International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

# Secure Social Network Based Healthcare

**Sreedevi B, V.Sellam**

***Abstract*: Healthcare system holds a huge amount of data due to the number of tests taken by the patients and are maintained in physical files or digital files in form of records. At the end of the treatment, a discharge summary of the files will be sent along with the patients. All the records of the patients are maintained in the hospital by MRD (Medico Record Department). Maintanence of records are of very high cost and data security, integrity should be maintained. When patients migrate from one hospital to another, they ought to provide their past records to the doctor for diagnosis. There is a very high probability for the patients to miss their records after many years. A social network based system can be developed in which the patient's data is stored in cloud and can be shared among the healthcare centres. Each hospital can send requests regarding a patients's past records to other hospital and records can be retrieved. This helps doctors to have a greater incite on the reports, and repeated tests are avoided for the search of the missing information. As medical records are very sensitive, security and privacy concerns are high. To secure data, blockchain is used in which the data are stored in off-chain and their hashes are stored on-chain. The data in off-chain are encrypted using Advanced Encryption Standard(AES).***

***Keywords* : *Advanced Encryption Standard, Blockchain, Cloud, Digital files, Medico Record Department.***

## I. INTRODUCTION

Electronic Medical Records(EMRs) has all the patient's clinical data like test reports etc. These records are maintained and managed by a system called Health Information System(HIS). They are capable of creating new EMR instances, store, query and retrieve the desired EMR instance. HIS provides a user interface at the front-end and has either centralised or distributed database at the backend. These records and systems are not feasible enough to provide mobility. These records are not portable with the patients. To provide portability, EMRs and HIS design are formalized. Electronic health Records(EHRs) allow patient's clinical data to move along with patient and be available to multiple healthcare centers.

There have also been initiatives to develop HIS and infrastructures that are able to scale and support future needs, as evidenced by the various national and international initiatives such as the Fascicolo Sanitario Elettronico (FSE) project in Italy, the epSOS project in Europe, and an ongoing project to standardize sharing of EHRs[9],[10],[1]. These provided way for Personal Health Records(PHRs) which provide instant data available to the patients, so that they can view the status of the records and data using a smart phone or a smart watch.

Cloud computing is a very good solution in which these clinical data of each patients can be stored in cloud regardless of any geographical locations. Data sharing between healthcare centres would be made possible by cloud, who all connected in a network. Cloud provides resource elasticity as needed by the hospital and also allows to handle big data by providing big data tools for managing and analysis of the data. Insights can be got from the analysis for research and diagnosis purposes.

Cloud is vulnerable to attacks and hackers can easily hack the data stored in the cloud. Therefore this gives rise to security and privacy concerns. This work presents solution as Blockchain which is a decentralized and distributed technology.

## II. SECURITY AND PRIVACY

Data is an asset which has all potential and it can be misused very easily. Particularly, clinical data are prone to misusing and frauds. As an example, in 2013, Yahoo experienced a data breach that put the information of over 3 billion users at risk, which is almost half of the entire human population. And this incident is just one example of countless data breach events [12]. Electronic Medical Record(EMR) data, suffers great risk. According to an investigation[12], many records being exposed and prone to threat are increasing every year. Healthcare data breaches are occurring at the rate of one per day. To prevent these frauds, privacy protection regulations, such as such as the Health Insurance Portability and Accountability Act (HIPAA) [13] in the United States or the General Data Protection Regulation (GDPR)[9].

There is one obstacle in sharing secure and privacy preserving clinical data:

### A. Data increasing at rapid speed:

Medical data such as X-ray images, genetic data are very large in size and their volumes are increasing at a rate of 20-40 percent every year. In 2015, an average healthcare provider in United States needed to manage 665 terabytes of patient information, 80 percent of which was unstructured medical images. Even worse, it is estimated that big data in healthcare will reach 25,000 petabytes in 2020 [10].

**Revised Manuscript Received on November 30, 2019.**
***** Correspondence Author
**Sreedevi B***, Student Pursuing her Bachelors in Computer Science and Engineering in SRM Institute of Science and Technology, Ramapuram, Chennai. India. Email: bsreedevibala@gmail.com
**Ms. V. Sellam**, Assistant Professor in the Department of Computer Science and Engineering in SRM Institute of Science and Technology, Ramapuram, Chennai, India.

The challenges include not only how to store such a massive amount of data with existing IT infrastructure, but also how to ensure its confidentiality and integrity.[12]

Blockchain can be used as a solution for the securing the clinical data. Blockchain is a public ledger where there is no centralised system. Each patient's clinical data is put in a block and all blocks are chained together. These blocks are immutable and provide high security.

Block chain technology basically works on 3 methodologies:

1) Private Key Cryptography: If two people need to transact over a network, they should hold same keys to decrypt the encrypted data. There are two keys , that is, private and public keys to have a secure digital identity. In this type of cryptology, it is the combination of both public and private keys. It provides strong authentication.

2) Distributed Network: No centralised authority or system. The transactions are controlled and provided to all the members connected to the network.

3) Protocol: Apart from authentication and authorization, certain protocol is involved. That is the consensus algorithm, proof of work which ensures that the next block in the blockchain is trustworthy.

## III. RELATED WORKS

[1] deals with, how the clinical data can be shared among the healthcare centres securely. The methodology used is blockchain. The data is stored in blocks which are immutable. All the medical data of the patients are maintained in the cloud. [2] gives a review of the traditional and recent methods to preserve or secure the medical data. It provides comparisons between the conventional form of securing data by using cryptology and new technology using blockchain. It classifies permission and permissionless blockchain approaches and analyses it advantages and disadvantages. [3] completely deals with the integration of blockchain with cloud to form a blockcloud. It provided all basic concepts of cloud and blockchain and how these two technologies can be combined to give a well secured cloud services and storage.

A record management system called MedRec to handle EMRs using blockchain technology is introduced by [4]. MedRec handles authentication and considers the sensitivity of the information for data sharing. This system encourages stakeholders(researchers, public health authority) to participate in the network as blockchain miners. Rewards are provided to the miners for securing the network by proof of work. A basic view of how cloud can be applied in health monitoring is given in [5]. The data is generated from the wearable sensors (bracelets or chains, etc) and stored in cloud, so that it can be monitored easily and actions are taken accordingly.

The concerns related to the security of Personal Health Records(PHRs) is discussed in [6]. It uses attribute based encryption to encrypt each patient's data before exposing it to the third party servers, that is, cloud. The challenges and opportunities of using cloud for storing healthcare related information is discussed in [7]. It deals with the growing trend of cloud computing technology with healthcare records. A cloud resource mediation service model is proposed in [8]. It plays as a trusted third party role among different tenants using the cloud. The proposed system prevents data leak from one tenant to another and thus having secure sharing of resources across various tenants in the cloud.

## IV. WORKFLOW

It consists of four hospitals, each of which is connected in a network. Each of these hospitals have their patient's reports and record details stored in cloud. Each healthcare centre has their own private cloud as it acts as a separate organisation and the clinical data can be very easily breached.

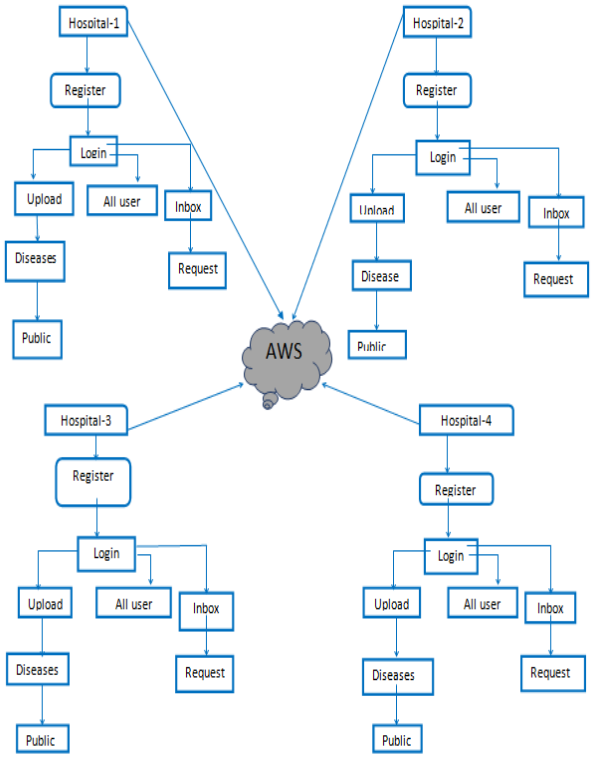


Fig. 1 Flow diagram

Healthcare organizations prefer private cloud as a deployment model. Each hospital stores the treatments of the diseases in cloud and the file owner is the doctor itself. If a Hospital-X needs any information about a patient's report and anything regarding treatment, it can send a request to any of the hospitals (eg. Hospital-Y) and wait for it's response. If only Hospital-Y accepts the request from Hospital-X, the reports and the treatments are sent to the hospital else the request is rejected and the reports are not sent. The acceptance of the request and rejection depends upon the Hospital's policies. If these patient's reports or clinical data are put in a block, these blocks from many patient's forms a blockchain. Therefore all the clinical data transactions from one hospital to another is very safe and secure.

In figure 1, first and foremost, all the hospitals have their own login account and if not, they register it newly. After logging in, request is sent to any one of the hospitals in the network. If the respective hospital accepts the request, then the reports are sent to the inbox of the hospital. The hospital checks its inbox and downloads the report for clinical analysis and to get insights of the past records.

## V. DETAILS OF THE PROCESS

Main aim of this work is to secure the shared clinical data of the patients. There are two parts,in which one is user side and another is admin side. In user side, data in the form of file is uploaded. In admin side, there exist totally four admins in which if the first user needs a file, acknowledgements of the other three members are needed. Only then they are allowed to use the file else the file is not accepted.The main motive is that, if the first user wants the file the other three member's acknowledgement is very important, only then the requester can use the file.

There are five processes- User Interface, Admin uploading details about treatment, Doctor searching for a new treatment, Sending request for a document, Request accepted by authentication.

User interface is the front-end and as a hospital, it has to register in one account under the database concord. After registering, for each and every healthcare center, a private key will be generated automatically. A CSP key will be generated automatically by using random key generation. After registering, as a doctor they have to login with the user credentials. A new researched treatments for any new or old disease can be uploaded with concern from the senior doctors in the hospital. All the process and the treatment methods are made into one document. While uploading, the content is encrypted and a private key is generated. These informations are stored in cloud. After uploading, the date and time of uploading the content is updated.

Any doctor can login using credentials. The new treatments for any new disease or an old disease given by the doctors of various healthcare centres can be viewed. To get those new treatments, a request can be sent from the account to respective hospitals. If those respective hospitals accepts the request, then they might access the treatment document else not. The desired document is chosen and the request is sent to the file owner. The file owner can accept or reject as it depends on him. If the request is accepted, they can view the document and the public key of the user will be sent to the file owner. For accessing the file, an CSP key and file view key should be entered for authentication and if both were correct then, the user can view the document.

## VI. IMPLEMENTATION

The clinical data can be secured by two methods. One is by using cryptological algorithms and other is by using blockchain. But there are few challenges faced by both of these methods when implementing these methods.

### A. Search on encrypted data

When the clinical data is encrypted and stored in the cloud, it becomes difficult to search the particular patient's record. A healthcare centre may have more than thousands of patient's records and if these all records are encrypted, search for a particular record becomes complicated. To get a record, all records must be decrypted before searching. This arises security and privacy problems. Otherwise, file owners have to send their keys for decryption before executing a query or first download the encrypted data and then decrypt it to execute query. Both these ways are impossible due to security and efficiency reasons.

### B. Immutability of the blockchain

Conceptually, blockchain is secure by design that provides the capability to achieve decentralized consensus and consistency, and resilience to intentional and/or unintentional attacks[1]. Key benefits of deploying a blockchain in this approach are as follows:

1. No need of any third party mediator, thus avoiding single point failure.
2. Patients can have control over their data;
3. Medical history as a blockchain data is complete, consistent, timely, accurate, and easily distributed;[1]
4. Any changes made to the blockchain are visible to allmembers of the network and all unauthorized modifications are easily detected.

But there are few limitations while storing the clinical data in the blockchain. Blocks in blockchain are immutable and once stored can never be altered or deleted. According to Article 17 of the General Data Protection Regulation has strengthened the rights of the individuals to request their personal to be erased[1]. One of the principles of the Organization for Economic Cooperation and Development privacy guideline, on which many data protection laws are based, provides the right-to-erasure to individuals[1]. Due to the sensitivity of the data, any healthcare centre planning to store the patient's data in the blockchain, cannot restrain from this obligation to erase personal data when asked for. But it is impossible in blockchain.

So the better solution is to combine both cryptography and blockchain to eliminate these problems. The concept is, off-chain storage of clinical data, where the data is stored outside the blockchain in the cloud, in encrypted form conventionally and the hashes of the data are stored in the blockchain. So the data stored off-chain can be secured by using Advanced Encryption Standard (AES), can be changed and erased if asked for by the patient. At the same time, the hashes of the clinical data stored in the immutable blocks provide authenticity and accuracy of the off-chain data. Therefore the medical records can never be breached or hacked thus providing high, strong security.

The off-chain medical records are encrypted using Advanced Encryption Algorithm. Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used. This algorithm has its own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software. It is extremely difficult to hackers to get the real data when encrypted by AES algorithm. AES has the ability to deal with three different key sizes such as 128, 192 and 256 bit and each of this ciphers has 128 bit block size. AES performs all its computations on bytes, not on bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes [15]. It uses different rounds for different bit keys. The number of rounds depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key [15].

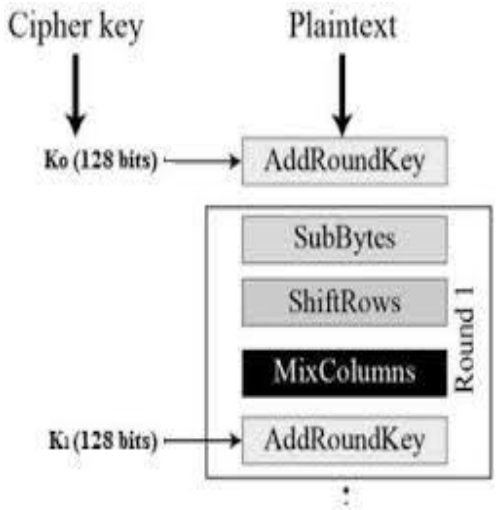


**Fig. 2 AES encrypting rounds[15]**

## VII. CONCLUSION

Medical information sharing with security and privacy has been a challenge. Many traditional methods use cryptological algorithms to secure data. But they are found to be inefficient because the medical data searchability becomes inefficient. As a new paradigm, blockchain has lots of advantages over traditional methods of encrypting. Even though blockchain serves very well in case of security and privacy, there are few challenges regarding record volume, record update and record erasure. As blocks are immutable, they can be used to store only the hashes of the medical data which on the other hand, can be encrypted using the most efficient AES algorithm. Therefore, this system provides a well secure way to transfer medical data from one hospital to another in a network.

## REFERENCES


1. C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, ‘‘Blockchain: A panacea for healthcare cloud-based data security and privacy?’’ IEEE Cloud Comput., vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.
2. Hao Jin, Yan Luo, Peilong Li and Jomol Mathew, “A Review of Secure and Privacy-Preserving Medical Data Sharing” IEEE, p. May 14, 2019.]
3. Nikita Sanghi, Rupali Bhatnagar, Gaganjot Kaur and Vinay Jain, “BlockCloud: Blockchain with Cloud Computing”, International Conference on Advances in Computing, Communication Control and Networking, p. 2018.
4. Asaph Azaria, Ariel Ekblaw, Thiago Vieira, Andrew Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management”2016 2nd International Conference on Open and Big Data (OBD), p.25-30, 2016.
5. Navya M S, A Nihitha, Anjan K Koundinya, “Cloud Based Application for Health Monitoring System Using Wearable Sensors, 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016.
6. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou, “Scalable and Secure of Personal Health Records in Cloud Computing Using Attribute Based Encryption”, IEEE Transactions on Parallel and Distributed Systems, vol.24, 2013.
7. Valentina Casola, Aniello Castiglione, Kim-Kwang Raymond Choo, Christian Esposito,“Healthcare-Related Data in the Cloud: Challenges and Opportunities”, IEEE Cloud Computing, vol. 3, 2016
8. Quratulain Alam, Saif U. R. Malik, Adnan Akhunzada, Kim-Kwang Raymond Choo, Saher Tabbasum, Masoom Alam, “A Cross Tenant Access Control Model for Cloud Computing: A Formal Specification and Verification”, IEEE Transactions on Information Forensics and Security, vol. 12, 2017.
9. (2016). General Data Protection Regulation. [Online]. Available: https://eugdpr.org/the-regulation/
10. W. Raghupathi and V. Raghupathi, ‘‘Big data analytics in healthcare: Promise and potential,’’ Health Inf. Sci. Syst., vol. 2, no. 1, p. 3, 2014.
11. BlockChain, https://en.wikipedia.org/wiki/Blockchain
12. (2018). Healthcare Industry Ranks 8th for Cybersecurity but Poor DNS Health and Endpoint Security of Concern. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/
13. (2017). Summary of the HIPAA Security Rule. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/
14. Coindesk,‖What is BlockChain Technology‖, https://www.coindesk.com/information/what-is-blockchain-technology
15. Advanced Encryption Standard. [Online]. Available:https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
16. Erl-Huei Lu, Kuo -Tsang Huang and Jung-Hui, “Word-Based AES Encryption Without Data Expansion” Journal of information science and engineering 32, p. 2016.


## AUTHORS PROFILE

**Sreedevi B** is a prefinal year student pursuing her bachelors in Computer Science and Engineering in SRM Institute of Science and Technology, Ramapuram, Chennai. She is an academic topper and got academic proficiency award and performace award. She is interested in Cloud computing technology and Big data analytics.

**Dr. V. Sellam** has overall experience of 9+ years in the field of Information Technology, Science & Technology Projects and in academic & administration. She has been a part of SRM group over 6 years and has served various academic and administrative roles. With six years of academic contribution and 4 years of research guidance, currently holds Sr. Assistant Professor. She has obtained her Ph.D in Computer Science and Engineering from SRM Institute of Science and Technology, Chennai And Masters from Annamalai University. Her research alignment is broadly in the areas of analysis and study of Agricultural Data Mining.