# Secured Medical Record Management System Using Cloud

**Indra Priyadharshini S[1], Ajay Yokesh T[2], Akash S[3], Jagadeeswaran E[4]**
[1]Assistant Professor, Dept of Computer Science and Engineering
[2, 3, 4]Dept of Computer Science and Engineering
[1, 2, 3, 4] R.M.K College of Engineering and Technology, Puduvoyal, India

***Abstract-*** *Cloud-based Secured Medical Record Management System (CB-SMRMS) majorly used for management of patient's individual health records. Cloud computing provide real-time data sharing in a cost-effective manner. Data security and privacy of maintaining personal health records are main problem for the wide usage of CB-SMRMS, since these information are highly sensitive, so it needed to be protected in highly secured manner. In this paper, we propose method using Standard Encryption technique for maintaining health record based on challenges in existing system. Indexes are indexed under separate symmetric keys throughout this process, and the authenticated data indexes from various service providers may even be combined across cloud without understanding the index material. It also offers powerful and privacy-conserving database processing with the submission of a single data database. Encrypted data will be processed by cloud from all associated service providers without understanding the content of their query.*

***Keywords***- Data Security, Encryption, Health Information Management, Profile Matching, Identity Based, Attribute Based, Decryption.

## I. INTRODUCTION

Fast access to health data allows for better health care services and contributes to improving quality of life. With rapid advances in cloud infrastructure, people become interested in utilizing mobile apps to view their health data from the cloud service. The main advantage of cloud storage is its unlimited capacity to store data and its ubiquitous nature. But the big challenge is data privacy and data security.

According to HIPAA (Health Insurance Portability and Accountability Act) it is recommended to keep health data to be confidential from unauthorized access. But the cloud is vulnerable to multiple assaults on protection and privacy. The biggest obstacle to cloud storage is the privacy and security issues. Several encryption techniques are used to solve privacy issues which add some control over unauthorized access to health information by user. Since after encryption the user can't perform plaintext search on encrypted file therefore it is difficult to retrieve the content in efficient way.

Consider the situation where the cloud consists of 2 GB of health information but consumer preferred to access 1 MB of sensitive information that is necessary to recover all the 2 GB of data then decrypt everything, so to ease data recovery from cloud storage, we need a scheme that enables users to scan for encrypted details across.

Using keyword search mechanism over encrypted file, the proposed system provides the efficient way to store and recover health data. We employ symmetric key algorithm to enforce the proposed method. We solve key management issue by exchanging hidden key to the user's mail ID.

## II. RELATED WORK

In this segment, we review similar cloud data sharing research and focus on the literature used to address the account revoking issue. We looked at previous similar research on mobile device convergence and cloud [1] [2].

Cong Wang et al [3] proposed a system to achieve less storage of space to store large amount of data and to reduce the cost for data sensing. They proposed following.

- Healthcare monitoring system must be effective.
- The system should be designed to be compatible with other data services, while providing possible extensible service interfaces [3].

E-health computing services are popularly used worldwide today. Protection for e health systems has to be given greater attention to patient's confidential health records. When we have a illness like pneumonia, we head to the hospital for diagnosis with a specialist [4]. The doctor must conduct a proper diagnosis of the state of our body to decide the disease with which we are affected, so that they can provide the necessary treatment. To provide treatment physicians need to handle many scanning images, previous medical records, etc., and these are challenging tasks and also

time consuming. E-health plays an important role in handling all these kinds of works; their main objective is to manage the healthcare information system. Securities are one of the major challenges in adapting E-Health systems around the world, because sensitive information is electronic health records [4].

The encryption can protect sensitive records. Key policy attribute based encryption performed to secure the data after dividing records to private and public domains. We are able to increase security by using session passwords and session regeneration. The use of one time password and session regeneration, respectively we can prevent eavesdropping and session hijacking.

So, in order to achieve efficiency and reliability, these technics are followed.

*A. Attribute based encryption*

Attribute Based Encryption (ABE) is an asymmetric encryption variant in depending on the attributes used [5]. The main purpose of this encryption is to provide security, flexibility in access control, scalability, and fine grain control of access. Secondly, secure information sharing is of the user on demand. Variants of Attribute Based Encryption can be used to solve those problems.

*B. Profile matching*

Profile matching is a method of comparing different user's personal profiles. User's profile also contain sensitive information, so ensure that private information is not leaked to third party [6]. Two mainstreams of ways were proposed.

- User's profile will be taken as a set of attributes which uses private set intersection to achieve attribute matching based sharing and encryption. For exchanging the minimal private information of participating users.
- The user profile as a vector is taken to measure social proximity [6]. Schemes for matching metrics. This is based on symmetric encryption.

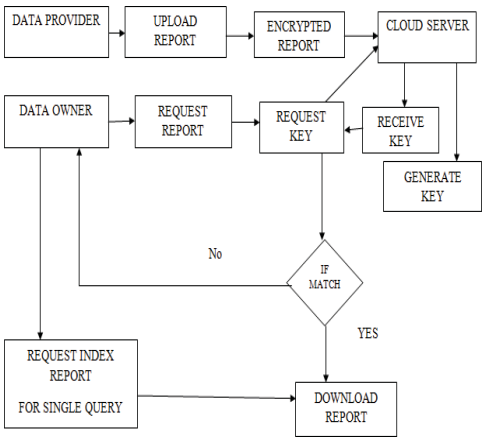
*C. Identity based encryption(IBE)*

Using various cryptographic algorithms used on the different data types, a patient's privacy is maintained highly secure. Maintaining electronic health records is the main goal before sharing them. The system being proposed is based on a web-based system with secure login and user registration. The cloud storage is used for flexible recovery and data classification as well as data encryption.

In these papers the researchers proposed a design for sharing electronic patient's health record in a cloud environment they first did survey and various specialists from the German medicinal services industry. Moving highly important records to the cloud still infers extreme security and protection risks. With this foundation, they display a secure novel design for sharing records of electronic patients in a cloud environment. Initially, they conducted systematic literature surveys and meetings with various specialists from the German medicinal services industry that allowed them to identify certifiable procedures and relate safety and protection needs. Taking into account these outcomes, they planned multi provider cloud mechanism that fulfils a large portion of the prerequisites by giving expanded confidentiality, integrity and availability of the healthcare records stored in the storage system. This design highlights secret sharing as a vital measure to disseminate the records of patients as shares with different cloud administrations, which can give greater redundancy.

## III. PROPOSED WORK

The proposed system is based on the Encrypted Multisource Database. The proposed framework allows multiple encrypted data indexes from the same patient's different health services to converge via cloud, without violating the privacy of the patient. The health data are stored in an encrypted form for data protection purposes and allowed with querying functionality over encrypted data.




*Block diagram of the proposed system*

*A. Architecture of the system*

- *DataOwner:* The DataOwner is one who wants to encrypt the file and upload to cloud server. DataOwner can be user or it may be an organization.
- *DataUser*: The DataUser is one who want to view or download the DataOwner health file. In order to view

health file user need to request cloud service provider and than cloud service share a secret key through which user can view or download health file.

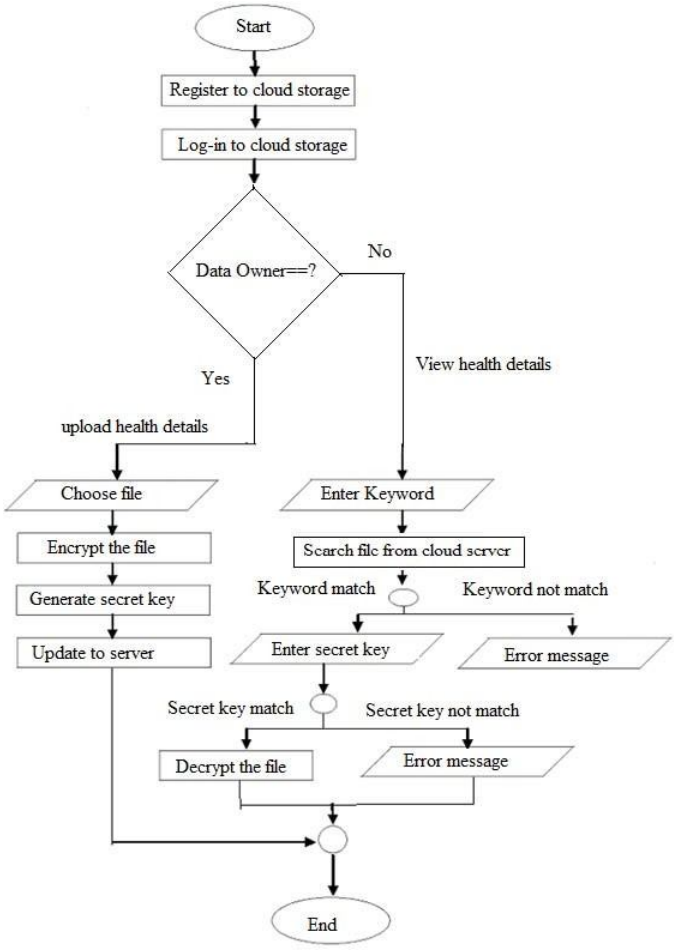
- *Cloud Server:* Cloud server can login directly to the application with username and password. Here cloud can view all the user details and owner details .The user details are encrypted. Cloud server administrator can view owner file details. All users' request for file will be shown here. Cloud can accept the request and sends file key to the user's mail id. After completing, administrators can logout the account.
- *Key Generator:* We are using one secret key for encryption and same for decryption because we are using AES scheme which is symmetric key encryption. the key management will be done by sending secret key to user's mail ID.

*B. Algorithm for AES encryption scheme*

Blowfish is a symmetric block cipher that can be used to replace DES or IDEA on drop-. It requires from 32 bits to 448 bits of a variable-length switch, rendering it suitable for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. This has been considerably studied since then, and is steadily gaining popularity as a good encryption algorithm. Blowfish is license-free and unpatented, and is available for all uses.

*C. Flowchart of the system*

There are two scenarios in this system one is the scenario for the data owner and the second is the scenario for the user. Both users should register with the cloud service provider when they send one password to the mail ID that they can log in to their cloud account. After login if data owner wish to upload health file than he is allowed to do by selecting 'upload health detail' link. Data owner need to enter his mobile number and key word for file than he can continue by selecting file from file directory the file must be in text format. After uploading the file on server the file will be encrypted and secret key will be generated and stored on to the cloud server.




*Flowchart of the system*

In second scenario if user wishes to view or download the data owners file than he has to select 'view health details via mobile' link their user must enter the mobile number of data owner and keyword of appropriate file for which user is requesting after matching the both criteria the file information will be displayed but the information will be in encrypted format to decrypt it user need to enter the secret key which is sent to his mail id. The user is allowed to download the file when he enters the secret key.

## IV. EXPERIMENTAL RESULTS

We have worked on two file types like Text file and Image file with different file sizes. We analyzed Text files of size 1mb, 10mb and 100mb which is in .txt format and Image files of size 1mb, 10mb and 100mb which is in .jpeg format.

First we used basic DES with PBE to encrypt files. For PBE encryption the key used to encrypt a file is chosen and then the same encryption and key used to decrypt the file. The tests we received were as follows.

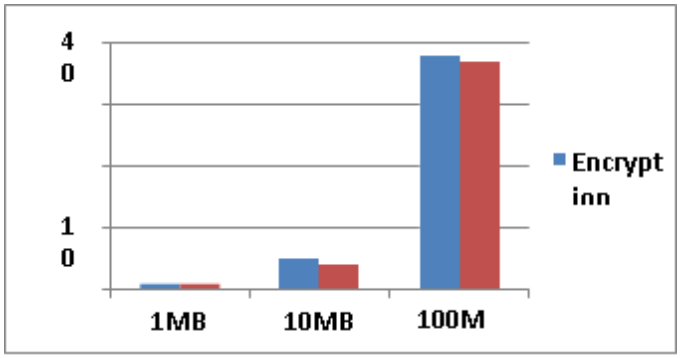



*Fig 1: Text File Encryption and Decryption using DES with PBE method.*

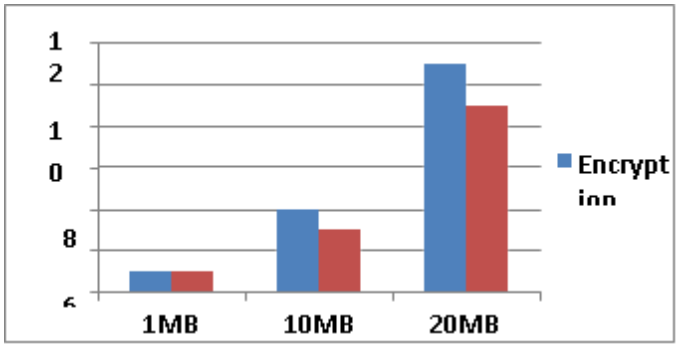



*Fig 2: Image File Encryption and Decryption using DES with PBE method.*

Second we used AES with PBE to encrypt data. In terms of reliability the AES encryption strategy is better than DES. In this we often use password and ID that is used for encoding purposes to initialize cipher and link.

By looking towards the results, the DES method is bit slower than AES encryption method. Then we attempted encryption and decryption with RSA algorithm for 1 mb text file first and it takes longer to encrypt and decrypt then we attempted with 10 mb text file and this RSA algorithm requires a ton more time. So we conclude that the RSA is relatively slower when dealing with large files. So, using RSA algorithm to encrypt and decrypt large files isn't a good idea. The results we obtained with technique of RSA encryption and decryption are as follows.

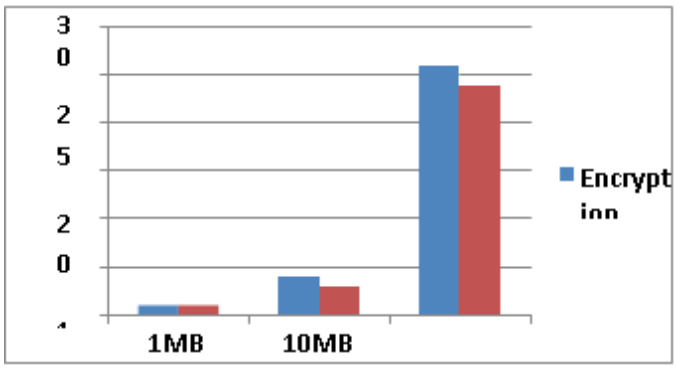



*Fig 3: Text File Encryption and Decryption using AES with PBE method.*

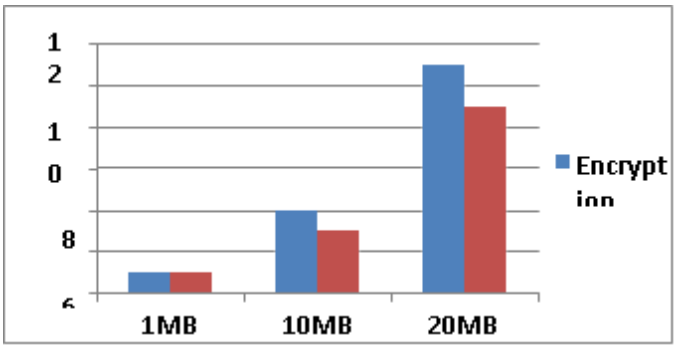



*Fig 4: Image File Encryption and Decryption using AES with PBE method.*

The RSA cryptosystem is therefore very slow to encrypt and decrypt large files compared to the DES and AES techniques but very secure than the AES and DES techniques.

## V. CONCLUSION

In this paper challenges and various security methods to protect privacy of health record on existing systems are discussed. These cloud based health record system used widely for patient's record management and also for quick reference for doctors about patient's health during operations. We provided privacy during data storage by encrypting the data at client side before storing it on remote cloud server. For our implementation we have chosen AES algorithm for encryption and decryption purpose. Since it is symmetric key encryption we are using same key for encryption and decryption. We also provided keyword search mechanism to make search over encrypted file. It also provides secures query processing in which user can submit a single data query without knowing its content in cloud.

## REFERENCES

[1] K. Ren, S. Yu, and K. Urs C. Wang, "Achieving usable and privacy assured similarity search over outsourced cloud data," in in Proc. IEEE Conf. Comput. Commun, Mar. 2012, pp. 451–459.

[2] Z. Yang, C.Wang, K. Ren, andW. Lou N. Cao, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in IEEE Int. Conf. Distrib. Comput. Syst, Jun. 2011, pp. 393–402.

[3] Cong wang,Bingsheng,KuiJanet,Chan wen Chen, "Privacy aware cloudassisted healthcare Monitoring system via compressive sensing", IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, July 2014.

[4] Xu An Wang,Jianfeng, FatosXhafa, Mingwu Zhang, Xiaoshuang Luo, "Cost-effective secure E-health cloud system using identity based Cryptographictechniques", Future generation computer system, Vol 67, Feb 2017,Pg 242-254.
[5] Shruthi ganesh, "Highly secured personal health record model", 2015 Online International Conference on Green Engineering and Technologies 2015.
[6] Qinlong Huang,Wei Yue, Yue He, Yixian Yang, "Secure Identity-based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing",IEEE,July 2018.