Multi-Authority Attribute Based Encryption for Personal Health Records in Secure Cloud Environment

C.A. PAVANI MCA, M.Tech (CSE), Ravi Mathey, Associate Professor and HOD of CSE Department, Vidya Jyothi Institute of Technology (VJIT)

Abstract: The revolution of medical field is sharing secure Personal Health Record (PHR) via the internet. Cloud computing has emerged as one of the most influential paradigms in the IT industry for last few years. Normally data owners and service providers are not in the same trusted domain in cloud computing. 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 the information could be exposed to those third party servers and to unauthorized parties. In the existing system, 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, leverage attribute based encryption (ABE) techniques to encrypt each patient’s PHR file. Patients only decide which set of users can access which set of files. All the files stored in clouds which are semi-trusted servers, are in the encrypted form and are confidential to other users. In proposed System, introduce the concept of Multi Authority Attribute-Based Encryption, where an arbitrary number of parties can be present to maintain attributes and their corresponding secret keys. Also two-level access control model introduced, that combines fine-grained access control, which supports the precise granularity for access rules, and coarse-grained access control, which allows the storage provider to manage access requests while learning only limited information from its inputs.

Keywords: Attribute Based Encryption, Multi Authority Attributed Based Encryption, PHR, Cloud Computing.

I. Introduction

A Personal Health Record (PHR) is a health record where health data and information related to the care of a patient is maintained by the patient. Patients control the health information in PHR and can get it anywhere at any time with Internet access. Cloud computing is a computing model, where resources such as computing power, storage, network and software are abstracted and provided as services on the internet. These services are broadly divided into three categories: Infrastructure-as-a-Service(IaaS), Platform-as-a-Service(PaaS), Software-as-a-Service (SaaS). Cloud computing provides on-demand self-service, in which the different business units are allowed to get the computing resources as they need without having to go through IT for equipment. It supports broad network access, which allows applications to be built in ways that align with how businesses operate today in mobile, multi-device, etc. It allows resource pooling, which allows for pooling of different computing resources to deliver the services to multiple users. It is highly elastic, which allows for quick scalability of resources depending on the demand. In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. In the existing system they propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, they conceptually divide the users in the system into two types of domains, namely public and personal domains. In the public domain, they use multi-authority 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. They propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. But it has some security issues. In our proposed system we introduce a two-level access control model that combines fine-grained access control, which supports the precise granularity for access rules, and coarse-grained access control, which allows the storage provider to manage access requests while learning only limited information from its inputs. This is achieved by arranging outsourced resources into units called access blocks and enforcing access control at the cloud only at the granularity of blocks. And also our solution handles the read and writes access control.

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. In the existing system they propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, they conceptually divide the users in the system into two types of domains, namely public and personal domains. In the public domain, they use multi-authority 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. The mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. Due to high cost of building and maintaining separate data centers, many PHR services are outsourced and provided by third party service providers for example, Microsoft Health Vault (UK). The Health Vault Program of Microsoft will allow users including individuals, health centers, hospitals etc. to gain access to the information on health related issues. The user interface will be simple, that would allow anyone to operate the program easily. But on the other hand, there is still less guarantee to protect one’s privacy statement. Many people do not wish to share their private health records and other information universally through the Health Vault.

II. Related Work

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. A file can be uploaded without key distribution and it is highly efficient. This is a single data owner scenario and thus it is not easy to add categories. C. Dong, [10] has explored that the data encryption scheme does not require a trusted data server. The server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the decryption keys. But in this scheme the server knows the access pattern of the users which allows it to infer some information about the queries. To realize fine grained access control, the traditional public key encryption 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 said solutions, one-to-many encryption methods such as attribute based encryption (ABE) can be used. In Goyal et. al's paper [11], data is encrypted under a set of attributes so that multiple users who possess proper key can decrypt. 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. Ming Li, Shucheng Yu, Yao Zheng and Kui Ren [1] 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, and leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, it 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.

III. Attribute-Based Encryption

Attribute-based encryption (ABE) is a recent promising cryptographic method proposed by Sahai and Waters in 2005 [20]. The ABE technique extends the identity-based encryption to enable expressive access policies and fine-grained access to encrypted data. In ABE, the access control decision is based on a set of attributes and the concept of access structure described as follows:

Universal attributes set \(U\): is the set of all attributes that describe data properties, user properties and environment properties.

Access structure: is an access policy that designs who can access to what. It is built from an access tree (T) which can be seen as a logical expression combining several attributes through AND, OR or other operators. Each non-leaf node of the tree represents a threshold gate, described by its children and the threshold gate value (AND, OR or other operators). Each leaf node of the tree is described by an attribute from \(U\) and a value. We give an example of an access tree which is derived from the following logical expression:

\[ (\text{speciality}=\text{physician} \land (\text{division}=\text{cardiology} \lor \text{cardiology}=\text{pulmonary}) \lor (\text{cardiology}=\text{gerontology} \land (\text{speciality}=\text{nurse} \lor \text{speciality}=\text{physician}))). \]

This expression means that data can be accessed by all physicians working in cardiology, pulmonary or gerontology divisions, as well as all nurses working in gerontology division have access. Key-Policy Attribute-Based Encryption (KP-ABE) [21] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [19] are the two main variants of ABE. KP-ABE assigns to each file a set of attributes to be encrypted, and assigns to each user an access structure, that represents his access scope, for data decryption. On the contrary, CP-ABE assigns to each file an access structure to be encrypted, and uses a set of attributes to generate the user’s key for data decryption. In medical systems, healthcare professionals are assigned particular roles (e.g. general practitioner, nurse), and through those role they get permissions to access to particular data. Implementing these policies is easier and more efficient using CP-ABE than using KP-ABE. Indeed, we can describe the role of each healthcare professional by assigning a combination of attributes. At the same time, we encrypt each file by an access structure that express the access policy. In what follows we present the basics of CP-ABE necessary for the understanding of our architecture. More extensive description of CP-ABE is available in [19]. A CP-ABE scheme consists of four fundamental algorithms: setup, encrypt, key generation, and decrypt. Setup: defines the universal attributes set \(U\) and computes the public key (PK) and the master key (MK). The public key (PK) is used in encryption and decryption algorithms. The master key (MK) is needed to generate secret keys in the Key
Fig 1 Access Tree

**Encryption (PK, M, A):** It takes as input the public key PK, a message M, and an access structure A built over the universal attributes set (U). This algorithm encrypts the message M according to the access policy that is defined by the access structure A, and gives as output the ciphertext CT. Only users having a set of attributes corresponding to the access structure A can decrypt the ciphertext (CT). Key generation (MK, S): This algorithm takes as input a master key MK and the user set of attributes S and generates the user's secret key SK. Decryption (PK, CT, SK): It takes as input the public key PK, the ciphertext CT and a secret key SK. It returns a message M that is plaintext of CT if the set of attributes corresponding to SK satisfies the access structure A of CT.

**IV. Authorized Private Keyword**

The problem of authorized private keyword searches (APKS) over encrypted PHRs in cloud computing. They make the following main contributions. First, they propose a fine-grained authorization framework in which every user obtain search capabilities under the authorization of local trusted 11 Authorities (LTAs), based on checking for user's attributes. The central TA's task is reduced to minimum, and can remain semi-offline after initialization. Using an obtained capability, a user can let the cloud server search through all owners' encrypted PHRs to find the records that match with the query conditions. Their framework enjoys a high level of system scalability for PHR applications in the public domain. To realize such a framework, they make novel use of a recent cryptographic primitive, hierarchical predicate encryption (HPE), which features delegation of search capabilities. Based on HPE they propose two solutions for searching on encrypted PHR documents, APKS and APKS+. The first solution enhances search efficiency, especially for subset and a class of simple range queries, while the second enhances query privacy with the help of proxy servers. Both schemes support multi-dimensional multi-keyword searches and allow delegation and revocation of search capabilities. Finally, they implement their scheme on a modern workstation and carry out extensive performance evaluation. Through experimental results they demonstrate that their scheme is suitable for a wide range of delay-tolerant PHR applications. To the best of their knowledge, their work is the first to address the authorized private search over encrypted PHRs within the public domain. The encryption schemes with strong security properties will guarantee that the patient's privacy is protected. However, adherence to a simple encryption scheme can interfere with the desired functionality of health record systems. In particular, they would like to employ encryption, yet support such desirable functions as allowing users to share partial access rights with others and to perform various searches over their records. In what follows, they consider encryption schemes that enable patients to delegate partial decryption rights, and that allow patients (and their delegates) to search over their health data. They shall propose a design that refers to as Patient Controlled Encryption (PCE) as a solution to secure and private storage of patients' medical records. PCE allows the patient to selectively share records among doctors and healthcare providers. The design of the system is based on a hierarchical encryption system. The patient's record is
partitioned into a hierarchical structure, each portion of which is encrypted with a corresponding key. The patient is required to store a root secret key, from which a tree of sub keys is derived. The patient can selectively distribute sub keys for decryption of various portions of the record. The patient can also generate and distribute trapdoors for selectively searching portions of the record. Their design prevents unauthorized access to patients’ medical data by data storage providers, healthcare providers, pharmaceutical companies, insurance companies, or others who have not been given the appropriate decryption keys.

V. Multi level Control Access

In this a hybrid solution suggest that offers a way to trade off privacy and efficiency guarantees. The basic idea behind it is to provide two levels of access control: coarse-grained and fine-grained. The coarse-grained level access control will be enforced explicitly by the cloud provider and it would also represent the granularity at which he will learn the access pattern of users. Even though the cloud provider will learn the access pattern over all user requests, he will not be able to distinguish requests from different users, which would come in the form of anonymous tokens. The fine-grained access control will be enforced obliviously to the cloud through encryption and would prevent him from differentiating requests that result in the same coarse-grained access control decision but have different fine-grained access pattern. The mapping between files and access blocks is transparent to the users in the sense that they can submit file requests without knowing in what blocks the files are contained. While most existing solutions focus on read request, we present a solution that provides both read and write access control. Choosing the granularity for the access blocks in the read and write access control schemes affects the privacy guarantees for the scheme as well as its efficiency performance.

Secure, scalable, and fine-grained data access control in cloud

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. 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. S. Yu, C. Wang, K. Ren, and W. Lou 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. They achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE).

VI. CONCLUSION

In this paper, we have proposed a Multi-Authority Attribute framework of secure sharing of personal health records in cloud computing by using MAABE. Considering partially trustworthy cloud servers, 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 greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize AABE to encrypt the PHR data, so that the patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Further enhancement could be done on an existing MAABE scheme.

References


C.A. Pavani completed Post Graduation in Computer Science Applications.

Ravi Mathey is a post-graduate specialized in Computer Science from BIT -Ranchi and he did Instrumentation technology in Andhra university. He has more than 20 years of experience in Research and Development; Presently he is working as a Associate Professor and HOD of CSE Department at Vidya Jyothi Institute of Technology (VJIT). His area of research is wireless embedded application, cloud computing, image compression techniques by using fractals and wavelets.