ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

Privacy Preserving Personal Health Record System

Akshayah. M[1], Akshaya. V[2], Azra Khan. S[3]

UG Scholar[1, 2, 3], Department of Computer Science and Engineering

Adhiyamaan College of Engineering, Hosur.

Abstract: The uprising of medical field is distribution secure, Personal Health Record (PHR) via the internet. Personal Health Record (PHR) is a health record where data and information related to the care of a patient is kept by the patient. The patient records should be maintained with high privacy and security. Secure sharing of personal health record protects the personal data from public access. It prevents third party authentication or man in the middle attack. Each authority is assigned with access permission for a particular set of attributes. The access control and privacy management is a complex task in the patient health record management process. Data owners update the personal data into cloud data centres. This project proposes a novel patient-centric framework and a suite of data access mechanisms to control PHRs stored in semi-trusted servers. To achieve fine grained and scalable data access control for PHRs, it leverages Attribute Based Encryption (ABE) techniques to encrypt each patient's PHR file. The proposed scheme could be extended to Multi Authority Attribute Based Encryption (MA-ABE) for multiple authority. It provides high degree of privacy.

Introduction

A Personal Health Record (PHR) makes it easy to gather and manage medical information in one accessible and secure location. Carrying paper records is a big drawback, rarely the patients have with them when they need. Personal Health Record system overcomes this problem by making the personal health record accessible anytime via a web enabled device, such as computer.

In an emergency, patient can quickly give emergency personal vital information about disease, medications and drug

allergies. Now a day, Personal Health Record has become a patient-centric model of health information exchange. A PHR service allows patients to create, manage and control their personal health data from one place through the web, which has made the storing, retrieving and sharing of the medical information more efficient.

Each patient will have full control of their medical records and can share their health data with different users from different domains which include healthcare providers, family members and friends. As the sensitive personal health information is highly valuable, the third-party storage servers are the targets of various malicious behaviours which may result in exposure of the PHI.

The main concern is about whether the patients could actually control the sharing of their sensitive PHR and other information, especially when they are stored on a third-party server which people may not fully trust. To ensure patient-centric privacy control over their own PHRs, encryption of data is necessary prior stage. The PHR owners themselves should decide how to encrypt their files and to allow which set of users to obtain access to each file.

The PHR and other files are available only to those users who are given the corresponding decryption key and are confidential to other users. The patient will always have the right to not only to grant, but also to revoke access rights when it is necessary. This scheme endeavours 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.

Related Work

1. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption

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.

In this project, it proposes 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, it leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, it focuses on the multiple data owner scenario, and divides 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 ABE. This 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 the proposed scheme.

2. Achieving Secure, Scalable, and Fine grained Data Access Control in Cloud Computing

To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents.

Existing work can be found in the areas of shared cryptographic file systems and access control of outsourced data. The Proposed system combining techniques of attribute-based encryption (ABE), proxy

re-encryption, and lazy re-encryption. The proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. The main issue with this scheme is that collusion between a malicious server and any single malicious user would expose decryption keys of all the encrypted data and compromise data security of the system completely. In addition, user access privilege is not protected from the proxy server. User secret key accountability is neither supported.

3. Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing

In this paper, it formulates and addresses the problem of authorized private keyword searches (APKS) on encrypted PHR in cloud computing environments. It first present a scalable and fine-grained authorization framework for searching on encrypted PHR, where users obtain query capabilities from localized trusted authorities according to their attributes, which is highly scalable with the user scale of the system.

The existing solutions of searchable encryption are still far from practical for PHR applications in cloud computing environments. First and foremost, they are limited both in the type of applications and system scalability.

It proposes two novel solutions for APKS based on a recent cryptographic primitive, hierarchical predicate encryption (HPE), one with enhanced efficiency and the other with enhanced query privacy. In addition to document privacy and query privacy, other salient features of this scheme include efficiently support multi dimensional, multiple keyword searches with simple range query; allow delegation and revocation of search capabilities.

4. Improving Privacy and Security in Multi Authority Attribute Based Encryption

Attribute based encryption (ABE) determines decryption ability based on a user's attributes. In a multi authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptions can require that a user obtain keys for appropriate attributes from each authority before decrypting a message.

Existing system uses a fuzzy IBE scheme, which allowed for some error tolerance

around the chosen identity. In more recent terminology, it would be described as a key policy (KP) ABE scheme that allows for threshold policies. Key-policy means that the encryptor only gets to label a cipher text with a set of attributes. The authority chooses a policy for each user that determines which cipher texts he can decrypt. A threshold policy system would be one in which the authority specifies an attribute set for the user, and the user is allowed to decrypt whenever the overlap between this set and the set associated with a particular cipher text is above a threshold.

The proposed system makes use of some

basic techniques in anonymous credential systems to protect the privacy of ABE users. In an anonymous credential system, users wish to obtain and prove possession of credentials while remaining anonymous. A multi-authority ABE system which requires a user to present his unique identifier to every authority would have severe privacy shortcomings.

Models

System Model:

The proposed system consists of Data Provider, Data Consumers and Cloud Service provider. Data providers use the storage capacity provided by CSP by uploading the encrypted files for exchange. Data consumers download a copy of data from cloud server and decrypt it by using his decryption key. Neither data provider nor the user is always online.CSP is always online and has storage capacity and computation power.

Security Model:

Always the server to be semi-trusted that is honest but curious as malicious access. That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. CSP to be semi trusted, i.e,"honest but curious". That means the cloud server will honestly perform the task delegated by the owner, but they will try to find out as much sensitive information in stored medical data as possible. At the same time, some users will also try to access the files beyond their scope of access privileges. For e.g., Drug companies may want to obtain the prescriptions of patients for understanding the buying patterns and boosting their profits. To do so they may collude with cloud servers for getting beneficial results. The Proposed work

focuses on fine grained access control in a cloud based medical data exchange.

Design Goals

The main goal is to achieve secure patient centric medical access control and secure key management at same time. The system guarantees negligible execution overhead on both the owner and user, while allowing guaranteed user revocation. The proposed method should prevent cloud servers from knowing both data file contents and access privilege information of user.

Existing System

In Existing system of 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 employee's private communications, or governments, who may wish to be able to view the contents of encrypted communications. For the secured sharing of personal health record, the data is stored in cloud server and the key management is provided by the single trusted authority based attribute-based encryption (ABE).

Using ABE policies are expressed based on the attributes of users or data, which enables a patient to selectively share their 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.

Drawbacks:

- It not only leads to load bottleneck, but also creates the key escrow problem.
- As it is a single trusted authority there may be user collision due to the confusion in key distribution.

- It is not secured to delegate the key management for all attributes to the single trusted authority.
- There is a chance of accessing the patient data by the illegitimate users or any unauthenticated members.
- Necessary algorithms required to prevent third party authentication or man in the middle attack are not employed here.
- Key management is very complex as it creates key escrow problem.

Proposed System

First, the system is divided into multiple security domains like Personal domain (PSD) and Public domain (PUD). Each domain controls only a subset of its users. For each security domain, one or more authorities are assigned to govern the access of data. For personal domain it is the owner of the PHR itself who manages the record and performs key management. This is less laborious since the number of users in the personal domain is comparatively less and is personally connected to the owner.

On the other hand, public domain consists of a large number of professional users and therefore cannot be managed easily by the owner herself. Hence it puts forward the new set of public Attribute Authorities (AA) to govern disjoint subset of attributes distributively.

A Multi-Authority ABE system is comprised of attribute authorities and one central authority. In this framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition two ABE systems are involved. For each PSD, the KP-ABE scheme is adopted; for each PUD, the proposed revocable MA-ABE scheme. Each data owner (e.g., patient)is a trusted authority of their own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in their PSD .Secondly, so as to achieve security of health records, a new encryption pattern namely Attribute based encryption (ABE) is adopted.

Data is classified according to their attributes. In certain cases, users may also be classified accordingly into roles. PHR owner encrypts their record under a selected set of attributes and those users that satisfy those attributes can obtain decryption key in order to access the data. However, in the new solution pattern, an advanced version of ABE called multi-authority ABE (MA-ABE) is used.

In this encryption scheme, many attribute authorities operate simultaneously, each handing out secret keys for a different set of attributes.

Advantages:

- It Avoids Key Escrow Problem.
- Third Party Authentication or Man in The Middle Attack Can be Prevented.
- Maintain Better Security And Privacy.
- Complexity of Key Management Greatly Reduced.
- Support Dynamic Policy Changes, Enforced Write Access Control.
- More Expressive File Access.
- Reduced Storage and Communication Cost.
- Enhances the System Scalability.
- High Degree of Privacy is guaranteed.

Conclusion

In this paper, we proposed a novel framework to share health records across personal and public domains. 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.

References

1. http://microsofthealthvault.com

2. Cryptography and Network Security, fourth edition by William Stallings.

3. Attribute Based Encryption with Fast Decryption by Susan Hohen Berger and Brent Wrest.

4. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Record”, 2009.

5. C. Dong, G. Russello, and N. Dulay, “Shared and Searchable Encrypted Data for Untrusted Servers”, Vol.19, 2010.

6. M. Li, S. Yu, N. Cao, and W. Lou, “Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing,” 2011.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

7. K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," 2011