International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 1 Issue 1 –AUGUST 2013.

Attribute based Encryption technique in Preserving Cloud based Health Records

G. Radhika Deepthi[#1], Bandla Srinivasa Rao[*2]

[#]*PG Scholar, Dept. of CSE, VRS & YRN College of Engg. & Technology, Chirala, AP*

[1] deepthi.radhika@gmail.com

[*]*Associate Professor & HOD, Dept. of CSE, VRS & YRN College of Engg. & Technology, Chirala, AP*

***Abstract*— Patient Health Records (PHR) consists of the patient's personal data and their diagnosis information. It should be maintained in the centralized server. The patient's records maintained with full security and privacy in the centralized server. In this privacy mechanism protects the sensitive attributes of the patients and in security schemes are used to protect the data from the public access. Patient Health Record is an emerging model for the patient's health information exchange. And it is outsourced to be stored at third parties in the cloud service providers. It could be exposed to the third party servers and to unauthorized parties or persons. So that the problems will rise in the following ways: risk in the privacy exposure, scalability in key management, flexible access and efficient user revocation. The most important challenges in the service as achieving the fine-grained cryptographically enforced data access control. In this paper, we proposed the novel approach of patient-centric framework and it mechanisms are used for the data access control and data of the patient's are stored in the semi trusted servers. To achieve the fine-grained and scalable data access control for PHR's by using the leverage attributes based encryption techniques. It is used to encrypt the data of the patients in the files. If we compared to the previous security data, this technique leads to the PHR system in the multiple security level or domains and consists of the multiple data owner and users. This key management reduces much more complexity when compared to the other system. 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.**

***Index Terms*— Personal health records, cloud computing, data privacy, fine-grained access control, attribute-based encryption.**

I. Introduction

Cloud computing [39], is an emerging paradigm in the computer industry where the computing is moved to a cloud of computers. The cloud computing core concept is, simply, that the vast computing resources that we need will reside somewhere out there in the cloud of computers and we'll connect to them and use them as and when needed. Cloud computing is the next general step in the evolution of on demand information technology services and products. Cloud computing is a means by which highly scalable and fully technology based services can be easily consumed over the internet on an as-needed basis. To a large extent, cloud computing will be based on virtualized resources. The convenience and efficiency of this approach, however, comes with security risks and data privacy. A significant barrier to the adoption of cloud services is thus user fear of confidential data leakage and loss of privacy in the cloud. Privacy is a important and fundamental human right that encompasses the right to be left alone, many techniques are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification etc.

In recent years, Patient Health Record (PHR) is an emerged technique in a cloud services provider. It is a patient-centric model for the patient health information exchange, control, storage and sharing the patient's personal data and their diagnosis information from one to other place through the web. Each patient is promised for the full control of their medical records and to share their health data with a wide range of users. Many PHR services are outsourced or provide due to the data or shared through the third parties in the cloud services provider.

There are many existing PHR services with many security and privacy risks which could be implode into wide adoption. Main concern of the services is to sharing the sensitive information of the patient's personal health records but the people don't trust fully the third party server. On the one hand, the existing healthcare regulations such as HIPAA is recently amended top the incorporate business associates. In this HIPAA, the cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information, the third-party storage servers are often the targets of various malicious behaviours which may lead to exposure. The PHR service provides to encrypt their files and to allow which set of users to obtain access to each file.

The goal of the exiting PHR system is the privacy is often in conflict. The authorized users may either need to access the PHR for personal use or professional purposes. The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be overwhelmed by the key management overhead. On the other hand, the existing PHR system, consist of the multiple owners who may encrypt according to their ways. An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority i.e., it cause the key escrow problem in the data's of the patients or in the services.

In this paper, we propose the patient-centric model for secure sharing of PHRs and it is stored on semi-trusted servers. The main focus of the proposing system is to address the complicated and challenging key management issues. In order to protect the personal health data from the untrusted server, we assume the attribute-based encryption (ABE) as the main encryption technique for the system. Using ABE policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date. We also introduce ABE (MA-ABE) in the public domain to improve the security level and in order to avoid the key escrow problem.

The rest of the paper is organized as follows. In Section II, we discuss about the related work of the PHR system. In Section III formally introduces our proposed system of the paper. In Section IV we summarize about the algorithm used in the PHR system. In Section V, we present the full simulation study of the proposed scheme. Finally, we conclude the paper and discuss future work in Section VI.

II. Related Works

In this section, we briefly discuss the works which is similar techniques as our approach but serve for different purposes.

Shilpa elsa abraham [40] in this paper Cloud computing environment supports storage spaces for patient health record management process. Data owners update the patient data into third party cloud data centers. The attribute based encryption (ABE) scheme is used to secure the patient records for selected sensitive attributes. Multiple owners can access the same data values. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism. The MA-ABE model is not tuned to provide identity based access mechanism. Distributed storage model is not supported in the MA-ABE model. The proposed system is designed to provide identity based encryption facility. The attribute based encryption scheme is enhanced to handle distributed attribute based encryption process. Data update and key management operations are tuned for multi user access environment.

Ming Li, Shucheng Yu, Kui Ren, and Wenjing Lou [41] In this paper, we propose a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patients' PHR data. To reduce the key distribution complexity, we divide the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically. Our proposed scheme is also flexible, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios.

Ayad F. Barsoum and M. Anwar Hasan [42] in the proposed system, a pairing based provable multi-copy data possession (PB-PMDP) scheme, which provides evidence to the customers that all outsourced copies are actually stored and remain intact. Moreover, it allows authorized users (i.e., those who have the right to access the owner's file) to seamlessly access the file copies stored by the CSP, and supports public verifiability. The proposed scheme is proved to be secure against colluding servers. We illustrate the performance of the PB-PMDP scheme through theoretical analysis, which is validated by experimental results. The verification time of our scheme is practically independent of the number of file copies. Additionally, we discuss how to identify corrupted copies by slightly modifying the proposed PB-PMDP scheme.

This paper is mostly related to works in cryptographically enforced access control for outsourced data and attribute based encryption. To realize fine-grained access control, the traditional public key encryption (PKE) based schemes [8], [10] either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used. In Goyal et. al's seminal paper on ABE [11], data is encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This potentially makes encryption and key management more efficient [12]. A fundamental property of ABE is preventing against user collusion. In addition, the encryptor is not required to know the ACL.

ABE based on the Fine-grained Data Access Control: A number of works used ABE to realize fine-grained access control for outsourced data [13], [14], [9], [15]. Especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). Recently, Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE [16] that allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users. In [17], a variant of ABE that allows delegation of access rights is proposed for encrypted.

EHRs. Ibraimi et.al. [18] applied cipher text policy ABE(CP-ABE) [19] to manage the sharing of PHRs, and introduced the concept of social/professional domains. In [20], Akinyele et al. investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline. However, there are several common drawbacks of the above works. First, they usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys. In fact, different organizations usually form their own (sub) domains and become suitable authorities to define and certify different sets of attributes belonging to their (sub) domains (i.e., divide and rule). Second, there still lacks an efficient and on-demand user revocation mechanism for ABE with the support for dynamic policy updates/changes, which are essential parts of secure PHR sharing. Finally, most of the existing works do not differentiate between the personal and public domains, which have different attribute definitions, key management requirements and scalability issues. Our idea of conceptually dividing the system into two types of domains is similar with that in [18], however a key difference is in [18] a single TA is still assumed to govern the whole professional domain

Chow [21] proposed a multiple-authority ABE (CC MAABE) solution in which multiple TAs, each governing a different subset of the system's users' attributes, generate user secret keys collectively. A user needs to obtain one part of her key from each TA. This scheme prevents against collusion among at most N − 2 TAs, in addition to user collusion resistance. However, it is not clear how to realize efficient user revocation. In addition, since CC MA-ABE embeds the access policy in users' keys rather than the cipher text, a direct application of it to a PHR system is non-intuitive, as it is not clear how to allow data owners to specify their file access policies. We give detailed overviews to the YWRL scheme and CC MAABE scheme in the supplementary material.

In addition, Ruj et al. [25] proposed an alternative solution for the same problem in our paper using Lewko and Waters's (LW) decentralized ABE scheme [26]. The main advantage of their solution is, each user can obtain secret keys from any subset of the TAs in the system, in contrast to the CC MA-ABE. The LW ABE scheme enjoys better policy expressiveness, and it is extended by [25] to support user revocation. On the downside, the communication overhead of key revocation is still high, as it requires a data owner to transmit an updated cipher text component to every non-revoked user. They also do not differentiate personal and public domains. In this paper, we bridge the above gaps by proposing a unified security framework for patient-centric sharing of PHRs in a multi-domain, multi-authority PHR system with many users. The framework captures application level requirements of both public and personal use of a patient's PHRs, and distributes users' trust to multiple authorities that better reflects reality. We also propose a suite of access control mechanisms by uniquely combining the technical strengths of both CC MA-ABE [21] and the YWRL ABE scheme [9]. Using our scheme, patients can choose and enforce their own access policy for each PHR file, and can revoke a user without involving high overhead. We also implement part of our solution in a prototype PHR system.

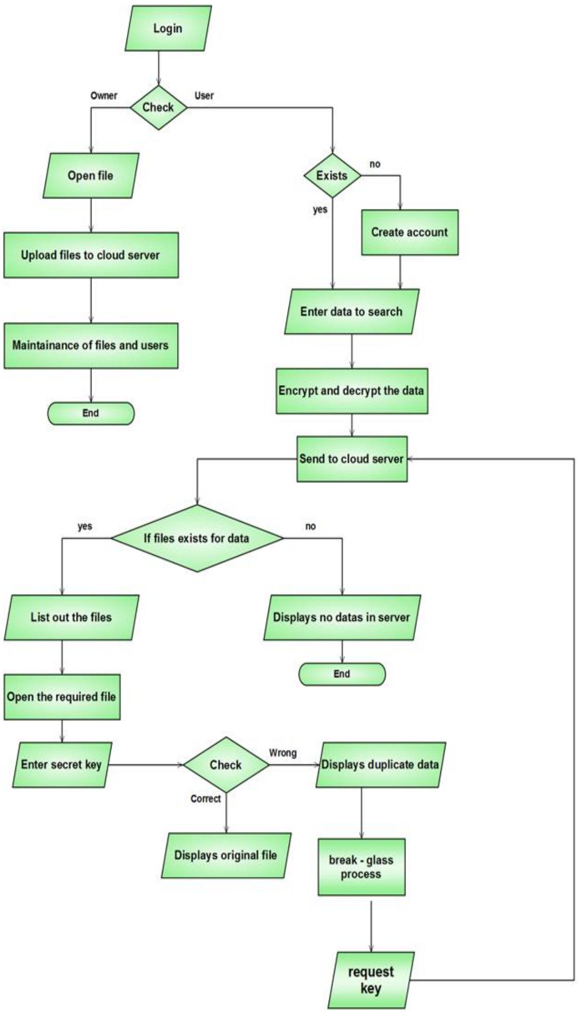
III. PROPOSED WORK

In this paper, we propose the patient-centric model for secure sharing of PHRs and it is stored on semi-trusted servers. The main focus of the proposing system is to address the complicated and challenging key management issues. In order to protect the personal health data from the untrusted server, we assume the attribute-based encryption (ABE) as the main encryption technique for the system. Using ABE policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date. The main contributions of this paper as follows:

Our first contribution of this paper is to propose the novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments. It works under the multi-owner settings. In this propose we address the key management challenges and security issues mainly. The two domains are used to handle for different types of PHR sharing personal data. The two domains are public and personal domains. Many of the patient's information sharing through the professional way by using managed distributively by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain.

We also introduce ABE (MA-ABE) in the public domain to improve the security level and in order to avoid the key escrow problem. We introduce the mechanism for the key distribution and encryption algorithms are used for the fine grained role based access policies during the file encryption. We augment the system into the MA-ABE by putting forward an efficient and its security. In this way, the patients have full privacy control over their personal, data and diagnosis information.

We also provides the analysis of the complexity and scalability of the proposed secure PHR sharing solution , in terms of computation, communication, storage and key management. We also compare our scheme to several previous ones in complexity, scalability and security. Furthermore, we demonstrate the efficiency of our scheme by implementing it on a modern workstation and performing experiments/simulations.



IV. CONCLUSION

In this paper, we proposed the effective novel framework for secure sharing of the personal data and patient's details in the cloud computing. The proposed framework addresses and overcome the problems are brought by the PHR owners and users. So, we greatly reduce the complexity in the key management and given the privacy guarantees to the users. This framework greatly reduces the issues and complexity in the data sharing when it is compared to the previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Last but not least, we increase an existing MA-ABE scheme to handle efficient and on-demand user revocation and proved it security in high. Through implementation and simulation, we show that our solution is both scalable and efficient.

V. REFERENCES

[1] 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," in SecureComm'10, Sept. 2010, pp. 89–106.

[2] H. L¨ohr, 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] 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.

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

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

[6] "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

[7] 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.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114.

[9] 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.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[12] Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEEWireless Communications Magazine, Feb. 2010.

[13] Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp. 417–426.

[14] 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.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010. S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[16] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC 2010, 2010.

[17] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.

[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.

[19] 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, 2010, http://eprint.iacr.org/.

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

[21] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.

[22] 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.

[23] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-based access control in social networks with efficient revocation," in ASIACCS, Hong Kong, March 2011.

[24] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

[25] Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT, pp. 568–588, 2011.

[26] “Indivo.” [Online]. Available: http://indivohealth.org/

[27] 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.

[28] Lewko and B. Waters, “Decentralizing attribute-based encryption,” Advances in Cryptology–EUROCRYPT, pp. 568–588, 2011.

[29] Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “Spins: security protocols for sensor networks,” Wirel. Netw., vol. 8, pp. 521–534, September 2002.

[30] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” Wireless Communications, IEEE, vol. 11, no. 1, pp. 38 – 47, feb 2004.

[31] N. Attrapadung and H. Imai, “Conjunctive broadcast and attribute-based encryption,” Pairing-Based Cryptography–Pairing2009, pp. 248–265, 2009.

[32] S. M¨ uller, S. Katzenbeisser, and C. Eckert, “Distributed attributebased encryption,” Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009.

[33] S. Chow, “New privacy-preserving architectures for identity-/attribute-based encryption,” PhD Thesis, NYU, 2010.

[34] Y. Zheng, “Key-policy attribute-based encryption scheme implementation,”

[35] “Privacy-preserving personal health record system using attribute-based encryption,” Master’s thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.

[36] Lynn, “The pbc library,” http://crypto.stanford.edu/pbc/.

[37] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010.

[38] Shraddha B. Toney and Sandeep U.Kadam,” Cloud Information Accountability Frameworks for Data Sharing in Cloud - A Review” International Journal of Computer Trends and Technology- volume4Issue3- 2013

[39] SHILPA ELSA ABRAHAM-“Distributed Attribute Based Encryption for Patient Health Record Security under Clouds”- International Journal of Computer Trends and Technology- volume4Issue3- 2013

[40] Ming Li, Shucheng Yu, Kui Ren, and Wenjing Lou-“ Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings”

[41] Ayad F. Barsoum and M. Anwar Hasan-“ Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers”.