ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

Investigation on Improving the Security of Public Health Record System in Cloud Computing

E. Kamalakannan[1] Arvind .K.S[2]

PG Scholar, Department of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamilnadu, India[1]

Assistant Professor, Department of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamilnadu, India[2]

ABSTRACT: In Cloud Computing we can integrate the lot of technology. But security is the serious concern while moving to the cloud. We need to provide the security for the cloud data. One of the sensitive information is Medical Records. Handling the medical records in cloud is a very complex one. There is the security threat in cloud computing. So overcome the security threat while maintaining the medical records we need to improve the security level of the PHR system in cloud computing. In this paper we made a Survey on Improving the Security of Public Health Record System in Cloud Computing.

Keywords: Cloud Computing, Medical Records, Public Health Record System.

I. INTRODUCTION

In this paper contains the survey on improving the Security on Public Health Records in Cloud Computing. Section2 includes the Literature Survey. That is the details about the overview of information given in the papers. Section3 contains the Techniques for Securing the PHR. Techniques are Attribute Based Encryption, Attribute Based Broadcast Encryption and Identity Based Encryption.

II. LITERATURE SURVEY

H. Lohr, A.-R. Sadeghi, provide the paper about the how to secure the Electronic Health Records and what are all the problems maintain the E-Health Records in Cloud Storage and also they gave the cryptographic scheme as well as key management for secure the Electronic Health Records [22]. M. Li, S. Yu, N. Cao, provides the paper on authorization for private keyword search over the encrypted cloud data. This paper provides detailed view for the keyword search which data is stored in cloud [23]. A. Sahai and B. Waters provide the initialization of Attribute Based Encryption as well as detailed about the Fuzzy Identity Based Encryption techniques [1]. M. Li, S. Yu, K., provides the excellent technique for accessing the data i.e. Fine Grained Access Control with the Multi Owners for accessing the records. This paper provides the scalability for the users for accessing the records [3].

Li, M., Lou,. provides the paper on how to secure the data and ensure the privacy of the data [2]. V. Goyal, A. Sahai, and B. Waters, provides the paper on the Fine Grained Access Control with the help of the Attribute Based Encryption. So this provides the detailed view about the scalable of users as well as confidentiality of the data [4]. Ming LiShucheng Yu, Yao Zheng, provides the scalability of the users and secure sharing as well as importantly

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

Revocable Attribute Based Encryption. This paper explains how public key cryptography used with the ABE as well as Fine Grained Access Control [5].

Y. Zheng provides the master thesis for the preserving the privacy of public health records in cloud computing. This paper gives the good understandable about the privacy of the health records to maintain in the cloud [6]. L. Ibraimi, M. Petkovic, S. Nikova, provides the detailed about the Ciphertext Policy with the use of Threshold property that is have to satisfied the condition [7]. S. Yu, C. Wang, and W. Lou, provides the data sharing based on attribute and revocation based on attributes [8]. S. Narayan, M. Gagne´, and R. Safavi-Naini, provides the preserving the privacy of the Electronic Health Records system with the use of the Attribute Based Infrastructure [9]. J. Bethencourt, A. Sahai,B. Waters, provides policy of cipher text with the Attribute Based Encryption [10]. J.A.Akinyele, C.U.Lehmann,provides the detailed about the self-protection of the Electronic Medical Records based on the attribute Based Encryption[11]. M. Chase and S.S. Chow, provides the important aspects of key distribution as well as maintenance of attribute that is Multi Authority [12]. X. Liang, R. Lu, provides the policy on cipher text as well as the more details about the revocations [13].

J. Hur also provides the Attribute Based Encryption with the revocation aspects [14]. A. Boldyreva, V. Goyal, and V. Kumar, provides the Identity Based Encryption with the revocation of IBE [15]. D. Boneh provides the identity based encryption with the concept of weil pairing algorithm aspects [16]. R. Canetti, S. Halevi, and J. Katz provide the different way that is chosen cipher text based on Identity Based Encryption method [17]. N. Attrapadung , provides the good approach that is Broadcast Based Encryption with the property of Conjunctive [18]. Jin Sun, Yupu Hu, provide the cipher text policy on the Broadcast Based Encryption [19]. Boneh D., Gentry. provides the detailed view of the Collusion Resistant on the Broadcast Based Encryption [20]. Zhang L., Hu Y., provide the paper on the Broadcast Based Encryption based on the Identity aspects [21].

III. TECHNIQUES FOR SECURING THE PHR

A. ATTRIBUTE BASED ENCRYPTION

Attribute Based Encryption [1][10][11][12] is the encryption technique which is used to solve the problems on outsourced data. The initial concept of the Attribute Based Encryption is keys of users and the cipher text are combined with the groups of attributes and using particular exact key only decrypt the cipher text. So there is the match between the cipher text and private as well as attributes. That stages they also used the Biometrics for strong protection.

Then the later years the Attribute Based Encryption [4][5][6][7][9] for one to many approaches [2] i.e. for particular information for many numbers of users with encryption schemes are evolved. This is the excellent technique for handle the many number of users i.e. it increases the scalability. So the Attribute Based Encryption technique can be used for securing the sensitive data like patient record over outsourced data in cloud computing with multi-owner [3]. So we having the excellent option that is Attribute Based Encryption are applicable for Fine Grained Access [4][5].

The most sensitive field is Medical field. So if the medical data is maintained with the Cloud is good one but we have to provide the N number of security for that data.

Figure1 is the Framework for Multiple Owner and Multiple Users and Multiple Authorities for Public Health Records System in Cloud Computing. The diagram clearly explains the system that is the patient can store the health record in cloud with the help of encrypted format. Patient is the data owner. So data owner having the all access rights on that data. So data owner can provide the access rights on the public domain users. The key distribution is controlled by the attribute authorities.

Here Multiple Attribute Authorities [4][5][12] (MAA) for separate domain. MAA maintains the attributes as well as key policy. In public domain except doctor all users are only having the read only rights. The doctor is the ultimate user in public domain so need to give the write option. The key will distribute via the attribute authority. And for Emergency scenario the Break Class Access [4][5] can maintain.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

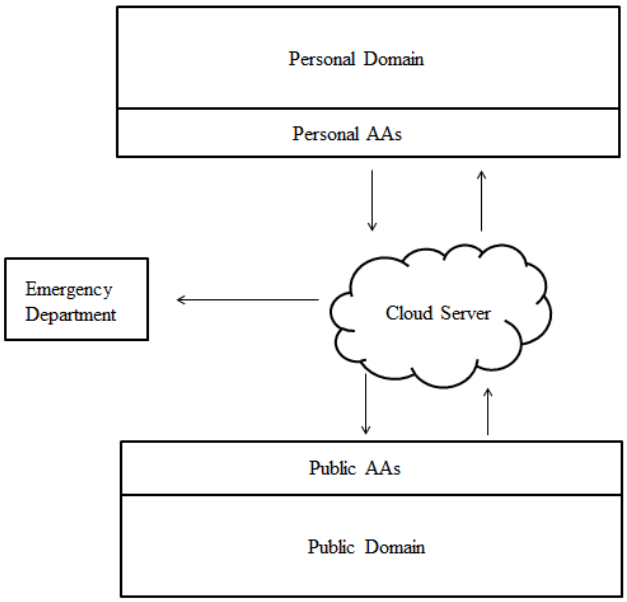

Fig1. Multi-Owner, Users, Authority for Public Health Records System in Cloud Computing [4] [5]

That is that emergency scenario based on the identity can break the normal formalities and can access the whole data from emergency department.

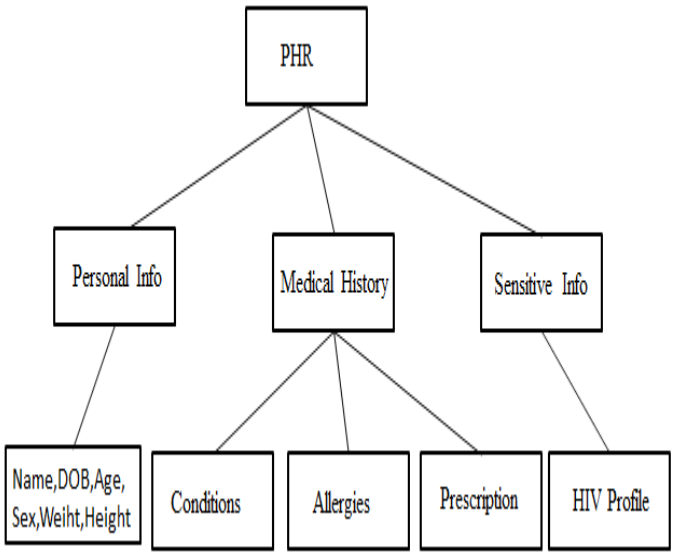

Fig2. The attribute hierarchy of Health Records [5]

Figure 2 is the diagram for Attribute Hierarchy of the Health files. This diagram clearly explains the hierarchy of Attributes which is going to be encrypted and stored in Cloud Storage.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

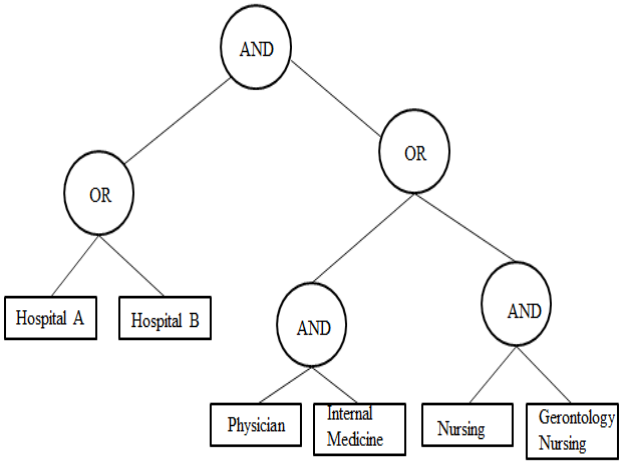

Fig. 3 Access Policy [4]

Figure 3 is the structures for access policy [4][10] which is under the arrangement of the Multiple Attribute Authority. Like Above diagram structure only the policy will assign and access rights are provided. If the policy break at any time means Revocation [8][13][14] will be taken at any time. This attribute based encryption more efficient in conjunctive property.

B. IDENTITY BASED ENCRYPTION

Identity Based Encryption [15][16][17] is better technology for protecting the secure access on the PHR. Because it does not requires the public key cryptosystem. So it's not depends any public key infrastructure. It based on E-mail or IP address for encryption. Efficient Revocation [15] is possible in the Identity Based Encryption. Fuzzy Identity Based Encryption [1] is method for like threshold value matching. In this scheme like set of attributes should be satisfied in matching. For example 10 out of 12 attributes have to satisfy. So the identity based encryption provides the strong authentication as well as confidentiality.

C. ATTRIBUTE BASED BROADCAST ENCRYPTION

Attribute Based Broadcast Encryption is special encryption technique for Direct Revocation without affecting the non-revoked users [18]. Attribute Based Broadcast Encryption is the Encryption technique for remove the limitations on the Multi-Authority system. In Abstract Based Encryption technique satisfies the Conjunctive property. Even Conjunctive Based Broadcast Encryption efficient in the pairing based cryptography Scheme [18]. Due to some real time limitations on MA-ABE we can move to Attribute Based Broadcast Encryption. ABBE supports the Disjunctive property as well as Conjunctive property.

Advantage of the Attribute Based Broadcast Encryption is it handles the both Cipher text-policy and key policy in efficient manner [19]. ABBE scheme is the strong collision resistant at the handling of cipher text [20]. It overcomes the limitations on ABE. The major advantage of the ABBE scheme is it's also possible to integrate the Identity i.e. Identity Based Broadcast encryption technique is better way to provide the authentication as well as confidentiality [21]. For the PHR System Attribute Based Broadcast Encryption technique is the better technique to protect the Records.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

IV. CONCLUSION

In this paper made a survey on the Improving the Security on Public Health Record System in Cloud Computing. And also made a detailed study about what are the techniques is needed for security the Health Record System. Attribute Based Encryption is the good technique to securing the Health records. It is efficient in the Conjunctive Property. But somewhat limitations on MA-ABE in real time with the property of Disjunctive as well as it had the little bit problem while revocation. Because it can be affect the non-revoked users. So move to the Attribute Based Broadcast Encryption. It satisfies the Disjunctive Property also and handles the revocation perfectly. Identity Based Encryption is the better way to provide the authentication for the Public Health Record System. My future work will be the using the ABBE scheme for securing the PHR system in Cloud Computing.

REFERENCES

[1] Sahai and B. Waters. "Fuzzy Identity Based Encryption.", In Advances in Cryptology – Eurocrypt, volume 3494 of LNCS, pages 457–473. Springer, 2005.

[2] Li, M., Lou,W., Ren, K., " Data security and privacy in wireless body area networks", IEEE Wireless Communications Magazine (February 2010).

[3] 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", Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10),pp. 89-106, Sept. 2010.

[4] 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.

[5] Ming LiShucheng Yu, Yao Zheng,Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE transactions on parallel and distributed systems, vol. 24, no. 1, january 2013.

[6] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption", master's thesis, Worcester Polytechnic Inst., 2011.

[7] 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.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[9] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure", Proc. ACM Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010.

[10]J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

[11]J.A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin, "Self-Protecting Electronic Medical Records Using Attribute-Based Encryption", Cryptology ePrint Archive, Report 2010/565, http://eprint.iacr.org/, 2010.

[12]M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009.

[13]X. Liang, R. Lu, X. Lin, and X.S. Shen, "Ciphertext Policy Attribute Based Encryption with Efficient Revocation", technical report, Univ. of Waterloo, 2010.

[14]J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July2011.

[15]A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation", Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[16]D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing", In CRYPTO, pages 213–229, 2001.

[17]R. Canetti, S. Halevi, and J. Katz., "Chosen-ciphertext security from identity-based encryption", In EUROCRYPT, pages 207–222, 2004.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

[18]N. Attrapadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption", Proc. Third Int'l Conf. Palo Alto on Pairing-Based Cryptography-Pairing, pp. 248-265, 2009.

[19]Jin Sun, Yupu Hu, and Leyou Zhang., "A Key-Policy Attribute-Based Broadcast Encryption", The International Arab Journal of nformation Technology, Vol. 10, No. 5, September 2013

[20]Boneh D., Gentry C., and Waters B., "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys", in Proceedings of the 25th Annual International Cryptology Conference, USA, pp. 258-275, 2005.

[21]Zhang L., Hu Y., and Mu N., "Identity-Based Broadcast Encryption Protocol for Ad-hoc Networks", in Proceedings of the 9th International Conference for Young Computer Scientists, Hunan, pp. 1619-1623, 2009.

[22]H. Lohr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud", Proc. First ACM Int'l Health Informatics Symp. (IHI 10), pp. 220-229, 2010.

[23]M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing", Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

BIOGRAPHY

Mr. E.KAMALAKANNAN

E. Kamalakannan is a Second year M.E CSE Student of Kalaignar Karunanidhi Institute of Technology, Coimbatore. He received B.TECH IT Degree in Chettinad College of engineering and Technology, Karur. He is doing Project in the area of Cloud Computing.

Mr. ARVIND .K.S

Arvind. K.S is working as Assistant Professor in Kalaingnar Karunanidhi Institute of Technology. He had received his Bachelor of Technology from Pondicherry University, Master of Engineering from Anna University Chennai and currently pursuing Research in Anna University Chennai. His field of Research is Cloud Computing and Information Security.