Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.894 – 900

RESEARCH ARTICLE

Personal Health Record Management Using Attribute Based Encryption

Sourabh S. Bhendawade[#], Ajinkya R. Ugale[#], Ravi S. Kurade[#], Hrushikesh S. Kate[#]

[#]Department of Computer Engineering, JSPM's Imperial college of Engineering and Research, Savitribai Phule Pune University

[1] bhendawade2308@gmail.com

[2] ajinkya.ugale143@gmail.com

[3] ravirajkurade@gmail.com

[4] hr007@gmail.com

Abstract: Cloud computing is newly formed technology in which resources of the computing infrastructure are used as services on web. It easily handles new challenges for the PHR data security and access to the PHR data when user wants to transmission of data for sharing on cloud, which is not between same trusted owners of data. To provide security against the unauthorized server, previously or existing method usually used is cryptography, encrypting the data using key which is only decrypted by the authorized user. It is hard to manage key arrangement and management of data. It is not suitable and well scale. The scalability and security related to access control of data still not remove. In this, the new access policy is introduced that the encryption is based on data attributes. Attribute Based Encryption method (ABE) used to encrypt each patient's PHR data file. It is different from previously used method of data outsourcing, in that we considering the multiple PHR data owner. This technique reduces the key arrangement problem of owner and user. We achieve the goal data security and sharing problem of data between multiple domain data owner is resolved. After extensive analysis and test results shows that our system technology are highly suitable and properly secure under the previous security techniques.[1],[2],[3].

Keywords—ABE encryption; Cloud computing; limb donnar; PHR data

1. INTRODUCTION

Cloud computing is a method of delivering technology to the user. Cloud computing pattern is very important in academia as well as in industry. By merging the set of existing and new methods from research and test areas such as visualization and Software Oriented Architecture (SOA).In cloud computing resources are provided as service to the user over internet. Cloud computing is also used in Business model to provide the services to the consumer. The business models provides the old as well new technology to the user, this term explain as Y as a service (YAAS) where Y could be a software, hardware or data storage. Y is provided as service to the user.[4]

Our approach is to encrypting the data before the transmission using the attribute based encryption. The PHR owner decides the access of the data to the users. The authorized person can use PHR data for their professional and public use. In this we divide the system into two parts public and private domain. To protect the PHR data we used attribute base encryption (ABE).

Attribute is very important in attribute based encryption scheme. Attribute based encryption build the access policy using the user's private key and describe the encrypted data with the users attributes.

Attribute based encryption as the two main advantages:

1) Communication overheads of the web are removed.

2) To provide the fine grained access control.

In recently years cloud has emerge to provide the many application based services satisfy the users requirements. Cloud provides the storage application in which the users are able to store the data on cloud and share it. And user can access this stored data from anywhere. We just have to pay money for required space on cloud. Cloud server is operated by the commercial provider. Storing the users data secure from storage server is not only option but it is the main requirement of the cloud user.

There are three types of cloud computing services

1) Software as a service (SaaS)

2) Platform as a service (PaaS)

3) Infrastructure as a service (Iaas)

We are using cloud for personal health record data storage only in our system.

1.1 Framework overview in PHR:

The main goal of this framework is to that provide security for accessing the data and management of data same time. The idea is divided the system into two parts i.e. public domain and private domain. Public domain consists of doctors, nurses and insurance companies. In personal domain user can give the authority for accessing or updating of data to its friend or closed relative.

In this both type we use ABE (attribute based encryption) for encrypting or decrypting the data. User in public domain access data with secret key indirectly by interact with system. The public domain consists no of user so it reduces the key management in both owner and user.

Each data owner is trusted of its own personal domain, which manage secret key and access the data. In personal domain attribute refers to intrinsic property of data. The user in personal domain is less so it reduces the burden of the owner. When encrypting the data owner need intrinsic properties.

The use of ABE is to encrypt data for safe storage. This data can access by authorized user from the server. On-demand user revocation is made possible in ABE.

2. Literature Survey

Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption [6]

- The author proposed that," Personal Health record management system is emerging patient centric model used for storing information on third cloud in encrypted format which is invisible for third party, And also to exchanging information which is stored on cloud. To ensure patients about storing information on cloud Attribute Based Encryption (ABE) technic is used."
- The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains and personal domains) according to the different users' data access requirements.[7]
- In existing system, there are multiple users who can encrypt information in their own ways, either using same cryptographic key or different cryptographic keys also there arrangement to done key ESROW in which data can decrypted present in this key hence there may be possibility third party can gain access.
- Information updates. A PHR user/owner can update their sharing policy for an existing PHR document by updating the attributes (or access policy) in the cipher text. The supported operations include add/delete/modify, which can be done by the server on behalf of the user.
- Break-glass. When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department. To prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergent access via the ED.[8][9]

3. Proposed System

Block Diagram:

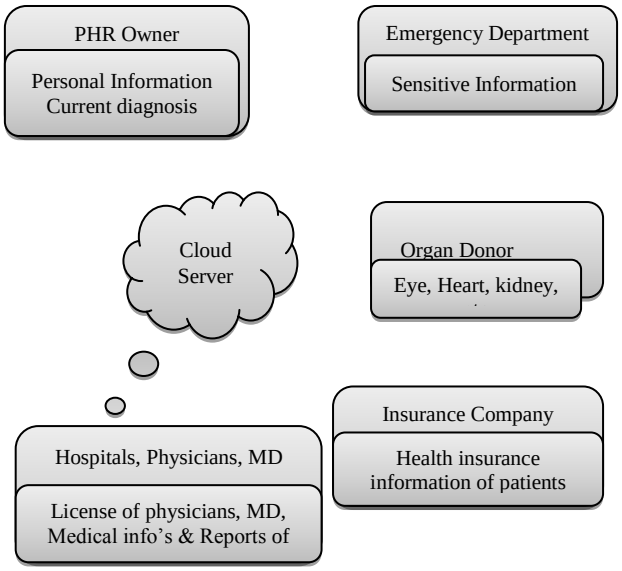


Fig 1:- Block Diagram

- We are trying to provide secure patient-centric personal health records (PHR) information which is stored on semi trusted web server and cloud server and finding the complex & challenging key management aspects. In order to provide more security to personal health data stored on a server for that purpose we are including attribute based encryption technique (ABE) as main encryption technique.

- In existing system there are multiple owners who create multiple encryption keys with their specific ways using different set of cryptographic keys, which leads complexity and key management issues. Using ABE we are able to access the terms and policies of particular person using id (attribute) which enables patients to respectively share PHR among all patients. we can encrypt users file without knowing complete list of users. The difficulties about encryption key generation are very rare.
- As per attribute based encryption we have to one unique id for each patient. A key which may valid only for one user which is not common among all. In India we consider then each person has its unique ADHAR CARD number. So now we are providing ADHAR CARD number as attribute for each person. Encryption is done through that attribute whenever we want to search the PHR the we have to just enter his ADHAR CARD number.
- Also we endeavoring the comparative search in which patient who can see another patients suffering from similar disease. It is up to patient to take treatment or not.

- We also trying to limb donation system which is another part of our project that may help In to find out the limb donor. This system is directly linked with donning camp while filling registration form it is optional for donor to donate his limb its not mandatory. Whenever some of donors will found then an email is directly sent to the needed donning camp. In future we make it as SMS based system.

4. MATHS MODULE

A] Identify the Cloud Infrastructure

$C = \{c1, c2, c3 \ldots.\}$

Where,

'C' is main set of number of clouds like c1, c2, c3…

B] Identify the Virtual Machine Monitors (VMM)

$V = \{vmm1, vmm2, vmm3 \ldots.\}$

Where,

'V' is main set of Virtual Machine Monitor's (VMM's) like vmm1, vmm2, vmm3…

$V \in C$ (V is a subset of C, such that cloud contains various virtual machine monitors)

C] Identify the Virtual Monitors

M = {vm1, vm2, vm3 …}

Where,

'M' is main set of Virtual Monitor's (VM's) like vm1, vm2, vm3…

M € V (M is a subset of V, such that virtual machine monitor have number of client machines as VM's)

D] Identify the Running Applications

A = {a1, a2, a3….}

Where,

'A' is main set of Running Applications like a1, a2, a3…

A € M (A is a subset of M, such that virtual machine can run number of applications defined by a1, a2, a3…)

E] Identify the Instructions

I= {i1, i2, i3…}

Where,

'I' is main set of instructions i1, i2, i3, … given to VM by VMM

The instructions are like, RESTART, LAUNCH, STOP, TERMINATE, CLOSE, etc.

F] Evaluate the Algorithm

Algo = {al1, al2, al3}

Where,

'Algo' is main set of algorithms al1, al2, al3

i.e {Analysis VM, Load Balancing, REJ}

al1: Analysis Virtual Machine: (this algorithm is used to analysis, running applications on VM, memory consumed by each application and hence total memory consumed)

Input:

- A set of running applications on VM, i.e. {A}
- A threshold value (M_{th}) against which VM was analyzed

Output:

- Status of VM in terms of memory and applications state

G] For running applications A on VM,

$$M_{tot} = M(a_1) + M(a_2) + M(a_3) + \ldots + M(a_n)$$

Where,

n = total number of running applications

$M(a_1)$ = memory consumed by running application a1 and similarly for $M(a_2)$ to $M(a_n)$

If $M_{tot} <<< M_{th}$, no need to implement any of remaining algorithm al2 &/or al3

al2: Load Balancing Algorithm: (this algorithm is implemented to balance the load between different machines i.e. VM's.

Input:

- Output of al1

Output:

- Instruction to VM
- Load balancing such that Application Shifting from source to destination machine

Let,
Identify the heavy application of VM

A_H = {set of heavy applications} = {a_{h1}, a_{h2}, a_{h3} . . . }

Where,
A_H € A (such that A_H is subset of all running applications on VM)

If (application was consuming more memory) then INSTRUCT SHIFT

This performs closing of application on VM_s (source VM =VM under monitor) safely and shifting to VM_d (destination VM = VM having capability to host application)

al3: REJ: Algorithm to Restart or close or terminate

Input:
- An output of algorithm al1

Output:
- Either application was terminated or restarted

Identify the failure applications
A_f = {set of failure application)

If (Application was not responding) then INSTRUCT TERMINATE
This performs termination of non responding application

Identify the Processes as P.
P= {p1, p2, p3, p4…..}

Where P is the main set of Processes p1, p2, p3, p4…..

P1 = {e1, e2}

Where

{e1=VM was added as client of VMM}
{e2=VM get login/connected with VMM}

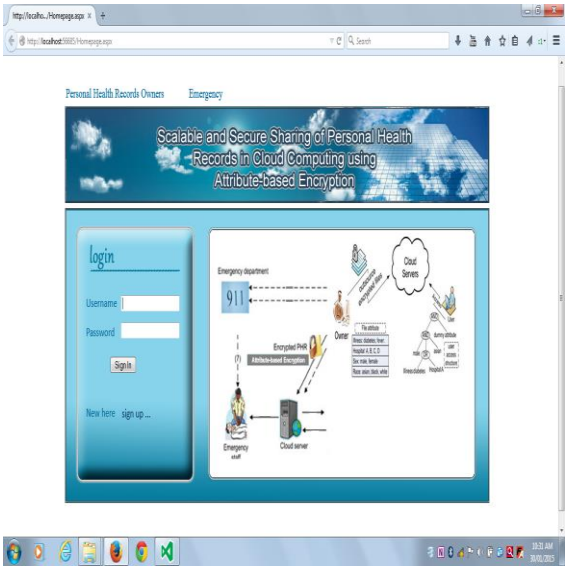
P2 = {e1}

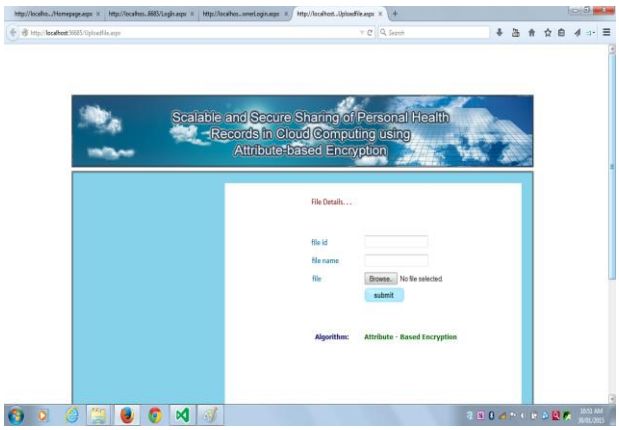
Where
{e1=check VM status}
P3 = {e1, e2, e3}
Where
{e1=check running applications}
{e2=summation of total consumed memory}
{e3=analysis against threshold value}

If (*Total consumed memory is near about threshold value*) then

P4 = {e1, e2, e3, e4}
Where
{e1=isolate the heavy applications}
{e2=check for heavier application}
{e3=check for capable destination VM}
{e4=Shift application from source VM to destination VM}
If (*application was not responding*) then
P5 = {e1, e2}
Where
{e1=check for failure application}
{e2= terminate failure application}

5. FINAL OVERWIEW





6. Conclusions

We conclude that the PHR management using attribute based encryption is reliable for the patients and doctors of today's busy world. The patients will not require to stand in such a big queue for the check-up. They can easily take an appointment by this PHR system. It also conclude that The patient can easily store there Personal Health Records i.e. PHR on Cloud Server by unique ADHAR CARD number. For security purpose this health records are stored in unreadable format on cloud. Health records storing on cloud server reduces marinating & managing file.

Distributed Attribute- Based Encryption," Proc. 11th Int'l Conf. Information Security and Cryptology (ICISC 08), pp. 20-36, 2009.

7. Acknowledgement

We are always thankful to our guide Prof. S. M. Tidke for his valuable discussion and constructive suggestions, which greatly contributed to our Paper. We sincerely thank our Head of Department (Comp.) Prof. S.R.Todmal for his reassuring encouragement throughout the preparation of our Paper. We are also grateful to our respected Principal Dr. Sachin Admane sir for his co-operation despite his busy schedule. Last but not the least we thank all the staff members of Computer Department for providing an excellent environment to undergo this Paper.

References

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10),

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] Cloud Computing Security: From Single to Multi-Clouds Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom*

[5] J. Li, K. Ren, B. Zhu, and Z. Wan, \Privacy-aware attribute-based encryption with user accountability," *Information on Security*, vol. 5735 of LNCS, pp. 347 Scalable and Secure Sharing of Personal

[6] Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE

[7] Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption by www.chennaisunday.com

[8] N. Attrapadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," Proc. Third Int'l Conf. Palo Alto on Pairing-Based Cryptography-Pairing, pp. 248-265, 2009

