Blockchain Based Smart Healthcare Systems in 5G Networks For Preventing Data Forgery

suji helen (sujihelen.cse@sathyabama.ac.in)
Sathyabama University https://orcid.org/0000-0001-6596-8205
C. Senthilsingh
Shadan Womens College of Engineering and Technology

Research Article

Keywords: Blockchain, IoT, Scalability, Security, Smart home, Smart contracts, Smart Agriculture, Health Monitoring

Posted Date: February 16th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-178651/v1

Blockchain based Smart Healthcare systems in 5G Networks

L.Sujihelen[1], C.Senthilsingh[2]
[1]Assistant Professor,Department of CSE, School of Computing
[1]Sathyabama Institute of Science and technology,Chennai
[2]Professor,Department of ECE,Shadan Women's College of Engineering and Technology,Hyderabad

Abstract:

The 5G networks are about to deploy it all over the world. This 5G technologies support by connecting the devices with rapid growth in network capacity, high QoS. Apart from this feature, 5G has more advantages in security, decentralization, transparency, data interoperability. The 5G network has millions of IoT devices are connected. With higher speeds these devices are enabled and worked with high speed. Blockchain is an important technology in the current trend. The Blockchain technology is used in more fields such as online payments, healthcare, smart contracts etc. Extending the technology of block chain to Internet of things (IoT) can have more features. The important issues in 5G technology is security because millions of IoT devices are connected and more confidential data is transferred. This data should be more secure using blockchain technology. This proposed system is to secure the data in smart healthcare systems using blockchain in 5G networks to prevent the data from forgery.

Keywords: Blockchain, IoT, Scalability, Security, Smart home, Smart contracts, Smart Agriculture, Health Monitoring.

1. Introduction

Mobile communication is to connect with other devices in various locations without any wires. It is an umbrella technology in which we can access the network at any time, any place, anywhere by any communication devices. The mobile communication technology has improved a lot from 1G to 5G technology [1][2]. Each technology will vary on speed, frequency, multiplexing, standards, switching, data transfer. 5G is the next technology which has more features such as high-speed internet connection, millions of IoT devices are connected, fast data transfer in uploading and downloading. One of the important of 5G technology is increased connectivity with more IoT devices. The millions of IoT devices are connected has low power consumption and high battery life. It will expand the broadband wireless services. According to the report by Ericsson in 2019, the 5G technology will have 45% of population coverage and the subscriptions is 1.9 billion. It uses optical fibers for the connectivity with the base station to increase the latency. The security and privacy of the 5G technology is high when compared with the 4G technology. The first application of the 5G technology is fixed wireless connection in home and magnify broadband services[3][4].

In 4G technology, we have very good features in more applications. The few services such as Smart IoT, AI that could not make in the previous generation. We need more data capacity and faster data which is required in few fields such as AI, big data, and smart IoT. It has a better connectivity to allow cross platform devices to speak to each other intelligently with data rate, connectionless services. The important three aspects are data transfer rate is faster in peak time, undisturbed connection, bandwidth free and fast data transfer for mobility [5]. 5G network has more features such as reliable, faster than 4G network. The data capacity is up to 10Gbps. The CDMA and BDMA are the two types of multiplexing used in 5G technology. The frequency is from 3 to 300 Ghz. The handoff supported is horizontal and vertical. The major features of 5G technology is lower battery consumption, lower latency, the applications combined with AI, it supports multimedia capability with AR/VR, more security, high data transfer rates are shown in Fig.1.

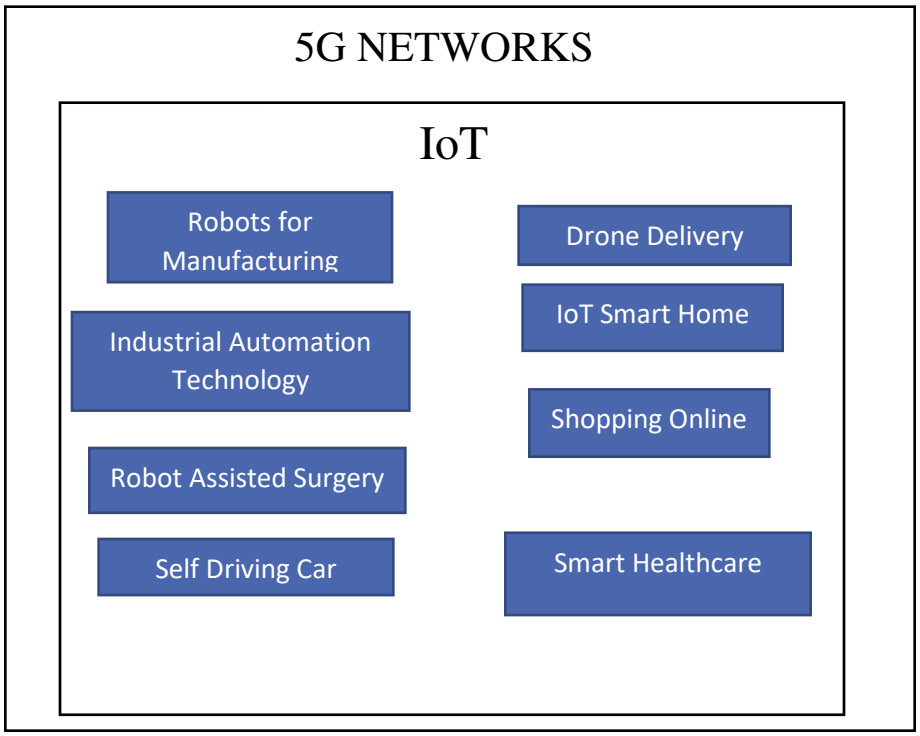

Fig.1 Features of 5G

1.1. Blockchain technology Overview

Blockchain allows a shared ledger with more secure management, in the network each transaction is stored and verified without any central authority. Blockchains are more secure when a transaction of a block is recorded. The blockchain has collection of blocks which is arranged in a chain. Each block chain is more secure by a cryptographic hash function. A block is added after verifying with all the blocks from the blockchain[6]. After validating a new block is added. The blockchain is categorized into three categories, private, public, permissioned and consortium blockchain. The advantages of blockchain has minting, increased capacity, security, immutability, faster settlement, decentralized system [7][15]. The core components of blockchain technology is node, transaction, block, chain, miners, consensus. The important key components of blockchain technology is summarized as follows:

Data block:

They are records of cryptocurrency transaction data. Blocks are linked to each other to form a blockchain. They appear in chronological order. Every block has a cryptographic hash of its preceding block.

Distributed ledger:

In Distributed ledger, each database is shared and replicated in peer-to-peer network. Each transaction is recorded by distributed ledger which is similar to the process of exchanging the data in the network participants. Within the blockchain ecosystem the database is shared for all the participants in the network. With the help of consensus mechanism all the participants in the network can achieve with agreement [8]. No outsider is required to play out the transactions in a distributed environment. Example, if a person joins in bitcoin applications, he should follow all the rules and regulations of the bitcoin application programming code. Any transactions can be exchanged with other members automatically without any third-party interaction [9]. Each record has a one-of-a-kind protected mark with timestamp in the distributed ledger. Due to this cryptographic signature which makes the ledger immutable and auditable.

Consensus algorithms: Consensus algorithm is a process of single data block among multiple unreliable nodes. Bitcoin blockchain is the example for the consensus applications.

Smart contracts: A programmable application which is run on a blockchain is called as smart contracts [10][11].
Decentralized:
This network is decentralized meaning no station is controlling or having no governing authority.
Cannot be corrupted: When a transaction is to be added then each node to be verified. After validating the node, it should be added in the ledger.

Enhanced Security:

As it eliminates the requirement for central authority, nobody can basically change any attributes of the system for their advantage.

1.2 5G and Block chain

Now a days, more IoT devices are connected and transfer the information through the communication channel without any user interaction. Due to this the data which is shared is not secured, data loss, connectivity issues etc. The connectivity issues are solved by 5G technology. In 5G IoT architecture has few issues such as scalability, security, network management, authentication, identity, lack of standards, interoperability. Few security issues are solved by blockchain technology [12]. In 5G technology, the blockchain has been interconnected with more IoT networks to provide more new chances to do more assistance and applications in new technology [13].This section has discussed about the blockchain for 5G IoT Applications [14][15]. The blockchain will support many applications are smart healthcare, smart city, smart banking, smart transportation, Smart grid, Smart Home, Manufacturing Industry, Internet of vehicles, Supply chain, Smart Agriculture, Smart Schools, Virtual Reality, Smart Contract which will be discussed as follows in fig.2.

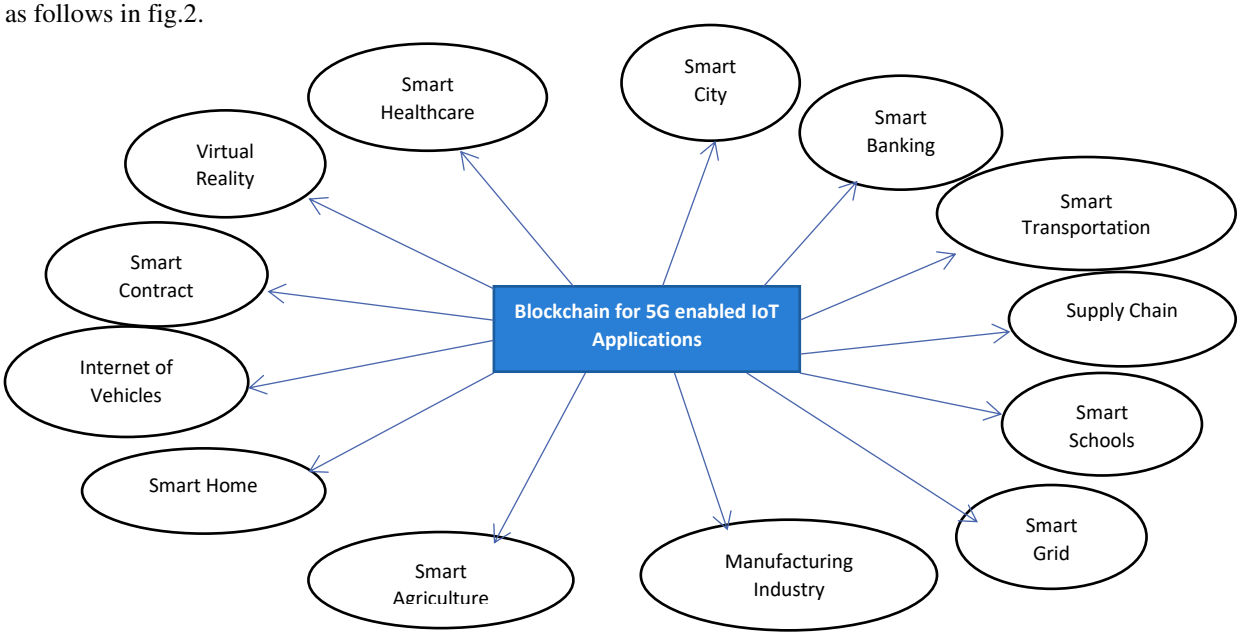

Fig. 2 Blockchain Applications

Smart Healthcare

Health care is an industrial sector where associations and clinical organizations give medicinal services administrations, medical equipment, medical coverage to encourage social insurance conveyance to patients. The integration of blockchain with 5G technology can propel current health care system and give more execution benefits

as far as better decentralization, security, protection, system simplifications for lower operational expenses. Blockchain can fuse with 5G advances. The softwarized framework can perform arrange works through NFVs, which advance IoT correspondence, while distributed computing can bolster quick social insurance conveyance administrations for early identification of patient wellbeing conditions. In such a 5G medicinal services situation, blockchain is utilized to manufacture a distributed database framework which can approve and record all exchanges (for example social insurance demand, understanding information) and store changelessly them in decentralized records. The job of blockchain in this work is to manage wellbeing information interoperability and security issues, for example, empowering powerful approved cooperation among patients and social insurance suppliers (specialists, insurance agencies), and conveying persistent information safely to an assortment of associations and gadgets.

Healthcare data should be more secure and should be more privacy. This data should be restricted from modification and destruction of stored data. If unauthorized person accessing the data then the data will be sold or misuse the data. In 5G technology, the size of the healthcare data increases, so the security mechanisms to protect the data should be also compelled.

2.Related work

The 5G technology is more benefits in more applications. One of the important applications is healthcare systems. The healthcare systems can be remote monitoring the patients. The information about the patients will be send to the care taker without any delay. This 5G technology deliver the information with high speed without reducing latency. This proposed system discusses about how to secure the data which is transform from patient to healthcare providers by using blockchain in 5G technology.

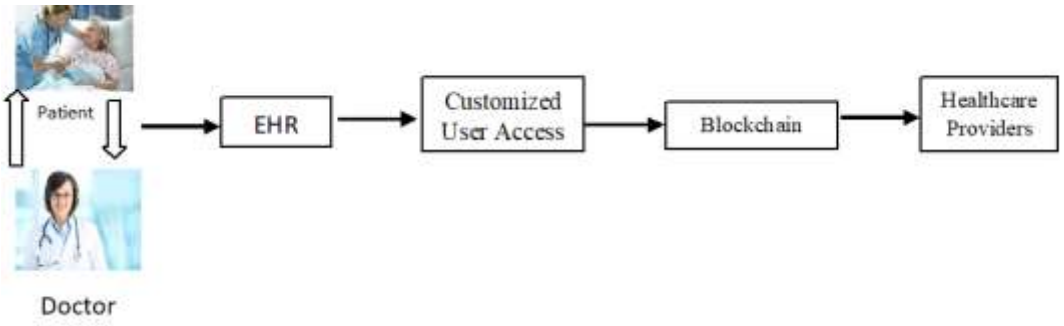

Fig.3 Architecture of Existing System

The data is generated from the patient and the doctor interaction. The primary data has medical history, current issues about the patient. The primary data has the medicines history, nursing care, reports about the patient. In the customized user access, it gives preference to the owner to access the data[16][17].

If the data is changed by unauthorized users then the medical suggestion and drugs suggested by doctors will leads to serious consequences, such as cause death, poisioning etc[18]. To avoid this issue more security is needed while transmitting and receiving the data. This proposed work focus on how securely data is transmitting and receiving and also it will avoid the man-in-the -middle attack. In the existing work, the primary data is generated from the patient and the doctor interaction[19][20]. The primary data has medical history, current issues about the patient. EHR has the medicines history, nursing care, reports about the patient. In the customized user access, it gives preference to the owner to access the data is shown in Fig.3.

More algorithms have already proposed for securing the health data using block chain techniques. A novel approach key management algorithm used to secure the healthcare data [21][22].

3.Proposed System

In 5G technology, millions of IoT devices are connected together and transferring the data to another device. If more data is transferring from one device to other device, it may lead to failure or less secure transmission. To

secure this data transmission more security algorithm is proposed. This proposed system discusses about how the data transmission is secured using blockchain in healthcare applications. Healthcare data should be more secure and privacy. Privacy means the person should have the rights to access or disclose personal information. In privacy itself assign who should be allowed to access the data.

In particular, the objectives are:

1. To reduce the computation time and encryption time
2. To design authentication protocol for protecting data transfer with less storage.

3.1 System Architecture

In this architecture, the patient is monitored remotely using healthcare IoT devices. These devices sense the patient such as heartbeats, Sleeping conditions, pressure, glucose level etc. These data is monitored by doctor and store in the cloud using blockchain. The data which is received should be verified from the authorized device. The patient can share his data with other hospitals also. Deployment of Smart Contracts is used to secure the transaction which is stored in the blockchain. In the architecture diagram, the entities used are patient, Cloud, Hospitals, agencies. Each patient is assigned by a patient id and each transaction about the patient is stored in the cloud. With the help of keys, the record can be accessed by the healthcare providers. This proposed system focus on how the data is stored securely and how it is accessed with more secure is shown in Fig.4.

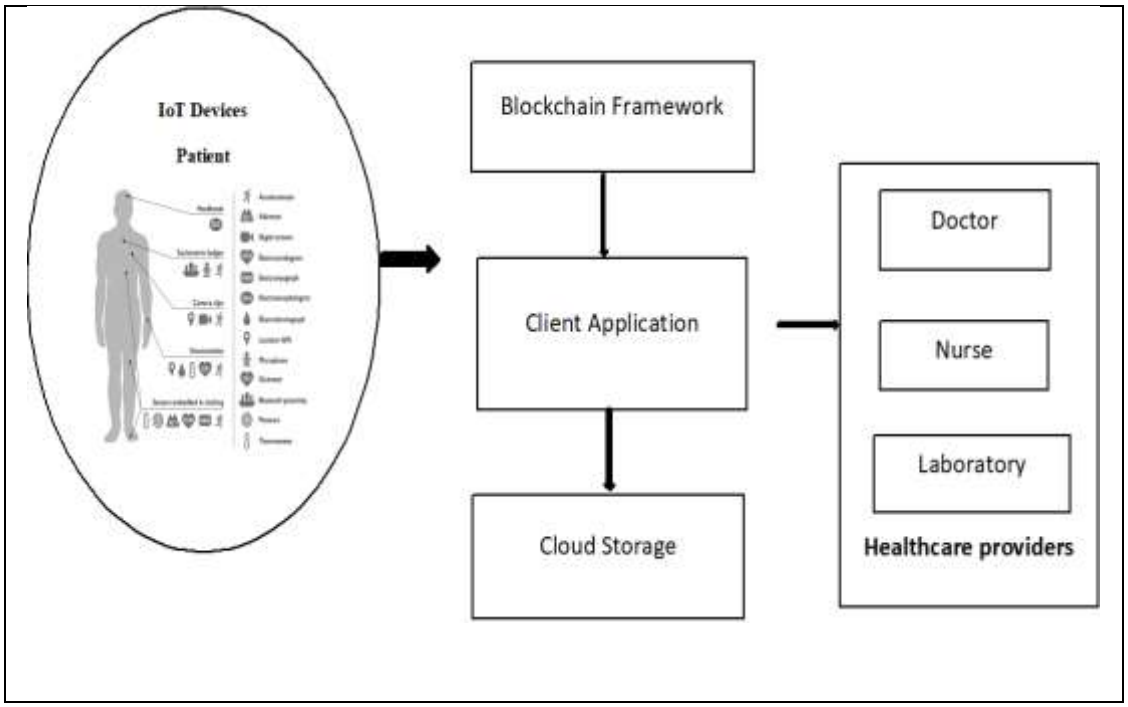

Fig. 4 Proposed architecture

The privacy is achieved by storing the records in encrypted format. The Hospitals/Agencies which wish to read the health record should approach the patient with their identity. Patient generates the key using **algorithm** and securely shares the key with the third party and shares the record.

Patient identity is a complex problem within healthcare, as a patient may registered multiple times with different accounts at same or different hospitals. This leads to fragmentation.

When the patient is in an unresponsive state, the key escrow technique will be used to solve the problem of accessing the record.

The record storage will be (Patient Id, Record, Record Hash, File Id, Date, Doctor Id, Disease Id, Parent record hash). The record structure of a patient is { patient id,data,hash1,fileid}. The record structure of a hospital/doctor {Hid/Did, key}. The Record transaction(hospital) has {Patient address, Service provider access, Record hash, File identity, Patient consent, Timestamp, Signature}. The key transaction(user/patient) is {Hospital/patient address, Public key, timestamp, signature}

3.2 Logical Flow Execution between patient to cloudserver using Blockchain

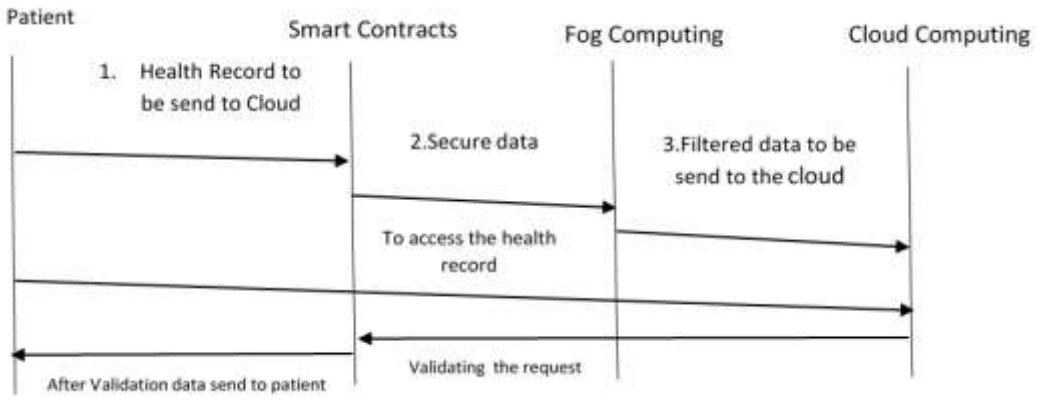

Fig.5 Logical flow execution between patient to cloudserver using blockchain

In Fig.5, the patient data should be stored in the cloud by using smart contracts. All the data is secured and stored in cloud. The filtered data to be send to the cloud. To access the health record with the help of proper validation the data is send to the patient or user who is requesting**.**

Algorithm:

Key Generation

In this proposed technique an ECC algorithm is used to achieve the security in blockchain using two parties P and Q . It has two points A and B.

- The parties contain the key A and B.
- P send a request message to Q. (message has its key A and B)
- Q accepts message from P
- calculates the value κ

$$\kappa = \frac{Y_B - Y_A}{Z_B - Z_A} \tag{1}$$

- Q computes the C value κ
- Q send message to P. (message has id and C value).
- C value is computed as :

$$Z_C = \kappa^2 - Z_A - Z_B \tag{2}$$

$$Y_C = (\kappa Z_A - \kappa Z_C) - Y_A \tag{3}$$

- P checks the C value.
- If it is equal, then P sent data to the Q.

```
function Assignkey ()
{
        if patient confirm data over blockchain then
        Generate a key K using ECC
        A<- Get values from ECC_Database
        a sends a Req message with A and B values appended to it

        b computes K from A and B

        b sends a reply with C
        Node a checks the C

        If

        {
                C=A+B

                Retum 1

        else
                Do nothing
        }
}
```

4.RESULTS AND DISCUSSION

The proposed system is discussed and the experimental results is evaluated is shown in table.1. Results are shown for performance latency, throughput, communication overhead etc.

Parameters	Value
Number of Patients	500
Total Record Size	2.5GB
Avg.Patient Record Size	50KB
Key Generation Algorithm	ECC
Blockchain size	667 GB

Table 1. Experimental Setup

The two performance metrics are used in this proposed system. The two metrics are communication overhead and computation overhead.

Communication overhead:

Number of messages and the total data need to be exchanged is calculated in communication overhead.

a) Number of exchanged messages:

The proposed system is compared with two algorithms RSA and Diffi hellman. The proposed system uses ECC algorithm. The ECC algorithm has less messages are exchanged are shown in Fig. 5. The number of messages exchanged is 6 for one transaction in proposed system. But in RSA and Diffi hellman has more messages are exchanged when compared with ECC algorithms is shown in Fig.6.

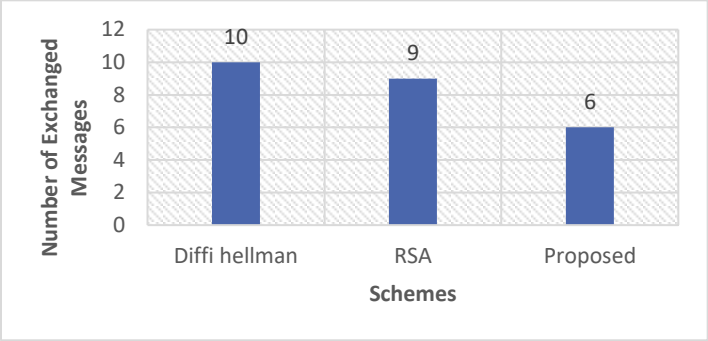

Fig.6 Number of Exchanged Message

b) Amount of data:

The amount of data used in the proposed system has occupies two bytes for identifier, q has 20 bytes, elliptic curve point occupies 20 bytes,for signatures occupies 20 bytes, and timestamp has 5 bytes. The proposed system decreases the no. of messages and the amount of data required to be exchanged is very less when compared with other algorithms is shown in Fig.7.

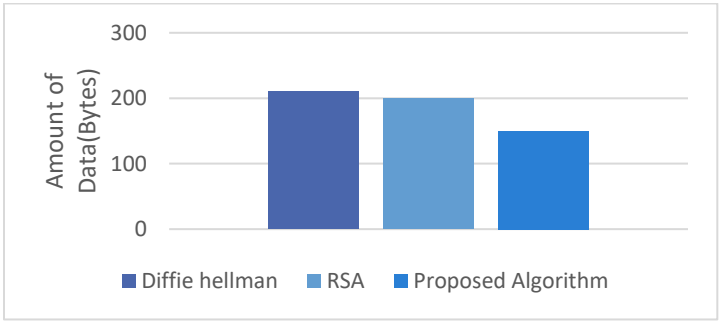

Fig.7 Amount of Data Transferred

Computation Overhead

The computation overhead is the time required for the 5G node to compute the required functions that are used in the authentication procedure. which decreases the congestion in the core network and decreases the security risks is shown in Fig.8.

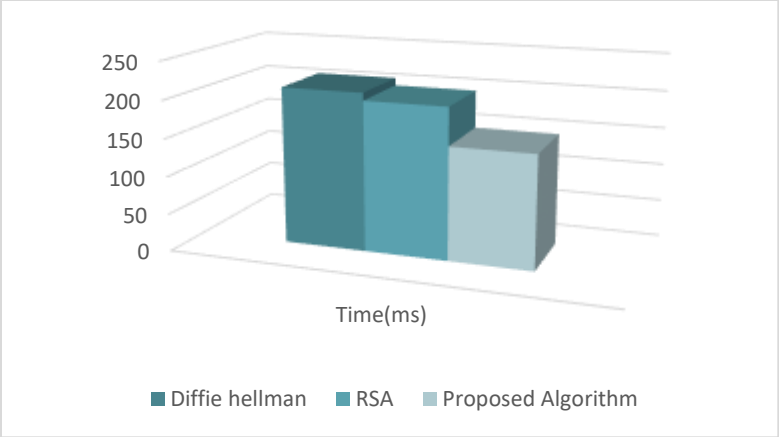

Fig.8 Computation Overhead

5.Conclusion

The 5G network has millions of IoT devices are connected. The Blockchain technology is one of the new technology used in more fields such as online payments, healthcare, smart contracts etc. Extending the technology of block chain to Internet of things (IoT) can have more features. The important issues in 5G technology is security. This data should be more secure using blockchain technology. The proposed system is to secure the data in smart healthcare systems using blockchain in 5G networks using the ECC algorithm. The proposed work is compared with the existing algorithms such as RSA and Diffie hellman. The two metrics are used to compare the performance. The proposed method secure more compared with the other algorithms.

Declaration

Funding: Not Applicable

Conflicts of Interest: Not Applicable

Availability of Data/Material :Not Applicable

Code Availability :Not Applicable

References

1. Panagiota D. Giotopoulou, The evolution of mobile communications: Movingfrom 1G to 5G, and from human-to-human to machine-to-machine communications, Nationaland Kapodistrian Universityof Athens, School of Science, November 2015.
2. Bharti Kalra and D.K. Chauhan, "A Comparative Study of Mobile Wireless Communication Network: 1G to 5G", *IJCSITR*, vol. 2, no. 3, pp. 430-433, July-September 2014.
3. Vivek Sanghvi Jain, Sanchit Jain, Lakshmi Kurup and Aruna Gawade, "Overview of Generations of Network: 1G 2G 3G 4G 5G", *IJCTA*, vol. 5, no. 5, pp. 1789-1794, September-October 2014.
4. Mohammed Alnaas, Elmabruk Laias, Saleh Alghol and Hosian Akeel, "An Overview of the Development of Mobile Wireless Communication Technologies", *American Journal of Computer Science and Engineering (AMCSE)*, vol. 5, no. 2, pp. 22-29, April 2018.
5. C. Jarray, A. Bouabid and B. Chibani, "Enabling and challenges for 5g technologies", *2015 World Congress on Information Technology and Computer Applications (WCITCA)*, pp. 1-9, 2015.
6. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5g security challenges and solutions", *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, 2018.
7. S. Li, L. Da Xu and S. Zhao, "5g internet of things: A survey", *Journal of Industrial Information Integration*, vol. 10, pp. 1-9, 2018.

8. A. Tabassum, M. S. Mustafa and S. A. Al Maadeed, "The need for a global response against cybercrime: Qatar as a case study", *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1-6, 2018.
9. S. K. Routray and K. Sharmila, *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 1-5, 2017.
10. M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman et al., "Blockchain technology: Beyond bitcoin", *Applied Innovation*, vol. 2, no. 6-10, pp. 71, 2016.
11. A. A. Zaidi et al., "OFDM numerology design for 5G new radio to support IoT eMBB and MBSFN", *IEEE Commun. Stand. Mag.*, vol. 2, no. 2, pp. 78-83, Jun. 2018.
12. D. Gomez-Barquero, D. Navrátil, S. Appleby and M. Stagg, "Point-to-multipoint communication enablers for the fifth generation of wireless systems", *IEEE Commun. Stand. Mag.*, vol. 2, no. 1, pp. 53-59, Mar. 2018.
13. A. Höglund et al., "Overview of 3GPP release 14 enhanced NB-IoT", *IEEE Netw.*, vol. 31, no. 6, pp. 16-22, Nov./Dec. 2017.
14. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," Journal of medical systems, vol. 42, no. 7, p. 130, 2018.
15. A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," Sensors (Basel, Switzerland), vol. 19, no. 2, January 2019. [Online]. Available: http://europepmc.org/articles/PMC6359727
16. A. Reyna, C. Mart´ın, J. Chen, E. Soler, and M. D´ıaz, "On blockchain and its integration with iot. challenges and opportunities," Future generation computer systems, vol. 88, pp. 173–190, 2018.
17. Yang Y, Ma M. Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Reencryption Function for E-health Clouds[J]. IEEE Transactions on Information Forensics and Security; 2016. pp.746–759
18. Li M, Yu S, Zheng Y. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24 (1):131–143.
19. Sun J, Wang X, Wang S, Ren L (2018) A searchable personal health records framework with finegrained access control in cloud-fog computing; PLoS ONE 13(11): e0207543. https://doi.org/10.1371/journal.pone.0207543 PMID: 30496194
20. Sun J, Ren L, Wang S, Yao X (2020) A blockchain-based framework for electronic medical records sharing with fine-grained access control. PLoS ONE 15(10): e0239946. https://doi.org/10.1371/journal.pone.0239946.
21. S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, 2017, pp. 464–467.
22. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on. IEEE, 2017, pp. 618–623

Figures

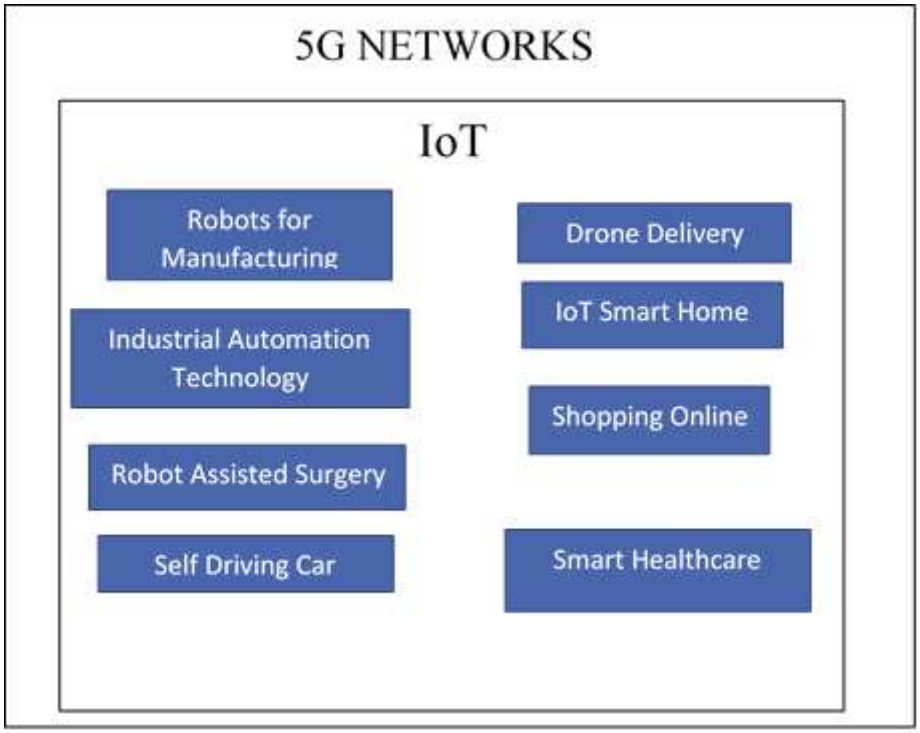

Figure 1

Features of 5G

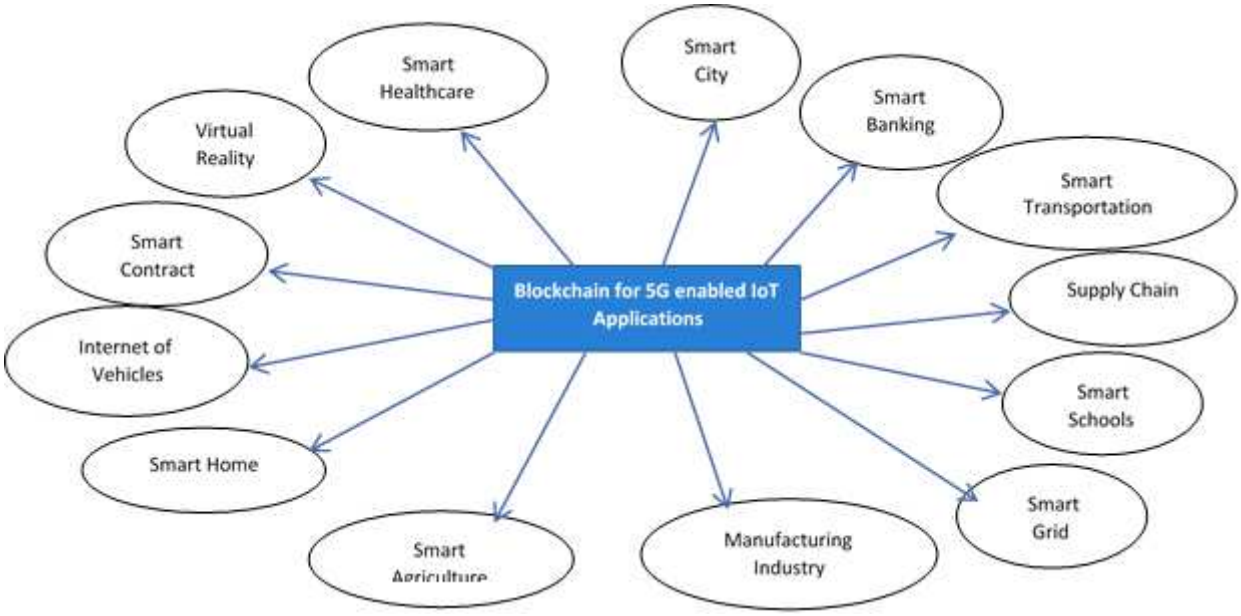

Figure 2

Blockchain Applications

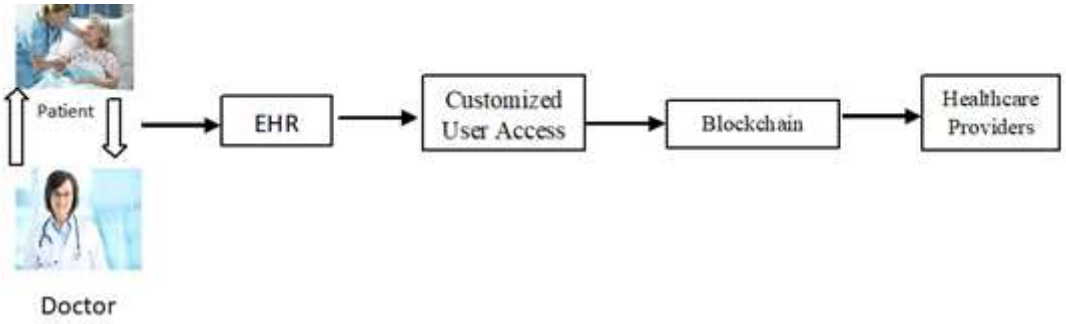

Figure 3

Architecture of Existing System

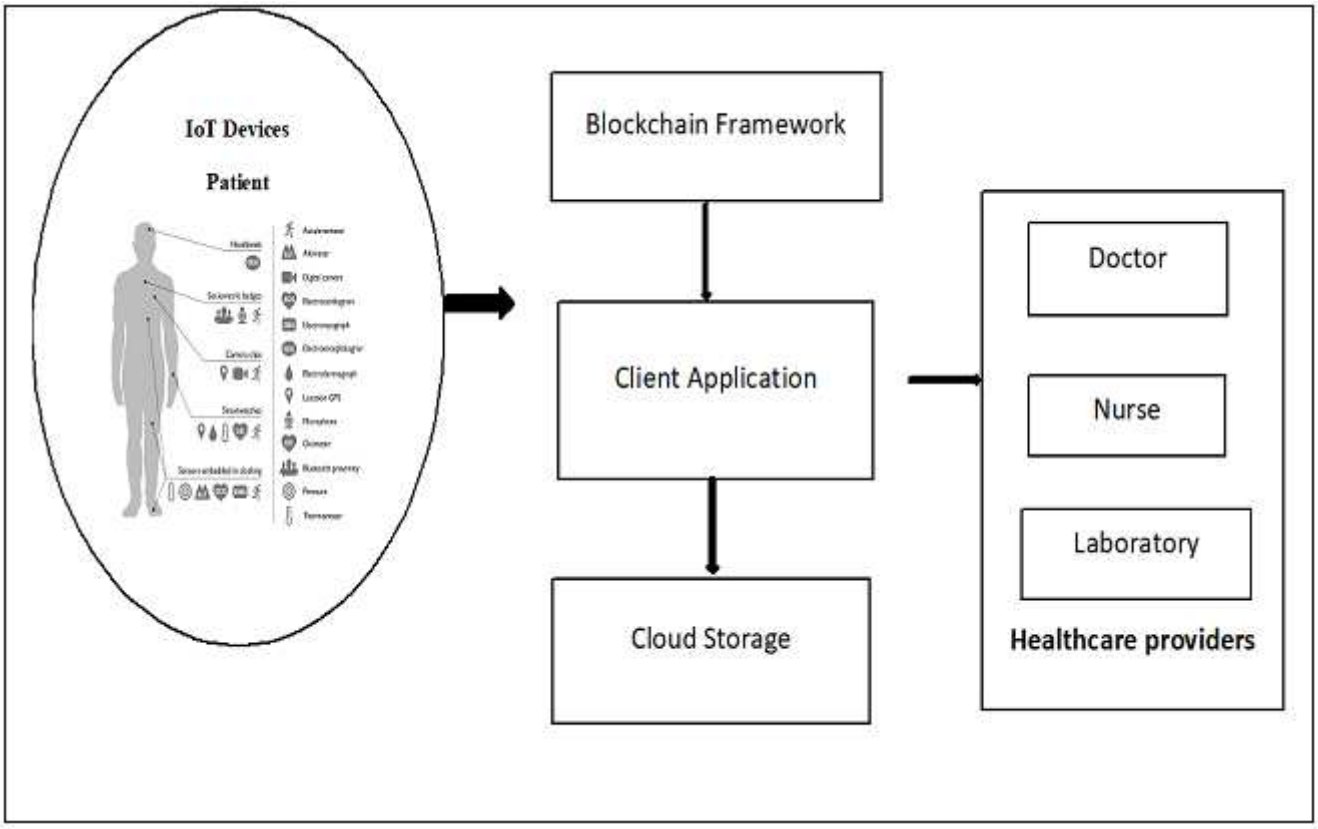

Figure 4

Proposed architecture

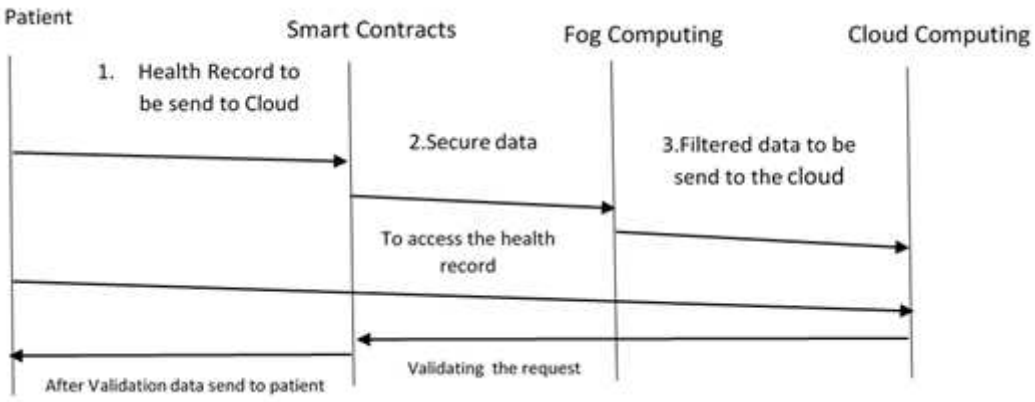

Figure 5

Logical flow execution between patient to cloudserver using blockchain

Figure 6

Number of Exchanged Message

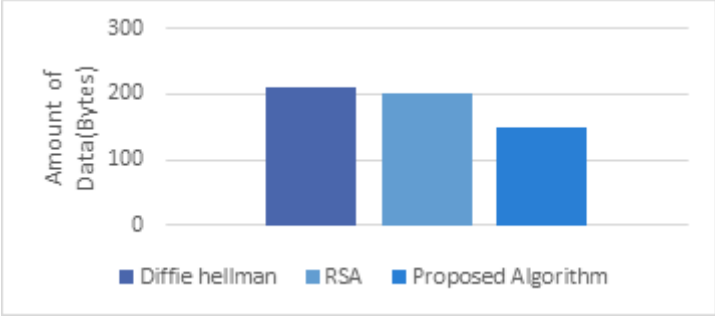

Figure 7

Amount of Data Transferred

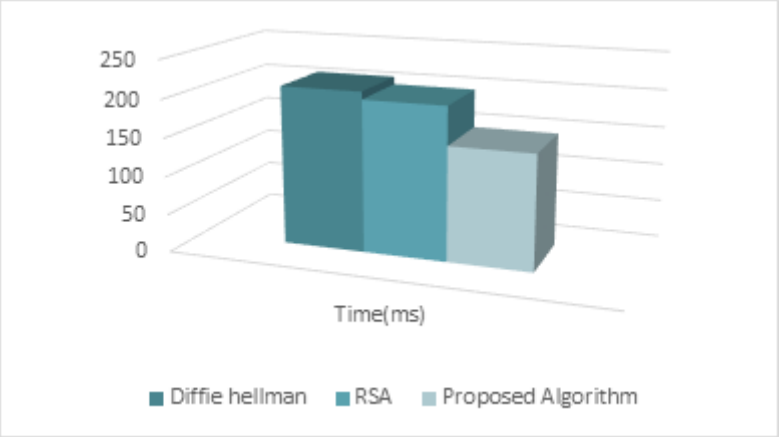

Figure 8

Computation Overhead