Research Paper : MEDICAL SCIENCE

SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS USING ENHANCED ATTRIBUTE BASED ENCRYPTION

M.Rajasekar ME (CSE), Nehru Institute of Technology, kaliyapuram, Coimbatore-641105.Ph:9047693733

S. Pathur Nisha ME (Ph D), Nehru Institute of Technology, kaliyapuram, Coimbatore-641105.Ph:9442464988

V.S.Thangarasu ME.Ph.D,VSB engineering college,Karur. Ph:9444021802

ABSTRACT

Personal health record (PHR) is a patient-centric model of health information-exchange. Personal Health Information outsourced to be stored at a third party, such as cloud providers. Some of the privacy concerns such as the Personal Health Information (PHI), is exposed to third party servers and to unauthorized parties. To give more assurance to the patient's own PHR's, encryption is done for the PHR's before outsourcing. Encryption gives more security to the PHR', by using Security policies Mechanisms. There are some risks such as Privacy exposure, scalability, flexible access and efficient user revocation. Most important challenge is to fine-grained and cryptographically enforced data access control. In this project, we propose a novel patient centric framework and a mechanism for data access control to PHR's stored in semi-trusted servers and to use the security policies algorithm to give more security. To achieve fine grained and data access control, attribute based encryption is used to encrypt each patient's PHR file. We are going to divide the users in the PHR system into multiple security domains which reduces the key management complexity for owners and users. By using multi-authority ABE, the patient privacy is guaranteed, with the secret key for the health record.

KEYWORDS Personal Health Information, Personal Health Records, break glass, multi authority ABE, Security policies algorithm

INTRODUCTION

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for our needs, we use a service over the Internet, at another location, to store our information or using its applications. Doing so may give rise to certain privacy implications. Cloud computing is a subscription-based service where we can obtain networked storage space and computer resources. One way to think of cloud computing is to consider our experience with email. Our email client, if it is Yahoo!, Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support our personal email account. When we want to access your email and log in, the most important part of the equation is having internet access. Our email is not housed on your physical computer; we access it through an internet connection, and can access it anywhere. If we are on a trip, at work, or down the street getting coffee, we can check your email as long as you have access to the internet. Our email is different than software installed on our computer, such as a word processing program. When we create a document using word processing software, that documents stays on the device we used to make it unless you physically move it. An email client is similar to how cloud computing works. Except instead of accessing just our email, we can choose what information we have access to within the cloud.

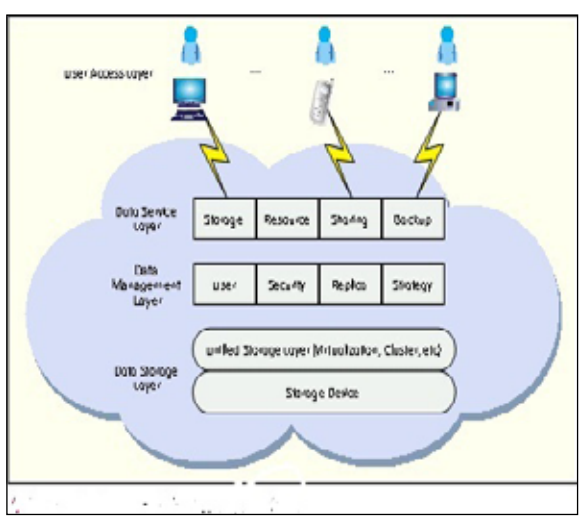


Fig1: Architecture of cloud data storage service

EXISTING METHOD

Due to the high cost of building and maintaining specialized data centers, many PHR services are outsource to or provided by third party service providers, for example, Microsoft health vault. While it is exciting to have convenient PHR services for everyone, there are many security and privacy risk.

Drawbacks :

There have been wide privacy concerns as personal health information could be exposed those third party servers and to unauthorized parties.Department of veterans Affairs database

containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization.

EXISTING ALGORITHM
HASING TECHNIQUE PSEUDO CODE
The function takes two inputs, key, which is an array of ASCII codes and

table_ sizewhich is the size of the address space

function hash(key, table_ size)

sum = 0; i = 0;

while (i < 12)

sum = sum + key[i] * 100 + key[i + 1];

i = i + 2;

end while

return sum mod table_ size

end function

Hashing 11

PROPOSED METHOD
A PHR service allows a patient to control her personal health data in one place through the web, which has made the storage and sharing of the medical information with more efficiency. The important approach would be to encrypt the data before outsourcing the record. Basically, the PHR owner herself should decide how to encrypt herself and to allow which set of users to obtain access to each file. A PHR record should be only available to the users, who gives the decryption key, while remain confidential to the rest of the users. Furthermore, the patient shall always retain the right to not only grant, but also revoke the access.

In PSD (personal domains), the owner used key- policy attributed based encryption and generates a secret key for their PSD users and in the PUD (public domain) the multi-authority attribute based encryption is preferred. We are going to give the security key to the PSD with high security. It's automatically created secret keys for individual patients.

PROPOSED ALGORITHM
ENCRYPTION/DECRYPTION ALGORITHM
It gives security to the PHR. Encrypts the Health Record and kept it on a cloud server. Take one Person's health record if it is not encrypted, then the record can be seen and can be modified by other persons. Using the available&suitable algorithm, the record cannot be modified and cannot be used by other persons.

MESSAGE DIGEST ALGORITHM 5
MD5 is a widely used cryptographic function with a 128- bit hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32-digit hexadecimal number.

MD5 processes a variable-length message into a fixed-length output of 128 bits.

STEPS
1. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit little endian integers),the message is padded so that its length is divisible by 512.
2. The padding works as follows: first a single bit, 1, is appended to the end of the message.
3. This is followed by as many zeros as are required to bring the length of the message up to 64bits fewer than a multiple of 512.
4. The remaining bits are filled up with a 64-bit integer representing the length of the original message, in bits.
5. The MD5 algorithm uses 4 state variables, each of which is a 32 bit integer (an unsigned longon most systems). These variables are sliced and diced and are (eventually) the message digest.

The variables are initialized as follows:
A = 0x67452301
B = 0xEFCDAB89
C = 0x98BADCFE
D = 0x10325476.

6. Now on to the actual meat of the algorithm: the main part of the algorithm uses four functionsto thoroughly goober the above state variables. Those functions are as follows:

F(X,Y,Z) = (X & Y) | (~(X) & Z)
G(X,Y,Z) = (X & Z) | (Y & ~(Z))
H(X,Y,Z) = X ^ Y ^ Z
I(X,Y,Z) = Y ^ (X | ~(Z))

Where &, |, ^, and ~ are the bit-wise AND, OR, XOR, and NOT operators

7. These functions, using the state variables and the message as input, are used to transform the state variables from their initial state into what will become the message digest. For each 512 bits of the message, the rounds performed (this is only pseudo-code, don't try to compile it) After this step, the message digest is stored in the state variables (A, B, C, and D). To get it into the hexadecimal form you are used to seeing, output the hex values of each the state variables, least significant byte first. For example, if after the digest:

A = 0x01234567;
B = 0x89ABCDEF;
C = 0x1337D00D
D = 0xA5510101

Then the message digest would be:

67452301EFCDAB890DD03713010151A5 (required hash value of the input value).

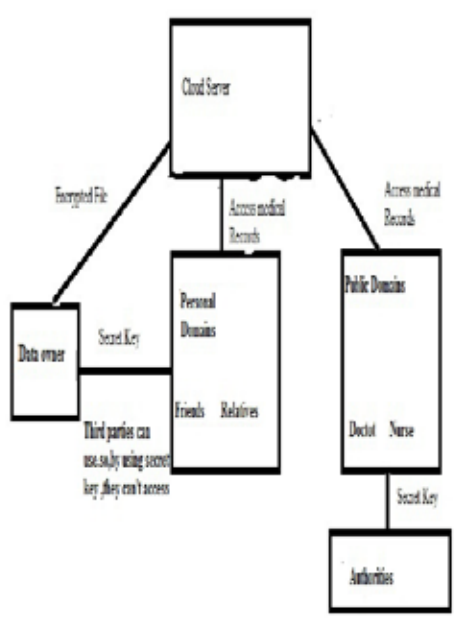


Fig 2: Proposed System Design

CONCLUSION

In this paper, we have proposed patient centric framework of secure sharing of personal health records in cloud computing. Considering partially used cloud servers, patients shall full control through encrypting their PHR files to allow fine-grained access. This framework brought the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the time, security and complexity of key management while enhance the privacy guarantees compared with previous works. We utilize the security policies algorithm to give more security to the PHR. We used ABE to encrypt the PHR data, so that patients can allow access as the private users, but not being able to use by the public users. Furthermore, encrypting the records will be safe and to give more security to the PHR will be using the Security policies algorithm.

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," in SecureComm'10, Sept. 2010, pp. 89–106. | [2] H. L¨ohr, A. -R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, sir. IHI '10, 2010, pp. 220–229. | [3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011. | [4] "The health insurance portability and accountability act." [Online]. Available: | http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp | [5] "Google, Microsoftsaysthe help stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/. | [6] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online]. Available: | http://articles.latimes.com/2006/jun/26/ health/he-privacy26 | [7] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," BMJ, vol. 322, no. 7281, p. 283, Feb. 2001. | [8] J. Benaloh, M. Chase, E. Horvitz, and K.. Later, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114. | [9] 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 | . [10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010. |