www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-2, April 2018
Research Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Autonomous PHR Sharing: A Patient Centric Scalable and Flexible e-Healthcare Framework

R. Bhavani[1], K. S. Suganya[2*], D. Yazhini Priyanka[3]

[1]Department of Computer Science and Engineering, Bannari Amman Institute of Technology,Erode, India
[2,3]Department of Information Technology, Bannari Amman Institute of Technology,Erode, India

Received: 06/April/2018, Revised: 14/April/2018, Accepted: 22/April/2018, Published: 30/Apr/2018

Abstract— An explosive growth of information technology and the widespread use of cloud computing in every field had paved the way for Personal Health Record (PHR) Systems in cloud computing. Microsoft Healthvault is the best choice of example which is a online personal health record service provided by the technology giant Microsoft where the users can store, access and maintain their personal records which is shared to the health care providers. Some critics argue that moving personal data application in cloud computing may compromise control over data. Hence the need for a secure PHR systems in cloud. Many frameworks for PHR have been proposed using traditional cryptographic techniques. But they lack in the aspect of efficiency, scalability and suitability required by the PHR systems. And also the multi owner scenario of PHR system does not go in with single owner scenario of traditional cryptographic techniques. Hence we propose a PHR framework where the patients have access control and privacy of their personal record using light weight 64 bit block cipher symmetric encryption algorithm and also divide the patient centric framework into multiple security domains to reduce the key distribution complexity. The proposed scheme is flexible as it allows break glass decisions in case of emergency scenario. But the system lacks integrity which can be ensured by using digital signature algorithm or Elliptic Curve Digital Signature Algorithm (ECDSA) scheme to achieve integrity of the personal health records.

Keywords—Personal Health Record, cloud computing, Microsoft Health vault, cryptographic techniques, Symmetric Encryption, break glass

I. INTRODUCTION

Cloud computing has become an integral part of both small and large organizations day to day business life which in turn resulted in its explosive growth. According to a recent survey conducted by Forbes [1], nearly 75 percent of the business users are using cloud platform in one way or another. Cloud storage is the most important services available to users here they can store large amount of data and access them anywhere ubiquitously on demand.

Before the time of technology, medical records of a patient were maintained in the paper format. After the growth of information technology, the data were computerized. Likewise health care information was digitized in the form of electronic health record which contains details of patient's health care information which was accessed by the health care professionals such as insurance people, physicians and doctors alone. Subsequently, patients (i.e.) people requisites the need for Personal Health Record which allows the patient to store, access and maintain their personal records and share them efficiently with health care professionals when needed which is totally different from electronic health care records maintained by hospitals and health care institutions. Microsoft Healthvault and Google Vault are the best choice of example for online personal health record service providers.

But the growth of Cloud computing as a centralized storage and management platform for PHR had also raised the issue of security and privacy. Henceforth many traditional cryptographic techniques such as symmetric cryptography like AES and public key cryptography like RSA were proposed for the use of security while sharing data in PHR systems. But the main concern in a PHR system is the need for privacy where the patients can lose control over their personal health data in cloud.

To overcome the difficulties of privacy leakage by the cloud providers, we propose a PHR framework where the patients are the owners and they are responsible for creating the decryption key using Attribute Based Encryption and share the key with authorized users here say doctors and health care personnel. The proposed frameworks also ensure that each owner has total control over their data. Further to reduce complexity of key distribution among many owners, the system is divided into security domains and each domain has a set of users and attributes as encryption primitive.

The rest of the paper is organized as follows. Section II discusses the related works to the problem statement chosen.Section III presents the proposed framework with system architecture. In Section IV, we analyze the security of proposed method by comparing with PKC method. In Section V, we give the implementation details of proposed system and its performance. Finally, we conclude the paper in Section VI.

II. RELATED WORKS

Traditional role based access control policy RBAC was used primarily in PHR systems to fine tune that can access the electronic health record. In RBAC, the access control was provided based on the roles played and their privileges as in [2]. Di Vimercati proposed the use of symmetric key cryptography where personal health data as stores in semi trusted server encrypted using symmetric encryption techniques. But the proposed solution had certain limitation with access control rights sharing and user revocation in [3].

Later on, public key cryptographic based solutions were considered. Benaloh proposed a PHR framework which advocates that encryption along with access control is needed to ensure security and privacy. So they have made use of hierarchical identity based encryption in which each label is regarded as an identity. However, the method proposed in [4] still had potentially high key management overhead. Dong proposed the use of keyword search over encrypted data using proxy encryption [5]. Access control can be enforced if every write and read operation involves a proxy server. But this method also had its limitation with fine grain control. Yao et al discussed the use of Multi-Source Order-Preserving Symmetric Encryption (MOPSE) which uses a privacy preserving query processing by using hierarchical data providers [9].

III. PROPOSED FRAMEWORK

To improve upon the scalability of the above solutions discussed in related works, traditional cryptographic block cipher has proposed in this framework Some of the most popular Block cipher encryption techniques are Rijandael and AES which makes use of many rounds of Substitution, Permutation and Transposition which achieves confusion and diffusion. The proposed lightweight encryption algorithm is a block cipher symmetric key encryption technique. The algorithm implements five rounds to make it lightweight and each round includes mathematical and logical operations such as shifting, swapping, substitution and Permutation which works over one nibble(4 bits of data from 64 bit block data). To achieve efficient confusion and diffusion, each round employs substitution diffusion functions with unique key of its own generated randomly. The proposed symmetric algorithm is implemented for one-to-many encryption model in which cipher-texts are not necessarily encrypted to single user, but can expanded for the use of multiple users.

Our proposed PHR framework under consideration consists of five types of parties that form a hierarchy: a cloud service provider, data owners, data consumers, a number of domain authorities and a trusted authority as shown in figure 1. In our system Ministry of Health represents trusted authority. There are two domain authorities called National Hospital Association and National Medical Association. Patients and doctors represent cloud data owners and cloud data consumers. Cloud provides data storage service and is managed by the cloud service provider.

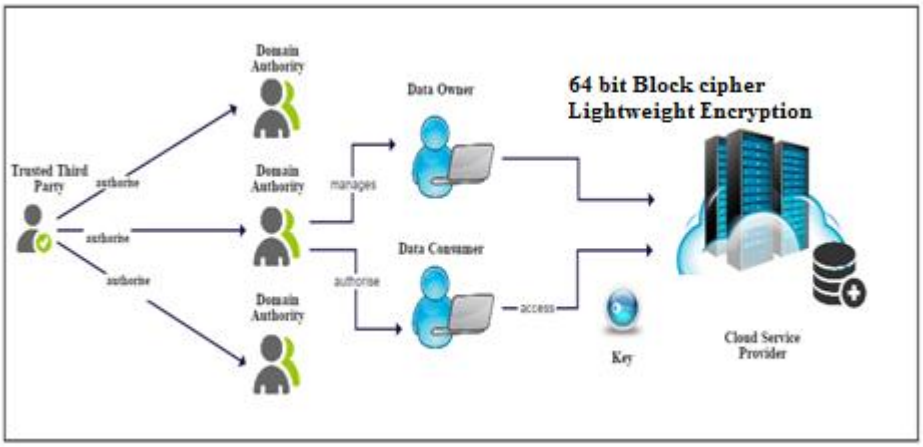

Figure 1. Proposed System Architecture

Data owners representing patients (and doctors) encrypt their medical record files and upload the same in the PHR cloud for sharing the PHR records with cloud data consumers. To access the shared PHR data files, cloud data consumers representing doctors (and patients) download the encrypted PHR files from the PHR cloud and then decrypt them to reuse the file for healthcare needs. Each cloud data owner/consumer is administrated by one domain authority as shown in figure 1. All the domain authorities are managed by master domain authority or main trusted authority. The master domain authority is the parent authority and they are very much responsible for managing top-level domain authorities in the proposed system framework. In the proposed system frameworks, cloud data owners and cloud data consumers

online availability is not needed always.PHR cloud is assumed to have major storage capacity and computation capabilities. Consequently, we assume that cloud data consumers have only reading permission. The personal health record data is encrypted using the proposed symmetric encryption scheme and break glass decision is used in case of emergency where the patient was not be available, then the next emergency contact personnel will be able to share the personal health record of the patient.

IV. SECURITY ANALYSIS

In this section, we compare our scheme with security feature of the one proposed in [3].

A. Flexibility:

When compared with [3] scheme, our scheme also achieves flexibility, by allowing the user to secure their personal health records over a easily accessible light weight encryption technique which provides better performance and efficient access to the health records securely.

B. Efficient User Revocation:

When compared with [3], this scheme also achieves efficient user revocation. The proposed security framework adds an random value to each user's key and employ multiple value assignments for this key. So we can refresh client's key by essentially increasing the value of the current key. We simply require a domain authority to keep up some state data of the client keys and maintain a strategic distance from the need to create and disseminate new keys consistently, which makes this plan more effective than existing schemes.

C. Scalability:

When compared with scheme in [3] our scheme also achieves scalability, by shifting the authority rights to subordinates and data owner which decreases the workload of root authority.

D. Fine-grained access:

When compared and contrasted with [3], our plan additionally accomplishes fine grained access control, by enabling data owner to define expressive and adaptable access policy for data files.

V. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

The performance and efficiency of the proposed system was compared with Symmetric Key based solutions proposed in [10] which use AES as their security method. With Personal sharing, each user has access to access their owned record. The parameter with which we measure the performance of our proposed system is efficiency and time and the results of our implemented framework is described in the figure 2 where the x axis denotes the time taken by the encryption technique and the y axis denotes the corresponding efficiency.

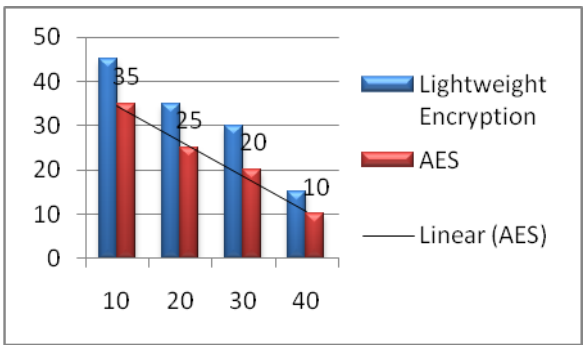

Figure 2: Comparison of Lightweight encryption with AES.

VI. CONCLUSION

In this paper, we have proposed a novel system of access control to acknowledge patient-centric privacy for personal health records in cloud computing. Thinking about in part dependable cloud servers, we contend that patients should have full control of their own privacy through encrypting their PHR documents to permit fine-grained get to. The structure tends to the unique challenges brought by numerous PHR owners and users, in that we enormously diminish the unpredictability of key management when the quantity of owners and users in the framework is huge. We use lightweight symmetric encryption to encrypt the PHR data, so patients can permit get to by personal users, as well as different users from various public domains with various professional parts, capabilities and affiliations.

REFERENCES

[1] Louis Columbus,2018,"Cloud Computing Survey," *Forbes* (26thDecember), at http://www.forbes.com/sites/louiscolumbus/2034/32/26/kpmgs-2034-cloud-computing-survey-enterprises-quickly-moving-beyond-cost-reduction-to-customer-driven-results/ , Accessed by 03 April 2018.

[2] Jin, J., Ahn, G.J., Hu, H., Covington, M.J. and Zhang, X., 2009. *"Patient-centric Authorization Framework for Sharing Electronic Health Records".* In the Proceedings of SACMAT '09 Proceedings of the 14th ACM symposium on Access control models and technologies pp. 325–334.

[3] Di Vimercati, S. D. C., Foresti, S., Jajodia, S., Paraboschi, S., & Samarati, P,2017," Over-encryption: management of access control evolution on outsourced data".In the Proceedings of the 33rd international conference on Very large data bases pp. 123-134.

[4] Benaloh, Josh, Melissa Chase, Eric Horvitz, and Kristin Lauter. "Patient controlled encryption: ensuring privacy of electronic medical records." In Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 103-114

[5] Dong, C., Russello, G., & Dulay, N. (2011),"Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, Vol.19,Issue.3, 367-397.

[6] Yu, S., Wang, C., Ren, K., Lou, W,"Attribute based data sharing with attribute revocation", In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security ASIACCS 2010 , pp 261-270 .

[7] Li, M., Lou, W., Ren, K.,"Data security and privacy in wireless body area networks",IEEE Wireless Communications Magazine, Vol.17,Issue.1,2010, pp 51-58.
[8] Goyal, V., Pandey, O., Sahai, A., Waters, B,"Attribute-based encryption for finegrained access control of encrypted data", In Proceedings of CCS 2006, pp. 89–98.
[9] X. Yao, Y. Lin, Q. Liu and J. Zhang, "Privacy-Preserving Search Over Encrypted Personal Health Record In Multi-Source Cloud," in IEEE Access, Vol. 6, Issue 2,pp. 3809-3823.
[10] V. Indhumathi and V. Prakasham, "On demand security for Personal Health Record in cloud computing,"In Proceedings of International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5.
[11] Sakshi kathuria,"A Survey on Security Provided by Multi-Clouds in Cloud Computing",International Journal of Scientific Research in Network Security and Communication,Vol.6,Issue.1,pp 23-28

Authors Profile

R.Bhavani is working as the assistant professor in the department of computer science in Bannari Amman Institute of Technology, Sathyamanagalam. She received her M.Tech and B.Tech degrees from Jawaharlal Nehru Technological University, Hyderabad in 2012 and 2010. Her area of research is Internet of Things and SQL.

Ms. K. S. Suganya pursed Bachelor of Technology from Kumaraguru College of Technology, Coimbatore, India in 2011 and Master of Computer Science and Engineering from Sriguru Institute of technology, Coimbatore, India 2015.She has worked as Programmer Analyst in Cognizant Technology Solutions between 2011 and 2013. She is currently working as Assistant Professor in Department of Information Technology, Bannari Amman Institute of Technology, since 2015. She is a life member of the Ired since 2015, and IAENG since 2015. She has published more than 15 research papers in reputed international journals including Thomson Reuters and Scopus (SCI & Web of Science) and international conferences including IEEE and it's also available online. His main research work focuses on Cryptography and Network Security, Cyberforensics and Cybersecurity, IoT and security issues in IoT. She has 3 years of teaching experience and 1.5 years of Industrial Experience.

D.Yazhini priyanka completed her M.Tech(Information Technology) and B.E(Computer Science and Engineering) degrees from Anna University, Chennai. Currently, she is working as the assistant professor in the department of Information Technology in Bannari Amman Institute of Technology. Her research fields are Big Data analytics and Internet of Things. She holds professional bodies membership in IEEE and IAENG. She has been published more than 5 papers in International Journal and Conferences.

