ISSN 23499842(Online), Volume 1, Special Issue 2(ICITET 15), March 2015
International Journal of Innovative Trends and Emerging Technologies

SCALABLE AND SECURE SHARING OF RECORDS IN CLOUD COMPUTING USING ATTRIBUTE-BASED ENCRYPTION

Mrs.M.SREEMAA AP[1], K.SOMAKRISHNAN[2], E.SHABIULLA[3]
[1,2,3]Department of Computer Science Engineering
[1,2,3]Surya group of institutions
[1]sachinshafi2727@gmail.com

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 semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) 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 multi-authority 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.

ARCHITECTURE

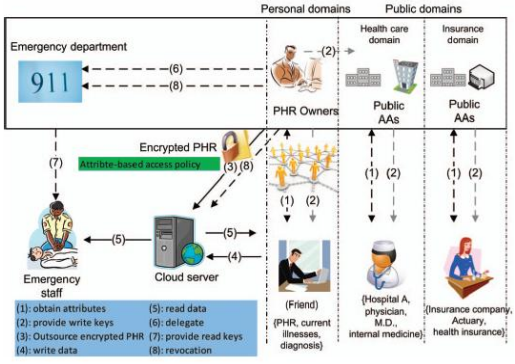


Fig. 1. The proposed framework for patient-centric, secure and scalable PHR sharing on semi-trusted storage under multi-owner settings.

EXISTING SYSTEM

In Existing system a PHR system model, there are *multiple owners* who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner who's PHR she wants to read would limit the accessibility since patients are not always online. 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., cause the key escrow problem).

Key escrow (also known as a "fair" cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

PROPOSED SYSTEM

We endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive.

Using ABE, access 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.

MODULES

1. Registration
2. Upload files
3. ABE for Fine-grained Data Access Control
4. Setup and Key Distribution
5. Break-glass

MODULES DESCRIPTION

Registration

In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader have access to.

Two ABE systems are involved: for each PSD the revocable KP-ABE scheme is adopted for each PUD, our proposed revocable MA-ABE scheme.

- PUD - *public domains*
- PSD - *personal domains*
- AA - attribute authority
- MA-*ABE* - multi-authority ABE
- KP-ABE - key policy ABE

Upload files

In this module, users upload their files with secure key probabilities. The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file encrypted both under a certain fine grained model.

ABE for Fine-grained Data Access Control

In this module ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of un revoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains 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.

Setup and Key Distribution

In this module 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)

There are two ways for distributing secret keys.

- First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc.
- Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs keygen of KP-ABE to generate the user secret key that embeds her access structure.

Break-glass module

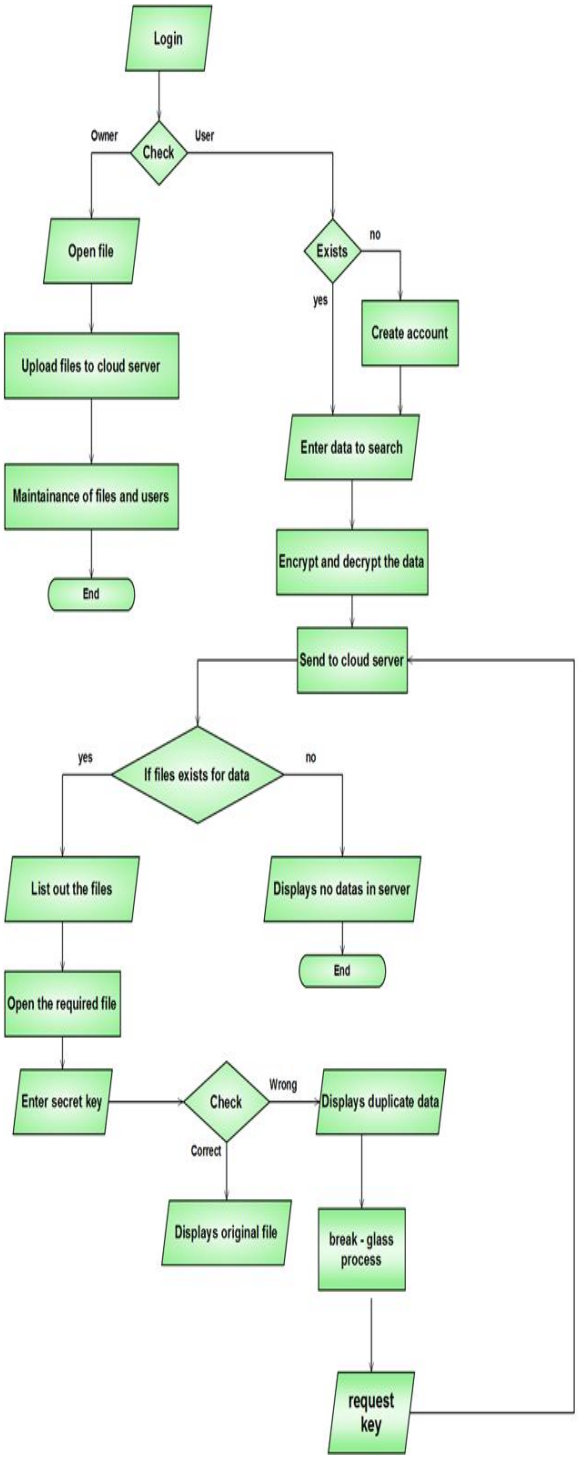
In this module when an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department ED to prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

On the other hand, when a user comes to drop a set of attributes that satisfy the access policy at some time instance, the corresponding attribute group keys are also updated and delivered to the valid attribute group members securely (excluding the user).

Then, all of the components encrypted with a secret key in the ciphertext are reencrypted by the storage node with a random , and the ciphertext components corresponding to the attributes are also reencrypted with the updated attribute group keys. Then, the user cannot decrypt any nodes corresponding to the attributes after revocation due to the blindness

resulted from newly updated attribute group keys.

FLOW DIAGRAM:



CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tole rant networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.

[2] M. Chuah and P. Yang, "Node density-based ada ptive routing scheme for disruption tolerant networks," in *Proc . IEEE MILCOM*, 2006, pp. 1–6.

[3] .M.B.Tariq,M.Ammar,andE.Zequra,"Mesag e ferry route design for sparse ad hoc networks with mobile n odes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.

[4] S. Roy and M. Chuah, "Secure data retriev al based on ciphertext policy attribute-based encryption (CP-ABE) s ystem for the DTNs," Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, "Performance evalu ation of content-based information retrieval schemes for DTN s," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.

[6] M. Kallahalla, E. Riedel, R. Swaminatha n, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing o n untrusted storage," in *Proc. Conf. File Storage Technol.*, 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P . Hartel, and W. Jonker, "Mediated ciphertext-policy attribute -based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 3 09–323.

[8] N. Chen, M. Gerla, D. Huang, and X. Hon g, "Secure, selective group broadcast in vehicular networks us ing dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Worksho p*, 2010, pp. 1–8.
[9] D.HuangandM.Verma,"ASPE:Attrib ute-based secure policy enforcement in vehicular ad hoc net works," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.
[10] A. Lewko and B. Waters, "Decentra lizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
[11] A. Sahai and B. Waters, "Fuzzy ide ntity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.