



# A Development of Medical Records Management System to Health Care Decision Makers using Cloud Technologies

S.Babu, K.Nagendra Babu, K.Chaitanya, Y.Siva Ganesh, MB.Mahesh

**Abstract:** *Electronic Health Record systems continue to be incorporated into health care facilities to reduce the problems and limits of paper-based methodology but their deployment has been slow due to high investment and storage costs. The Enterprise Electronic Cloud-based Health Record System is planned, created and checked for recording, recovering, chronicling and surveying patients and other clinical records. Cloud Data fills in as a coordinative information bank over every single authoritative emergency clinic, middleware gives a typical stage to all electronic health record frameworks between remote medical clinics while a security approval server gives access to approves clients and denies unapproved clients access to records or assets in the system. In this model, complex mixes are redistributed to open cloud servers, leaving nearly the whole intricate of private key generator, sender and beneficiary. In addition, PKG communication costs with users have been optimized. In addition, we are building a comprehensive library called libabe compatible with mobile devices, and the access control mechanism is distributed in a logical environment, including public cloud servers, a laptop and an inexpensive mobile device with interactive resources.*

**Keywords:** *Information sharing system, attribute based encryption, cloud, Medical Record.*

## I. INTRODUCTION

As an appealing worldview for advanced data processing, Electronic Medical Record benefits patients to acquire clinical treatment of high caliber and effectiveness and empowers specialists and patients to helpfully share clinical records, e.g., clinical history, medicine and hypersensitivities, radiology pictures and individual wellbeing data and so on. To diminish the expense of keeping up specific server farm and accomplish information sharing, the EMR frameworks can redistribute clinical records to open cloud, where specialists and patient sweep store, oversee and share clinical records. As a creative cryptographic arrangement, quality

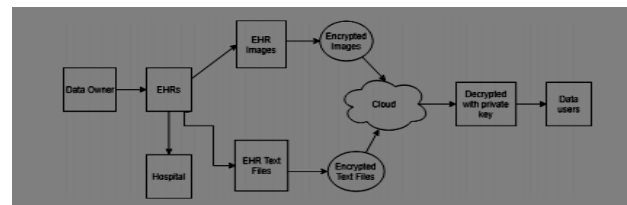
based encryption (ABE) coordinates adaptable access control with encryption usefulness. The adaptability signifies that each and every document can be encoded with an adaptable access policy. It presents the customary access control model of ABE. Specifically, figure content strategy ABE (CP-ABE) that is thoughtfully nearer to RBAC can possibly be applied in ERM frameworks. So as to meet the instantaneousness and versatility, specialists utilize cell phones to make, read and update clinical records anyplace, whenever. A specialist is relegated with a few qualities dependent on his/her job, for example, "Medical procedure", "Chief", "Male" etc., and utilizes a cell phone to scramble patients' clinical records related with get to strategy, e.g., "Pediatrics" ("Doctor" – "Head-nurture"), before transferring to the EMR cloud. Different specialists who have private keys containing qualities can decode encoded clinical records if the traits fulfill the entrance arrangement.

## II. RELATED WORK

### A.Review On Securing Medical big Data In Health Care Cloud,2019

- E health is one of the emerging fields of the healthcare industry.
- E health being is one of the rising fields of the human services industry.
- To analyze a patient, doctors need a patient's clinical record containing huge sight and sound information. Dynamic access Electronic Medical Record ought to be put in the cloud and furthermore bolstered by versatility.
- It has numerous focal points, faces numerous security issues, and its hacking is viewed as the most exceedingly awful of the wellbeing information in the cloud
- A study was led on different strategies for acquiring enormous clinical information in the cloud.
- Health care data can be put away and gotten to utilizing the bait procedure.

### Architecture:



**Fig: 2.1 Architecture of securing medical big data in health care**

Revised Manuscript Received on April 17, 2020.

\* Correspondence Author

**S.Babu\***, CSE, V R Siddhartha Engineering College, Vijayawada, Andhra Pradesh. Email: [sallagundlababu@gmail.com](mailto:sallagundlababu@gmail.com)

**K.Nagendra Babu**, CSE, VRSEC, Vijayawada, Andhra Pradesh. Email: [nag47.kolusu@gmail.com](mailto:nag47.kolusu@gmail.com)

**K.Chaitanya**, CSE, VRSEC, Vijayawada, Andhra Pradesh. Email: [chaitanyachitti29@gmail.com](mailto:chaitanyachitti29@gmail.com)

**Y.Siva Ganesh**, CSE, VRSEC, Vijayawada, Andhra Pradesh, Email: [sivaganesh062@gmail.com](mailto:sivaganesh062@gmail.com)

**MB.Mahesh**, CSE, VRSEC, Vijayawada, Andhra Pradesh, Email: [maheshmbm777@gmail.com](mailto:maheshmbm777@gmail.com)

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

**Data Owners:-**The client whose subtleties are to be put away in the cloud will be the proprietor of the his/her information. On the off chance that a patient visits a facility or any medical clinic for any reason, it would have been simple if the emergency clinic or the center has as of now the records of that specific patient, on the off chance that so no time will be squandered in the correspondence telling about his clinical history.

**HER's:-** They are the records or information of a patient which is put away in a computerized group. The subtleties including both the individual just as the clinic records.

**Encryption:-** It is performed before putting away the information into the cloud.

**Cloud Storage And Retrieval:-** After the fruition of the encryption procedure, the encoded records can be put legitimately to the cloud. It fills in as the capacity for all the information according to the pre-requisite.

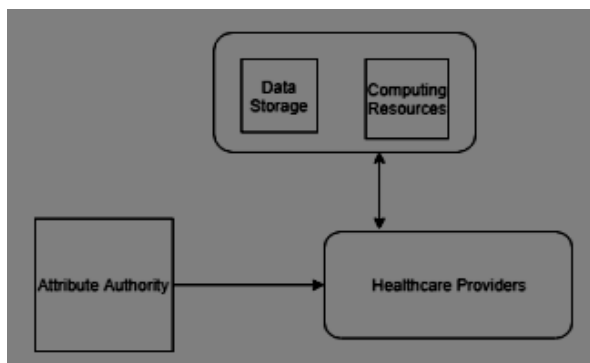
**Decryption:-**The decoding of the information are performed just when those information or the records are recovered from the cloud. The records are unscrambled with the assistance of a key which will be available with the specialist.

**B. Cloud Storage For Electronic Health Records Based On Secret Sharing With Verifiable Reconstruction Outsourcing ,2018**

Utilizing Electronic Health Records (EHRs) is presently a generally illogical practice in social insurance frameworks. By using enlivening advantages, for example, adaptability and minimal effort, cutting distributed storage has become a well known answer for keeping enormous quantities of EHRs packing neighborhood stockpiling. Be that as it may, putting away delicate data, for example, wellbeing records in the cloud presents perilous security and protection dangers. Right now, propose a novel distributed storage framework for EHRs that totally ensures information protection through Shamir's Privacy division. Right now, EHR is separated into numerous parts by the human services community, and the segments are shared on various cloud servers.

Upon receipt of the EHR, the health care center captures the components from the participating cloud servers and then creates the EHRs.

**Architecture**



**Fig: 2.2 Architecture of cloud storage for Electronic Health Records**

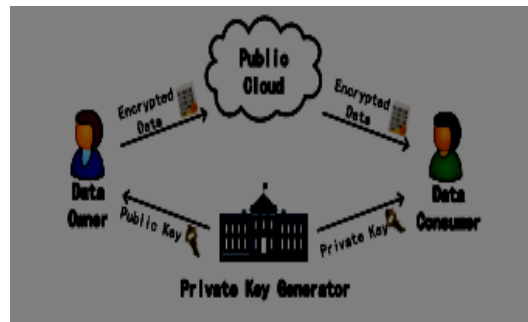
**Description:**

The cloud comprises of two dynamic segments, one is information stockpiling and the other is a processing device. Clouds can be gotten to through the web-based

interface and at any number of clients in the expert clinical field. The cloud likewise produces get to arrangements for all figure archives. Clients can just utilize the administrations after the confirmation procedure. They are liable for record transferring and information encryption. The keys are made required. After the age of catches, catches are conveyed to social insurance suppliers. By utilizing those keys the information can be gotten to. As the name suggests, encryption depends on trait.

**C. Efficient Fine Grained Data Sharing Mechanism for Electronic Medical Records System With Mobile Devices, 2018**

**Archeicture:**



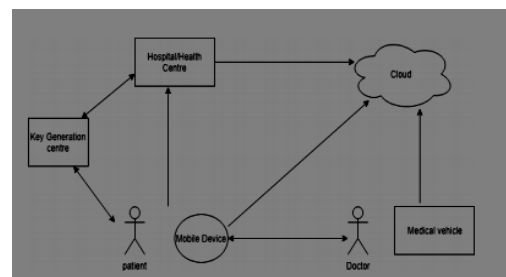
**Fig: 2.3 Sharing Mechanism For Electronic Medical Record**

**Description:**

Sharing computerized clinical records in broad daylight distributed storage with cell phones helps patients (specialists) find (give) high-caliber and effective treatment. In any case, difficulties, for example, ensuring information security, sharing of touchy information, legitimate assignment of specialists, accomplishing ideal execution, despite everything bring about accomplishing great fundamental access control in the Electronic Medical Record (EMR) framework. Right now, propose another entrance control strategy and a productive method to share EMR information, which at the same time accomplishes the highlights depicted above and is reasonable for administration restricted cell phones. In the model, complex transmissions are sent to open cloud servers, leaving no unpredictable key generator (PKG) complex, sender and beneficiary. What's more, PKG correspondence costs with clients have been streamlined.

**D. Design of Secure Medical Data Sharing System via an Authorized Mechanism, 2017**

**Architecture:**



**Fig: 2.4 Design of a secure medical data sharing system Architecture**

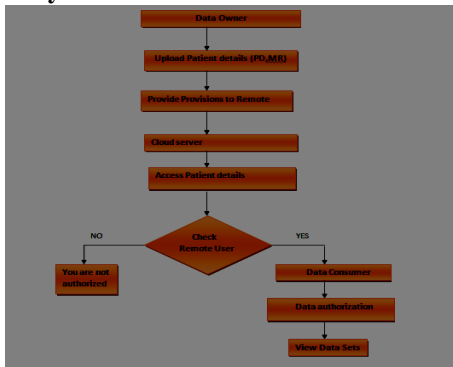


Electronic clinical records can be handily kept up through the fast advancement of medicinal services innovation and distributed computing. However, the security of patient data is at present a stressing issue. Despite the numerous books examined, these books despite everything face numerous security challenges. Therefore, we propose a "cloud-based authentication system". In our program, we permit individuals to utilize the advanced improvement strategy to accomplish shared information. By the way, the "unique finger impression biometric include and advanced mark" are utilized to guarantee the security of clinical data in our framework.

### III. METHODOLOGY

The information proprietor transfers their information in the cloud server. The client can possibly get to the information record with the scrambled key if the client has the benefit to get to the document. The cloud specialist co-op deals with a cloud to give information stockpiling administration. All the legitimate clients in the framework can uninhibitedly question any intrigued encoded and decoded information.

#### Proposed System:



- The information proprietor transfers their information in the cloud server.
- The client can possibly get to the information record with the scrambled key if the client has the benefit to get to the document.
- The cloud specialist co-op deals with a cloud to give information stockpiling administration.
- All the legitimate clients in the framework can uninhibitedly question any intrigued encoded and decoded information.

This area presents the philosophy plan of the cloud based electronic clinical record framework.

- i. Cloud-based EHR: Pooling different medicinal services IT assets into huge mists to encourage simplicity of record sharing.
- ii. Authentication: Security is accomplished using passwords.

The cloud-based endeavor electronic wellbeing record framework is introduced in cloud. The framework comprises of two significant parts which are: the cloud-based framework and the E-wellbeing online interface.

- Cloud-Based System: The cloud-based framework comprises of a focal database server, Unifier Interface Middleware and an Authentication Server.
- Cloud Central Database Server: This goes about as the bound together information bank for all the teaming up

medical clinics. The Infrastructure as a Service (IaaS) cloud datacenter contains the focal database server as the information archive for putting away electronic clinical records and recovering patient data.

#### Encryption Decryption Process:

❖ Right now use TDES logarithm: For the encryption and unscrambling procedure of information in the cloud.

❖ Data Encryption Standard (DES) is a block cipher algorithm that takes plain content in squares of 64 bits and changes over them to cipher text utilizing keys of 48 bits. It is a symmetric key calculation, which implies that a similar key is utilized for encoding and decoding information.

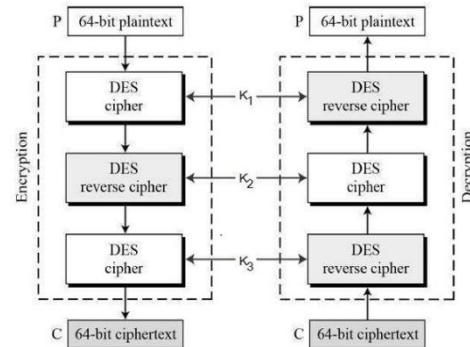


Fig: Triple DES

- Scramble the plaintext squares utilizing single DES with key K1.
- Presently unscramble the yield of stage 1 utilizing single DES with key K2.
- At long last, encode the yield of stage 2 utilizing single DES with key K3.
- The yield of stage 3 is the ciphertext.
- Unscrambling of a ciphertext is an invert procedure. Client initially decode utilizing K3, at that point encode with K2, lastly unscramble with K1.

### IV. RESULT

From the examination of papers we used to build up a clinical record the board framework to medicinal services leaders utilizing cloud technologies.

#### Home Page:

It is the primary page of the clinical records the board framework.



#### Data Owner:

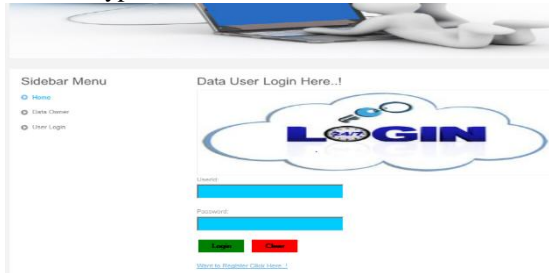
The owner can upload the file and records, they have the overall details of the files and records. The owner have the look at users request and sends the secret key for an encryption file or record.







**USER LOGIN:** Before view the file, the user have to register and then login. Now they can search for the files and sends the request to the data owner for the acceptance of the file for the decryption of the file.



**Secret Key:**

to me  
File and Secret Key : fever.txt Key is 6253187



**Decrypted File:**



**V. CONCLUSIONS**

In this work, we propose a structured way to share EMR program data, It is not limited to access to data privacy, effective unauthorized access control, and authority shipping simultaneously, but also suitable for low-cost mobile devices. In addition, we developed a library called libabe compatible with Android devices, and us to use our process in a realistic situation. The test results show that our system is efficient, efficient and economical. In the future, we will focus on building efficient way to work.

**REFERENCES**

1. Kalyani Sudheep, Sandy Joseph “Review on Securing Medical Big Data in Healthcare Cloud ” IEEE june 2019.
2. Hui Ma ,Rui Zhang ,Guomin Yang ,Zishuai Song ,Kai He ,Yuting Xiao “ Efficient Fine-Grained Data Sharing Mechanism for Electronic Medical Record Systems with Mobile Devices ” IEEE june 2018.
3. Hanlin Zhang,Jia Yu ,Chengliang Tian ,Pu Zhao ,Guobin Xu ,Jie Lin “ Cloud Storage for Electronic Health Records Based on Secret Sharing With Verifiable Reconstruction Outsourcing ” IEEE JULY 2018.

4. Chin-Ling Chen , Jin -Xin Hu ,Chun-Long Fan ,Kun-hao Wang “ Design of a secure medical data sharing system via an authorized mechanism ” February 2017.
5. A. Castiglione, A. D. Santis, B. Masucci, F. Palmieri, A. Castiglione, and X. Huang, “Cryptographic hierarchical access control for dynamic structures,” IEEE Transactions Information Forensics and Security, vol. 11, no. 10, pp. 2349–2364, 2016.
6. R. Zhang, H. Ma, and Y. Lu, “Fine-grained access control system based on fully outsourced attribute-based encryption,” Journal of Systems and Software, vol. 125, pp. 344–353, 2017.
7. A. Castiglione, A. D. Santis, and B. Masucci, “Key indistinguishability versus strong key indistinguishability for hierarchical key assignment schemes,” IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 4, pp. 451–460, 2016.
8. S. Hohenberger and B.Waters, “Online/offline attribute-based encryption,”in Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014, pp. 293–310.

**AUTHORS PROFILE**



**S. Babu** done M.Tech degree in CSE from V R Siddhartha Engineering College, Vijayawada, India. His area of interests includes Web Technologies and Data Mining. He has 11 years of teaching experience as Assistant Professor in CSE at VR Siddhartha Engineering College, Andhra Pradesh, India.



**K.Nagendra Babu** is currently pursuing B.Tech at VRSEC (Autonomous), Vijayawada, Andhra Pradesh. His area of interest include Object Oriented Programming.



**K.Chaitanya** is currently pursuing B.Tech at VRSEC (Autonomous), Vijayawada, Andhra Pradesh. Her area of interest include Web Technologies.



**Y.Siva Ganesh** is currently pursuing B.Tech at VRSEC (Autonomous), Vijayawada, Andhra Pradesh. His area of interest include Database Security.



**MB.Mahesh** is currently pursuing B.Tech at VRSEC (Autonomous), Vijayawada, Andhra Pradesh. His area of interest include Web Technologies.