International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 23 (2015) pp 43378-43383

Flexible, Scalable and Fine Grained Access Control for Medical Data in Cloud Using Attribute Based Encryption

Lakshmi Mohanan

PG Scholar, Department of Computer Science and Engineering, Adi Shankara Institute of Engineering & Technology Kalady, India laks.mohanan @gmail.com

Ajay Basil Varghese,

Assistant Professor, Department of Computer Science and Engineering Adi Shankara Institute of Engineering & Technology Kalady, India ajaylalau @gmail.com

Abstract-
The widespread adoption of Personal Health Records (PHR)/Electronic Health Records (EHR) has greatly improved the quality of healthcare systems world over. Cloud computing with its storage scalability and cost effectiveness has been the driving force technology behind this shift. Since usage of cloud for healthcare involves entrusting the patient health records to cloud providers, there are increased concerns of safety and security of outsourced health data. Many approaches including cryptographic and non cryptographic techniques have been suggested to ensure the privacy of health records stored and exchanged using cloud. Among them the Attribute Based Encryption (ABE) and its different variations have been successful in providing flexible and fine grained access control to health data. But most of them incur high key management overhead, inflexibility in implementing complex access control policies and less efficient user revocation methods. The purpose of this research paper is to provide a scalable, flexible and fine grained access control mechanism for outsourced health records in cloud. This is achieved by categorizing the users of the system into personal and professional security domains. For professional domain, a Hierarchical Attribute Set based Encryption (HASBE) is employed and for the personal domain Key Policy Attribute Based Encryption (KP-ABE) is used. This achieves the needed scalability and fine grainedness for professional domain and simplicity of key management in personal domain. An analysis of the proposed method in terms of its performance is also provided.

Keywords: Cloud computing; ABE; HASBE; KP-ABE; cloud data security.

Introduction

Information technology has greatly aided in revolution-izing the health care industry. IT introduced the use of electronic health records (EHRs) and personal health records (PHR) for patient data-keeping, instead of paper records. The PHRs and EHRs, both are the electronic versions of patient health information, former controlled by patients[1] and latter by healthcare providers. American Recovery and Reinvestment Act (ARRA) stipulates that all healthcare organizations must implement the use of electronic health records by 2015. Furthermore, Health Insurance Portability and Accountability Act (HIPAA) mandates certain physical, network, and process security measures that needs to be in place and followed to ensure confidentiality and integrity of health data. If these mandates are not satisfied, penalties will ensue. Therefore, healthcare professionals have no choice but to march into the digital world.

Cloud Computing is a prominent technology that has revolutionized the way services are delivered to the end users. Cloud can bring the benefits of reduced costs, on-demand access, scalability, flexibility etc. to healthcare sector. The HIMSS Cloud Analytics Survey of healthcare service providers in the US, finds that 83% of American Healthcare providers use some form of cloud. However healthcare data has stringent requirements for security, con-fidentiality, availability along with the need to conform to government and industry regulations (HIPAA and ARRA). While cloud services offers advanced technical solutions at lower costs, issues of privacy and security needs to be addressed effectively

To address the safety concerns of health data in cloud, this paper proposes a method where, users are categorized into security domains public and personnel. For personnel domain (PSD) which includes family and friends a Key Policy ABE (KP-ABE) scheme is used to manage the secret keys and access right. On the other hand, PUD will consist of users who access the health records based on their pro-fessional roles like doctor, nurses, medical researchers etc. and a Hierarchical Attribute Set Based Encryption (HASBE) can be leveraged for managing users in PUD.

Related Work

There have been numerous privacy preserving approaches in cloud which may be categorized into 1) cryptographic approaches 2) non-cryptographic approaches, which are dis-cussed in the subsequent sections.

A. Non Cryptographic Approaches

The major non-cryptographic approaches in cloud, that use certain policy-based authorization are described here. Kamran et al. proposed [2] a watermarking scheme for right protection of EMR systems that computes a water-mark which when inserted into the EHR does not alter its vital/diagnostic

features hence preventing misdiagnosis. Currently this method is limited to only numeric values and calculating the watermark for each feature requires multiple iterations through the full database. Secure health data application software based on virtual machines is presented in [3] called MyPHRMachines. After uploading the PHRs on MyPHRMachine, the patient access the PHRs through Virtual Machine (VM) to delegate the access rights selectively to individual caregivers. But this technique can lead to numerous personal application islands, in which each patient collects heterogeneous PHR data and application software and lack of internet access for the VMs in which the data and software prevents it from accessing other web services.

B. Cryptographic Approaches

The cryptographic approaches commonly used in the e-Health cloud-based systems to protect data use encryption schemes, like Public Key Encryption (PKE), Symmetric Key Encryption (SKE) and Attribute Based Encryption (ABE).

***PKE based approaches*:**

The PKE technique utilizes two separate keys; one is private while the other is public. In many cases, PKE is used in conjunction with the SKE for better computational efficiency. In the security model pro-posed by Liu et al. [5] a reference security model for EHR collection, storage and verification is proposed. Although this model combining various techniques provides ample security, key management and distribution is hard to address. [6] talks about a digital rights management approach for health record privacy, which requires client side agent to enforce security, which limits it. Method for enhancing accountability of electronic health record usage via patient-centric monitoring is introduced in [7] that utilizes concept of Universal Designated Verifier Signatures (UDVS). But this technique assumes that the health data is first created by record issuers that have knowledge about the contents of records, hash values, and signatures and hence can be misused by them.

***SKE based approaches*:**

Unlike PKE, SKE has the same keys for encryption as well as decryption. The SKE-based schemes can effectively secure data and protect its confidentiality but may require additional procedures to implement the access control. A mechanism for unlinkability between the patients and electronic medical records in the cloud environment is presented by Li et al. [9]. The patients electronic medical records are encrypted through the SKE and are stored anonymously. The doctors use digital signatures to process the patient health records after the treatment for storage at the cloud. A dynamic access structure to enforce precise access control over the PHRs in multiuser cloud environment is introduced by Chen et al. [8]. The health records are encrypted and decrypted through Lagrange multipliers using the SKE. Major advantages of this approach is the automatic revocation of the users and reduced complexities of key management.

***ABE based approaches*:**

ABE is a cryptographic primitive based on the PKE where the messages are encrypted and decrypted on the basis of attributes. The major advantage of ABE over other techniques is that it allows fine grained access control policies to be specified and enforced. The two major categories of ABE are 1) Key Policy Attribute Based Encryption (KP-ABE) 2) Ciphertext Policy Attribute Based Encryption (CP-ABE). In KP-ABE, the policies are specified in the users key, while the ciphertext is associated with attributes. In contract to this, CP-ABE[18] has policy associated with the ciphertext and attributes with the user key. In both cases, the user can decrypt the document only if the attributes satisfy the policy.

In [11] Liu et al. proposes a form of attribute based encryption for scalable and secure sharing of PHR. The major feature is the use of MA-ABE for the public domains and KP-ABE for personal domains. This scheme does not fully address user revocation and key management problems. CAM [12] for mobile health data monitoring aims to preserve privacy of the clients and the mobile health (mHealth) service providers relies on homomorphic encryption and outsourcing decryption. This method can be used only for specific patients who needs continuous monitoring using sensor devices. For multiauthority cloud storage DAC-MACS [13] is proposed where new multiauthority CP-ABE scheme with efficient decryption is constructed with main computation outsourced using a token-based decryption method. Provides design of an efficient immediate attribute revocation method for multiauthority CP-ABE scheme that achieves both forward security and backward security.

Proposed System

The main objective of the proposed scheme is to provide scalable, flexible and fine grained access control with less complex key management and user revocation. The general overview of the scheme is given in the below section.

.

A. Overview of Proposed Scheme

The system users are divided into two security domains personnel and public domain as in the method adopted by Li in [11]. Personnel users (PSD) can be friends/relatives and are granted access directly by the data owner. The number of users in this domain are limited in number. Public domain (PUD) users access the health records for professional purpose like doctors, medical researchers, goverrnment officials etc. The number and the type of users in this domain cannot be determined in advance and can be large. Li proposes the KP-ABE scheme for personnel domain and MA-ABE for public domain. While KP-ABE suits the personnel domain because of the limited number of users, MA-ABE is limited due to its complex user revocation and limitation in specifying key attributes. To overcome this, our paper proposes to use HASBE[16] scheme for the pubic domain in place of MA-ABE. Hence for each PSD YWRLs revocable KP-ABE [15] scheme is used while for each PUD HASBE [16] scheme is proposed. This combination reduces the burden of key management for the data owner, while effectively securing the health data in the public domain.

B. KP-ABE in personnel domain

For personnel domain YWRLs revocable KP-ABE [15] is used. The system first defines a common universe of data

attribute categories for every PSD, like ”basic pro-file”,”medical history ”,”allergies” and ”prescriptions”. Each PHR owners client application generates its pub-lic/master keys. A user in PSD obtains the secret key by sending a request to the PHR owner. Based on attributes allowed by the PHR owner, the policy engine automatically derives an access structure, and generates user secret key that embeds this access structure using keygen of KP-ABE. The keys size is linear with the category of files they can access. In addition, the data attributes can be organized in a hierarchy for efficient policy generation, that leads to fine grained capability. Each PHR document is labelled with a set of attributes and also encrypted using these attributes. The owners upload encrypted PHR files to the cloud server. The data readers download PHR files from the server, and can decrypt the files only if they have suitable attribute-based keys that satisfy the attributes of the encrypted file. This is depicted in Fig. 2

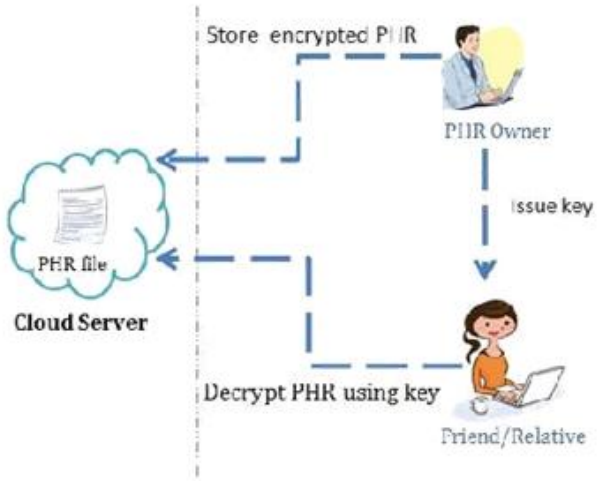

Figure 1. KP-ABE in personnel domain

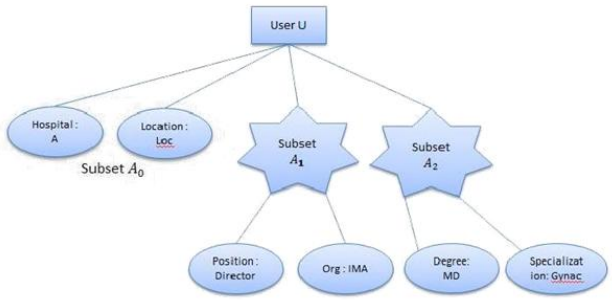

Fig.2. Key structure

C. HASBE in public domain

In the public domain, for realizing scalable, flexible, and fine-grained access control HASBE scheme[16] is proposed instead of MA-ABE by Li [11]. This scheme has a top-level trusted authority (TA), responsible for managing the top level domain authorities (DA) under it. These DA’s can represent different domains like insurance, government, medical etc. and can manage sub DAs under them or can directly manage users. These DAs are responsible for issuing keys to the users under them. Neither the data consumers nor the data owners need to be online always while the TAs and the DAs and the cloud service provider needs to be always online. This hierarchical organization of domain authorities help achieve the needed scalability by utilizing the cloud resources.

Key Structure

The DA generates the keys for the users. A recursive set based key structure as in [17] where each element of the set is either a set or an element corresponding to an attribute. The depth of the key structure is the level of recursions in the recursive set, similar to definition of depth for a tree. For a key structure with depth 2, members of the set at depth 1 can either be attribute elements or sets but members of a set at depth 2 may only be attribute elements. The example shown in Fig. 3 shows a key structure with depth 2. The key structure defines unique labels for sets in it. If there are m sets at depth 2 then a unique index i where 1 i m is assigned to each set. The set at depth 1 is referred to as set 0. Using this convention, a key structure of depth 2 can be represented as A = A_0; A_1; ::A_m, where A_0 is the set at depth 1 while A_i is the ith set at depth 2, for 1 i m. When trying to satisfy a given policy, a user may only use attribute elements within a set, but may not combine attributes across the sets by default. However, if the encryptor has designated translating nodes in an access structure, users can combine attributes from multiple sets to satisfy the access structure. This leads to flexibility in specifying the access policy. At the same time different values for expiration time attribute can be assigned under different sets, that makes user revocation efficient.

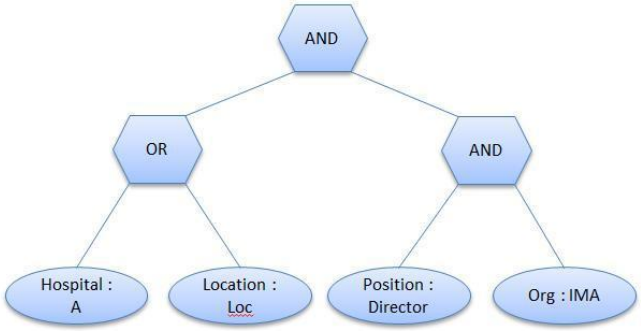

Figure 3. Access structure

Access Structure

The tree access structure[17] has the leaf nodes represent attributes and nonleaf nodes threshold gates. Each nonleaf node/threshold gate is defined by its children and a threshold value. Let num_x be the number of children and k_x indicate threshold value of node. A sample access tree is shown in Fig. 4. The threshold gates are AND and OR and have threshold values of 2 and 1, respectively. As mentioned earlier the access structure can also have translating nodes that lets users restrict/allow combining attributes from different sets to satisfy the policy and thus leading to flexible design.

The key structure that can satisfy the access structure associated with the encrypted record can decrypt that record. The overall scheme is depicted in figure 4. This scheme

achieves scalability due to the hierarchical organization of DA's. Flexibility of the scheme comes from the above mentioned access structure that helps you restrict combining attributes from different sets or allow it. ABE is inherently fine grained and allows you to specify the attributes in a hierarchically organized way and to a very low level.

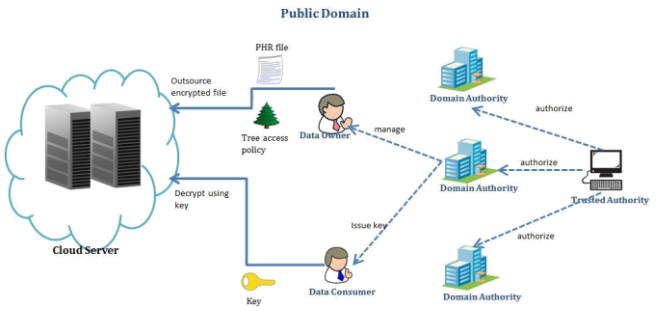

Figure 4. HASBE in public domain

Implementation & Experimental Results

This section describes the implementation details along with result of the experiments conducted in studying the method.

A. Implementation

We have implemented separate toolkits for HASBE and KP-ABE schemes along with corresponding graphical user interfaces. The KP-ABE toolkit was developed using Pairing Based Cryptography library (http://crypto.stanford.edu/pbc/). The HASBE toolkit was developed extending the toolkit (http://acsc.csl.sri.com/cpabe/) developed for CP-ABE [18] which uses also uses Pairing-Based Cryptography library. Then comprehensive experiments are conducted on a laptop with intel core 1.40-GHz CPU and 4-GB RAM, running Windows 8.

B. Experimental Results

This sub-section describes the experimental results for both kpabe and hasbe toolkit.

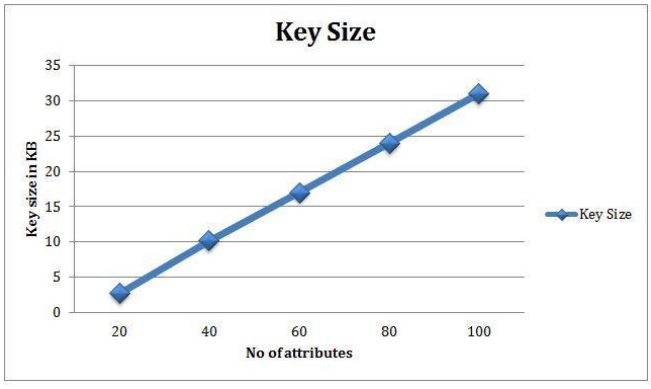

Figure 5. KP-ABE Key Size

KP-ABE:

Fig 5 shows the key size corresponding to the number of attributes in kp-abe. As can be seen from the figure the key size increases linearly with the number of attributes in the key. The plot for the key generation time is given in Fig 6 that shows that the time increases linearly with the no of leaf nodes in the policy defined for the ciphertext. Even with a policy having 100 leaf nodes, the maximum time taken would be below 6 seconds. Encryption and decryption time plots are given by Fig 7 and 8 respectively. Both the plots show a linear increase of time with respect to the increase in the number of leaf nodes in the policy.

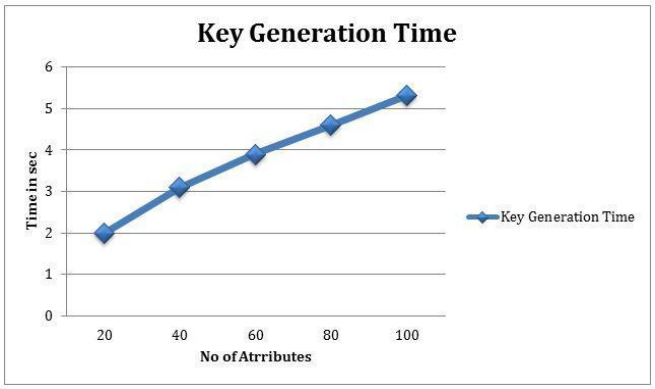

Figure 6. KP-ABE Key Generation Time

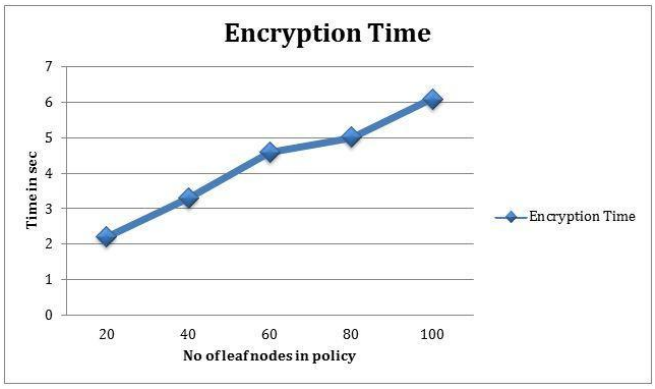

Figure 7. KP-ABE Encryption Time

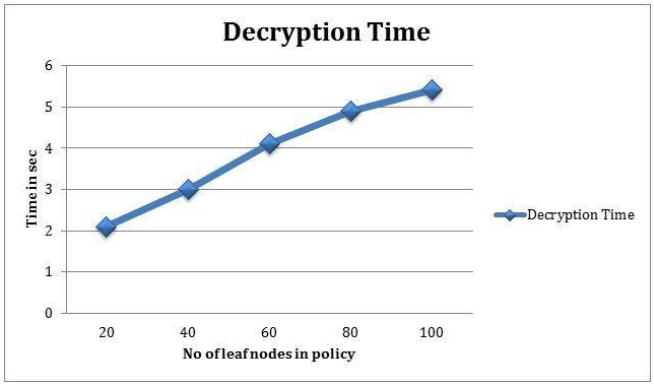

Figure 8. KP-ABE Decryption Time

HASBE:

The key size plot for HASBE is given in Fig 9 which shows the key size corresponding to the number of attributes which

increases linearly. The plot for the key generation time is given in Fig 10 that shows that the time increases linearly with the no of leaf nodes in the policy defined for the ciphertext. Even with a policy having 100 leaf nodes, the maximum time taken would be below 7 seconds. Encryption and decryption time plots are given by Fig 11 and 12 respectively. Both the plots show a linear increase of time with respect to the increase in the number of leaf nodes in the policy.

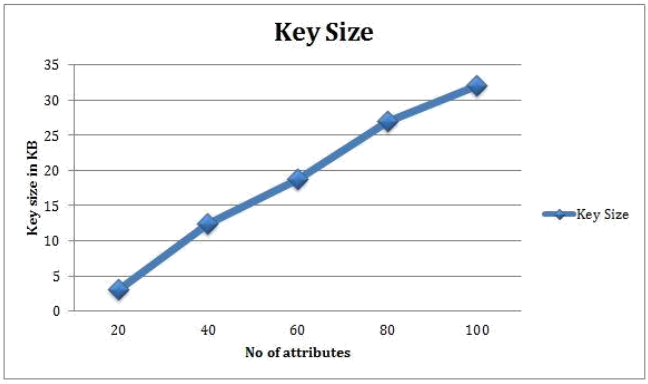

Figure 9. HASBE Key Size

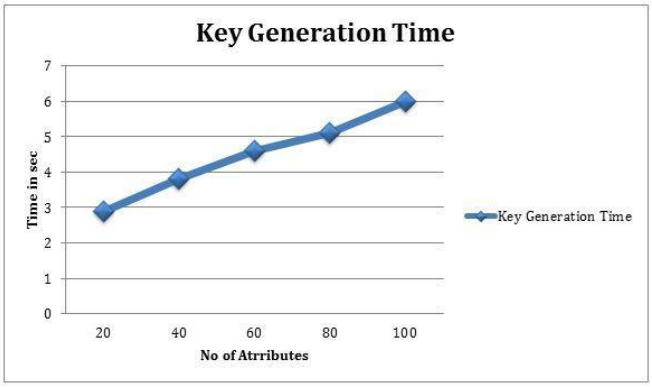

Figure 10. HASBE Key Generation Time

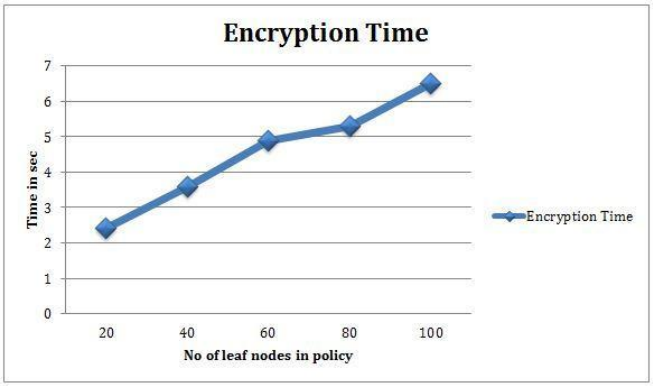

Figure 11. HASBE Encryption Time

Conclusion

This paper aims at proposing a flexible, scalable and fine grained access control mechanism with lower key management and user revocation complexities. For this two different ABE variants are utilized. The systems users are divided into the public and personnel security domain. For personnel domain KP-ABE is proposed with the key issuing handled by the data owner himself.

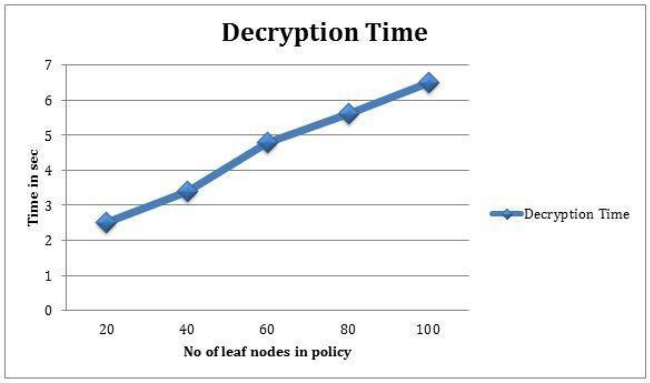

Figure 12. HASBE Decryption Time

For public domain flexible, scalable and fine grained scheme HASBE is utilized. Because of the property of multiple value assignments for expiration time attribute user revocation is achieved efficiently. This scheme effectively achieves lower key management overhead for the data owner at the same time providing flexible and fine grained access control in the public domains. The exper-imental results also show that the additional functionality provided does not impact the system performance beyond unacceptable levels.

Acknowledgment

The authors would like to thank ASIET, Kalady for all the infrastructure support provided in completing our work. We would also like to extend our sincere gratitude to Prof.Rajaram, HOD, CSE Dept ASIET for his immense support and encouragement. We also wish to express our thanks to Prof. Abraham Varghese for his constant feedback and guidance.

References

[1] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, A research agenda for personal health records (PHRs), J. Am. Med. Informat. Assoc., vol. 15, no. 6, pp. 729736, 2008.

[2] M. Kamran and M. Farooq, An information-preserving wa-termarking scheme for right protection of emr systems, IEEE Trans. on Knowledge and Data Eng., Nov. 2012.

[3] P. V. Gorp and M.Comuzzi, Lifelong personal health data and application software via virtual machines in the cloud, IEEE J. Biomed. Health Informatics, vol. 18, no. 1, pp. 110, Jan. 2014.

[4] R.Wu, G.-J. Ahn, and H. Hu, Secure sharing of electronic health records in clouds, in Proc. 8th IEEE

Int. Conf. Collabo-rative Comput., Netw., Appl. Work-sharing, 2012, pp. 711718.

[5] R. Zhang and L. Liu, Security models and requirements for healthcare application clouds, in Proc. IEEE 3rd Int. Conf. Cloud Comput., Jul. 2010, pp. 268275.

[6] M. Jafari,R. S.Naini, andN. P. Sheppard, A rights management approach to protection of privacy in a cloud of electronic health records, in Proc. 11th Annu. ACM Workshop Digital Rights Manag., Oct. 2011, pp. 2330.

[7] D. Mashima and M. Ahamad, Enhancing accountability of electronic health record usage via patient-centric monitoring, in Proc. 2nd ACM SIGHIT Sympo. Int. Health Informat., Jan. 2012, pp. 409418.

[8] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, Secure dynamic access control scheme of PHR in cloud computing, J. Med. Syst., vol. 36, no. 6, pp. 40054020, 2012.

[9] Z. R. Li, E. C. Chang, K. H. Huang, and F. Lai, A secure electronic medical record sharing mechanism in the cloud computing platform, in Proc. 15th IEEE Int. Sympo. Consum. Electron., Jun. 2011, pp. 98103.

[10] A. Sahai and B. Waters, Fuzzy identity based encryption, Adv. Cryptol. Eurocrypt, vol. 3494, pp. 457473, May 2005.

[11] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131143, Jan. 2013.

[12] H. Lin, J. Shao, C. Zhang, and Y. Fang, CAM: Cloud-assisted privacy preserving mobile health monitoring, IEEE Trans. Inf. Forensics Security, vol. 8, no. 6, pp. 985997, Jun. 2013.

[13] Kan Yang, Xiaohua Jia, Kui Ren, and Bo Zhang. DAC-MACS: Effective data access control for multi-authority cloud storage systems. In INFOCOM, 2013 Proceedings IEEE, pages 2895 2903, 2013. 2, 9

[14] Yue Tong, Jinyuan Sun, Chow S.S.M., Pan Li, Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability, IEEE J. Biomed. Health Informatics, vol. 18, no. 2, pp. 419 - 429, Mar. 2014.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing, Proc. IEEE INFOCOM 10, 2010.

[16] Wan, Zhiguo, Jun'E. Liu, and Robert H. Deng. "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing." Information Forensics and Security, IEEE Transactions on 7, no. 2 (2012): 743-754

[17] R. Bobba, H. Khurana, and M. Prabhakaran, Attribute-sets: A practically motivated enhancement to attribute-based encryp-tion, in Proc. ESORICS, Saint Malo, France, 2009.

[18] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007.