Scalable and Secure Sharing of Personal Health Records:A Review

Anagh Kumawat[1], Ashish Kumar Hoskery[2], Saurabh Mathur[3], Vishwajeet Kumar[4], Shyamala G[5]

[1 2 3 4]Department of Computer Science and Engineering, BMSCE

[5]Department of Computer Science and Engineering, BMSCE, Assistant Professor

Abstract-Personal Health Records(PHR) is an emerging patient-centric model of health information exchange, which is many times outsourced to be stored at a third party, such as cloud service. There have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized group. To reassure the patients' control over access to their own PHRs, it is a potential method to encrypt the PHRs before outsourcing. Yet, issues such as threat of solitude exposure, scalability in key management, amenable access and efficient user revocation, have remained the most significant challenges toward achieving fine-grained, photographically compulsory data access control.

A survey on novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To accomplish fine-grained and scalable data access control for PHRs, leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file is used. These works in secure data outsourcing, focus on the various data owner scenario, and segregate 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 promised simultaneously by exploiting multi-authority ABE. Dynamic changes of access policies or file attributes, supports systematic on-demand user/attribute revocation under emergency scenarios can be included.

INTRODUCTION

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service let a patient to create, manage, and control his personal health data in one place through the web, which makes storage, retrieval, and distribution of the medical information more efficient. Especially, each patient is promised full control of his medical records and can share his health data with a wide variety of users, including doctors, family members or friends. Due to the high price of building and maintaining specialized data centers, multiple PHR services are outsourced to or provided by third-party service providers. Recently, architectures of storing PHRs in cloud computing have been proposed.

While it is exciting to have convenient PHR services for everyone, there are multiple security and privacy risks which could impede its wide adoption. Due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to subjection of the PHI. As a famous incident, a Department of Veterans Affairs database containing delicate PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without their consent. To ensure patient-centric privacy control over their own PHRs, it is crucial to have fine-grained data access control mechanisms that work with semi-trusted servers.

A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHR owner himself should decide how to encrypt his files and to allow which set of users to obtain access to each file. A PHR file should only be accessible to the users who are given the corresponding decryption key, while remain intimate to the rest of users. Moreover, the patient shall always retain the right to not only accord, but also revoke access privileges when they feel it is necessary.

History of Personal Health Records

Computerized Personal Health Records (PHRs) have existed for more than a decade. But it was not until late 2007 when large technology companies such as Microsoft and Google began to offer PHR products. That initial growth was followed in 2008 by the establishment of Dossia, a consortium of large employers created to offer PHRs to their employees.

A large number of other PHR vendors have recently introduced new PHR products to the market to connect consumers with their healthcare information identifying this market activity, Congress for the first time addressed privacy and security requirements for PHRs in the American Recovery and Reinvestment Act of JANUARY 2011 MEMBER BRIEFING HEALTH INFORMATION AND TECHNOLOGY PRACTICE GROUP 2 2009 (ARRA) under Title XIII, Health Information Technology for Economic and Clinical Health Act (HITECH Act).

1 Early experiences with Personal Health Records

In recent years, Personal Health Record (PHR) has e-merged as a patient-centric model. By using PHR service we enable the patient to create and control his/her PHR at a single place using cloud, thus paving way for more efficiency which has made storage, retrieval and sharing of personal health record uncomplicated. The benefit of PHR service is that each patient has full control of his/her medical records and share the corresponding or relevant information to various users which include health providers, family members and friends. Many PHR services are deployed to third party cloud servers due to disadvantage of high cost of building and maintaining data centers. For example, Microsoft HealthVault1.

2 Modernization in the confidentiality protection of Personal Health Records

There have been extensive confidentiality concerns as personal health information can be exposed to the third party servers. A feasible method is to encrypt the Personal Health Record before outsourcing and guarantee the patients' control over access to their own Personal Health Record. A novel patient-centric framework and a suite of mechanisms were proposed [2] for data access control of the Personal Health Record stored in semi-trusted servers. To encrypt each patient's Personal Health Record file, they leverage Attribute Based Encryption techniques.

3 Authorized Private Keyword Search over Encrypted Data in Cloud Computing

The confidentiality of the deployed data is protected by Attribute Based Encryption, but it also upsurges much complications in performing effective searches over encrypted information. The existing PHR solutions does not support adequate searches with complicated query conditions, and taking into consideration of various facts because of the potential privacy leakages about the data owners to the data users or the cloud server. M Li, S Yu, N Cao, W Lou introduced a solution called, "Accredited Private Keyword Search " over encrypted cloud data . This proposed solution paved way for efficient multi-dimensional keyword searches with range query and revocation of search capabilities

4 Shared and searchable encrypted data for untrusted servers

The main disadvantage of Encrypting and decrypting sensitive data at the client side is that it involves high computation overheads if only a small amount of the data is required, for example, selecting a record in a database on a keyword search. C Dong, G Russello, N Dulay proposed a solution that support encrypted queries over encrypted data. They also introduced an encryption scheme where each valid user in the system has his own keys to encrypt and decrypt data. This solution enables keyword search that facilitate the server to return only the encrypted data that amuse an encrypted query without decrypting it.

.

5 Enforcing Multi-user Access Policies to Encrypted Cloud Databases

Cloud computing has the advantage that it offers companies unlimited data storage at attractive costs. However, Sensitive data like medical data, business or government data cannot be stored as a plaintext on the cloud. Companies need new mechanisms to query the encrypted data without revealing anything to the cloud server, and to impose access policies to the data. Prevailing security methods does not allow complicated encrypted queries over encrypted data in a multi-user mode. Instead, they are limited to keyword searches. M Lon, X Liang[5] shows the implementation of a scheme that allows making SQL-like queries on encrypted databases in a multi-user mode, meanwhile allowing the database owner to assign different access rights to users.

6 Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings

M Li, S Yu [6] propose a novel framework for access control to PHRs. To enable access control for PHRs, they utilize attribute based encryption (ABE) techniques to encrypt PHR data of each patient. To curtail the key distribution complication, they divide the system into multiple security domains, where each domain manages only a subgroup of the users. Thus, each patient has full control over her own privacy, and the key management complication is reduced dramatically.

7 Ciphertext Policy Attribute Based Encryption with Efficient Revocation

Ciphertext Policy Attribute based Encryption (CP-ABE) can be widely applied to realize access control in many applications including medical systems and education systems. For example, the sensitive medical data, strongly related to patients' privacy must be accessed only if the users are authorized with patients' consent; solutions of exams in the education online system also should be only read by professors or specified teaching assistants. The CP-ABE scheme deals with this condition, by encrypting the target information with expressive access policies, such as "Medicine" and "Physician", "Professor" or ("Computer Science" and "Teaching Assistant").In fact, CP-ABE can provide a perfect solution to an access control system by taking into notice, competent distributing, access control and data confidentiality.

.

8 Attribute based data sharing with attribute revocation

Ciphertext-Policy using Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for fine-grained access control of shared data. In CP-ABE, each user is correlated with a set of attributes and data are encrypted with access structures on attributes. A user can decrypt a ciphertext if and only if his attributes satisfy the ciphertext access structure. In this paper, as compared to existing schemes, S Yu, C Wang[8] proposed solution enables the authority to revoke user attributes with minimal effort. They achieve this by uniquely integrating the technique of proxy re-encryption with CP-ABE, and allow the authority to delegate most of laborious tasks to proxy servers.

9 Secure management of Personal Health Records by applying attribute-based encryption

L Ibraimi, M Asim [9] present a new variant of ciphertext-policy attribute-based encryption (CP-ABE) scheme which is patient/organizational access control policies. The data is encrypted in CP-ABE according to an access policy over a set of attributes. The access policy determines which attributes a user needs to have in order to decrypt the encrypted data. after the data has been encrypted, it can be safely stored in an untrusted server such that everyone can download the encrypted data but only authorized users who satisfy the access policy can decrypt. The attributes can be from two security domains: social domain (e.g. family, friends, or fellow patients) and professional domain (e.g. doctors or nurses).

10 Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

To keep sensitive user data confidential against non reliable servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to valid users. However, in doing so, these solutions absolutely introduce a heavy computation overhead on the data owner for key distribution and data management. The problem of simultaneously achieving fine-grainedness, scalability, and data privacy of access control actually still remains unresolved. It addresses this challenging open issue by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.

11 Ensuring Privacy and Security in Data Sharing under Cloud Environment

An important application of data sharing in cloud environment is the storage and retrieval of Patient Health Records (PHR) that maintain the patient's personal and diagnosis information. These records should be protected with privacy and security for safe retrieval. The privacy mechanism takes care of the delicate attributes. The security schemes are used to save the data from public access. The data are allowed to be retrieved only by certified individuals. Each party is accredited with access permission for a set of attributes. Data owners update the Patient Health Record into third party cloud data centers. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism due to its vast access.

12 DACC: Distributed Access Control in Clouds

MB Buntin, MF Burke [12] proposed a new model for data storage and access in clouds. Their scheme avoids storing multiple encrypted copies of same data. In their framework for secure data storage, cloud stores encrypted data (without being able to decrypt them). The main novelty of their model is addition of key distribution centers (KDCs). They propose DACC (Distributed Access Control in Clouds) algorithm, in which one or more KDCs distribute security key to data owners and users. KDC provides access to peculiar fields in all records. Thus, separate keys of owners is replaced by a single key. A certain set of attributes is assigned to owners and data users .The data owner encrypts the data with the attributes it has and stores them in the cloud. The users with identical set of attributes can retrieve the data from the cloud. Attribute-based encryption has been applied by them which is based on bilinear pairings on elliptic curves. This proposal is collusion secure; two users cannot together decode any data that none of them has individual right to access. DACC also backs revocation of users, without redistributing keys to all the users of cloud services. They show that their approach results in lower communication, computation and storage overheads, compared to existing models and schemes.

13 Securing the E-Health Cloud

Modern information technology is increasingly used in healthcare with the goal to improve and enhance medical services and to reduce costs. In this situation, the outsourcing of computation and storage resources to general IT providers (cloud computing) has become very attractive. E-health clouds offer new possibilities, such as easy and universal access to health data, and opportunities for new business models. However, they also carry new risks and raise challenges with respect to security and privacy aspects. several shortcomings of current e-health solutions and standards are pointed out by the author. The client platform security are not being addressed, which is a crucial aspect for the overall security of e-health systems. To fill this gap, they present a security architecture for establishing privacy domains in e-health infrastructures. Their solution provides client platform security and appropriately combines this with network security concepts. Moreover, SE Abraham[11] discuss further open problems and research challenges on security, privacy and usability of e-health cloud systems.

14 Cloud-based Storage Solutions

There has been some work carried out in designing storage and file management systems for e-Health Cloud. Guo et al. [14] put forward a Cloud-based intelligent hospital file management system (HFMS) that aims to improve some of the limitations which characterize the traditional hospital management systems (HMS). Such limitations include limited storage capacity of some of the hardware devices and slow performance of the hardware due to the huge amount of data, the backup models, and the resource distribution across dissimilar platforms.

The proposed Cloud-based HFMS consists of a master server and multiple blocks of servers. Huge files are divided into fixed-sized blocks and each block is backed up by three blocks. The master server supervises the file system meta-data that includes namespace, access control, file-block mapping and physical address of pertinant information. This model is claimed to adopt low-cost server clusters with the flexibility to allow the applications to overcome the physical boundaries, maximizing the throughput of total systems resources as needed.

15 Cloud Gains Traction In Healthcare

Healthcare providers are increasingly recognizing that the cloud empowers them to minimize costs, enhance agility, and improve insights. And so many people are investing heavily and expanding their cloud initiatives. By 2020, 80% of medical data will "pass through the cloud at some point in its lifetime, as providers seek to utilize cloud-based technologies and infrastructure for data collection, gathering, analytics and decision-making," according to IDC Health Insights. More appealing for IT professionals, that same year the United states healthcare cloud market will reach $3.54 billion, compared with $903.1 million in 2013, Frost & Sullivan predicted..

16 PEACE: An efficient and secure patient-centric access control scheme for eHealth care system

In this paper, an efficient and secure patient-centric access control (PEACE) scheme is proposed for the emerging electronic health care (eHealth) system. In order to guarantee the privacy of patient personal health information (PHI), define different access privileges to data requesters according to their roles, and then allocate different attribute sets to the data requesters. By using these non-identical sets of attribute, build the patient-centric access policies of patient PHI. The PEACE scheme can assure PHI integrity and confidentiality by adopting digital signature and pseudo-identity techniques. It include identity based cryptography to aggregate remote patient PHI securely. Vast security and performance analyses demonstrate that the PEACE scheme is able to achieve desired security requirements at the cost of an acceptable communication delay.

17 SAGE: a strong privacy-preserving scheme against global eavesdropping for ehealth systems

The eHealth system is envisioned as a promising approach to improving health care through information technology, where security and privacy are critical for its success and large scale deployment. Here we propose a strong privacy-preserving Scheme against Global Eavesdropping and spy , named SAGE, for eHealth systems. The presented SAGE can attain not only the content oriented privacy but also the contextual privacy against a strong global adversary. Extensive analysis demonstrates the usefulness and practicability of the proposed scheme.

18 Security Models and Requirements for Healthcare Application Clouds

With the widespread use of electronic health record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community. Cloud computing paradigm is one of the accepted health IT infrastructure for facilitating EHR sharing and EHR integration. Here, we discuss important concepts related to EHR sharing and integration in healthcare clouds and analyze the arising security and privacy issues in access and management of EHRs.

EHR security reference model for managing security issues in healthcare clouds is described, which emphasize three important core components in securing an EHR cloud. The development of the EHR security reference model through a use-case scenario and describe the corresponding security countermeasures and state of art security techniques that can be applied as basic security guards.

19 Access control for cloud-based eHealth social networking: design and evaluation

eHealth is being rapidly deployed. Reduced cost and greater productivity attract government and healthcare enterprise to transit from traditional healthcare service to eHealth service. The widespread deployment of eHealth and the development of next generation of eHealth services led to security and privacy concerns. Y Bai, L Dai, S Chung discuss these security problems and propose a high-level security framework that captures required features in the next-generation eHealth infrastructure.

Their framework consists of the following: (i) an adaptive trust-aware tag-based privacy control to specify which data to share and whom to share with. (ii) a decentralized authorization that relies on trust propagation protocol to provide robust and resilient access control enforcement; and (iii) a hybrid trust management mechanism that addresses access control information depository on a cloud server. It administers user-defined access control not only in a distributed environment but also in a privacy-preserving manner so as to minimize the disclosure of privileges and of access policies

20 Managing of health record protection for unreliable servers

In the modern times, there has been a rising attentiveness in applying attribute based encryption to safe electronic healthcare records. To carry out patient-centric health record sharing, a core prerequisite is that every patient can manage who are allowed to access to their health records documents. New approach of attribute based encryption based structure was introduced for patient-centric secure contribution of health records in cloud computing setting, under situation of multi-owner.

The structure handle various types of health record sharing applications' needs, while incur negligible key management transparency for owner as well as users. The introduced system protection was measured in terms of privacy assurance, access control granularity with quite a lot of existing works and it attains forward confidentiality and protection of write access control and achieves high confidentiality assurance as well as on demand revocation.

Conclusion

A novel framework of secure sharing of Personal Health Record has been proposed in this paper. In order to deal with partially trustworthy cloud servers, patients should have complete control over their own privacy through encrypting their PHR files to allow fine-grained access. The complexity of key management are being reduced despite having multiple PHR owners and users. ABE technique has been used to encrypt PHR data so that patients can allow access not only by personal users, but also various users from public domains with different personal roles, qualifications and affiliations. Furthermore MA-ABE scheme has been enhanced to handle efficient and on demand user revocation. This solution is both scalable and efficient.

Acknowledgements . The work reported in this paper is supported by the BMSCE college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the *MHRD, Government of India*

REFERENCES

[1] : JD Halamka, KD Mandl… - Journal of the American …, 2012 - jamia.oxfordjournals.org
[2] : J Myers, TR Frieden, KM Bherwani… - … Journal of Public Health, 2010 - ncbi.nlm.nih.gov
[3] : M Li, S Yu, N Cao, W Lou - Distributed Computing Systems (…, 2011 - ieeexplore.ieee.org
[4] : C Dong, G Russello, N Dulay - Journal of Computer Security, 2011 - IOS Press
[5] : M Ion, G Russello, B Crispo - Policies for Distributed Systems …, 2011 - ieeexplore.ieee.org
[6] : M Li, S Yu, K Ren, W Lou - Security and Privacy in Communication …, 2010 - Springer
[7] : X Liang, R Lu, X Lin, XS Shen - 2010 - bbcr.uwaterloo.ca
[8] : S Yu, C Wang, K Ren, W Lou - Proceedings of the 5th ACM Symposium …, 2010 - dl.acm.org
[9] : L Ibraimi, M Asim, M Petkovic - Wearable Micro and Nano …, 2009 - ieeexplore.ieee.org
[10] : S Yu, C Wang, K Ren, W Lou - INFOCOM, 2010 Proceedings …, 2010 - ieeexplore.ieee.org
[11] : SE Abraham, R Gokulavanan - International Journal of Computer …, 2013 - ijcat.com
[12] : MB Buntin, MF Burke, MC Hoaglin, D Blumenthal - Health affairs, 2011 - Health Affairs
[13] : H Löhr, AR Sadeghi, M Winandy - … of the 1st ACM International Health …, 2010 - dl.acm.org
[14] : J Wu, L Ping, X Ge, Y Wang, J Fu - Intelligent Computing and …, 2010 - ieeexplore.ieee.org
[15] : M Trivedi, V Suthar - International Journal of User-Driven Healthcare …, 2013 - igi-global.com
[16] : M Barua, X Liang, R Lu, X Shen - … (INFOCOM WKSHPS), 2011 …, 2011 - ieeexplore.ieee.org
[17] : X Lin, R Lu, X Shen, Y Nemoto… - Selected Areas in …, 2009 - ieeexplore.ieee.org
[18] : R Zhang, L Liu - Cloud Computing (CLOUD), 2010 IEEE 3rd …, 2010 - ieeexplore.ieee.org
[19] : Y Bai, L Dai, S Chung… - Security and …, 2014 - Wiley Online Library
[20] : S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-based access control in social networks with efficient revocation," in ASIACCS, Hong Kong, March 2011