RESEARCH ARTICLE OPEN ACCESS

Secure Cloud Architecture for Medical Wireless Networks

Mrs. G.Mohana Priya[1], G.Selva Jeba[2]
[1]Assistant Professor , [2]PG scholar,[1,2]Department of Computer Science and Engineering Velammal College of Engineering and Technology Madurai

ABSTRACT
In the recent decade, cloud computing with wireless technologies such as tablets, smartphones, laptops in healthcare has gained ever-increasing popularity. Healthcare system helps in the management of healthcare services such as collection, storage and accessibility of the medical records. Healthcare data are highly sensitive, which have to be protected from unauthorized access. Anytime and anywhere access to information has become a defacto requirement which is fulfilled by cloud computing. However, privacy has become a major issue in the cloud services. In order, to overcome the security issues against unauthorized access, the proposed system provides security mechanisms which makes use of effective cryptographic algorithms to achieve confidentiality, integrity and fine grained access control to medical data. This is achieved using Multi Attribute Authority Ciphertext Based Encryption technique with multi central authority which overcomes the drawback collusion resistance of using Ciphertext Attribute Based Encryption technique . This technique is more scalable, efficient and secure.

***Keywords*:** Healthcare, cloud, ciphertext attribute based encryption, multi attribute authority, multi central authority**.**

I. INTRODUCTION

The world is driven by the digital technology. Smart phones have transformed our daily lives and our communication ways. The Medical sector which has enormous amount of data needs to be digitized in the form of electronic health records, hospital patient administrative system, laboratory systems etc.

Cloud computing deals with various issues of cloud services when is accessed by portable devices in wireless environment. The Healthcare data is relatively sensitive compared to other data which need at most supervision. When Cloud services are accessed by the mobile devices additional challenge like security arises. Providing the security and privacy for the medical data is an interesting topic to deal with.

A healthcare information system (HIS) is an important support tools in the management of health care services. It refers to any system that captures, stores, manages information related to the health of individuals.

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user 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, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file.

The paper is organized as follows. Section II gives the System model. Section III gives the system architecture. Finally we give the conclusion in section IV.

II. SYSTEM MODEL

Cloud Computing is a commercial extension of computing resources which provides scalable resources and economic benefits to its users over the internet. It acts as software and provides data access and storage services which don't need the knowledge of the end users physical location and the systems configuration that provides the computing resources. In Cloud Computing, the users use the web browsers as an interface, while the software and data are stored on the remote servers and hence it is device independent.

In recent years, many healthcare organizations have started using wireless networks for efficient supervision of patient health. Many healthcare organizations and insurance companies have also started using the electronic medical record (EMR) system by which the medical records are maintained in a centralized database in the form of an electronic record and the records are stored in the cloud. Applications deployed on the cloud for manipulate electronic medical records.

The general scope of our work is to propose a secure architecture to integrate the healthcare cloud with wireless network technology.

Attribute Based Encryption (ABE)

The concept of attribute based encryption was first proposed by Amit Sahai and Brent Waters. In Attribute-based Encryption (ABE) scheme, attributes play a very important role. Attributes have been exploited to generate a public key for encrypting data and have been used as an access policy to control users' access. Using ABE schemes can have the advantages: to reduce the communication overhead of the Internet, and to provide a fine-grained access control. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold value d. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it use the access of monotonic attributes to control user's access in the system.

Cipher Text Policy Attribute Based Encryption(CP-ABE)

In a CP-ABE scheme, each user is associated with a set of attributes based on which the user's private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt.In this scheme whenever we are encrypting a message M, the encryptor specifies an access structure which is expressed in terms of a set of selected attributes for M. The message is then encrypted based on the access structure such that only those whose attributes satisfy this access structure can decrypt the message. Unauthorized users are not able to decrypt the cipher text even if they collude. A CP-ABE scheme consists of the following four algorithms:

Setup: This is a randomized algorithm that takes a security parameter as input, and outputs the public parameters PK and a master key MK. PK is used for encryption and MK is used to generate user secret keys and is known only to the central authority.

Encryption: This is a randomized algorithm that takes as input a message M, an access structure T, and the public parameters PK. It outputs the cipher text CT.

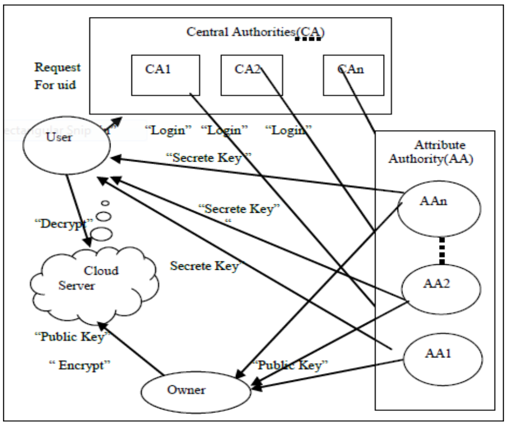
Ken Gen: This is a randomized algorithm that takes as input the set of a user (say X)'s attributes SX, the master key MK and outputs a secret key SK that identifies with SX.

Decryption: This algorithm takes as input the cipher text CT, a secret key SK for an attribute set SX. If SX satisfies the access structure embedded in CT, it will return the original message M.

Drawbacks of the most existing CP-ABE schemes are single Central Authority(CA) did not manage any attribute but responsible for issuing user unique id (UID).This CA must have capacity to decrypt any Cipher Text(CT) on the cloud.

To overcome such a drawback here we can replace single CA to multi CA.in this paper we design secure cloud storage by providing access to the files using CPABE scheme.

III. SYSTEM ARCHITECTURE



CA Setup

The CA setup the system by running the CA set up algorithm. Each CAi accept both user & AAi registration for particular attribute domain.

User Registration

CAi first assign uidi to user. Also generate 2 random number uidi, uidi' using RSA algorithm, .Then generate global secrete keys are GSKi= uidi and GSK'i=aidi
Then global public keys are
GPKi= uidi and GPK'i=aidi

CAi also generate certificate(uidi) for user.CAisend global public key and global secrete key & certificate to user, that is set of (GSKi, GPKi, uidi).

Aai Registration

Every AAishould register to respective CAi, during
system initialization. If AAi is legal authority in the system,then CAi first assign a global attribute authority id aidi tothis AAi. Then CAi send the global public /secrete key ofeach user(GSKi, GPKi) to AAi, which can be used toverify the certificates of users issued by CAi.

Data Encryption by Owner

Owner send request to AAi for upload data by submitting ID, file, attribute set and policy structure, then AAi check for legal owner. If he is valid owner then AAi send public key to the user according to its role or identity.

Data Decryption by User

User send request to CAi using secrete public key pair GPKi, GSKi, UIDi.By submitting this certification (UID) to AAi,then AAi check for legal user. If he is valid user then AAi send attributes to the user according to its role or identity.

IV. CONCLUSION

Main goal of this system is to provide security against decrypting every cipher text by single central authority in Multi Attribute Authority - Attribute Based Encryption with single Central Authority system. In which different attribute authorities are managed by central authority according to their attribute domain. And no authority can independently decrypt any Cipher Text. And this can achieve more security as compared to Multi Attribute Authority Attribute Based Encryption single CA.

REFERENCES

[1]. Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, Yacine Challal. Secure and Scalable Cloud-based Architecture for e-Health Wireless Sensor Networks. International Conference on Computer Communication Networks (ICCCN), Jul 2012.

[2]. Minakshi V.Shinde,Prof.H.A.Hingoliwala, Secure Cloud Storage using Multi Attribute Authority with Multi Central Authority, International Journal on Recent and Innovation Trends in Computing and Communication, April 2015.

[3]. Annapurna Patil, Ashwini D V, Tulasi Srinivas, A Mobile Cloud based Approach for Secure Medical Data Management, International Journal of Computer Applications (0975 – 8887) Volume 119 – No.5, June 2015.

[4]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Journal of Future Generation Computer Systems 25 (6) (2009) 599–616.

[5]. Y. Wen, X. Zhu, J. Rodrigues, C. W. Chen, Cloud mobile media: Reflections and outlook, Multimedia, IEEE Transactions on 16 (4) (2014) 885–902.

[6]. S. Pandey, W. Voorsluys, S. Niu, A. Khandoker, R. Buyya, An autonomic cloud environment for hosting ECG data analysis services, Future Generation Computer Systems 28 (1) (2012) 147–154.

[7]. M. Barua, X. Liang, R. Lu, X. Shen, ESPAC: enabling security and patient-centric access control for eHealth in cloud computing, International Journal of Security and Networks 6 (2/3) (2011) 67–76.

[8]. D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, L. Alem, A platform for secure monitoring and sharing of generic health data in the cloud, Future Generation Computer Systems.

[9]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu, Plutus: Scalable secure file sharing on untrusted storage, Proceedings of the 2nd USENIX Conference on File and Storage Technologies, USENIX Association, Berkeley, CA, USA, 2003, pp. 29–42.

[10]. J. Benaloh, M. Chase, E. Horvitz, K. Lauter, Patient controlled encryption: ensuring privacy of electronic medical records, in: Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW ’09, New York, NY, USA, 2009, pp. 103–114.

[11]. W. Wang, Z. Li, R. Owens, B. Bhargava, Secure and efficient access to outsourced data, in: Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW ’09, New York, NY, USA, 2009, pp. 55–66.

[12]. J. Han, W. Susilo, Y. Mu, Identity-based data storage in cloud computing, Future Generation Computer Systems 29 (3) (2013) 673–681.

[13]. A. Sahai, B. Waters, Fuzzy Identity-Based encryption, in: Lecture Notes in Computer Science, Vol. 3494, 2005, pp. 457–473.

[14]. V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: Proceedings of the 13th ACM conference on Computer and communications security, CCS ’06, New York, NY, USA, 2006, pp. 89–98.

[15]. A. D. Brucker, H. Petritsch, S. G. Weber, Attribute-Based encryption with BreakGlass, in: Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices, Springer Berlin Heidelberg, 2010.