DIGITAL HEALTH CARE SYSTEM FOR MEDICAL REPORT/CERTIFICATE SHARING

Student, Komal S. Raut, Final year ME, Dept. of Computer Science Engineering,
Sipna College of Engineering and Technology, Amravati,Maharastra , India.

Abstract— The health care services industry is always showing signs of change and supporting new advancements and advances. This paper describes our blockchain architecture as a new system solution to supply a reliable mechanism for secure and efficient medical record exchanges. It is going to revolutionize the e- Health industry with greater efficiency by eliminating many of the intermediates as we know them today. Digital Health Care (DHC) reform suggests a new consumer paradigm in data and information processing. Here user can distribute or access of network collaborative cares to centralized repository of personal health records.

The new approach in this paper is to explore the Advanced Block-Chain paradigm for e-Health record keeping and while addressing the special needs of patient privacy. As society is moving towards peer networking and on-line practices, we are going to combine the best parts of two worlds in both the healthcare regulation and the technology revolution while formulating advanced solutions.

Keywords— Block chain, Medical Report Data Accessibility, e-Health system, reliability, security; blockchain, architecture.

I .INTRODUCTION

The Block chain is the fastest growing technology through various applications in a secure manner. The various implementations make use of block chain technology among stakeholders. Banking, healthcare services, and supply chain management utilize this technology for its immense potential and secure data sharing management. Mainly, block chain technology plays a major role in the medical and healthcare system. Because of the decentralized and distributed technology, Block chain provides security services inhealthcare. Block chain innovation deals with the human service administrations to give secure information sharing among different partners, information interoperability, adaptable and speedy charging.

In Today's world, the technology has a rapid growth in its upcoming future with a widespread digital transformation by making a better replacement every day. Internet of things, detecting advancements, and 5G are the quickest developing innovation gives a markable commitment to human service administrations. The centralized design in current health care services is not so secure among the various medical services, which provides a delay in accessing the data and it has a major risk in leakage of information. In such a case, the medical reports can be archived without the knowledge of the patient. Accessing the data in a secure manner within the network is the major issue in current health care maintaining system.

For accessing the data, Block chain is the efficient way and a promised technology. Electronic, Health/Medical Record (EHR/EMR) is the current online healthcare serviceswhich play a key role in maintaining and storing the data, which has a major issue in leakage of patient 's information. In block chain technology, the information is stored as a ledger feature which can monitor the patients in accessing the medical records. This becomes the major reason for the development of Block chain technology. In Block chain technology, not only provides security and easy accessibility, but also gives other production elements in the administrations and furthermore pursues privacy, respectability, and verification.

The purpose of our e-Health research program is to develop next generation healthcare digital service solutions to improve patient outcomes, decrease costs, and address the complexity of challenging e-Health problems in security, reliability, efficiency and flexibility. As demands of healthcare spending outgrow many countries' GDPs, there are urgent needs to adapt the e-Health technological services to meet the demands not only in numbers but also in improvement of social interactive norms. Recent advancements in e- Health research have enabled interoperable and scalable networking, applications, and services for effective sharing of electronic health records, flexible data representation including semantic metadata, and more efficient services that access such health data[1].

I. LITERATURE REVIEW

There have been a variety of research studies associated with efficient utilization of block chain in healthcare. Electronic medical remedy approaches for manual and remote access of medical reports and protecting the privacy of the records are the most essential fields of application where Block chain technology can create value. The MedRec in which a decentralized method for utilizing block chain mechanical skill is received to deal with the EHR/EMR and furthermore gives a potential contextual analysis of block chain usage in social insurance, which gives a model to EHR/EMR. Moreover, MedShare gives the trustless method for sharing the clinical reports among an assortment of specialist organizations utilizing block chain. Thus, the examination network characterizes the exceptional systemsfor accessing the records safely utilizing block chain innovation [2].

The medical report of a patient is viewed as relatively sensitive and wants a secure and safer ability to guard the data. In this manner, the putting away, sharing and overseeing restorative reports can be executed in secure ways. These problems are already proposed by using a number of mechanisms, for example, numerous authentication schemes, which leads to fulfilling the need of efficient and secure access of medical reports, manageability, and other safety requirements. These options had been useful in providing a variety of protection necessities under preferred healthcare scenarios. But these strategies in current healthcare technology are no longer enough due to the fact the patient has been exploited by means of various entities via distinct means except their consent. This is to discover a variety of security solutions based on block chain based health care approaches [3].

II. Proposed Work

A) Architecture

Block chain reports verification system was developed based on relevant technology. The system's application will be programmed on the public block chain platform. In the system, three groups of users are involved in the system Doctor1 (who issue reports), Doctor2(who uses/analyze reports) and patient, have access to the system. When patient meet with any diagnosis then doctor1 will generate its report based on its medical tests and based on treatment given to him. After generating documents and reports that can be shared with its authenticity.

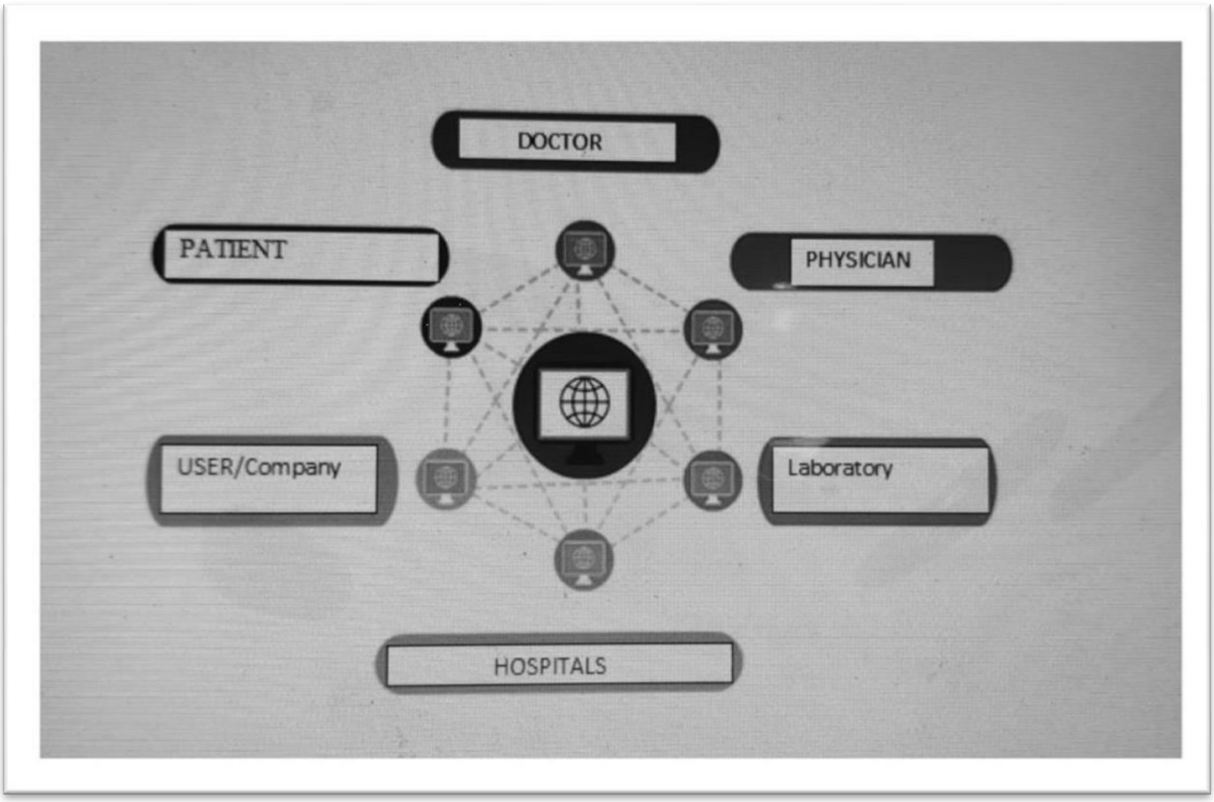

Fig. 1: Working Mechanism

The project implement detail is as follows:

- Firstly, the patient goes under diagnosis and generates health records like verity of medical test reports, existing hereditary problem details, current disease treatment details etc. Users can also going to generate some documents medical certificate/ treatment Result or any other documents through the diagnosis treatment system. Then the patient requests for the medical reports, certificate, medical related document, treatment related documents, prescription from doctor. The Issuing authority (doctor) verifies the credibility of the patient and grants the particular file or document.

- Secondly, the granted certificate/document will be uploaded to web portal and its respective hash code is generated. This uploaded document can shared with the help of sharable link.

- In next step after successfully uploading document on web portal its generated hash code will be upload in the block of public block chain by authority (doctor), once the documents hash is stored in the block they become impossible to fix or to modify by anybody. While uploading data in the block of public block chain it will be done with some patient id which will be unique and constant for patient for overall its life spanof patient. The patient id can be it's adhering number or its permanent mobile number.

- In Fourth step, any other doctor (doctor 2) or any other user which inquiries for verification of documents medical reports that can be shared easily and validated effectively. This can be done by downloading each and every certificated from web portal and its hash will be generated again once this new hash is generated this hash has to be match with previously generated hash value which is uploaded by authority(doctor) so that proves validity of documents with easy share ability.

- In case of alteration of any documents data by patient or any other intruder then the new hash value will be different from original one so this will leads to detection of document forgery.

B) Importance of block chains in healthcare

The advantages of blockchain technology, according to the National Institute of Standards and Technology (NIST), include its tamper-resistant nature, the decentralizednature of the digital ledgers, and the impossibility of changing a published transaction subsequently within the user community that shares the ledger. This technology is also called digital ledger technology (DLT). Key concerns with blockchain applications in healthcare include:

- Network infrastructure security at all levels
- Identity verification and authentication of all participants
- Uniform patterns of authorization to access electronic health information

DLT can be applied in many healthcare areas, but all activity within healthcare is not linked to transactions. However, public blockchains cannot be used to store private information such as identifying health data, because the data in them is widely accessible. This transparency mandates that providers consider privacy issues to ensure protected health information (PHI).

Secondly, blockchain technology is vulnerable to some types of attacks, though it offers inbuilt protection against others. The blockchain code lays it open to zero day attacks and bugs, as well as social engineering. Thus, information security must be paid intensive attention especially when used in healthcare.

Blockchain technology should not be used indiscriminately in healthcare, since its data is immutable. Large files, or those which change often, may be kept out. All identifying data should be kept off the chain. DLT experts comment, ―With new regulations on the rise, such as the General Data Protection Regulation (GDPR), in conjunction with regulations that have been around for more than a decade, such as HIPAA, patient privacy is now a standard when considering processing any form of PHI.‖

The benefits of using blockchains, relative to traditional methods of healthcare database management systems, include decentralized management, unchangeable databases, data provenance, traceable data, robust data, availability of data to any authorized user, while keeping it out of the hands of unauthorized users by encryption that is dependent on a patient's private key.

C) Importance of Ganache Software

Ganache is used for setting up a personal Ethereum Blockchain for testing your Solidity contracts. It provides more features when compared to Remix. Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development. You can use Ganache across the entire development cycle; enabling you to develop, deploy, and test your dApps in a safe and deterministic environment. Ganache is a personalized blockchain for Ethereum development. It can be used to run tests, execute commands, and inspect states while controlling how the chain operates.

It allows developers to use a private Ethereum blockchain and have full control over it. On this local blockchain users can run tests, execute commands, and inspect state while controlling how the chain operates. There the developers have the ability to perform all actions that they would do on a testnet or mainnet even without an internet connection. The tool provides convenient functionality such as advanced mining controls and a built-in block explorer. Ganache can show the accounts, transactions, mnemonic phrase, and all otherimportant things. There are two versions of this local blockchain – one with graphical interface and Ganache-CLI (with Command Line Interface). Many developers find Ganache useful for smart contracts' testing and this tool with yummy name is becoming more and more popular.

D) Blockchain

A blockchain is a data structure where the records are stored in a linked sequence of blocks. This sequence forms a distributed ledger, which means it is replicated in multiple machines, called nodes, that communicate to one another. The nodes form a peer to peer network where every update to the ledger must be accepted by the network using a consensusprotocol. The consensus protocol assures that everybody has the same view on the status of the system.

The technology was introduced in 2008 as the foundation of a cryptocurrency called Bitcoin, with the aim to solve the double spending problem and allow value exchange between peers without the mediation of a third-party central authority. In fact, before Bitcoin,it was impossible to securely transfer value online, from one party to another, without relying on a trusted authority such as banks or card issuers. The new crypto currency solved the problem by employing security techniques, including hashing, public keys, and anonymity, inorder to replace the need of trust with cryptographic proof and consensus [4].

E) Algorithms Used

1) Consensus mechanisms

Blockchain presents all the characteristics of a distributed system because the computation is done concurrently by different entities, without the assistance of a global clock. In addition, any process can fail at any point during the execution. According to the theory of distributed systems [2] there are two types of failures: crash (or stop) failure and Byzantine failure. The former is the simplest to assess and consists of a node crashing without resuming, thus leaving the network. The rest of the processes can spot a faulty node because it suddenly stops replying to messages. a consensus process, tolerant to faults, must be in place to ensure the continuity and correctness of the system. In blockchain, the consensus is needed to agree on the total order of transactions and the block that must be added to the chain.

The equivalence between the Proof of Work protocol proposed in Bitcoin and the consensus in distributed systems was formalized in the work of Garay [6]. Therefore, the parties in a blockchain network can be formally considered as replicated state machines that execute logic. The consensus is the mechanism by which the state machines agree on the order of messages sent. This mechanism is usually referred to as atomic broadcast and is needed by the state machines to be able to produce the same output, given the same input. The output can be the same only if the logic is deterministic and identical for each machine. The determinism is also necessary to detect faults: in fact, a replica that produces a different output can be considered as misbehaving [7].

2) Proof of Work

The full description of a proof of work consensus was first introduced as the fundamental way to agree on the order of transactions in the Bitcoin network. It needs a distributed timestamp server to demonstrate that a transaction has come before another and that an entity has not spent the same amount of money in other transactions. The approach to solve this problem consists of finding a value that, when hashed with an algorithm like SHA- 256, presents an output with a number of leading zero bits. In the context of a block, the goal is to increment a nonce so that the block's hash has a number of leading zeros greater than theone required by the system. It has been proved that there is no efficient algorithm to solve this matematical puzzle. Therefore, the only approach is to increment the nonce until the output satisfies the requirements. Finding the solution proves that some work has been done by a CPU and guarantees that a block cannot be modified without repeating the process [5][8].

The time required to solve the puzzle grows exponentially with the number of required zeros. In addition, the longer the chain, the more difficult becomes to change a blockbecause it requires to prove the work for that block and all the subsequent ones. It would be possible only if a set of malicious attackers has a computing power greater than the rest of thenetwork [9]. This implies that a network is secure as long as it is composed by a majority of honest nodes. Blockchain implementations based on proof of work compensate the increase of hardware performances by adjusting the difficulty to the speed of the network: if the number of appended blocks in one hour is too high (computed with a moving average), the difficult is increased, decreased otherwise [10].

3) Proof of Stake

Another set of consensus algorithms is the one represented by Proof of Stake (PoS). It was initially proposed as an energy-efficient alternative to Bitcoin's PoW to reach consensus in public blockchains. In fact, PoW has proven to be incredibly inefficient in terms of energy used as all the nodes in the network must prove the work, but only one is eventually able to add a new block. To solve the problem while ensuring security and decentralization, PoStakes advantage of a group of validators (a subset of the blockchain network) taking turns to propose, vote, and add new blocks to the chain. To become a validator, one has to send a specific transaction that locks its coins into a vault. The vault opens only once the validator has managed to add a block. Therefore the algorithm requires the participants to hold coins (value in the form of a crypto currency) to put at stake to join, as well as to track them [10][11].

IV. IMPLEMENTATION

After the designing of a basic out system we executed many set of test cases for performance evaluation. In first case we choose health record of file size 1 MB, this health record is selected as a document in our system, then hash of the file is calculated also this hash is uploaded to block of blockchain along with document ID. The time required for calculating hash of the file and uploading the hash in the blockchain is measured. The same set of action is repeated for 2MB file size 5 MB file size and for different file sizes which are available in following table 1 and its time required in second is measured.

File Size	Time (Sec)
1 MB	2.18
2 MB	2.75
5 MB	3.24
10 MB	3.67

20 MB	3.88
50 MB	4.12
100 MB	4.35
500 MB	5.14

Table 1: Time required calculating and uploading Hash to block chain

In second scenario the performance evaluation of retrieving block of the information from block-chain is measured. We downloaded different blocks of information which was uploaded in the first case for different file size and here we calculated time required to download block from blockchain and retrieve information from block. Just statistic for different file size and time required to evaluate their information is calculated which is shownin Table 2

File Size	Time (Sec)
1 MB	2.12
2 MB	2.33
5 MB	2.16
10 MB	2.59
20 MB	2.71
50 MB	2.79
100 MB	2.86
500MB	2.97

Table 2: Time required downloading hash from block chain

V. RESULT ANALYSIS

a. Uploading Documents

Following table 1 shows time required to calculate and upload hash of the medical report/ certificate to the block of block chain. It is observe that that time required for the 1MB of the files required 2.1sec where is if we are increasing the file size then the time consumption also increases. But if you are doubling the size of the file then time consumptionis not getting double, It is increasing congratulatory. Comparing with 500 MB file size time requirement is only 5.14sec whereas for 1 MB file size it is only 2.18 sec

Following graph shows time requirement for different file size, after observing the slope ofthe graph it is clear that time consumption is not increasing in the ratio of increasing files size

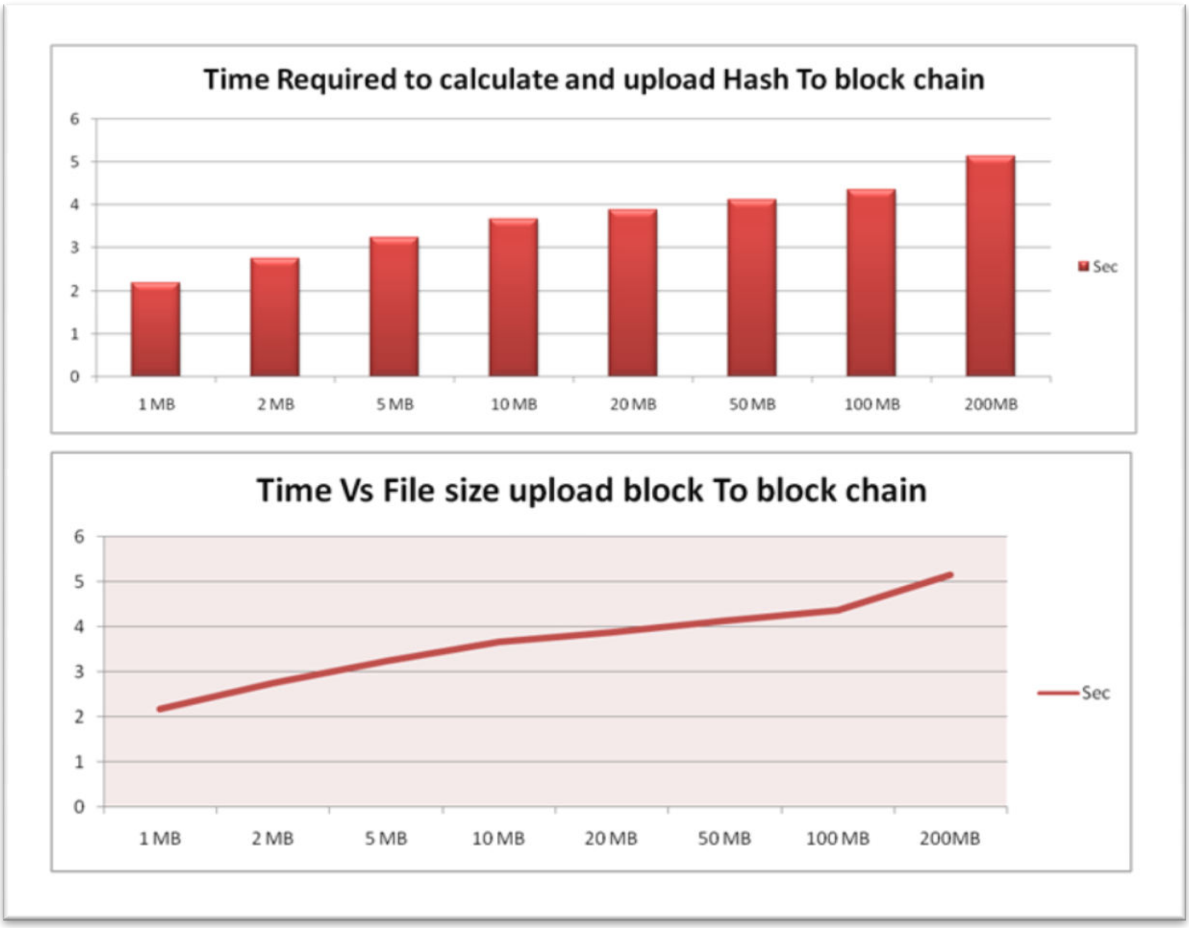

Fig. 2: Time required calculating and uploading Hash to block chain

b. Downloading Documents

In the following figure shows the time required to download Hash from blockchain. In the X-axis represents the different samples of file size and Y-axis represents number of time in seconds for downloading hash to blockchain. doctor uploads the report or medical certificate on blockchain and its calculate hash code in the particular time period, when patients download the result file from website during this process downloading the file inthe particular time period depending on the file size.

Following fig. 3 show time required in to Sec for different file size. It is observed that as file size is increasing then time doesn't increases in each case. Comparing 1MB file size with 500MB file size time required is 2.12 and 2.97sec which is nearly equal only difference is Milisec so we can conclude that time requirement for downloading the hash from blockchain is notdirectly dependent on file size.

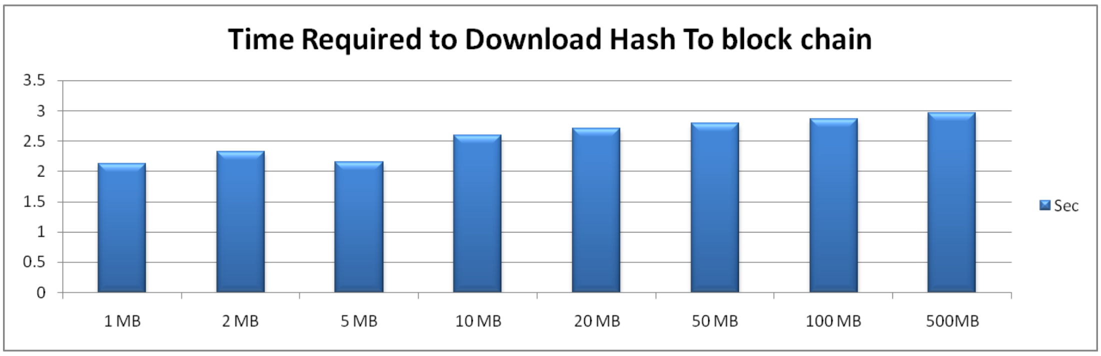

Fig. 3: Time required download Hash from block chain

VI. CONCLUSION

It is concluded that most of the goals which were set for the project has been met by this project i.e. –an authentication & data sharing of medical report using Blockchain security‖ and it is believed that implementation of the project will be able to satisfy the requirement of user.

Thus, the authentication & data sharing of medical report using Blockchain security issuccessfully done.

VII. FUTURE WORK

A distributed ledger where the records are stored in a linked sequence of blocks and are theoretically difficult to delete or tamper with made possible to design and implement new solutions for more failure-resistant applications adopting a distributed and decentralized philosophy, in contrast with the central ones based on cloud infrastructures or even local solutions. The future work includes the extension of the current smart contact and theaddition of others to improve the lookup and support the additional features required by an EHRs management solution.

REFERENCES

[1] M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. C. Wong, –Data security and privacy management in healthcare applications and clinical data warehouse environment,‖ in2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), Feb 2016, pp. 5– 8.

[2] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, –Big data security and privacy in healthcare: A review,‖ Procedia Computer Science, vol. 113, pp. 73 – 80, 2017, the 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017) / The 7th International Conference on Current and Future Trends of

Information and Communication Technologies in Healthcare (ICTH-2017) / AffiliatedWorkshops.

[3] N. Kahani, K. Elgazzar, and J. R. Cordy, ―Authentication and access control in e-health systems in the cloud,‖ in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security ril 2016, pp. 13–23.

[4] M. Braunstein and B. Todd, ―Disruptive Technology in the Healthcare Space‖, GaTech Seminar on technology innovation in the healthcare space, Atlanta, Georgia, on Febuary 10, 2016.

[5] W. Liu, ―Wireless Access and Wireline Integration: OAM&P Architecture with ITU-tML Technologies‖, IEC Broadband Wireless Report, International Engineering Consortium, December 2004.

[6] S. Nakamoto, "Bitcoin P2P e-Cash Paper". Originally published in The Cryptography Mailing List (Mailing list), on October 31, 2008.

[7] W. Liu, ―Digital Health Care (DHC) Information Technology Infrastructure Framework‖, IEEE Consumer Communications Network Conference, Las Vegas, January 2010.

[8] Mary Sumbawa Christo, Amigo Marjoram A, Parthia Strathy G, Piranha C and Raj Kumara M "An Efficient Data Security in Medical Report using Block Chain Technology" International Conference on Communication and Signal Processing IEEE, April 4-6, 2019, India.

[9] M. Mettler, ―Blockchain technology in healthcare: The revolution starts here,‖ in 2016 IEEE 18th International Conferenceon e-Health Networking, Applications and Services (Healthcom),Sept 2016, pp. 1–3.

[10] W. Liu, S. Zhu, T. Mundie, and U. Krieger, ―Advanced blockchain architecture for e- health systems,‖ in e-Health Networking,Applications and Services (Healthcom), 2017 IEEE 19thInternational Conference on. IEEE, 2017, pp. 1–6..

[11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, ―Medrec: Using blockchain for medical data access and permissionmanagement,‖ in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 25–30.

[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ―Medshare: Trust- less medical data sharing among cloud service providers via blockchain,‖ IEEE Access, vol. 5,pp. 14 757–14 767, 2017.IEEE Criteria for Class IE Electric Systems (Standards style), IEEE Standard 308, 1969.

[13] Komal Suresh Raut, “An Authentication & Data Sharing of Medical Report Using Blockchain Security”, International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132x ,V713-2116,Volume-7,Issue-3,2021.