International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-1, June 2013

Secure Sharing of Health Records in Cloud Using ABE

Nithya.E, TousifAhamed Nadaf

Abstract— In recent years, Personal health record (PHR) has emerged as a patient-centric model of health information exchange. This stands in contrast with the more widely used electronic medical record, which is operated by institutions (such as a hospital) and contains data entered by doctors or billing data to support insurance claims. Individual Patient is the owner of the PHR. The main purpose of a PHR is to provide accurate and complete summary of an individual's medical history which is accessible online. Especially, each patient is promised the full control of his/her medical records and can share his/her health record with a wide range of users, including healthcare providers, family members or friends. PHR is often outsourced to be stored at a third party, such as cloud providers. To assure the patients' control over the access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Heretofore, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation have remained, which are some of the most important challenges toward achieving fine-grained, cryptographically enforced data access control.

Index Terms— Personal Health Record, Data Privacy, Attribute Based encryption, Cloud Computing.

I. INTRODUCTION

In an emerging IT industry healthcare is the one of the most important sector. Existing healthcare systems are built on workflow that consists of paper medical records, duplicated test results, on digitized images, handwritten notes. Hospitals and providers are facing the risk of capacity shortage to securely store and share patient medical records and information. Health information Exchange (HIE) is the provision of exchanging healthcare information within or across organization. Eg: Interacting with lab or ordering tests/receive results, transmitting prescriptions from physicians to pharmacies, sharing patient health history between physicians, relaying data from patient's home medical devices to physicians and giving patients access to their health information. An Electronic Medical Record (EMR) is the effective capture, dissemination, and analysis of medical and health related information for a single patient [1]. All participants in the health care delivery system have a stake in efficient information flows. They include health care providers, insurers, government agencies, claims processors, and patients. Indeed, Electronic Medical Records managed by individuals are termed Personal Health Records (PHRs). PHRs capture all relevant personal health details, including diagnoses, X-Rays, and similar items into a single repository. Using EMRs, doctors can review patient histories and charts, obtain laboratory results, generate referrals for specialist consultations, prescribe medicines, and diagnose images all without the use of paper. The main components of an EMR are shown in Fig 1.

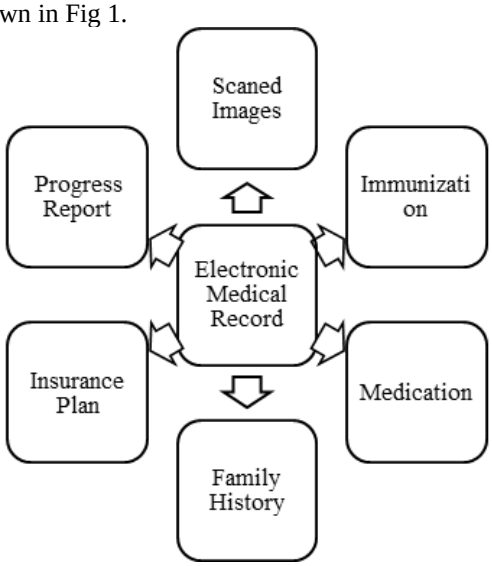

Fig 1 Electronic Medical Record System

Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, Cloud computing [2] technology can simplify the complex medical records exchange procedure between different systems, and save the device setup expenses for smaller hospitals. It can provide an exchange platform that all hospitals and clinics can use, and can serve as electronic medical data storage [3]. Large companies like Google and Microsoft are building medical record clouds such as Google health and Microsoft Health Vault [4]. Through the health care cloud of the cloud platform, patients need only one interface to find out their complete medical history, instead of having through different hospitals at the risk of finding only a partial medical history. The benefits of putting health data in a cloud based system [5] include:

A. Data Portability

Using Cloud based medical data exchange; it is easier to access and share data between patients and doctors and between specialists.

B. Better security

Data and medical records are not stored at the normal location. Instead, data is stored in a safe, HIPAA-compliant secure cloud location allowing for convenient, secure access from any location with the benefit of off-site disaster recovery.

Manuscript published on 30 June 2013.
***Correspondence Author(s)
Asct Prof Nithya.E, Department of Computer Science, Dr. Ambedkar Institute of Technology, Bangalore, India.
Tousfiahamed Nadaf, Department of Computer Science, Dr. Ambedkar Institute of Technology, Bangalore, India.

C. Enormous storage capacity

With cloud-based systems, doctors and clinicians do not have to own hardware and software. Additional data storage is available as needed.

Cloud computing inevitably poses new challenging security threats [6] for number of reasons. The use of the cloud for healthcare, including electronic medical records, personal health records, and healthcare treatment expands the protection of personal information based on the Health Insurance Portability and Protection Act (HIPPA).Firstly, existing cryptographic primitives for the purpose of data security protection cannot be directly used because it will loss the user's control of data under Cloud Computing. Therefore, security of correct data storage in the cloud must be conducted without knowing the whole data. Secondly, Cloud Computing cannot be considered as a third party data warehouse [7]. To ensure storage security under dynamic data environment is hence an important matter.

To protect the confidential medical information in cloud, encryption is used. But it requires exchange of decryption keys among the data owners and users. It is not good for the data owner to remain online for providing decryption key to registered users. The solution is to delegate the distribution task to cloud server. The risk of privacy violation increases when decryption keys are distributed via cloud storage provider. The main problem with this solution is the increase in load of asymmetric encryption on the data owner.

For securing medical records stored in cloud and achieving fine grained access control, the proposed scheme combines Key Policy based encryption, along with Proxy Re-encryption.KP-ABE[8] mainly concentrates on access control policy and PRE [9] delegates task of decryption key distribution to cloud server. By uniquely combining these cryptographic techniques this scheme realizes a secure medical record exchange through cloud platform with minimum overhead on data owner.

II. RELATED WORK

A. Patient Controlled Encryption

[10] is a privacy preserving medical health record system. In PCE data is stored as hierarchical structure on a remote server and patient has no direct control on these data. However, PCE facilitates sharing and searching of the encrypted data in the remote location. The proposed scheme can be realized using symmetric and asymmetric encryption algorithms, with their inherited benefits and limitations.

B. PEACE: An Efficient and Secure Patient-centric Access Control Scheme for eHealth Care System

[11] The proposed scheme in this paper is an efficient and secure patient-centric access control (PEACE) scheme for the emerging electronic health care (eHealth) system. In order to assure the privacy of patient personal health information (PHI), different access privileges are defined to data requesters according to their roles, and then assign different attribute sets to the data requesters. By using these different sets of attribute, construct the patient-centric access policies of patient PHI. The PEACE scheme can guarantee PHI integrity and confidentiality by adopting digital signature and pseudo-identity techniques. It encompasses identity based cryptography to aggregate remote patient PHI securely. Extensive security and performance analyses demonstrate that the PEACE scheme is able to achieve desired security requirements at the cost of an acceptable communication delay.

C. Vimercati et al

[12] proposed a solution for *Securing data storage on untrusted servers using key derivation methods* [13]. In this proposed scheme, each file is encrypted with a symmetric key and each user has given a secret key. To grant the access privilege for a user, the owner creates corresponding public tokens from which, together with his secret key, the user is able to derive decryption keys of desired files. The owner then transmits these public tokens to the semi-trusted server and delegates the task of token distribution to it.

D. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems [14]

The paper proposes an access control mechanism using cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. And demonstrate how to apply the proposed mechanism to securely manage the outsourced data. The analysis results indicate that the proposed scheme is efficient and secure in the data outsourcing systems.

There are several Attribute-Based encryption schemes proposed, including the BSW scheme introduced by Bethencourt et al. in [15], the CN scheme of Cheung and Newport in[16] and the CP-ABE scheme proposed by Ibraimi et al. in [17]. The first two schemes present a set of disadvantages (e.g. BSW requires many pairings and exponentiation operations due to the large number of polynomial interpolation required to reconstruct the secret, the size of cipher text and secret key in CN increases with the number of attributes in the system, etc.) which makes them not appropriate for a PHR system. The third scheme ([17]) was proved by the authors to be efficient and secure, fact that motivates our choice for implementing it as a basis for the PHR system access control.

III. DISADVANTAGES IN EXISTING SYSTEM

- There is no proper policy management for file access, so that unauthorized users can also able to access the sensitive data.
- There is no proper encryption decryption concept the files stored in the semi-trusted cloud can able to leak the information to others.
- There is no structured way to access the file for personal & professional purpose.

IV. MODULES USED

A. Admin Module

This module is used to control all the process. Administration is a dynamic work in every field. The initial meaning of administration is the running of a business or system. In every step of your business, it needs administration. To run faster in the technological scenario a business need to administer.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Admin is a super user who creates the PHR Data Owner user and maintains the cloud servers' configurations. He has the writes to Add, Edit or Delete any number of Data owners.
Once the Admin logged in he has following functions.

- *Login Module*
- *Attribute Values*
- *Policy Management*
- *PHR Owners*
- *Key Generation*
- *Transaction Details*
- *Change Password*

B. PHR Data Owners

PHR Data Owner is a person who will store the files in cloud which in turn accessed by the authorized Data Users. Data Owners are like Patient who will upload all the files in the system. Whenever the file is uploaded it will be encrypted by the system using PHR Data Owners Encryption Key.
PHR Data Owner has to specify the Hierarchical Access Policy for each and every file. Access policies are set using Domain Attribute and Designation Attribute.
PHR Data Owner can able to create the Data User and he has to send them Attribute based Decryption Key. Attribute based Decryption Key means it contains the PHR Data Owners Decryption Key and Data users Attribute Set (Domain, Designation).
Once the PHR Data Owner logged in he has following functions. When you submit your final version, after your paper has been accepted, prepare it in two-column format, including figures and tables.

- *Login Module*
- *File Upload*
- *Attribute based Key Distribution through e-mail*
- *Transaction Details*
- *Change Password*

C. PHR Data User

PHR Data user are the data access users, suppose PHR Data owner is a Patient and then data users are comes into domains like Hospitals, Insurance, Friends, Emergency. Each data user has two attribute one is Domain and another one is designation.
Data user will receive their access key (Attributed based Decryption Key) from respective data owner through email.
With the help of the access key they can able to download the files for which they have access, remember access control is set by PHR data owner.
Suppose the data user wants to download any file, first he has to select the file from the list and the system ask for the access key, After system getting the access key it will separate the Attribute Set from the key and check for the access rights, if the user has the access he can download the encrypted file which in turn decrypted using the decryption key and download to the data consumer local system.
Once the Data Consumer logged in he has following functions.

- *File Download*
- *PHR Owner ID Input*
- *o Key Input*
- *Verifying ID and Input Key*
- *Listing the file based on Access Policy*
- *Encrypted File Download from cloud to web server*
- *Decrypting the file in web server*
- *File download to local system*

V. PROPOSED SCHEME

The main goal 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 according to the different users' data access requirements. The domains consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, domains can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each domain, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

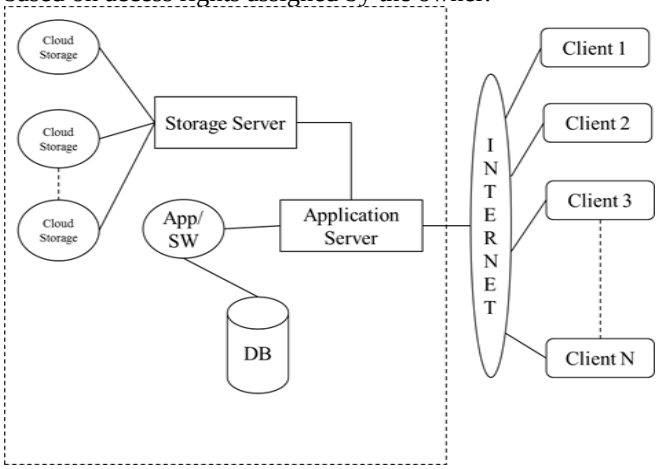

Fig 2 Architecture Diagram

This is a web based application developed in MVC three tier architecture. This system is developed with cloud computing technology.
Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network. Cloud computing entrusts remote services with a user's data, software and computation.
End users access cloud-based applications through a web browser on a light-weight desktop while the application software and user's data are stored on servers at a remote location.
In this system there are three type of end user Admin, Data Owner & Data Consumer.
Basically this system need two servers in cloud, one will act as a Cloud Application Server where the application software is running. Another one is Cloud Storage Server where the encrypted data files are stored.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

User has to access the application which is running in cloud application server with proper URL on web browser. Each user has their unique user id and password to enter into their session. Once the user enters into their session, all the relevant functions they can use. At a time any number of users can able to access the application, it has the capability to handle more than one user at a time. The application will encrypt the file and store the encrypted file in cloud storage server and also it is like a gateway, any user has to pass the application to place a file in cloud and to retrieve the file from cloud.

VI. BENEFITS

Having a personal health record can be a lifesaver, literally. In an emergency you can quickly give emergency personnel vital information, such as a disease you're being treated for, medications you take, drug allergies, and how to contact your family doctor. A personal health record not only allows you to share information with your care providers but also empowers you to manage your health between visits. For example, a personal health record enables you to:

- Track and assess your health. Record and track your progress toward your health goals, such as lowering your cholesterol level.
- Make the most of doctor visits. Be ready with questions for your doctor and information you want to share, such as blood pressure readings since your last visit.
- Manage your health between visits. Upload and analyze data from home-monitoring devices such as a blood pressure cuff. And remind yourself of your doctor's instructions from your last appointment.
- Get organized. Track appointments, vaccinations, and preventive or screening services, such as mammograms.

VII. USER INTERFACE

When the application is started an admin/user, will be greeted by the screen in Figure 3. At this point, it is imperative that a connection with the database is possible before proceeding. After this, the following Figures 4-11 shows the related operations of Admin, User and Data Access Member.

Fig 3 Home Page

Fig 4 Admin Profile Page

Fig 5 Policy Management

Fig 6 Key Generation

Fig 7 Attribute Values

Fig 8 Key Distribution

Fig 9 File Upload

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Fig 10 Transaction

Fig 11 File Download

VIII. CONCLUSION

Proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access to different domains with different professional roles, qualifications and affiliations. Furthermore, we enhance an existing ABE scheme to handle efficient and on-demand user revocation, and prove its security.

REFERENCES

1. Saman Iftikhar, Wajahat Ali Khan, Maqbool Hussain, Muhammad Afzal, Farooq Ahmad," Design of Semantic Electronic Medical Record (SEMR) system as SaaS service model for Efficient Healthcare",IEEE 3rd International conference on cloud computing 2010,pages 344-347.
2. Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, "A Break in the Clouds: Towards a Cloud Definition," in ACM SIGCOMM Computer Communication Review, Volume 39, Number 1, January 2009
3. Zhuo-Rong Li1, En-Chi Chang1, Kuo-Hsuan Huang1, Feipei Lai2," A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform," IEEE 15th International Symposium on Consumer Electronics 2011, pages 450-457.
4. Microsoft health vault http://www.healthvault.com/
5. R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," Proceedings of IEEE 3rd International Conference on Cloud Computing, 2010, pages 268-275.
6. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS '09, 2009.
7. Yves Giard, André Lessard "Decisions about switching to cloud computing should be based on sound practices despite any limitations" http://www.camagazine.com/archives/print-edition/2010/may/regulars/camagazine36546.aspx
8. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. Of CCS'06, 2006
9. Ran Canetti and Susan Hohenberger. Chosen-ciphertext secure proxy re-encryption. Cryptology,ePrint Report 2007/171, 2007.
10. Benaloh, J, Chase M., Horvitz E., and Lauter K.(2009) Patient controlled encryption: ensuring privacy of electronic medical records. Proceedings of the 2009 ACM workshop on Cloud computing security, New York, NY, USA, pp. 103{114, CCSW '09, ACM.
11. X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC 2010, 2010.
12. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proc. of VLDB'07, 2007.kjnk
13. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005.
14. J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactionson Parallel and Distributed Systems, vol. 99, no. PrePrints,2010.
15. John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP '07, pages 321{334, Washington, DC, USA, 2007. IEEE Computer Society.
16. Ling Cheung and Calvin Newport. Provably Secure Ciphertext Policy ABE. CryptologyePrint Archive, Report 2007/183, 2007. http://eprint.iacr.org/.
17. Luan Ibraimi, Qiang Tang, Pieter Hartel, and Willem Jonker. Ecient and Provable Secure Cipher text-Policy Attribute-Based Encryption Schemes. In Proceedings of the 5th International Conference on Information Security Practice and Experience, ISPEC '09, pages 1{12,Berlin, Heidelberg, 2009. Springer-Verlag.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)