Secure Identity Based, Privacy Preserving Encryption & Search for Health Record in Multi Cloud

S. S. Shedshale[1] A.B.Rajmane[2]
[1,2]Department of Computer Science and Engineering
[1,2]Ashokrao Mane Group of Institutions, Vathar, India

Abstract— In the past few years, cloud computing has developed very quickly. A large amount of data is upload and stored in remote public cloud servers which cannot fully be trusted by users. Especially, more and more enterprises would like to manage their data by the aid of the cloud servers. However, when the data outsourced in the cloud are sensitive, the challenges of security and privacy becomes urgent for wide deployment of the cloud systems. Cloud computing and social networks are changing the way of healthcare by providing real-time data sharing in a cost-effective manner.
Keywords: encryption, profile matching, indexing, cloud computing, distributed server

I. INTRODUCTION

Secure Identity Based, Privacy Preserving Encryption & Search for Health Record in Multi cloud systems have great potential in facilitating the management of individual health records, Security and privacy, indexing and identity-based data sharing, profile matching. In this paper we consider a multi-source system in multiple data providers such as hospitals and patients, doctors, specialist are authorized by individual data owner to upload their personal health data to an untrusted public cloud.

Cloud computing and social networks are changing the way of healthcare by providing real-time data sharing in a cost-effective manner. However, data security issue is one of the main obstacles to the wide application of mobile healthcare social networks, since health information is considered to be highly sensitive.

The patients will send their data to system, after that system will outsource their encrypted health records to cloud storage with an identity-based broadcast encryption technique, and share them with a group of doctors in a secure and efficient manner.

In this paper we propose the distributed cloud computing technique for storing data in an secure way, We will then present an attribute-based conditional data re-encryption construction which permits the doctors who satisfy the pre-defined conditions in the cipher text to authorize the cloud platform to convert a cipher text into a new cipher text of an identity-based encryption scheme for specialist without leaking any sensitive information. Furthermore, we can provide a profile matching mechanism based on identity-based encryption with an equality test, which helps patients to find friends in a privacy-preserving way and achieves flexible authorization on the encrypted health records with resisting the keywords guessing attack, we also provide indexing facility for fast access of information.

II. EXISTING WORK

Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing [1] author introduced a secure data sharing and profile matching scheme for the MHSN in cloud computing. First, they realize secure data sharing in MHSN with IBBE cryptographic technique, which allows the patients to store EHRs to cloud securely and share them with a group of doctors efficiently. Then present an attribute-based CPRE mechanism in MHSN, which allows doctors who satisfy the pre-defined conditions to authorize the cloud to convert a stored ciphertext into a new ciphertext under IBE for the specialist, without leaking any sensitive information

The limitation of this survey is, less security because there is no distributed server is used.as well time-consuming process.

A. Privacy-Preserving Search Over Encrypted Personal Health Record in Multi-Source Cloud [2]

In this consider a multi-source CB-PHR system in which multiple data providers such as hospitals and physicians are authorized by individual data owners to upload their personal health data to an entrusted public cloud. The health data are submitted in an encrypted form to ensure data security, and each data provider also submits encrypted data indexes to enable queries over the encrypted data.

This survey has limitation of security and user profile classification.

B. Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record [3]

This system proposed a secure data sharing scheme to ensure the privacy of data owner and the security of the outsourced cloud data. The proposed scheme provides flexible utility of data while solving the privacy and security challenges for data sharing. The security and efficiency analysis demonstrate that the designed scheme is feasible and efficient.

This survey has limitation of slow performance. Create a gap in effective data storing

C. Security and Privacy-Preserving Challenges of E-Health Solutions in Cloud Computing [4]

In this system proposed 1) EHR security and privacy 2) security and privacy requirements of e-health data in cloud 3) diverse EHR cryptography and non-cryptography approaches, to maintain the integrity and confidentiality of patient's information

The limitation of this survey is cyber security. Key related research issues as well as Less Efficiency.

D. Privacy-Preserving Indexing and Query Processing for Secure Dynamic Cloud Storage [5]

Investigate new privacy-preserving indexing and query processing protocol which meets a number of desirable properties, including the multi-keyword query processing with conjunction and disjunction logic queries, practically high privacy guarantees with adaptive chosen keyword attack

security and forward privacy and support of dynamic data operation

This survey has limitation of Difficult to implement and Less Performance.

E. PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks [6]

In this framework called PAAS which leverages user's verifiable attributes to authenticate users in eHealth systems while preserving their privacy issues. In this system, instead of letting centralized infrastructures take care of authentication, there scheme only involves two end users. it also offers authentication strategies with progressive privacy requirements among patients or between patients and physicians. Based on the security and efficiency analysis, it shows framework is better than existing eHealth systems in terms of privacy preservation and practicality

F. Cipher text-Policy Attribute-Based Encryption [7]

In this system for realizing complex access control on encrypted data that call Cipher Text-Policy Attribute-Based Encryption. By using these techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, these methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys.

G. Identity-Based Proxy Re-Encryption [8]

Author addressed the problem of Identity-Based proxy re-encryption, where cipher texts are transformed from one identity to another. These schemes are compatible with current IBE deployments and do not require any extra work from the IBE trusted-party key generator. In addition, they are non-interactive and one of them permits multiple re-encryptions. Their security is based on a standard assumption (DBDH) in the random oracle model

H. Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption [9]

In this system author proposed novel patient-centric framework and suite of mechanism for data access control to PHR's stored in semi-trusted servers Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient use revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for PHRs, leverage ABE techniques to encrypt each patient's PHR file. Data owner update the personal data into third party cloud data centers.

Title	Publication year	Author	Limitation
Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare social network in cloud computing	2018	QINLONG HUANG, YIXIAN YANG	1. singlecloud services provider/server 2. Time consuming
Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record	2018	HUAQUN WANG	1. Difficult to implement 2. Less Performance.
Security and Privacy-preserving challenges of e-health solutions in cloud computing	2018	Shekha chenthara, khadakar ahmed	1. Key related research issues. 2. Less Efficiency.
Privacy-preserving indexing and query processing for secure dynamic cloud storage	2018	Minxin Du , Qia Wang	Query efficiency and query privacy is less
PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks	2012	Linye gueo,chi zhang	1. Social connection is not available 2. central storage
Cipher text-Policy Attribute-Based Encryption	2012	Amit sahai,john	1. provide secure under the generic group 2. moderate loss of efficiency
Identity-Based Proxy Re-Encryption	2014	Matthew green,Giuseppe ateniese	1. unidirectionality 2. non-interactivity
Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption	2014	y.b.gurav,manjiri desmukhh	1. key management overhead 2. data owner is also trusted authority.

Table 1: Existing systems

In the above table 1 shows the all information related to existing system which we are referred for this survey paper.

III. PROPOSED SYSTEM ARCHITECTURE

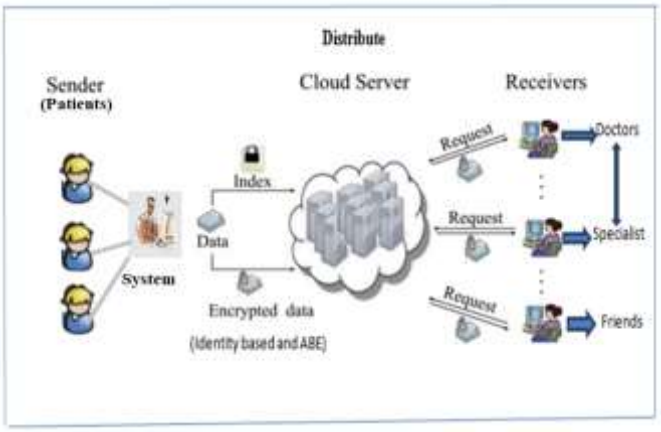

Fig 1: System Architecture

In the proposed architecture sender (Patients) want to outsource their data on a distributed cloud server in a secure and effective manner. Then for this patient first enter his/her data into Secure Identity Based, Privacy Preserving Encryption system, after that system will encrypted their data for security purpose for that identity-based encryption and attribute-based encryption technic is used. Indexing by using Btree is added after encryption for efficient search record system. Then encrypted data is stored on distributed cloud servers. Doctors, specialist and friends with same attributes are the act as receivers. When receivers want to access data then decryption process is applied. In fig.2 shows how the data will flow in the proposed system

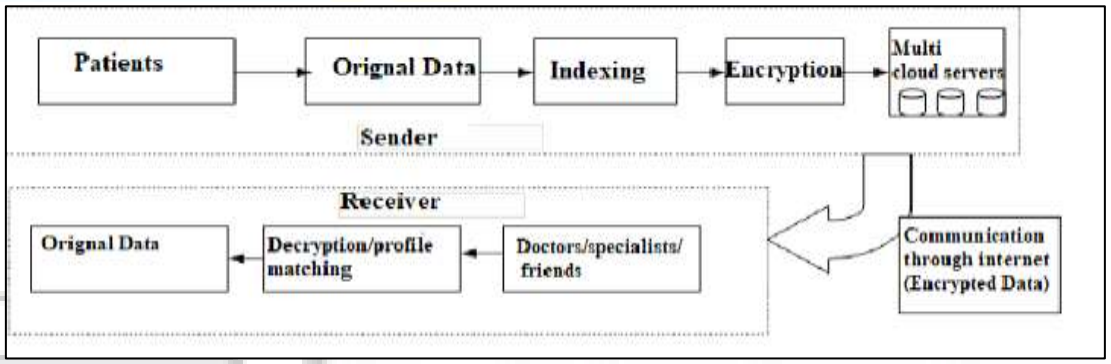

Fig. 2: Data flow in the proposed system

In the above fig.2 shows how data will flow in the Secure Identity Based, Privacy Preserving Encryption & Search for Health Record in Multi cloud systems system patients will store his/her data into the system then this data will be encrypted and stored into the multi cloud, indexing is applied while storing the data, after that in the receiving end receiver will decrypt the data and get the original data. Receiver should be doctors, specialist or friends.

IV. METHODS USED

A. Key Generation:

The central authority will generate the secret key SK for each entity with identity ID by running KeyGen algorithm.

B. Data Encryption:

In order to protect the security of data in Identity Based, Privacy Preserving Encryption system, the patient will run Enc algorithm and outsources the result. First, the patient chooses a random EK to encrypt data with symmetric encryption algorithm, and generates result. Then the patient will choose a set doctors, identities, and picks a random k to protect the data based on IBE.

C. Re-Encryption Key Generation:

If the doctor will need to collaborate with the specialist with identity IDs, he then runs ReKeyGen algorithm to randomly and secret key SK

D. Data Re-Encryption:

The system will run reEncy algorithm, with the re-encryption request from authorized doctors

E. Data Decryption:

By using decryption algorithm and key data will be decrypted into the original form.

F. Profile Matching:

The system will determine whether the ciphertexts of two patients contain the same data according to the authorization type. Equality test profile matching scheme will use for it.

V. ALGORITHMS USED

A. Attribute-based Encryption Algorithm

Attribute-Based Encryption (ABE), a generalization of identity-based encryption that incorporates attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that multiple users who possess proper can decrypt.

Attribute-based encryption (ABE) is an expansion of public key encryption that allows users to encrypt and decrypt messages based on user attributes the general scheme consists of four stages, for each of them has its own algorithm.

B. Identity based Encryption-

ID-based encryption, or identity-based encryption (IBE), is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its

decryption key from a central authority, which needs to be trusted as it generates secret keys for every user

C. BTree Indexing Algorithm

When we think about the performance of a database, indexing is the first thing that comes to the mind. B-Tree is a self-balancing search tree. In most of the other self-balancing search trees, it is assumed that everything is in main memory. To understand the use of B-Trees, we must think of the huge amount of data that cannot fit in main memory. When the number of keys is high, the data is read from disk in the form of blocks. Disk access time is very high compared to main memory access time. The main idea of using B-Trees is to reduce the number of disk accesses

D. Equality Test Profile Matching Algorithm

By using this method patients can communicate with others. Specially, patient can find similar patients with profile matching mechanism and communicate their symptoms and medication this done by using IBE with equality test

In the following table 2 shows the basic comparison between different encryption algorithms

Factor	RSA	DES	3DES	ABS
Created by	Ron rivert, Adishamir	IBMin 1975	IBMin 1975	Vincent rajunen,jon daeman
Key length	Depend on no of bits N=p*q	56 bit	168 bit 112 bit	128,192,256 bit
Round(s)	Variables	64bits	64bits	128bits
Cipher type	Asymmetric Block cipher	symmetric Block cipher	symmetric Block cipher	symmetric Block cipher
Speed	Slowest	Slow	Very slow	Fast
Security	Least secure	Not secure enough	Adequate security	Excellent security

Table 2: comparison between encryption algorithms

VI. CONCLUSION

In this paper made a survey on the Improving the Security on Public Health Record System in Cloud Computing. ~~And~~ also made a detailed study about what are the techniques is needed for security the Health Record System. Attribute Based Encryption is the good technique to securing the Health records. Identity Based Encryption is the better way to provide the authentication for the Public Health Record System. This system will improve the healthcare through its convenient data sharing. Secure identity based, privacy preserving encryption & search for health in multi cloud system represents a significant role in today's health care system. With secure data storing and sharing.

REFERENCES

[1] Qinlong Huang ,WEI YUE ," Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud" Computing" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8403204
[2] L. Guo, C. Zhang, J. Sun, and Y. Fang, ''PAAS: A privacy-preserving attribute-based authentication system for eHealth networks,'' in Proc. 32nd Int. Conf. Distrib. Comput. Syst., Macau, China, Jun. 2012
[3] A. Abbas and S. U. Khan, ''A review on the state-of-the-art privacypreserving approaches in the e-health clouds,'' IEEE J. Biomed. Health Informat., vol. 18, no. 4, pp. 1431–1441, Apr. 2014
[4] C. Delerablée, ''Identity-based broadcast encryption with constant size ciphertexts and private keys,'' in Proc. 13th Int. Conf. Theory Appl. Cryptol. Inf. Secur., Kuching, Malaysia, 2007, pp. 200–215
[5] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-policy attribute-based encryption,'' in Proc. IEEE Symp. Secur. Privacy, Berkeley, CA, USA, May 2007, pp. 321–334.
[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ''Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,'' IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013
[7] M. Green and G. Ateniese, ''Identity-based proxy re-encryption,'' in Proc. 5th Int. Conf. Appl. Cryptogr. Netw. Secur., Zhuhai, China, 2007, pp. 288–306
[8] S. Yu, C. Wang, K. Ren, and W. Lou, ''Achieving secure, scalable, and fine-grained data access control in cloud computing,'' in Proc. IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–9.
[9] M. Barua, X. Liang, R. Lu, and X. Shen, ''ESPAC: Enabling security and patient-centric access control for eHealth in cloud computing,'' Int. J. Secur. Netw., vol. 6, nos. 2–3, pp. 67–76, 2011.
[10] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, ''Secure and fine-grained access control on e-healthcare records in mobile cloud computing,'' Future Gener. Comput. Syst., vol. 78, pp. 1020–1026, Jan. 2017

