Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.452 – 456

SURVEY ARTICLE

SURVEY ON USER REVOCATION AND FINE GRAINED ACCESS CONTROL OF PHR IN CLOUD USING HASBE

T.Radhika[1], S.Vasumathi Kannagi[2]

[1]PG Scholar, Computer Science and Engineering & Anna University, India
[2]Assistant Professor, Computer Science and Engineering &Anna University, India
Radhikaa216@gmail.com; Vasumathi.arun@gmail.com

Abstract-Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing Attribute-Based Encryption (ABE) have been proposed for access control of outsourced data in cloud computing, however, most of them suffer from inflexibility in implementing complex access control policies. The proposed scheme used is Hierarchical Attribute-Set-based encryption by extending cipher text-policy Attribute-Set-Based Encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, ASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the Cipher text-Policy Attribute-Based Encryption (CP-ABE) scheme and analyze its performance and computational complexity. We introduced the ASBE scheme for realizing scalable, flexible, and fine-grained access control in cloud computing. The ASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. ASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes.

Keywords: *HASBE; Cloud Computing; PHR; User Revocation*

I. INTRODUCTION

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. **C**loud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing, and service-oriented architecture.

Cloud computing holds the promise of providing computing.

- The great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computing extensive applications and usage in the future.
- One of the prominent security concerns is data security and privacy in cloud computing due to its Internet- based data storage and management.

In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is usually a commercial enterprise which cannot be totally trusted. Data represents an extremely important asset for any organization, and enterprise users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors.

II. LITERATURE SURVEY

Shucheng Yu have proposed **"Achieving Secure, Scalable, And Fine-Grained Data Access Control In Cloud Computing"** enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. We achieve our design goals by exploiting a novel cryptographic primitive, namely key policy attribute-based encryption (KP-ABE) and uniquely combine it with the technique of proxy re-encryption (PRE) and lazy re-encryption. User secret keys are defined to reflect their access structures so that a user is able to decrypt a ciphertext if and only if the data file attributes satisfy his access structure. Such a design also brings about the efficiency benefit, as compared to previous works, in that, the complexity of encryption is just related the number of attributes associated to the data file, and is independent to the number of users in the system; and data file creation/deletion and new user grant operations just affect current file/user without involving system-wide data file update or re-keying. One extremely challenging issue with this design is the implementation of user revocation, which would inevitably require re-encryption of data files accessible to the leaving user, and may need update of secret keys for all the remaining users.

Cong Wang, Kui Ren and Shucheng Yu have proposed **"Attribute Based Data Sharing With Attribute Revocation"** for IBE, which is also applicable to KP-ABE and fuzzy IBE . Ciphertext-policy attribute based encryption (CP-ABE) is a public-key cryptography primitive that was proposed to resolve the exact issue of fine-grained access control on shared data in one-to-many communications. In CP-ABE, each user is assigned a set of attributes which are embedded into the user's secret key. A public key component is defined for each user attribute. When encrypting the message, the encryptor chooses an access structure on attributes, and encrypts the message under the access structure via encrypting with the corresponding public key components. However, it is not clear whether the proposed scheme is applicable to CP-ABE.

Ming Li, Ning Cao, Shucheng Yu*y* and Wenjing Lou have proposed **"Authorized Private Keyword Search Over Encrypted Personal Health Records in Cloud Computing"** is a fine-grained authorization framework in which every user obtain search capabilities under the authorization of local trusted 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. Our framework enjoys a high level of system scalability for PHR applications in the public domain. To realize such a framework, we make novel use of a recent cryptographic primitive, hierarchical predicate encryption (HPE), which features delegation of search capabilities. Based on HPE we propose two solutions for searching on encrypted PHR documents, APKS and APKS+ . We consider a cloud computing environment which hosts the PHR service. There are three entities in the system: data owners/users, trusted authorities, and the cloud server. In this paper, owner refers to a special type of user, i.e., a patient who creates her PHR records, and wants them to be stored in the cloud server such that her privacy is preserved. The "users" generally refers to those who can perform searches over the encrypted PHR database, and in this paper we consider the users to be from the public domain, i.e., who are usually not personally known by an owner, and need to access or search over the PHRs due to their professional responsibilities.

Josh Benaloh, Kristin Lauter, ric Horvitz and Melissa Chase have proposed **"Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records"** refer 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 subkeys is derived. The patient can selectively distribute subkeys for decryption of various portions of the record. The patient can also generate and distribute trapdoors for selectively searching portions of the record. Our 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. We assume that a patient's record is organized into a hierarchical data structure. There are multiple ways to decompose medical data into a hierarchical representation based on the use of different ontologies.

Ting-Yu and Winnslett.M have proposed **"A Unified Scheme for Resource Protection in Automated Trust Negotiation"** in centrally managed security domains. Every entity that can take actions within such a system has one or more identities in that domain. The system grants or denies an entity's requests to access certain resources according to its access control policies and the authenticated identities of the requester. underlying assumption is that entities in the system already know each other. Therefore, trust can be easily established based on each other's identity. Further without obtaining a local identity, an entity will not be able to interact with the system and gain access to the system's resources.
As we move towards a globally internetworked infrastructure, open systems like the Internet provide an environment where two or more parties who are virtually strangers to each other can make connections and do business together. Such interactions often involve release of sensitive information and remote access to a party's local resources. Mutual trust between the two parties is crucial in such an environment. Obviously, establishing trust based on identity is not a feasible approach. Parties may come from different security domains and they often will not have any preexisting relationship.

Amit Sahai, Brent Waters, Carnegie Mellon and John Bethencourt have proposed **"Ciphertext-Policy Attribute-Based Encryption"** in which, a user will only be able to decrypt a ciphertext if that user's attributes pass through the ciphertext's access structure. In this work, we provide the first construction of a ciphertext-policy attribute-based encryption (CP-ABE) to address this problem, and give the first construction of such a scheme. In our system, a user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message in our system, they specify an associated access structure over attributes. At a mathematical level, access structures in our system are described by a monotonic "access tree", where nodes of the access structure are composed of threshold gates and the leaves describe attributes. We note that AND gates can be constructed as n-of-n threshold gates and OR gates as 1-of-n threshold gates. Furthermore, we can handle more complex access controls such as numeric ranges by converting them to small access. Traditionally, this type of expressive access control is enforced by employing a trusted server to store data locally. The server is entrusted as a reference monitor that checks that a user presents proper certification before allowing him to access records or files. However, services are increasingly storing data in a distributed fashion across many servers. Replicating data across several locations has advantages in both performance and reliability. The drawback of this trend is that it is increasingly difficult to guarantee the security of data using traditional methods; when data is stored at several locations, the chances that one of them has been compromised increases dramatically.

Kristin Lauter has proposed **"Automated Trust Negotiation using Cryptographic Credentials"** have been developed to address oblivious signature. Oblivious signature based envelope, hidden credentials, and secret handshakes can be used to address the policy cycle problem. Oblivious Attribute Certificates (OACerts), private credentials, and anonymous credentials together with zero-knowledge proof protocols can be used to prove that an attribute satisfies a policy without disclosing any other information about the attribute. Certified input private policy evaluation (CIPPE) [20] enables A and B to determine whether A's attribute values satisfy B's policies without revealing additional information about A's attributes or B's policies. While these credential schemes and associated protocols all address some limitations in ATN, they can be used only as fragments of an ATN process. For example, a protocol that can be used to handle cyclic policy dependencies should be invoked only when such a cycle occurs during the negation process. A zero-knowledge proof protocol can be used only when one knows the policy that needs to be satisfied and is willing to disclose the necessary information to satisfy the policy. An ATN framework that harnesses these powerful cryptographic credentials and protocols has yet to be developed. In this paper, we develop an ATN framework that does exactly that. Our framework has the following salient features. **Separation of credential disclosure from attribute disclosure***:* In several credential systems, including private credentials anonymous credentials, and OACerts, a user's attribute values are not stored in the clear; instead, they are stored in a committed form in her credentials. When the commitment of an attribute value is stored in a credential, looking at the commitment does not enable one to learn anything about the attribute value. Therefore, A credential holder can disclose her credentials without revealing the attribute values in them. For example, consider a digital driver license certificate from Bureau of Motor Vehicles(BMV) consisting of name, gender, DoB, and address.

Brunelli.D have proposed **"Cloud Computing And Emerging IT Platforms:Vision, Hype, And Reality For Delivering Computing As The 5th Utility"** consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements without regard to where the services are hosted or how they are delivered. Several computing paradigms have promised to deliver this utility computing vision and these include cluster computing, Grid computing, and more recently Cloud computing. At present, it is common to access content across the Internet independently without reference to the underlying hosting infrastructure. This infrastructure consists of data centers that are monitored and maintained around the clock by content providers. Cloud computing is an extension of this paradigm wherein the capabilities of business applications are exposed as sophisticated services that can be accessed over a network. Cloud service providers are incentivized by the profits to be made by charging consumers for accessing these services. Consumers, such as enterprises, are attracted by the opportunity for reducing or eliminating costs associated with "in-house" provision of these services. However, since cloud applications may be crucial to the core business operations of the consumers, it is essential that the consumers have guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) brokered between the providers and consumers. Providers such as Amazon, Google, Salesforce, IBM, Microsoft, and Sun Microsystems have begun to establish new data centers for hosting Cloud computing applications in various locations around the world to provide redundancy and ensure reliability in case of site failures. Since user requirements for cloud services are varied, service providers have to ensure that they can be flexible in their service delivery while keeping the users isolated from the underlying infrastructure. Recent advances in microprocessor technology and software have led to the increasing ability of commodity hardware to run applications within Virtual Machines (VMs) efficiently. VMs allow both the isolation of applications from the underlying hardware and other VMs, and the customization of the platform to suit the needs of the end-user .While convenient, the use of VMs gives rise to further challenges such s the intelligent allocation of physical resources for managing competing resource demands of the users.

Amit Sahaiz, Brent Waters, Omkant Pandeyy and Vipul Goyal have proposed **"Attribute-Based Encryption For Fine-Grained Access Control Of Encrypted Data"** in which, each user's key is associated with a tree-access structure where the leaves are associated with attributes. A user is able to decrypt a cipher text if the attributes associated with a cipher text satisfy the key's access structure. The primary difference between our setting and secret-sharing schemes is that while secret-sharing schemes allow for cooperation between different parties, in our setting, this is expressly forbidden. For instance, if Alice has the key associated with the access structure \X AND Y", and Bob has the key associated with the access structure \Y AND Z", we would not want them to be able to decrypt a cipher text whose only attribute is Y by colluding. To do this, we adapt and generalize the techniques introduced by to deal with more complex settings. We will show that this cryptosystem gives us a powerful tool for encryption with fine-grained access control for applications such as sharing audit log information.

Amit Sahai and Brent Waters have proposed **"Fuzzy Identity-Based Encryption"** is a new type of Identity-Based Encryption that we call Fuzzy Identity-Based Encryption in which we view identities as a set of descriptive attributes. In a Fuzzy Identity-Based Encryption scheme, a user with the secret key for the identity is able to decrypt a cipher text encrypted with the public key 0 if and only if and 0 are within a certain distance of each other as judged by some metric. Therefore, our system allows for a certain amount of error-tolerance in the identities. Fuzzy-IBE gives rise to two interesting new applications. The first is an Identity-Based Encryption system that uses biometric identities. That is we can view a user's biometric, for example an iris scan, as that user's identity described by several attributes and then encrypt to the user using their biometric identity. Since biometric measurements are noisy, we cannot use existing IBE systems. However, the error-tolerance property of Fuzzy-IBE allows for a private key to decrypt a cipher text encrypted with a slightly different measurement of the same biometric. Secondly, Fuzzy IBE can be used for an application that we call "attribute-based encryption".In this application a party will wish to encrypt a document to all users that have a certain set of attributes. Any user who has an identity that contains all of these attributes could decrypt the document. The advantage to using Fuzzy IBE is that the document can be stored on an simple un trusted storage server instead of relying on trusted server to perform authentication checks before delivering a document.

Mrinmoy Barua and Xiaohui Liang have proposed **"Principles of Policy In Secure Groups"** a group security policy defined as a statement of the entirety of security relevant parameters and facilities used to implement the group. This best fits the viewpoint of policy as defining how security directs group behavior, who are the entities allowed to participate, and which mechanisms will be used to achieve mission critical goals. Note that this definition is not restricted to electronically distributed statements; policy is often the result of system design and configuration. This paper considers the definition and requirements of security policies in groups. A number of principles for the design of policy services in group communication are identified. These principles are the result of a systematic analysis of the policy requirements unique to secure groups and those common to both peer and group communication. We reason about the security of arbitrary policy through the application of known principles and the reduction of group behavior to pair-wise operations.

III. CONCLUSION

Here 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.

REFERENCES

[1] Kui Ren, Ming Li, Shucheng Yu, Wenjing Lou, Yao Zheng, and “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption” IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013.

[2] Cong Wang, Kui Ren, Shucheng Yu and Wenjing Lou “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, INFOCOM, 2010 Proceedings IEEE,march 2010.

[3] Cong Wang, Kui Ren, Shucheng Yu “Attribute Based Data Sharing with Attribute Revocation”, ASIACCS '10 Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security 2010.

[4] Amit Sahaiz, Brent Waters, Omkant Pandeyy, Vipul Goyal “Attribute-Based Encryption for Fine-Grained Access Control”, CCS '06 Proceedings of the 13th ACM conference on Computer and communications security 2006 .

[5] Ming Li, Ning Cao, Shucheng Yu*y* and Wenjing Lou “Authorized private keyword search over encrypted personal health records in cloud computing”,Distributed Computing Systems (ICDCS), 2011 31st International Conference, June 2011.

[6] Josh Benaloh, Kristin Lauter, ric Horvitz, Melissa Chase “Patient controlled encryption: ensuring privacy of electronic medical records”, CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security.

[7] Ting-Yu,Winnslett.M, “A Unified Scheme for resource protection in automated trust negotiation”, Security and Privacy 2003 Proceedings, May 2003.

[8] Amit Sahai, Brent Waters, Carnegie Mellon, John Bethencourt “ciphertext-policy attribute-based encryption”, Security and Privacy, May 2007.

[9] Kristin Lauter “Automated trust negotiation using cryptographic credentials utility cloud computing and emerging it platforms:vision, hype, and reality for delivering computing”,Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference Dec 2010.

[10] Brunelli.D “Cloud computing and emerging it platforms:vision, hype, and reality for delivering computing as the 5th utility “, Volume 25, Issue 6, June 2009.

[11] Amit Sahai, Brent Waters, “fuzzy identity-based encryption” ,CCS '08 Proceedings of the 15th ACM conference on Computer and communications security 2008.

[12] Mrinmoy Barua, Xiaohui Liang,“Principles of policy in secure groups PEACE: An Efficient and Secure Patient-centric Access Control Scheme for eHealth Care System”,Computer Communications Workshops,IEEE Conference April 2011.