Investigation on PHR Security over Patient Centric Data using Time Stamp Server

Birru Devender[1] Dr. Syed Abdul Sattar[2]
[1]Scholar [2]PhD (ECE), PhD (CS) Director R & D, Professor
[1,2]Department of ECE
[1]Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, India [2]Nawab Shah Alam Khan College of Engineering & Technology, New Malakpet, Malakpet, Hyderabad. T.S. India

Abstract— *Now a days Cloud Computing is emerging solutions for storing and sharing of information in the cloud environment, where computing resources including process and storage is provided by a third party service provider i.e. they are semi-trusted in domain thus raise serious concern of individual privacy for the Adoption of cloud computing technologies. Where in the presented system in order to privacy protection concerned surveys of research categorized as privacy by policy, privacy by statistics, and privacy by cryptography applied on various public and personal domain. However, the privacy concerns and data sharing requirements on different parts of the medical data may be distinct ways it losses data integrity and authenticity when data are encrypted using an (Attribute Based Encryption)ABE scheme under KP-ABE and CP-ABE , key management is difficult if there is access levels are more from various backgrounds where in Health Domain . As our proposed system a novel access control scheme is proposed with Fine-grained access control which is patient centric includes Timestamp, ACP (Access Control Policies) and TTAA (Trusted Timestamp Attribute Authorities) which address the challenges of presented system.*

Keywords— PHR, timestamp server, fine grained access control

I. INTRODUCTION

Cloud computing is defined as global network where resources are shared by across different network and cloud computing offers many services among IaaS (infrastructure as a service), PaaS (Platform as a Service) and SaaS (software as a service) in this work using public cloud and DaaS (Database as a service) are implementing, in general public cloud accessed by everyone like DriveHQ and DropBox are example for public clouds. And using database service any user Maximum 1GB of data he can store in public cloud. And same way he can access freely across the world. Due to public and global access of cloud the PHR owner need to provide efficient security. Generally PHR system has multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners‟ PHRs. The users may come from various aspects; like, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners‟ data. Correctness of the PHI in the cloud is put at risk due to the following reasons. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they still face a broad range of both internal and external threats to data integrity. Outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may spoil the successful deployment of the cloud architecture. And the major issues in cloud is Personal health records security and PHR owner un able to controlling his sensitive personal records in cloud storage due to lack of security provided by cloud service provider and the major requirement in cloud computing is access control the PHR owner should enable access control over his data without any issues. Our Proposed work is to improve the privacy preserving PHR framework utilizing Attribute Based Encryption (ABE) with fine-grained approach with precise (accurate) time stamp Server for reliable patient data. Some of the key issues are given mentioned below. This research concentrates user privacy while outsourcing their data in cloud storage systems, a user may hold attributes issued by multiple authorities and the owner may share data with users administrated to different authorities. For instance, in an E-health system, the medical data may be shared only with a user who has the attribute of "Doctor" issued by a hospital and the attribute "Medical Researcher" issued by a medical research center. Some CP-ABE schemes have been proposed for such multiauthority systems. However, due to the inefficiency of computation, they cannot be directly applied to construct the data access control scheme. Basically, there are two operations in access control that require efficient computation, namely coarse grained approach and fine grained approach.

The key idea is to divide the system into multiple security domains is to avoid from high key management complexity for each owner and user (namely, public domains and personal domains (PD)) according to the different users' data access requirements. This research concentrates user privacy while outsourcing their data in cloud storage systems, a user may hold attributes issued by multiple authorities and the owner may share data with users administrated to different authorities. For instance, in an E-health system, the medical data may be shared only with a user who has the attribute of "Doctor" issued by a hospital and the attribute "Medical Researcher" issued by a medical research center. Some CP-ABE schemes have been proposed for such multiauthority systems. However, due to the inefficiency of computation, they cannot be directly applied to construct the data access control scheme. Basically, there are two operations in access control that require efficient computation, namely coarse grained approach and fine grained approach.

The key idea is to divide the system into multiple security domains is to avoid from high key management complexity for each owner and user (namely, public

domains and personal domains (PD)) according to the different users' data access requirements.

II. PROBLEM STATEMENT

Generally PHR system has multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners" PHRs. The users may come from various aspects; like, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners" data. Correctness of the PHI in the cloud is put at risk due to the following reasons. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they still face a broad range of both internal and external threats to data integrity. Outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may spoil the successful deployment of the cloud architecture. Our Proposed workis to improve the privacy preserving PHR framework utilizing Attribute Based Encryption (ABE) with fine-grained approach with precise (accurate) time stamp Server for reliable patient data.

III. IMPLEMENTATION

This research concentrates user privacy while outsourcing their data in cloud storage systems, a user may hold attributes issued by multiple authorities and the owner may share data with users administrated to different authorities. For instance, in an E-health system, the medical data may be shared only with a user who has the attribute of "Doctor" issued by a hospital and the attribute "Medical Researcher" issued by a medical research center. Some CP-ABE schemes have been proposed for such multiauthority systems. However, due to the inefficiency of computation, they cannot be directly applied to construct the data access control scheme. Basically, there are two operations in access control that require efficient computation, namely coarse grained approach and fine grained approach.

The key idea is to divide the system into multiple security domains is to avoid from high key management complexity for each owner and user (namely, public domains and personal domains (PD)) according to the different users' data access requirements.

A. Personal Domain (PD)

Personal Domain is used for Outsourcing the data by the data owners, data owners initially encrypts the data with content keys by using symmetric encryption techniques. Then, the owner defines the access policies with timestamp over attributes from multiple users and encrypts content keys under the policies. They do not trust on the server to do data access control. Instead, they assume that the server may give the data to all the users in the system. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the fine grained access policy with time stamp defined in the ciphertext and satisfied by the fine grained policy; then user is able to decrypt the ciphertext for the sake of Read or Write or Read-Write Operations.

B. Public Domains (PUD)

The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, and medical researchers. In practice, a PUD (Public Domains) can be mapped to an independent sector in the society, such as the health care, government, or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHR (Patient Health Record) s based on access rights assigned by the owner

1) Timestamp Server:

Time stamping service is primitive service in our methodology which protects data confidentially by providing data availability in Cloud Server with a specified time frame afterword's data will be unavailable once time excides which protects high security by data availability.

The objectives of this paper are to:

1) improving PHR framework efficiency and Privacy among multiple authority access
2) Prevention of Unauthorized Users by providing secure patient-centric PHR access and efficient key management using Fine-graininess of Access Control
3) Performing Attribute Revocation using forward and backward security.
4) Achieving authenticity and data integrity
5) Implementing Time stamp functionality for data availability and Security.
6) Updating attribute access Policy dynamically7 by TTAA behalf of Cloud Server.

IV. RESEARCH METHODOLOGY

This research concentrates user privacy while outsourcing their data in cloud storage systems, a user may hold attributes issued by multiple authorities and the owner may share data with users administrated to different authorities. For instance, in an E-health system, the medical data may be shared only with a user who has the attribute of "Doctor" issued by a hospital and the attribute "Medical Researcher" issued by a medical research center. Some CP-ABE schemes have been proposed for such multiauthority systems. However, due to the inefficiency of computation, they cannot be directly applied to construct the data access control scheme. Basically, there are two operations in access control that require efficient computation, namely coarse grained approach and fine grained approach.

The key idea is to divide the system into multiple security domains is to avoid from high key management complexity for each owner and user(namely, public domains and personal domains (PD)) according to the different users' data access requirements.

A. Personal Domain (PD)

Personal Domain is used for Outsourcing the data by the data owners, data owners initially encrypts the data with content keys by using symmetric encryption techniques. Then, the owner defines the access policies with timestamp over attributes from multiple users and encrypts content keys under the policies. They do not trust on the server to do

data access control. Instead, they assume that the server may give the data to all the users in the system. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the fine grained access policy with time stamp defined in the ciphertext and satisfied by the fine grained policy; then user is able to decrypt the ciphertext for the sake of Read or Write or Read-Write Operations

B. Public Domains (PUD)

The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, and medical researchers. In practice, a PUD(Public Domains) can be mapped to an independent sector in the society, such as the health care, government, or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHR(Patient Health Record)s based on access rights assigned by the owner

1) Timestamp Server:

Time stamping service is primitive service in our methodology which protects data confidentially by providing data availability in Cloud Server with a specified time frame afterword's data will be unavailable once time excides which protects high security by data availability.

V. CONCLUSION

In this work proposed time stamp server over patient centric data in multi-health care domains where group of doctors and patients share their personal heath records while sharing personal heath records the personal health record owner must be enable access control and policies over cloud shared personal heath records, and the PHR owner can control his data over encrypted cloud data. First PHR owner encrypt he personal heath record under set of policies and he upload to the cloud and doctor or user who want to download the personal health records they first get the secrete key from the owner and they can download the personal health records from cloud after downloading using secrete key they can decrypt but if any policies changes then the PHR owner with help of trusted third party auditor (TTA) will generate new keys to the un revoked users while revoked user secrete key remains same and revoked user can't download the PHR so in this process the TTA will update the attributes whenever user polices changes and PHR owner can define attributes with time stamp using this a particular user attributes will expiries in certain time period and in this process using asymmetric encryption personal health record will encrypt and keys will distribute to the corresponding to the users via secure channel.

REFERENCES

[1] Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, pp. 62–91.

[2] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M.Wu, andD.W.Oard, "Confidentiality-preservingrank-ordered search," in Proceedings of the 2007 ACM workshop on Storage security and survivability. ACM, 2007, pp. 7–12.

[3] Advanced SaaS Security Measures, Overview of BlueTie Security, SaaS Security White Paper,December 2012.

[4] AbhaSachdev and MohitBhansali,"Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications 67(9), April 2013.): pp19-23 Published by Foundation of Computer Science, New York, USA.

[5] Akhilesh Kumar Shrivas, S.K.Singhai and H.S. Hota," An efficient decision tree model for classification of attacks with feature selection", IJCA, vol84, No.14, Dec 2013.

[6] ArezooJahani, Leyli Mohammad Khanli, SeyedNaserRazavi," W_SR: A QoS Based Ranking Approach for Cloud Computing Service," Department of Electrical and Computer Engineering, University of Tabriz, Iran.

[7] A. Goscinski, M. Brock, "Toward Dynamic and Attribute Based Publication, Discovery and Selection for Cloud Computing," Future Generation Computer Systems, Vol. 26, No. 7, pp. 947-970, 2010.

[8] Almulla, S.A.;ChanYeobYeun," Cloud computing security management" Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on; 05/2010

[9] B.Arun,S.K.Prashanth,"Cloud Computing Security Using SecretSharingAlgorithm",Indian Journal of research, Volume : 2 , Issue : 3 , March 2013, pp 93-94.

[10] BinaKotiyal,PritiSaxena, R.H.Goudar,Rashmi.M. Jogdand," A 5 Level Security Approach for Data Storage in cloud", IJCA,Vol. 54-No11, September 2012 pp 29-34.

[11] Brunette, G., &Mogull, R.: Security guidance for critical areas of focus in cloudcomputing v2.1. Tech.rep., CSA,December 2009.