ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

SMHRW: Secure Maintenance of Health Records in Well Organized Way

P.Murali[1], T.VenkataRathnam[2]

M. Tech (CSE), SSITS, Rayachoty, A.P, India[1]

Assistant Professor (CSE Department), ITS, Rayachoty, A.P, India[2]

Abstract: This paper presents implementation of personal health records based on cloud computing systems as it is a sharing personal heath record in third party system such as cloud. Security is provided using balanced Encryption. For maintaining the patient's information we are providing centralized server for Personal Health Record (PHR). Personal Health Records can be accessed by different types of people with high privacy and security. The security authentications are used to protect the personal data from public access. Patient records can be accessed by different people like medical history, insurance people. Access permissions are provided for particular set of attributes with high security. All the files should be stored in cloud which are semi-trusted servers these, are in encrypted form and also re confidential to other users. There are various issues such as risks of privacy exposure, efficient user revocation, flexible access, scalability in key management and efficient user revocation, the most important challenge is achieving in depth cryptographically enforced data access control. For well organizing of health records we follow the technique attribute mean value to fill the missing values(or) fields and to achieve in depth and scalable data access control for personal health records stored in semi trusted servers, we can use ABE techniques to encrypt each patient's medical record files. Numerous PHR owners access the same data values in many times. The proposed scheme in this paper is Multi Authority Attribute Based Encryption (MA-ABE) and dynamic modification of access policies, file attributes, break glass access under emergency conditions and it supports on demand attribute revocation. Results are provided with efficiently security and sharing manner.

Index Terms: Cloud Computing, Personal Health Records, Data Privacy, Attribute Mean, Multi Authority Attribute-Based Encryption

I. INTRODUCTION

What is Data? Data is a raw fact or unprocessed information (or) Data is a collection of facts, such as values or measurements. Record is when related data is being processed, filed and kept, that is a record. A record is made in the form of data. Organizing Data: When data is collected from a survey or designed experiment, they must be organized into a manageable form. Data that is not organized is referred to as raw data. The organizing data can be displayed in the form of Tables, Graphs, Bar charts, pie charts, Histograms etc.

Maintenance of Data: In this paper we suggest that the health records data can be maintained in secured way. Here the security we are providing encryption and decryption.PHR owner can provide the encryption keys to doctors, patients, hospitals. By using the decryption keys the PHR users can access their files. Remote Accessing of Information: Here we are saying that PHR users (patients, doctors, hospital management, and insurance companies) can access their files remotely through cloud by using some applications. The users can easily access their information through the provided keys.

II. RELATED WORK

Attribute Based Encryption was introduced along with cryptography called fuzzy identity-based encryption (FIBE) [7] by Sahai and Waters. Both ABE and FIBE are based on bilinear maps (pairing). In ABE system, users' private keys and cipher text are labeled with sets of descriptive attributes and access policies respectively, and a particular key can decrypt a particular cipher text only if associated attributes and policy are matched**.**

Key policy Attribute Based Encryption: The key-policy attribute-based encryption (KP-ABE) was first introduced in 2006 by Goyal et al. [2] In this cryptography system, cipher text are labeled with sets of attributes. On the other hand Private keys are associated with access structures. A private key can only decrypt a cipher text whose attributes set is authorized set of the private key's access structure. Key-policy attribute-based encryption is a cryptography system built upon bilinear map and linear secret sharing schemes.

Multi Authority Attribute Based Encryption: In a multi-authority ABE system [9], we are having many attribute authorities to a PHR owner, and users. A group of system wide public parameters available to everyone. A user can choose to go to an AA(Attribute authority), proves that it is entitled to some of the attributes handled by that authority, and request their corresponding decryption keys. This authority will run the attribute key generation algorithm, and return the results to the user. Any user can also choose to encrypt a message; in this case he uses the public parameters together with an attribute set of his choice to form the cipher text. Any user who wants to decrypt message he can choose decryption keys according to an appropriate attribute set can use them for decryption purpose.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

III. PHR MODEL FRAME WORK

Problem Definition: To show a Novel patient-centric scalable and secure data sharing framework for cloud-based PHR systems. Multiple PHR owners and PHR users needed to design PHR system .The PHR owners refer to patients who have full control over their own PHR data, The PHR owner and PHR users can create, manage and delete it. Users are a friend, a caregiver or a researcher. Users access their PHR documents through the semi trusted server in order to read or write to someone's PHR, and a user can access simultaneously multiple owners' data but without the permission they can't delete it. For the Security reasons system is preloaded with some public (or) private key pair. This PHR Project objective is in terms of security and performance is to attain data confidentiality by restricting unauthorized user from encrypting/decrypting a PHR document. To support on demand revocation. Restricting write Access control only to owner in key management system should be highly scalable

IV. PROPOSED SOLUTION

Personal Health Record Owner: The PHR owner registers his personal information in the system. When a PHR user request for registration into the server in the semi trusted server PHR user requests the user's registration at the time of registration user provides a public key and a secret key.PHR owner stores the user's data into the server by encrypted format by using key policy based encryption. The PHR owner refers to patients and they have full control on their own PHR data, they can create, manage, control and delete it. The PHR owner is having their own choice related to either the data may be public or private. The private data will be available at PHR owner. The private data can be view only secret key of associated PHR owner submits to the server. Whenever the PHR owner keeps his data as public the public authority people will view his data by using their secret key. Here the public authority is hospitals, doctors, insurance companies, physicians. Sensitive data is kept as private i.e. confidential this data can't be viewed by any other person in the PHR system. And also here I am proposing Data ware housing cleaning technique for PHR records. If there is any missing attributes in the PHR records we can apply attribute mean to fill the missing values or fields. And also most probable value to fill in the missing values (or) fields.

Public Authority Agents: Public Authority Agents (PPAs) can view the data of a Public and Personal Information with the help of PHR Owner. The PAAs Maintains the PHR Owner and the user's Personal Information. Using the MA based encryption PPA's can send secret key to an user who request for data of a patient(PHR owner) through emergency conditions.PHR owners can access their particular session only with the help of provided key. The Public Authority Agents (PPAs) have control over their public data of PHR.PPA's don't have permission to write or change PHR owner data. Here PPAs can only view and read PHR owner data. By using MA-ABE we can implement break glass access for emergency conditions, here the break glass access is temporary access to the PHR data of a PHR owner for PPAs.

Search User: Here the search users are like physicians, doctors are interested to view the PHR data for their research available in PHR server. They did not keep PHR data into their systems but interested to accessing the other PHR owner's data and getting useful information from them. While the users register their personal information into the server after successful registration he gets a secret key. A PHR server is provided to explore the Patients Health Records (PHR owners). He can view them by providing his Private Key generated by Generic Anonymous Key Issuing Protocol of MA ABE. Whenever a user enters a correct secret key he can view his/her PHR data. If the user enters incorrect key and tries to access by giving wrong moles rate will be counted and the user is blocked and we did not allow to login permananently. If the user gives login credentials correctly he can view the PHR data. The user if enters the correct Secret key He can able to view the PHR data.

Algorithms of for KP-ABE with improvement are discussed as below:

(1) KP-ABE Setup (A): Outputs public key PK and Master key MK for A as set of attributes Associate for each attribute in A with attributes universe as U = {1, 2... n}. It defines a bilinear group G1 of prime order p with a generator g, a bilinear map e: G1 × G1 -> G2 which has the Properties of bilinearity, computability, and non-degeneracy. Associate each attribute i ∈ U with a number ti and also chose y uniformly at random in Zp* and y.

The public key is:

PK = (T1 = gt1, ..., T1 = gt|U | , Y = e(g, g)y)

The master key is:

MK = (t1,…, t|U |, y)

(2) KP-ABE Encryption (M, γ, PK): M message in GT with a set of attributes γ , PK is public Key , outputs Cipher Text E. Choose a random value s in Zp. Encrypt a secret message M in GT with a set of attributes γ.

The cipher text is: E = (γ, E‟ = MY s, {Ei = Tis} where i∈ γ)

(3) KP-ABE Key Generation (A, MK): This algorithm output a secret key D embedded with an access structure T. The access structure A is realized by the following three steps:

1. For root node r, set value secret = y. mark all node un-assigned and mark root node assigned.
2. Recursively, for each assigned non-leaf node,

a) If the operator is ^ (and) and its child nodes are noticeable un-assigned, let n be the number of child nodes, set the value of each child node, except the last one, to be si ∈ Zp, and the value of the last node to be sn = s -∑ si . Mark this node assigned.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

b) If the operator is V (or), set the values of its child nodes to be s. spot this node assigned 4) KP-ABE Decryption (E, D) this algorithm takes as input the cipher text E encrypted under the attribute put U, the user˝s secret key SK for entrée tree T, and the public key PK. Finally it output the message M if and only if U satisfies T.

Basic Algorithm of the MA-ABE with improvement is:

(1) Key Issue (Attributes, MK, PK). This algorithm, the AAs together actively generates a secret key for a user. For a user with (secret) ID u, the secret key is in the form:
SKu = ⟨Du = g^Ru, {Dk;i = g^(qk(i)/tk,i) , Verk,i} k∈{1…N} ⟩
where Ru is a universal ID for user u, and qk(0) = Σk vk −Ru.

(2) Encryption (M, PK, attributes []): This algorithm take a message M, PK and a set of attributes and outputs the cipher text E as follows:
CT = [E0 = M·Y^ s,E1 = g2^s, {Ck;i = Tk;i^s, Verk;i};k∈{1..N}]

(3) Decryption (*CT, SKu*): This algorithm takes as input a cipher text *CT* and a user secret key *SKu*. If for each AA *k*,If the version of the attribute in SK and CT matches, algorithm pairs up the $D_{k;i}$ and $C_{k;i}$ and reconstructs $e(g1, g2)^{sq_k}(0)$. After multiplying all these values together with $e(Du,E_1)$, *u* recovers the blind factor Y^s and thus gets *M*.

(4) Update Parameter: This algorithm updates an attribute to a new version by redefining its system public key and master key components. It also outputs to a proxy re-encryption key and re-secret-key between the old version and the new version of the attribute.

(5) Update Secret Key: This algorithm translates the secret key component of attribute i in the user secret key SK from an old version into the latest version using re-secret-key generated in step 4

(6) ReEncryptFile: This algorithm translates the cipher text component of an attribute i of a file from an old version into the latest version using proxy- encryption key generated in step 4.

V. ADVANTAGES

Security: No one can access the users profile without providing the user secret key. The PHR owner allows accessing read or writing permissions only the members of personal and public domain can access the records. The data will be high secured by using MA-ABE the information is encrypted before outsourcing. For decrypting the information also they need a secret key.

Storage: The encrypted data will store in cloud server for better output The entire information will be stored in semi trusted server. In the cloud server requested attributes are encrypted .The records are divided into attributes for memory allocation it saves the memory space.

Portability: PUD and PSD user can access their information anywhere in the world at any time. Encrypted data stored in semi trusted servers. It greatly reduces their cost for accessing their information. Easy access for under emergency conditions.

VI. CONCLUSION

Personal health Records needs the security because attackers and hackers stolen the PHR data. It causes the risks to the patients and PHR owners. So we are going to provide security for to protect information from unauthorized access. Patients (PHR users) having complete control and privacy on their own records. These control and privacy provide through encryption techniques. A unique challenge produced by PHR users and PHR owners such as and key management complexities and security are effectively reduced by using DES encryption.ABE is used for encrypt the PHR's data, so that PHR users (patients)

Can allow accessing not only to their personal user's public domain and professional's access that PHR data with decrypt keys. On demand user revocation and break glass technique provided with security is also achieved.

REFERNCES

[1] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW ˝09, 2009, pp. 90–114.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS ˝06, 2006, pp. 78–110.

[3] A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin. Self-protecting electronic medical records using attribute-based encryption on mobile device. Technical report, Cryptology ePrint Archive, Report 2010/565, 2010. http://eprint. iacr. Org/2010/565.

[4] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 34–76.

[5] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009. Pp.121-142

[6] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[7] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded,"http://articles.latimes.com/2006/jun/26/health/he-privacy26, 2006.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

[9] M. Vijayapriya Dr. A. Malathi , M. Phil. Research scholar PG & Research Department of Computer Science" Multi Authority Attribute Based Encryption for Personal Health Record". International Journal of Computer Trends and Technology (IJCTT) - volume 4 Issue 8- August 2013

[10] C. Cachin, I. Keidar, and A. Shraer, ―Trusting the cloud,‖ SIGACT News, vol. 40, no. 2.

BIOGARPHIES

P.Murali Was born in Andhra Pradesh, India in 1984.He received bachelor degree, B.Tech (CSE) from the University of JNTU, Hyderabad, in 2006.He is currently pursuing Master degree, M.Tech (CSE) in Sri Sai Institute of Science &Technology, Rayachoty.