International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.10, October 2015 DOI:10.15693/ijaist/2015.v4i10.35-38

Enhanced USB Security in Secure Sharing Personal Health Record using Attribute Based Encryption

Anju P R
Department of Computer Science and Engineering
Adi Shankara Institute of Engineering and Technology
Kalady

Deepika M P
Department of Computer Science and Engineering
Adi Shankara Institute of Engineering and Technology
Kalady

Abstract—Personal Health Record (PHR) is plays a vital role in every human life. PHR is concentrating centralized-patient model for exchanging health information ,which is to be stored at a middle third party. In this paper the PHR is stored in a semi-trusted serves. The person who can keep his PHR need to guarantee that it must be secure. Because it is more secure document according to a human being. The PHR can be accessed by an authorized person who get the access from the PHR owner.

But authentication which plays an important role while owner uploading or updating his PHR. The owner who only can modify the record .PHR had a proposed method ,which will include a encryption- decryption i.e cryptographic mechanisms for providing the security and authentication mechanisms in both public and private domain. The PHR is kept in a semi-trusted servers. So we need additional secondary level of authentication, even though it had encrypted and decrypted method for security and a primary checking.

So we propose a new idea to give such efficient authen-tication, mechanisms by providing a external hardware, as USB device. We add a small sized software inside the USB ,which will ensuring the secondary authentication ,while it connecting any computer device after primary authentication. This will ensure the high degree of privacy for the PHR.

Index Terms—PHR Personal Health Record

I. INTRODUCTION

AS the proverb 'health is wealth' says, heath is the most important asset than any of the living being can have. In today's world, due to food habits and irregular routine most of the individuals face different kind of health issues. This is when we will need a health record of a complete individual which not only gives the complete record of the health of an individual but also the faster diagnostic method.

The health record consist of various details of the parameters of a human body. It is one of the most important thing that an individual should have as it can be used in case of diagnosis of any health issues whether sudden or gradual. Keeping a health record by your own can in a way deliver you peace of mind as your health details will be updated with the routine check ups.

Maintaining a personal health record have various advantage such as diagnosis and analysis of disease, treatment etc. The disease can be diagnose at early stage. Most of the disease diagnosed at its early stage are curable. Hence maintaining a personal health record can even keep you away from serious disease.

For providing the secure access of the PHR , we can use cryptographic methods ,such as encryption and decryption. In proposed methods use Attribute Based Encryption(ABE) mechanism for security.

The owner credentials will select to make the key for encryption and decryption by using SHA. The owner can give the access key sending through mail. The access key will generate by taking details of requested user for that purpose we also use ABE. The administrator have the power to block and unblock unauthorized users by checking it with primary credentials.

II. RELATED WORK

The proposed system that provide to access the PHR record by external entity which the permission of the PHR owner. But it may reside some security problem when the external entities accessing the record unmannerly. Even though the unauthorized access and malicious access can be detected by the PHR owner by alerting him through the Email messages. But this have no as much security. So we need to arise the strength of the security level.

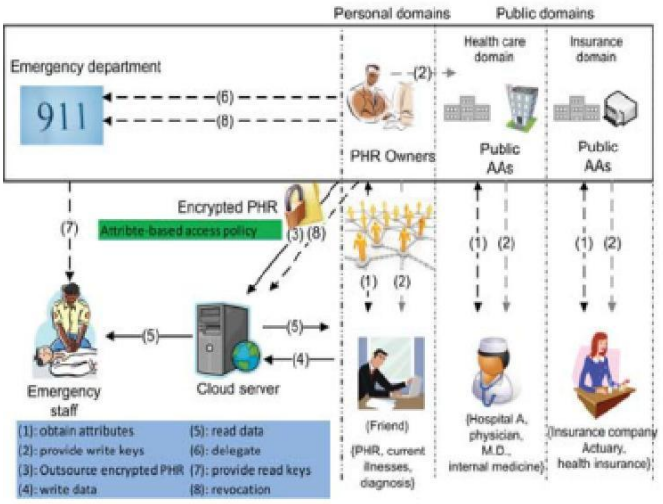

Fig. 1: Architecture of PHR using ABE[1]

So for future enhancement we propose a better and scalable method for keeping PHR.

We had image security, Data mining security, Network security for authenticated security area. All of these concepts which include the direct data entry in the form of textual format or image format for security. But nowadays , these all are have some kind of trouble or disadvantages ,if these are unfortunately matching with malicious entry. Like any variation in pixels in an image or any modification in textual format. So more chance to get break the authentication. So we need a security mechanism to overcome all of these difficulty.

In this new concepts , we completely replace the data entry format like textual or image. Instead of that we introduce a external hardware concepts. For example ,In real life if we have a car key , we believe ourself that it will never stole by other if there is no such other duplicate key is exist. If we lost that key we can realize that. Similarly, in the case of hardware it can easy realizable ,when any issue will arise than in the case of software. Because everything is being to a system that may get a chance to modify without the awareness of the owner.

So we need to introduce a hardware for future enhancement. But before choosing a hardware we deeply think about that which hardware is more suitable for this purpose. For that we analysed many hardware devices ,such as RFId ,fingerprint devices in punching machine and card reader systems in many organizations. But all of these have many disadvantages ,as following,

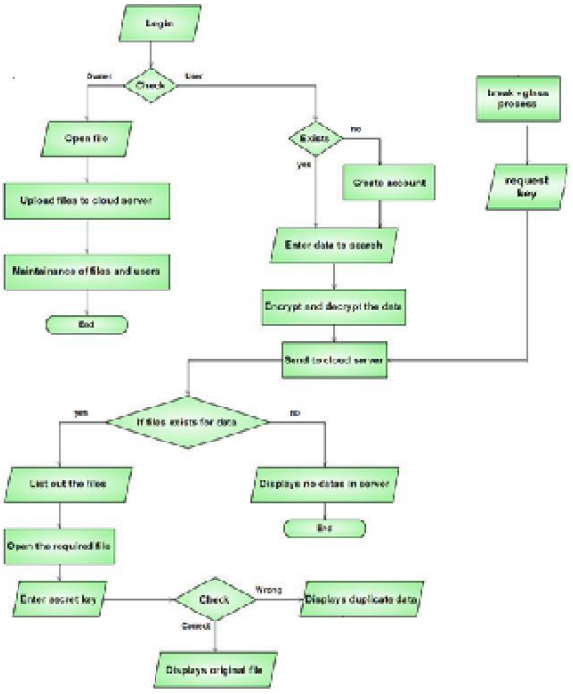

Fig. 2: Architecture of PHR using ABE[1]

1) More Expensive
2) Not much user friendly
3) People who have not much knowledge about that systems.
4) Carrying is difficulty

For easiest usage and manageable working ,we can choose less expensive hardware that is USB device.

III. FEASIBILITY ELEMENTS

Much storage space
Easy to carry
Less expensive
More user friendly
Easy to format

IV. SCOPE

The question is that how USB device will change a security mechanisms for a PHR owner in future enhancement. This paper is actually is the answer.

Any Electronic device that have a manufacturing ID or machine ID. This ID in the case of USB device is called PNP (Plug and Play)device ID. This will be recognized from the USB device. And it add at the time of owner registration. At each time owner login to the website , by providing username and passwords. But instead of this primary credentials ,

it will show a secondary authentication mechanisms by asking a question to plug in a USB.

If USB connected is not authenticated one, the USB will get reject and user can not enter into the site. Thus USB will act as a secondary front and security. The USB is a hardware token device. So we need to develop a application code to read the USB ID for secondary security.

In real time , we use ATM machine to withdraw money by inserting ATM card. ATM is a Windows machine. But here we implementing it as a web application. If we generate a code for a window machine to reading a USB , the difficulty is that , USB must insert into that machine only. We want to host the project into the web , the code generated may placed in the server, situated anywhere in the world. So the owner can not travel to plug in the USB where the code is situated.

So in order to correlate this into web , we develop a small exec named keyfinder i.e software for reading ID from USB. The size of the exec is a matter because we can download this software through mobile phones also. So the size of the exec should be below 115 KB. After developing this, its executable file is add into the website and complete the hosting.

As the result , the client or owner use the application from any system. After the first primary security is completed , and reaches the secondary security (i.e, USB mechanism). The system will automatically say that please download this USB finder. So the owner or client will click and download that small sized software and run it. At the time , if we plug in a USB device , the USB ID will be read and can check by matching with credentials provided at the time of registration. If the matching successful , then only the owner can enter into the application.

There are generally two different methods for getting the serial number of a USB-based device.

An “easy” way using Windows Management Instrumentation (WMI), and

A “hard” way using the Win32 APIs.

There are advantages and disadvantages for both methods

One is slow but simple to implement, the other is fast (and potentially provides more informa-tion) but is difficult to implement. Here we uses WMI technique to get USB serial number.

The WMI technique uses a series of ”re-lationships” that exist between several WMI classes. We start with the Win32 LogicalDisk class, track it to the Win32 DiskPartition class (which itself is just a relationship class).

Windows Management Instrumentation (WMI) is perhaps one of the best kept secrets in the IT world. It is a very powerful set of tools that you can use to gather information, configure settings, and manage PCs either locally or across the network. It truly is ”management” and ”instrumentation” of Windows.

WMI is the Microsoft implementation of an industry-based Web-Based Enterprise Manage-ment (WBEM) initiative. The Distributed Man-agement Task Force (DMTF) now sets the standards for WMI.

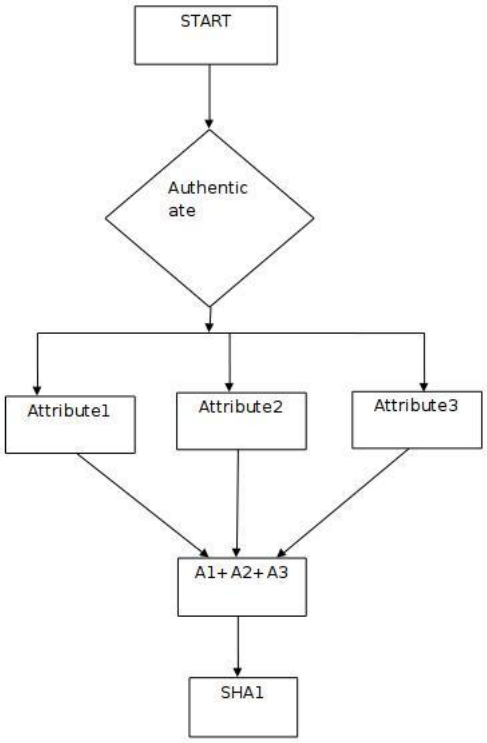

Fig. 3: Flowchart demonstrating ABE encryption

There are WMI ”namespaces” for performing operations on the registry, operations on the file system, discovering and configuring hardware, and manipulating settings of Windows itself.The system is extensible, so a new WMI ”provider” can be added during the install of an application (like SQL Server or Internet Information Service). The default

namespace (called ”root*n*cimv2”) contains over 500 classes in the following categories

Computer system hardware Operating System

Installed Applications

Internal WMI Service settings Performance Counter

Helper Classes

The WMI data is accessed via a relational database. Like any database, there are schemas, data types, primary keys, table relationships, etc.

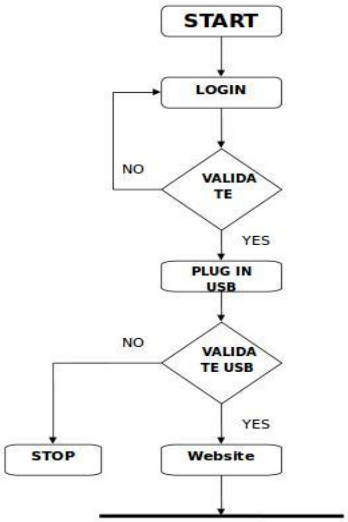

Fig. 4: Flowchart of PHR using ABE[1]

V. ALGORITHM

Steps

Create a class named *USBDriveSerialNumber* for getting USB key.

1) Inside that class create four function named
   getSerialNumberFromDriveLetter
   matchDriveLetterWithSerial
   parseSerialFromDeviceID
   getValueInQuotes
2) End

VI. CONCLUSION

The PHR is more helpful in human being.But its protection is considerable factor. We already have a primary authentication in any security level.But which is not much trustful and consistent. So an additional authentication is needed in secondary level. We propose a new concepts by using USB device with a software which will take care of the secondary authentication.Thus we get a strong security over our secret personal health record.

REFERENCES

[1] K. Ren M. Li, S. Yu 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*, 2010.

[2] Y. Zheng K. Ren M. Li, S. Yu and W. Lou. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Transactions on Parallel and Distributed Systems*, 24(1), 2012.

[3] Khobragade Pranjali Ghodake Shubhangi, Joshi Priyanka and Chandak Manjiri. Scalable and Secure Sharing of data Cloud Computing Using Attribute-Based Encryption. *International Journal of Multidisciplinary Research and Development*, 2(4), 2015.

[4] M. Gagne S. Narayan and R. Safavi-Naini. Privacy Preserving EHR System Using Attribute-Based Infrastructure . *Proc. ACM Cloud Computing Security Workshop*, 2010.

[5] X. Lin X. Liang, R. Lu and X.S. Shen. Patient Self-Controllable Access Policy on Phi in Ehealthcare Systems. *Proc. Advances in Health Informatics Conf*, 2010.

Author Profile

Anju P R is currently doing her master's de-gree in Technology, specializing in Computer Science and Engineering at Adi Shankara In-stitute of Engineering and Technology, Kalady. Her areas of interest include network security, cryptography and steganography.

Deepika M P is currently working at Adi Shankara institute of Engineering and Tech-nology as Assistant Professor in Information Technology Department. Received her M.Tech degree in Software engineering from CUSAT. Her area of interest is in Visual Cryptography