



PERSONAL HEALTH RECORD SHARING IN CLOUD USING ADDITIVE HOMOMORPHIC ENCRYPTION VIA SECURE ALTERNATE VIABLE ALGORITHM

S.R.Lyernisha ^{#1}, Dr. T.Jaya ^{*2}

[#]PG Scholar, Department of Electronics and Communication Engineering (Communication and Networking),
CSI Institute of Technology, Thovalai.

^{*}Professor, Department of Electronics and Communication Engineering,
CSI Institute of Technology, Thovalai.

Abstract—Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage additive homomorphic encryption(AHE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key

management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. 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

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users,



including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault.¹ Recently, architectures of storing PHRs in cloud computing have been proposed. While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust.

The complexities per encryption, key generation, and decryption are only linear with the number of attributes involved. However, to integrate AHE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are nontrivial to solve, and remain largely open up-to-date. To this end, we make the following main contributions:

1. We propose a novel AHE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multiowner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains.
2. In the public domain, we use multiauthority ABE (MA-ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system.
3. We provide a thorough analysis of the complexity and scalability of our proposed secure PHR sharing solution, in terms of

multiple metrics in computation, communication, storage, and key management. We also compare our scheme to several previous ones in complexity, scalability and security.

II RELATED WORKS

A number of works used AHE to realize fine-grained access control for outsourced data. Especially, there has been an increasing interest in applying AHE 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-AHE that allows direct revocation. However, the ciphertext length grows linearly with the number of unrevoked users. In a variant of AHE that allows delegation of access rights is proposed for encrypted EHRs. Ibraimi et al. applied ciphertext policy AHE (CP-AHE) to manage the sharing of PHRs, and introduced the concept of social/professional domains. In, Akinyele et al. investigated using AHE to generate self-protecting EMRs, which can either be stored on cloud servers or cellphones 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.

III FRAMEWORK FOR PATIENT-CENTRIC, SECURE AND SCALABLE PHR SHARING



In this section, we describe our novel patient-centric secure data sharing framework for cloud-based PHR systems.

A. Problem Definition

We consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage, and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. The users may come from various aspects; for example, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data.

B. Overview of Our Framework

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains and personal domains) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government, or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner. In both types of security domains, we utilize AHE to realize cryptographically enforced, patient-centric PHR access.

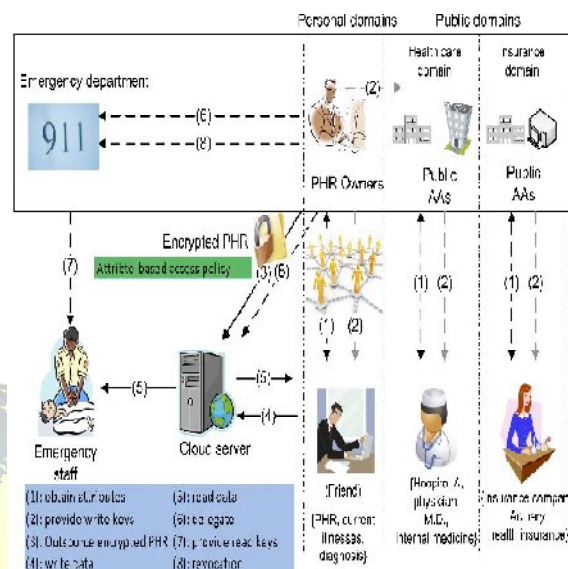


Fig. 1. The proposed framework for patient-centric, secure and scalable PHR sharing on semitrusted storage under multiowner settings.

C. Details of the Proposed Framework

In our framework, we use secure alternate viable algorithm which provides encryption using a single encryption key with multiple decryption keys. Hence only one encrypted file will be stored in cloud server whereas different decryption keys will be provided to the users. Hence this reduces memory needed for a file very efficiently

D. System setup and key distribution.

The system first defines a common universe of data attributes shared by every PSD, such as "basic profile," "medical history," "allergies," and "prescriptions." An emergency attribute is also defined for break-glass access. Each PHR



owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-network (HSN) (which could be part of the PHR service; e.g., the Indivo system). In addition, the data attributes can be organized in a hierarchical manner for efficient policy generation. When the user is granted all the file types under a category, her access privilege will be represented by that category instead. For the PUDs, the system defines role attributes, and a reader in a PUD obtains secret key from AAs, which binds the user to her claimed attributes/roles. For example, a physician in it would receive "hospital A, physician, M.D., internal medicine" as her attributes from the AAs. In practice, there exist multiple AAs each governing a different subset of role attributes. For instance, hospital staffs shall have a different AA from pharmacy specialists.

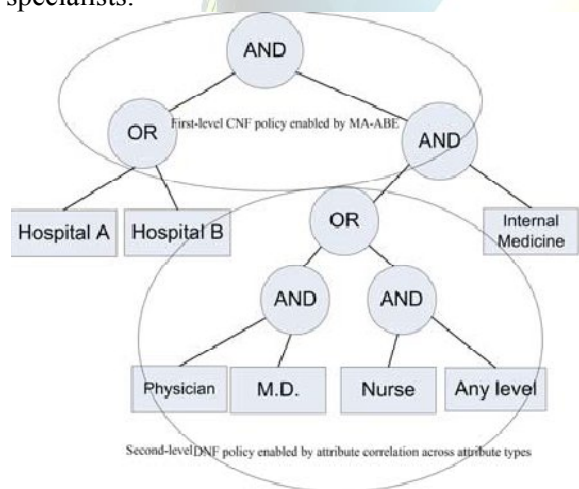


Fig.2 An example policy realizable under our framework using SAV, following the enhanced key generation and encryption rules.

IV SECURITY ANALYSIS

In this section, we analyze the security of the proposed PHR sharing solution. First we

show it achieves data confidentiality (i.e., preventing unauthorized read accesses), by proving the enhanced MA-ABE scheme (with efficient revocation) to be secure under the attribute-based selective set model. We have the following main theorem. In addition, our framework achieves forward secrecy, and security of write access control. For detailed security analysis and proofs, please refer to the online supplementary material, available online, of this paper. We also compare the security of our scheme with several existing works, in terms of confidentiality guarantee, access control granularity, and supported revocation method, etc. Our scheme achieves high privacy guarantee and on-demand revocation. The conjunctive policy restriction only applies for PUD, while in PSD a user's access structure can still be arbitrary monotonic formula. In comparison with the RNS scheme, in RNS the AAs are independent with each other, while in our scheme the AAs issue user secret keys collectively and interactively.

V SCALABILITY AND EFFICIENCY

A. Storage and Communication Costs

First, we evaluate the scalability and efficiency of our solution in terms of storage, communication, and computation costs. We compare with previous schemes in terms of ciphertext size, user secret key size, public key/information size, and revocation (rekeying) message size. Our analysis is based on the worst case where each user may potentially access part of every owners' data.

B. Computation Costs

Next, we evaluate the computational cost of our scheme through combined implementation and simulation. We provide the first implementation of the GPSW KP-ABE scheme and also integrated the ABE algorithms



into a prototype PHR system, Indivo. The GPSW KP-ABE scheme is tested on a PC with 3.4 GHz processor, using the pairing based cryptography (PBC) library. The public parameters are chosen to provide 80 bits security level, and we use a pairing-friendly type-A 160-bit elliptic curve group. This parameter setting has also been adopted in other related works in AHE.

VI CONCLUSION

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with 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. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

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," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), Sept. 2010.
- [2] H. Lohr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), 2010.
- [3] 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.
- [4] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," <http://www.ihealthbeat.org/Articles/2009/4/8/>, 2012.
- [5] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded," <http://articles.latimes.com/2006/jun/26/health/he-privacy26>, 2006.
- [6] 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, Feb. 2001.
- [7] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), 2009.
- [8] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," Pairing-Based Cryptography-Pairing, 2009.
- [9] 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.
- [10] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for



Untrusted Servers,” J. Computer Security, vol. 19, 2010.

[11] 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), 2006.

[12] M. Li, W. Lou, and K. Ren, “Data Security and Privacy in Wireless Body Area Networks,” IEEE Wireless Comm. Magazine, vol. 17, no. 1, Feb. 2010.

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

[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,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’10), 2010.

[16] S. Narayan, M. Gagne’, and R. Safavi-Naini, “Privacy Preserving EHR System Using Attribute-Based Infrastructure,” Proc. ACM Cloud Computing Security Workshop (CCSW ’10), 2010.

[17] X. Liang, R. Lu, X. Lin, and X.S. Shen, “Patient Self-Controllable Access Policy on Phi in Ehealthcare Systems,” Proc. Advances in Health Informatics Conf. (AHIC 10), 2010.

[18] L. Ibraimi, M. Asim, and M. Petkovic, “Secure Management of Personal Health Records by Applying Attribute-Based

Encryption,” technical report, Univ. of Twente, 2009.

[19] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), 2007.

[20] 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.