu, P.; SivaSai, J.; Ijaz, M.; Bhoi, A.; Kim, W.; Kang, J. Classification of skin disease using deep learning neural networks with mobilenet V2 and LSTM. *Sensors* **2021**, *21*, 2852. [CrossRef] [PubMed]
4. Nagasrinivasu, P.; Rao, C.S. A multilevel image encryption based on duffing map and modified DNA hybridization for transfer over an unsecured channel. *Int. J. Comput. Appl.* **2015**, *120*, 1–4. [CrossRef]
5. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.-S. IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors* **2018**, *18*, 2796. [CrossRef]
6. Samaila, M.G.; Neto, M.; Fernandes, D.A.B.; Freire, M.M.; Inácio, P.R.M. Challenges of securing Internet of Things devices: A survey. *Secur. Priv.* **2018**, *1*, e20. [CrossRef]
7. Ray, D.; Ligatti, J. Defining injection attacks. In *Information Security. ISC 2014. Lecture Notes in Computer Science* 2014; Chow, S.S.M., Camenisch, J., Hui, L.C.K., Yiu, S.M., Eds.; Springer: Cham, Switzerland, 2014; Volume 8783.
8. Chen, J.; Liang, G.; Cai, Z.; Hu, C.; Xu, Y.; Luo, F.; Zhao, J. Impact analysis of false data injection attacks on power system static security assessment. *J. Mod. Power Syst. Clean Energy* **2016**, *4*, 496–505. [CrossRef]
9. Hasan, M.; Islam, M.; Zafir, I.I.; Hashem, M. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet Things* **2019**, *7*, 10059. [CrossRef]
10. Oza, A.D.; Kumar, G.N.; Khorajiyeh, M.; Tiwari, V. Snaring cyber attacks on IoT devices with honeynets. In *Computing and Network Sustainability. Lecture Notes in Networks and Systems* 2019; Peng, S.L., Dey, N., Bundele, M., Eds.; Springer: Singapore, 2019; Volume 75.
11. Sumra, I.A.; Bin Hasbullah, H.; Bin AbManan, J.-L. Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey. In *Advances in Intelligent Systems and Computing*; Springer: Singapore, 2015; Volume 306, pp. 51–61.
12. Chenthara, S.; Wang, H.; Ahmed, K. Security and privacy in big data environment. In *Encyclopedia of Big Data Technologies*; Springer: Singapore, 2019; pp. 1487–1495.
13. 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]
14. Wu, H.; Cao, J.; Yang, Y.; Tung, C.L.; Jiang, S.; Tang, B.; Liu, Y.; Wang, X.; Deng, Y. Data management in supply chain using blockchain: Challenges and a case study. In Proceedings of the 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 29 July—1 August 2019; pp. 1–4.
15. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
16. El-Rashidy, N.; El-Sappagh, S.; Islam, S.M.R.; M El-Bakry, H.; Abdelrazeck, S. Mobile Health in Remote Patient Monitoring for Chronic Diseases: Principles, Trends, and Challenges. *Diagnostics* **2021**, *11*, 607. [CrossRef]
17. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218–2188. [CrossRef]
18. Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access* **2018**, *6*, 11676–11686. [CrossRef]
19. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-based data preservation system for medical data. *J. Med. Syst.* **2018**, *42*, 141–141:13. [CrossRef]
20. Rahurkar, S.; Vest, J.R.; Menachemi, N. Despite the spread of health information exchange, there is little evidence of its impact on cost, use, and quality of care. *Hdl. Aff.* 2015, 34, 477–483. [CrossRef]

21. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. BlobHIE: A BLOCKchain-based platform for healthcare information exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2018; pp. 49–56.

22. Ozgur Catak, F.; Catak, E.; Kuzlu, M.; Cali, U. Security concerns on machine learning solutions for 6G networks in mmWave beam prediction. *arXiv* 2021, arXiv:2105.03905.

23. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* 2020, 166, 102693. [CrossRef]

24. Rahimi, S.; Zargham, M. Security analysis of VPN configurations in industrial control environments. In *Critical Infrastructure Protection, V ICCIP* 2011; Butts, J., Shenoi, S., Eds.; Springer: Berlin, Germany, 2011; pp. 73–88.

25. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* 2020, 135, 106382. [CrossRef]

26. Panigrahi, R.; Borah, S.; Bhoi, A.; Ijaz, M.; Pramanik, M.; Kumar, Y.; Jhaiveri, R. A consolidated decision tree-based intrusion detection system for binary and multiclass imbalanced datasets. *Mathematics* 2021, 9, 751. [CrossRef]

27. Panigrahi, R.; Borah, S.; Bhoi, A.; Ijaz, M.; Pramanik, M.; Jhaiveri, R.; Chowdhary, C. Performance Assessment of supervised classifiers for designing intrusion detection systems: A comprehensive review and recommendations for future research. *Mathematics* 2021, 9, 690. [CrossRef]

28. Surendran, S.; Nassef, A.; Beheshti, B.D. A survey of cryptographic algorithms for IoT devices. In Proceedings of the 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 4 May 2018; pp. 1–8.

29. Choi, J.; Kim, J.; Sung, J.; Lee, S.; Lim, J. Related-key and meet-in-the-middle attacks on triple-DES and DES-EXE. In *Computer Vision; Springer Science and Business Media: Berlin/Heidelberg, Germany, 2005; Volume 3481, pp. 567–576.*

30. Li, R.; Jin, C. Meet-in-the-middle attacks on 10-round AES-256. *Des. Codes Cryptogr.* 2015, 80, 459–471. [CrossRef]

31. Roche, T.; Lomné, V.; Khalifallah, K. Combined fault and side-channel attack on protected implementations of AES. In *Transactions on Petri Nets and Other Models of Concurrency XV; Springer Science and Business Media: Berlin/Heidelberg, Germany, 2011; Volume 7079, pp. 65–83.*

32. Mahanta, H.J.; Khan, A.K.; Mukhopadhyay, S. Modular exponentiation with inner product to resist higher-order DPA attacks. *Innov. Syst. Softw. Eng.* 2019, 16, 87–97. [CrossRef]

33. Hunn, S.A.Y.; Naziri, S.Z.B.M.; Idris, N.B. The development of tiny encryption algorithm (TEA) crypto-core for mobile systems. In Proceedings of the 2012 IEEE International Conference on Electronics Design, Systems and Applications (ICEDSA), Kuala Lumpur, Malaysia, 5–6 November 2012; pp. 45–49.

34. Hong, S.; Hong, D.; Ko, Y.; Chang, D.; Lee, W.; Lee, S. Differential cryptanalysis of TEA and XTEA. In *Privacy Enhancing Technologies*; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2971, pp. 402–417.

35. Salehani, Y.E.; Youssef, A. Differential fault analysis of Hummingbird. In Proceedings of the 10th International Conference on Security and Cryptography, Sanya, China, 10–12 December 2011; pp. 357–361.

36. Kobayashi, E.; Suzaki, T.; Minematsu, K.; Moriai, S. TWINE: A lightweight block cipher for multiple platforms. In *Selected Areas in Cryptography; Springer: Berlin/Heidelberg, Germany, 2012; p. 7707.* [CrossRef]

37. Biriyukov, A.; Derbez, P.; Perrin, L. Differential analysis and meet-in-the-middle attack against round-reduced TWINE. In *Transactions on Petri Nets and Other Models of Concurrency XV; Springer Science and Business Media: Berlin/Heidelberg, Germany, 2015; Volume 9054, pp. 3–27.*

38. Beaulieu, R.; Shors, D.; Smith, J.; Treatman-Clark, S.; Weeks, B.; Wingers, L. The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 7–11 June 2015; pp. 1–6.*

39. Dwivedi, A.D.; Morawiecki, P.; Srivastava, G. Differential cryptanalysis of round-reduced SPECK suitable for internet of things devices. *IEEE Access* 2019, 7, 16476–16486. [CrossRef]

40. Shanmugam, D.; Selvam, R.; Annadurai, S. Differential power analysis attack on SIMON and LED block ciphers. In *Transactions on Petri Nets and Other Models of Concurrency XV; Springer: Cham, Switzerland, 2014; Volume 8804, pp. 110–125.*

41. Sahai, A.; Brent, W. Fuzzy identity-based encryption. In *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; pp. 457–473.*

42. Kumar, N.S.; Lakshmi, G.R.; Balamurugan, B. Enhanced attribute based encryption for cloud computing. *Procedia Comput. Sci.* 2015, 46, 689–696. [CrossRef]

43. Celik, A.; Tetzner, J.; Sinha, K.; Matta, J. 5G device-to-device communication security and multipath routing solutions. *Appl. Netw. Sci.* 2019, 4, 1–24. [CrossRef]

44. Adnan, M.H.; Zukarnain, Z.A. Device-to-device communication in 5G environment: Issues, solutions, and challenges. *Symmetry* 2020, 12, 1762. [CrossRef]

45. Ismail, L.; Materwala, H. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry* 2019, 11, 1198. [CrossRef]

46. Shuaib, K.; Saleous, H.; Zaki, N.; Dankar, F. A layered blockchain framework for healthcare and genomics. In *Proceedings of the 2020 IEEE International Conference on Smart Computing (SMARTCOMP), Bologna, Italy, 14–17 September 2020; pp. 156–163.*
47. Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-layer blockchain-based security architecture for internet of things. *Sensors* 2021, 21, 772. [CrossRef]

48. Hang, L.; Kim, D.-H. Design and implementation of an integrated IoT blockchain platform for sensing data integrity. *Sensors* 2019, 19, 2228. [CrossRef]

49. Zhang, Y.; Wen, J. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Netw. Appl.* 2017, 10, 983–994. [CrossRef]

50. Reyna, A.; Martin, C.; Chen, J.; Soler, E.; Diaz, M. On blockchain and its integration with IoT: Challenges and opportunities. *Futur. Gener. Comput. Syst.* 2018, 88, 173–190. [CrossRef]

51. Niu, Z.; Li, Q.; Ma, C.; Li, H.; Shan, H.; Yang, F. Identification of critical nodes for enhanced network defense in MANET-IoT networks. *IEEE Access* 2020, 8, 183571–183582. [CrossRef]

52. Khalifeh, A.; Abid, H.; Darabkh, K.A. Optimal cluster head positioning algorithm for wireless sensor networks. *Sensors* 2020, 20, 3719. [CrossRef]

53. Qiu, Q.; Liu, S.; Xu, S.; Yu, S. Study on security and privacy in 5G-enabled applications. *Wirel. Commun. Mob. Comput.* 2020, 2020, 1–15. [CrossRef]

54. Basin, D.; Dreier, J.; Hirschi, L.; Radomirovic, S.; Sasse, R.; Stettler, V. A formal analysis of 5G authentication. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–18 October 2018; pp. 1383–1396.

55. Seok, B.; Park, J.; Park, J.H. A lightweight hash-based blockchain architecture for industrial IoT. *Appl. Sci.* 2019, 9, 3740. [CrossRef]

56. Seok, B.; Sicato, J.C.S.; Erzhena, T.; Xuan, C.; Pan, Y.; Park, J.H. Secure D2D communication for 5G IoT network based on lightweight cryptography. *Appl. Sci.* 2019, 10, 217. [CrossRef]

57. Jamil, F.; Hang, L.; Kim, K.; Kim, D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics* 2019, 8, 505. [CrossRef]