International Journal of Advanced Technology and Innovative Research

ISSN 2348–2370
Vol.07,Issue.08,
July-2015,
Pages:1472-1474

www.ijatir.org

A Novel on Personal Health Record in Cloud by using MA-ABE

A. RUPA[1], ASHISH LADDA[2]

[1]PG Scholar, Dept of CSE, Balaji Institute of Technology & Science, Warangal, TS, India, Email: annam.rupa@gmail.com.
[2]Asst Prof, Dept of CSE, Balaji Institute of Technology & Science, Warangal, TS, India, Email: ashishladda@gmail.com.

Abstract: Cloud computing, is an emerging computing environment which allows users to remotely store the data in one centralized place. This facilitates on demand scalable services as well as efficient management and sharing of data. However, there have been wide privacy concerns as data is outsourced to third party servers and to unauthorized users. The best way to ensure confidentiality of the data in the cloud is to utilize encryption/decryption for data in transit and data at rest. Data encryption/decryption technique can be applied on both coarse grained level and fine grained level but in both techniques it is required to give another party your private key. Hence Key management becomes a critical issue and the cloud provider require policies and procedures in place for storage, generation and archival of private keys. To achieve scalability in key management, flexible access and efficient user revocation an attribute based encryption (ABE) technique has been recently popularized. Using ABE records are encrypted at fine-grained level instead of coarse grain level which helps in scalable data access control. The paper discusses the use of cloud computing and cryptographic techniques i.e. (ABE) for Personal health record (PHR).PHR is an upcoming patient-centric model for storing patients' e-record in one centralized place. It allows patients to create, manage, control and share their health information with other users as well as health care providers. In additional it allows patients to provide Read/Write access based on users attribute.

.

.**Keywords:** Attribute based encryption, cloud computing, MA-ABE, Personal Health Record.

I. INTRODUCTION

One of the biggest advantages of cloud computing is that users can access data stored in the cloud anytime and anywhere using any device. Considering these merits of cloud computing an idea of PHR model is put forth. Personal health record (PHR) is an upcoming patient-centric model for storing patient's e-record in one centralized place. It allows patients to create, manage, control and share their health information with other users as well as health care providers. The other long term benefits are easy management of personal health information, freedom of sharing only relevant information with authorized care providers and lastly to maximize health benefits. For better usage patient can upload health measurements directly from their devices or can also import their health records from hospital EHR System. Considering the value of sensitive PHI and as cloud services do not come under covered entities[1], there exist health care regulations such as HIPAA [2] which is recently amended to incorporate business associates rules. Current date leading third party service providers are Microsoft HealthVault1, Google Health or Web MD. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers' .A best suited approach would be to encrypt the data before outsourcing. A PHR should only be available to set of users with the alternative decryption key while it should not be exposed to rest of the users. The patient shall retain the rights to grant as well as revoke the access rights [3].The users can be further categorized as Personal and Professional. Personal include family members and friends while Professional cover the large scope like medical doctors, pharmacists, and researchers, etc. Professional category requires potentially large scale key management if done by single authority. To avoid this problem a PHR system with multiple owners is put forth [4],[5]. They may encrypt according to their own ways, possibly using different sets of cryptographic keys. The paper focuses on patient centric and secure sharing of PHR records with multi-owner environment on a semi trusted server and try to minimize the complexity of key management.

II. RELATED WORK

A. Existing System

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability[6] in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically[7] enforced data access control.

B. Proposed System

In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs

stored in semitrusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously [8][9] by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

III. IMPLEMENTATION

The general flow will be user through web application will login into the system. The user credentials will be checked against login database system. System will verify that to which domain user belongs to. On that basis attribute authentication[10] system will grant read/ write access. A system attains data confidentiality by restricting unauthorized user to ac acess PHR document from personal domains. PHR owner have the right to request their PHI in format of their choosing. In additional security by providing Read/Write access based onattribute of Users document/ PDF / Image format. The owner is provided with two options such as PHR document can be filled either through Template or as Form. AES is a symmetric block cipher algorithm, the successor of the des. It's used to encode files, documents, etc. It works fast and is very sure. For encoding and decoding you use the same key. It is resistance against all known attacks. The method of Rijndael Algorithm[11][12] is as follows

- From the 128-bit key, Rijndael generates 10 keys of 128 bits each.
- These keys are placed into 4x4 arrays.
- The plain text is also divided into 4x4 arrays (128 bits each).
- Each of the 128-bit plain-text items is processed in 10 rounds (10 rounds for 128-bit-keys, 11 for 192, 13 for 256).
- After the 10th round the code is generated.
- Each single byte is substituted in an S box and replaced by the reciprocal on GF (2 8).
- Then a bit-wise modulo-2 matrix is applied, followed by an XOR operation with 63.
- The lines of the matrices are sorted cyclically.
- The columns of the matrix multiplication are interchanged on GF (2 8).
- The sub keys of each round are subjected to an XOR operation.

The system can be analyzed on various parameters like Security, scalability and efficiency. Data confidentiality analysis will be done and achieved by using the enhanced MA-ABE scheme (with efficient revocation) to be secure under the attribute based selective-set model. Comparison with existing schemes, the owner can decide the format of PHR document provides by user's attribute.

IV. EXPERIMENTAL RESULTS

Fig1. Registering as physician, nurse,PHR user technician.

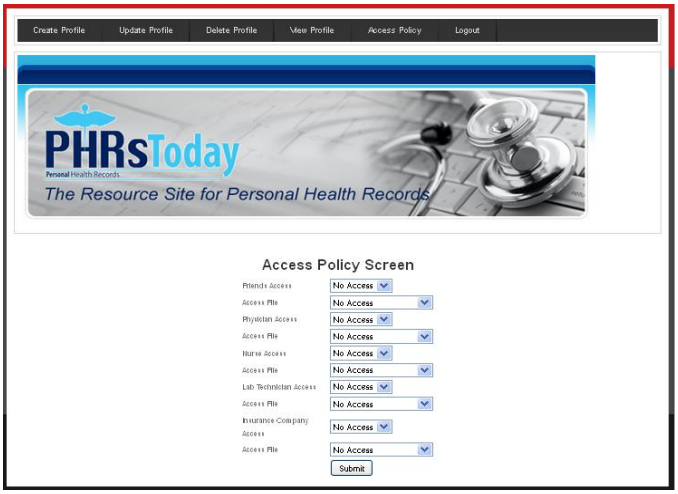

Fig2. Accessing Polacy.

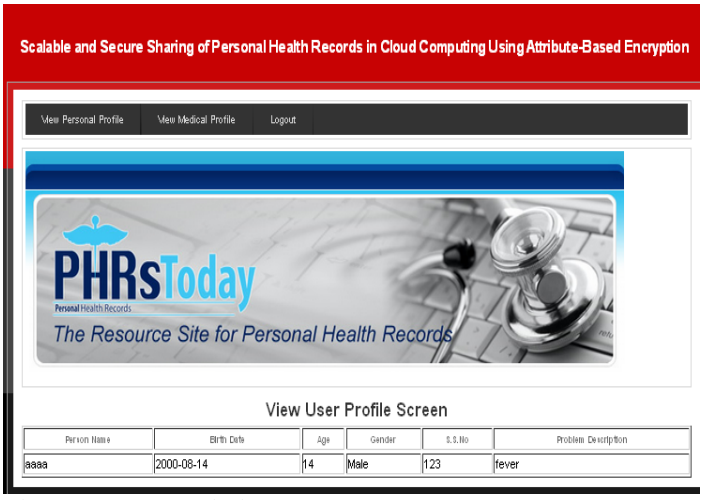

Fig3. Access Permissions.

Fig4. View Medical History.

V. CONCLUSION

This paper proposes the platform for sharing of personal health records in the secure and scalable manner by using Cloud computing. To enhance the fully patient centric concept and its privacy each PHR file is encrypted which also allows fine grained data access. The owner shall have complete control to their document providing access to specific users from various domains with formats of the document. Furthermore, a variation of ABE scheme that is MA-ABE is used to manage efficient and on-demand user revocation, dynamic policy changes and security.

VI. REFERENCES

[1] "Google, microsoft say hipaa stimulus rule doesn't apply to them,"http://www.ihealthbeat.org/Articles/ 2009/ 4/8/.

[2] "The health insurance portability and accountability act."[Online].Available:http://www.cms.hhs.gov/HIPAAGenInfo/01Overview.asp

[3] 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.

[4] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

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

[6] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J Computer Security, vol. 19, pp. 367-397, 2010.

[7] 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),pp. 89-98, 2006.

[8] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm.Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.

[9] Ming Li., Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou" Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption "IEEE SYSTEMS,vol.xx,No.xx,2012

[10] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W.Jonker,"Ciphertext-policy attribute-based threshold decryption with delegation and revocation of user attributes," 2009.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

[12] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp.121– 130.

Author's Profile:

A. Rupa Currently doing M.Tech in Computer Science & Engineering at Balaji Institute of Technology & science, Warangal, India. Research interests include Data Mining Network Security & Cloud Computing etc.,
Mail id: annam.rupa@gmail.com,
Mobile no:9491828455

Ashish Ladda, Mtech from JNTU Hyderabad in 2013, Experience :4+ years, Designation: Assistant professor at Balaji Institute of Engineering Sciences-Narsampet, Interested areas: Network Security & cloud computing, Email id:ashishladda@gmail.com.