Cloud Based Secure Storage Dynamics for Personal Health Records

Sravan Kumar.Ch[#1], Srikanth Sreerama[*2]

[#1]*M.Tech, Computer Science Engineering, MLRIT, Hyderabad, Andhra Pradesh, India*
[#]*Associate Professor, Department of CSE, MLRIT, Hyderabad, Andhra Pradesh, India*

Abstract-Cloud computing has become an attractive and viable solution for outsourcing data. People can use cloud storage in pay per use fashion without capital investment. Enterprises from various industries are moving their data to cloud. Personal Health Records (PHRs) is a new model pertaining to health domain which has huge data that can be outsourced to cloud. Unlike data of other domains, the data of healthcare domain is highly sensitive. The patient's control over his record is very important. To achieve this PHR is encrypted before outsourcing it to cloud storage. There are many concerns pertaining to security such as privacy. Therefore scalable and secure sharing of such data is essential. Recently Li et al. proposed a scheme known as Multi-Authority ABE, which is based on Attribute Based Encryption (ABE). This encryption mechanism when used before outsourcing to cloud ensures that the data owner is assured complete security to his sensitive data. Concurrent and scalable sharing beside high degree of privacy is guaranteed in this scheme. In this paper we implement the scheme proposed by Li et al. with a prototype application that demonstrates the proof of concept. The empirical results revealed that the scheme is effective and support scalable and secure sharing of PHRs.

Index Terms--PHR, cloud computing, data privacy, attribute based encryption

I. INTRODUCTION

PHR (Personal Health Record) has become a model which is patient centric for exchanging health information. This is a service which enables patients to tcreate and manages their own health records. In this approach patients have full control over the medical records that are shared with other users. Other users include healthcare providers, friends, insurance companies and friends. As it is very expensive to build data centres, it is good idea to outsource PHR services the data to cloud storage. There are many cloud service providers like Microsoft, IBM, Oracle, Amazon, Google and so on. Of late there are many architectures that came into existence [1], [2] for outsourcing PHRs into cloud. These frameworks allow the users of PHR to outsource data to cloud storage. However, they could not address the security problems thoroughly. Patients should be able to control their own PHR records though they are shared to other parties. In order to make it possible HIPAA kind of health care regulations came into existence [3]. As the data of PHRs is very sensitive, it is essential that strict security measures are in place to ensure complete integrity of data. There was an incident of security issue with PHR records which recorded stolen records of 26.5 million military veterans [4].

Fine grained access control is required in order to control access to PHRs in a distributed environment. This is because the servers of cloud are semi-trusted in nature. Solution to this problem is encryption data before it is outsourced. The PHR owner should be able to decide how to encrypt. Only the users who know the decryption key can access the PHR files. The patients or PHR owners have right not only to grant files but also revoke them when required [5]. There are multiple PHR owners,who can grant access to their PHRs by encrypting in their own way using various cryptographic keys [6], [7]. Every user who wants to gain access to PHR has to obtain security keys from the owner. This will reduce security risk. An alternative to this CA for key managementwhere single authority,in this paper multiple authorities are used. The proposed system is basedon Attribute Based Encryption (ABE). Use ABE all access policies are made using attributes concept. An attribute is a set of columns that are determined to grant or revoke permissions. This will help in managing the users and the credentials easily. Each PHR owner is able to provide access to friends, trusted authorities and also hospital staff in case of emergency.

The main contributions in this paper include MA-ABE based framework which is patient-centric that allows sharing of PHR among multiple users with fine grained access control; each authority can give sharing rights to other users based on their description. This will help completely secure access to PHR and also ensure that the whole access system is patient centric. The remainder of the paper is

structured as follows. Section II provides review of literature. Section III provides a schematic overview of the proposed architecture. Section IV presents prototype implementation details. Section V presents experimental results while section VI concludes the paper.

II. PRIOR WORKS

In this paper our work is related to cryptographic access control using attribute based encryption for enforcing fine-grained access control. The public key encryption schemes which are used traditionally are not sufficient to use with the PHR system which is based on ABE as they result in high key management overhead. Set of attributes are used to encrypt and share data. By doing this key management can be done efficiently [8]. User collision prevention is an important feature of ABE where the program needs not to know ACL.

ABE is used by number of researchers [7], [9], [10], [11]. There has been increased usage of this kind of encryption to PHRs. There is a variant of ABE known as CP-ABE [12], [13] which has direct revocation provision. Another variant of ABE which was recently proposed by Yu et al. [7] is used to outsource PHR data to cloud. It also supports the data owner to revoke access rights when they are no longer needed by a user. It does mean that the PHR owner can revoke access rights that have been bestowed to users at will. An ABE where PHR owners can revoke access rights is known as Revocable ABE. However, it is a challenging task implementing revoking provision in the ABE. Instead of periodic revocation, immediately on – demand revocation is available with CP-ABE. Recently, Li et al. [14] proposed a new scheme for outscoring PHR data to cloud with complete security. The scheme is known as MA-ABE (Multi-Authority ABE). It is a multi-domain and multi-authority PHR system.

III. SCHEMATIC OVERVIEW OF PROPOSED SCHEME

The proposed scheme is meant for secure and scalable sharing of patient health records. Our scheme is based on the scheme proposed by Li et al. [14] which makes use of ABE as underlying theme. However, the proposed scheme is multi-authority based ABE. The schematic overview of the scheme is as shown in figure1.

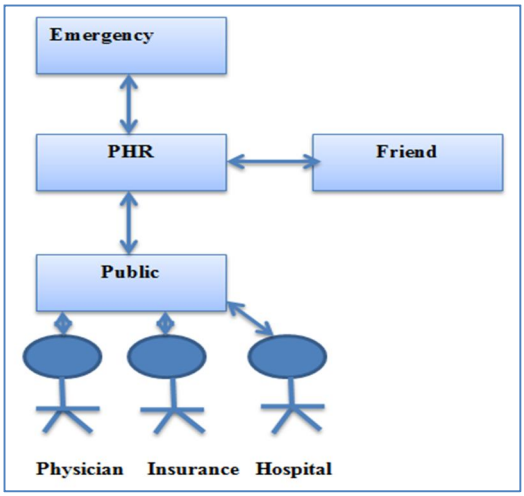

Fig. 1 – Schematic overview of the scheme

As can be seen in fig. 1, PHR is actually owned by patients. A patient can operate the system online and give find grained access to his friends, public attribute authorities and emergency personnel of hospital. All kinds of access policies are based on attributes. Attributes are very convenient to share PHRs. No user has full access to PHR generally as the access is given based on attribute requirements. Each attribute is nothing but a set of columns whichare relevant. For instance each PHR might have attributes like personal information, medical history, examination, insurance information and sensitive information. Again each attribute is made up of a set of columns or fields. For instance medical history is made up of conditions, allergies, prescriptions. The access policy is encryption based. The physician, insurance staff and hospital staff are known as public domain users. Patient might have friends. They are known as private domain users.

The operations involved in the system are system setup and key distribution, PHR encryption and access, user revocation, policy updates, and break-glass security. The key distribution process generates a public key and secret key for every user. The encryption and access policies are based on the attributes available. The user revocation is possible when PHR owner wants to revoke any particular user on his PHR. Then that user can't access PHR details. Policy updates are possible from time to time to improve the ABE security scheme. Break – glass security is applied to emergency personnel where they can take directly details from PHR owner. This emergency access helps them to serve better. More technical details of the scheme are found in [14].

IV. PROTOTYPE IMPLEMENTATION

We built a prototype application that demonstrates the efficiency of the proposed framework that can be used to outsource PHRs in patient centric fashion. The application is built in such a way that it works in distributed environment. It is a web based prototype. The environment used to build the application is a PC with 2GB RAM, core 2 dual processor running Windows 7 operating system. The platform used to built application is Microsoft .NET. The programming language used is C#. Some key functionalities of the prototype are presented via the screens presented in fig. 2 and fig. 3.

Fig. 1 –Shows Key Generation as part of MA-ABE system

As seen in fig. 2 it is evident that the new registration of a user needs security keys that are used further to manage and access PHRs. In fig. 3 demonstrates the usage of ABE in terms of encryption and decryption. The generated keys are sent to the user in a secure fashion.

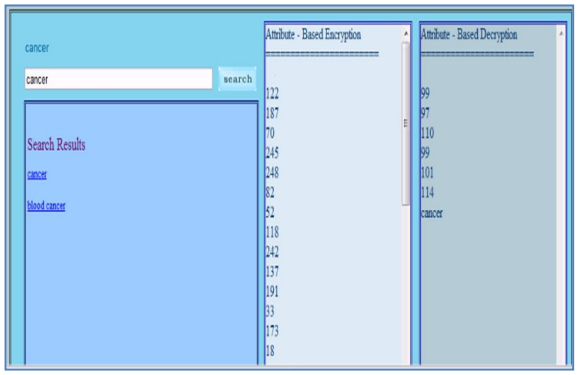

Fig. 3 –ABE and ABD results

As can be seen in fig. 3, there is provision for encryption and decryption. The encryption and decryption processes are pertaining to ABE. The ABE is an efficient scheme that has been enhanced in this paper as described earlier.

V. EXPERIMENTAL RESUTLS

We made experiments with our system. Then the results are compared with other works such as RNS [15], NGS [12], HN [16], BCHL [6] and VFJPS [17]. The results revealed that our system outperforms previous works in terms of cipher text size, user secret key size, public key or information size, and revocation message. Figure 4 presents the results of experiments.

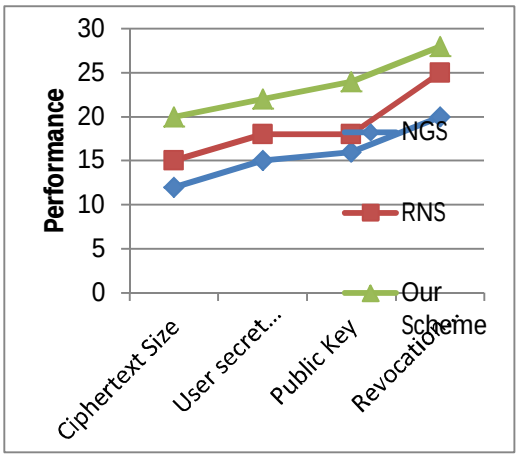

Fig. 4 –Experimental Results

As can be seen in figure 4, the result of the proposed scheme is compared with RNS and NGS. As per the results the proposed system is more secure and scalable in terms of ciphertext size, user secret key size, public key, and revocation message.

VI. CONCLUSION

In this paper we implement a framework for secure and scalable sharing of PHRs in cloud. As the cloud servers are un-trusted, the patients should have privacy to their out sourced data. Moreover the schemeshould be patient centric. As the personal health records are highly sensitive in nature, patient should have full control over health record while giving fine grained and control access to other parties. In the proposed system multiple PHR owners and other users are involved. We aim at reducing complexity and improve privacy guarantees. To achieve this by improving ABEinto MA-ABEthis also has user revocation.Our framework is influence by the work of Li et al. [14]. We built a prototype application which is patient centric and demonstrates the proof of concept. The empirical results revealed that the application is effective as it gives scalable and secure access to health records.

References:

[1] 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.
[2] H. Lohr, A.-R.Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.
[3] "Google, microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.
[4] "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
[5] 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.
[6] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical record- s," in CCSW '09, 2009, pp. 103–114.
[7] 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.
[8] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Communications Magazine, Feb. 2010.
[9] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp. 17–426.
[10] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible 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] S. Narayan, M. Gagń , and R. Safavi-Naini, "Privacy preserving e
ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.
[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.
[14] Ming Li Member, IEEE, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", IEEE, 2012.
[15] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.
[16] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no.PrePrints, 2010.
[17] 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 VLDB '07, 2007, pp. 123–134.

AUTHORS

Authors

Sravan Kumar.Ch, he is pursuing M.Tech (CSE)in MLRIT , Hyderabad, AP, INDIA. He has received B.Tech Degree in Computer Science and Engineering. His main research interest includes Cloud Computing and Datamining.

Srikanth Sreerama. He is currently with the Department of Computer Science and Engineering, MLRIT, Andhra Pradesh, India. He is having 7 years of teaching experience**.** His main research interest includes Cloud Computing and Data Mining.