PROVIDING SECURITY TO PERSONAL HEALTH RECORD IN CLOUD COMPUTING USING ABSTRACT BASED ENCRYPTION

Anamika Datta1, Dharmendra Singh2, Abhishek Dalal3, Tanuj Kumar Singh4

Computer Science & Engineering (BE), Brindavan college of Engineering, Bangalore, Karnataka.

1. dattasonu145@gmail.com, 2.jatboy.singh@gmail.com, 3.Debnathabhishek441@gmail.com, 4.Tanuj.542@gmail.com

Abstract: **This paper present the design and help to implement Personal Health Record(PHR) using such as cloud. Personal Health Record allows people to coordinate their lifelong health information and even they can access this information from anywhere as its Web based application. To provide security we used Attribute based Encryption for Personal Health Record. Here Attribute Based Encryption will encrypt the data before outsourcing to third party. Here we focus on Multi Authority Attribute Based Encryption (MA-ABE) also which any polynomial number of independent authorities to monitor attribute and distribute secret keys. Our scheme provides high degree of patient's privacy as well as gives PHR owner full control of his/her data. Here our proposed system is highly efficient security and performance analysis.**

Keywords: Personal health record, multiple authority, Attribute authorities, cloud computing, Key management, fine-grained data access control.

I. INTRODUCTION

PHR is an emerged-centric model which takes care of health information and also them to exchange their information with each other through web. It enables the patient to create, manage & retrieve the data with the help of web because of high cost & maintaining data many PHR services outsourced to third party services. While using this service we mainly concern on security and privacy issues. As we storing the data to third party this is not fully trusted. Hence to overcome from this we encrypt the data before outsourcing and PHR owner will only decide that which user will get access to which data in his Personal Health Record. PHR owner will provide the decryption key to the user and PHR file should available to those users only. Personal Health data that is stored in semi trusted server will be protected by Attribute Based Encryption as main encryption primitive.

II. RELATED WORK

At the early stages the traditional encryption techniques were applied to the personal health record and now days the advanced encryption techniques such that attribute based encryption and its different variation are used. To improve the security we are using one-to-many encryption method such as Attribute Based Encryption. Attribute Base Encryption is used to prevent against user collusion.

A. *Public key encryption:*
The public key encryption method was the most traditional method applied to the PHR for the security of the data. But it made the high key-management problems and also this method was very less scalable.

B. *MultiAuthority Attribute Based Encryption (MA-ABE):* This method allows n number's of independent authority to distribute secret key and monitor all attributes. Encryptor can choose decryption key and set of attributes and then he will able to decrypt the data as he is having decryption key of given attribute.

ISSN: 2278-0181

C. *Cipher Text Policy Attribute Based Encryption (CP-ABE):* This method is used to keep encrypted data confidential. Cipher text attribute based encryption is an attribute based encryption technique which allows the data owner to encrypt the data based on an access policy, which will be based on the attributes of the user or the data. So, the decryption is possible when the secret key is matching with the access control policy.

D. *Attribute Based Encryption (ABE):* Here attributes defines an object very efficiently just an identity of an object works. Attribute base Encryption provides security to the database. Here we provide both cipher text & secret key which will be associated with attributes.

E. *Key-policy based encryption:* It is an attribute based encryption in which the data are associated with the attributes, for each of which a public key component is defined. In this method, each user will be assigned to an access structure which will
.specify which type of cipher texts the key can decrypt. The secret key is defined to reflect the access structure. So the user will be able to decrypt a cipher text if and only if the data attribute satisfy that user's access structure.

III.THE EXISTING SYSTEM

In the existing system the Cipher-Text attribute based encryption (CP-ABE) is used which is a variation of attribute based encryption scheme. The data owner is uploading the data to the cloud server after encrypting the data according to the access control policy [7] defined with the set of attributes. This encrypted data can be decrypted by the user only if the attributes of that user satisfies the access control policy P.

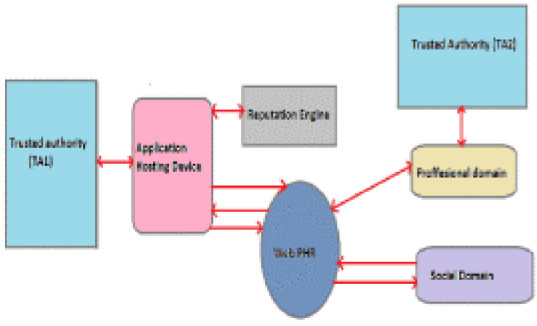

Fig.1 The existing PHR-system

The working principle:

1. At first the key-generation algorithm will run by the both the trusted authority by using CP-ABE scheme.
2. The professional domain users will obtain their secret keys according to their attributes defined in the system.
3. The patient will create the measurement data by the help of devices and tools and which will send to the application hosting devices like personal computer or mobile phones.
4. The hosting device will encrypt this data after the categorization according to an access policy.
5. The encrypted data will send to the web PHR repository.
6. When the user wants to see this data, they can download the encrypted data from the server and can decrypt them locally by using the secret key.

IV. PROBLEM DEFINITION

The problem is being extended to a wider range, where a number of PHR owners and users are involved. The owners refer to patients whose medical related data are being controlled and the users are those who try to access them. There exists a central server where owners place their sensitive medical data, and attempted by users to gain access. 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. This leads to the need of Multi-Authority Attribute Based Encryption (MA-ABE).

A. *Prevention of Unauthorized Users:* An important requirement of efficient PHR access is to enable "patient-centric" sharing. This means that the patient should have the ultimate control over their personal health record. They determine which users shall have access to their medical record.

B. *Fine Grained Access Control:* Fine grained access control should be enforced in the sense that different users are authorized to read different sets of documents. The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute.

V. PROPOSED SYSTEM

Above problems can be resolved by using this proposed system. Personal Health Record is a web based application that allow user to access and coordinate their health information for life long. Here we mainly concert how to provide proper security to the data present in the cloud. Hence we propose unique authentication and encryption technique. Proposed system is provide fine-grained access and users are classified into two security domain called personal security domain and public security domain System achieves data confidentiality by providing enhance MA-ABE scheme. Cloud server plays a main function by providing interface between application and user and authentic user will have user name and password and if user is authentic then only he/she get access to their record.

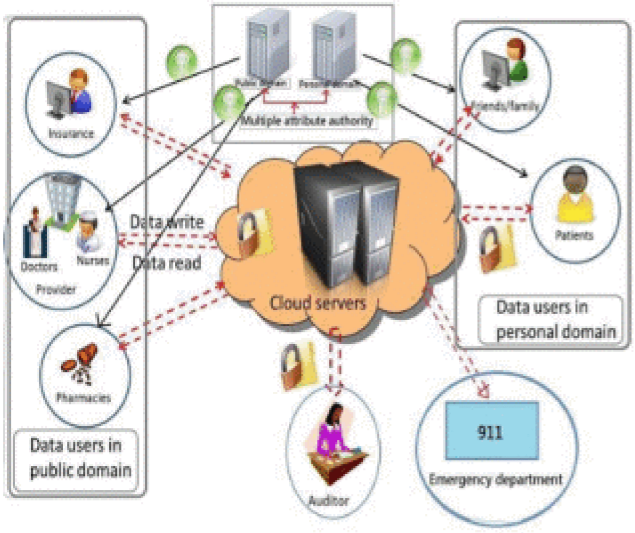

Fig2: Proposed System

VI. ATTRIBUTE BASED ENCRYPTION

Using Attribute Based Encryption we are providing security to database, so that data can be shared and stored on cloud server, before storing data at third party we have to encrypt data. In Attribute Based Encryption cipher text labeled with set of attributes and private key is associated, that control which cipher text a user has to decrypt. Using Attribute Based Encryption, policies are made which based on attributes of user or data, which enables patient to share their Personal Health Record.

A. SYSTEM FLOW DIAGRAM

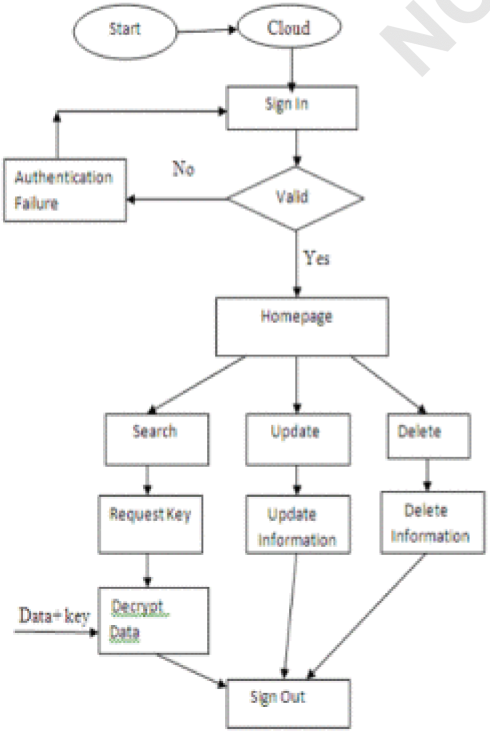

Fig 3: System Flow Diagram

B. SYSTEM ARCHITECTURE DIAGRAM

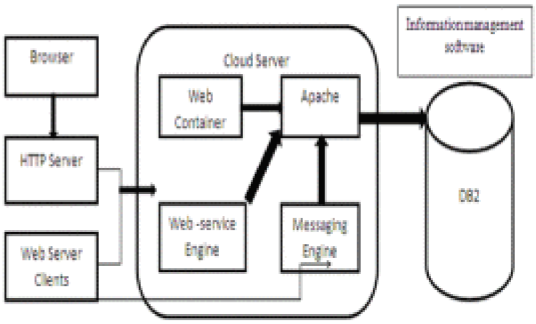

Fig 4: System Architecture Diagram

C. ATTRIBUTE HIERARCHY

We are using Attribute Based Encryption for providing security, we use following PHR's attribute hierarchical structure.

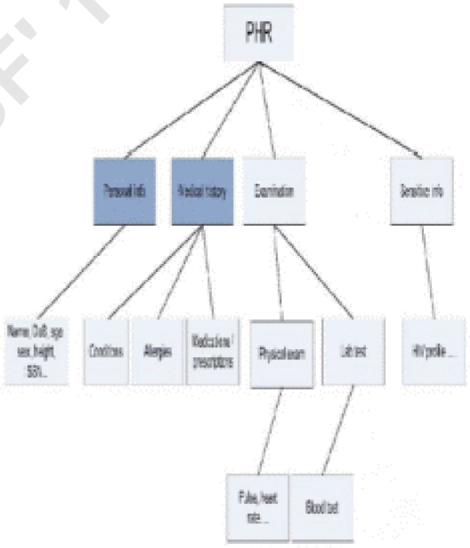

Fig5: Attributes

VII.CONCLUSION

Provide securities to protect information from unauthorized access. This paper approach existing Personal Health Record system for providing more security using Attribute Based Encryption. As well as cloud computing storage and sharing secure is highly utilized by users.

ACKNOWLEDGMENT

The satisfaction and euphoria that accompany successful completion of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crowned our efforts with success. We feel delighted to have this page to express our sincere thanks and deep appreciation to our guide, Prof SOUMYALATHA for valuable guidance.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM"10, 2010

[3] S. Narayan, M. Gagn'e, and R. Safavi-Naini, "Privacy preserving phr system using attribute-based infrastructure," ser. CCSW '10, 2010

[4] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06)