International Journal of Engineering Research and General ScienceVolume 2, Issue 5, August – September 2014
ISSN 2091-2730

A Design for Secure Data Sharing in Cloud

Devi D[1], Arun P S[2]

[1]Research Scholar (M.Tech), Dept of Computer Science and Engineering, Sree Buddha College of Engg, Alappuzha, Kerala, India

[2]Assistant professor, Dept of Computer Science and Engineering, Sree Buddha College of Engg, Alappuzha, Kerala, India

E-mail- devidharman@gmail.com

Abstract— Cloud computing, which enables on demand network access to shared pool of resources is the latest trend in today's IT industry. Among different services provided by cloud, cloud storage service allows the data owners to store and share their data through cloud and thus become free from the burden of storage management. But, since the owners lose physical control over their outsourced data, there arise many privacy and security concerns. A number of attribute based encryption schemes are proposed for providing confidentiality and access control to cloud data storage where the standard encryption schemes face difficulties. Among them, Hierarchical Attribute Set Based Encryption (HASBE) provides scalable, flexible and fine grained access control as well as easy user revocation. It is an extended form of Attribute Set Based Encryption (ASBE) with a hierarchical structure of users. Regarding integrity and availability, HASBE is not sufficient to provide the data owner with the ability to perform checking against missing or corruption of their outsourced data. So, this paper extends HASBE with privacy preserving public auditing concept which additionally allows owners to securely ensure the integrity of their data in the cloud. We are using homomorphic linear authenticator technique for this purpose.

Keywords— Cloud Computing, Access control, Personal Health Record, HASBE, Integrity, TPA, Homomorphic Linear Authenticator.

INTRODUCTION

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Three distinct characteristics differentiate cloud service from traditional hosting. It is sold on demand- giving the cloud consumer the freedom to self-provision the IT resources, it is elastic - which means that at any given time a user can have as much or as little of a service as they want, the service is fully managed by the provider-the consumer needs nothing but a personal computer and Internet access. Other important characteristics of cloud are measured usage and resilient computing. In measured usage cloud keep track of usage of it's IT resources and the consumer need to pay only for what they actually use. For resilient computing, cloud distributes redundant implementations of IT resources across physical locations. IT resources can be pre-configured so that if one becomes imperfect, processing is automatically handed over to another redundant implementation.

Infrastructure as a Service(IaaS), Platform as a Service(PaaS), and Software as a Service(SaaS)are the major service oriented cloud computing models. Cloud storage is an important service of cloud computing which allows data owners to move data from their local computing systems to the cloud. The physical storage spans across multiple servers and locations. People and organizations buy or lease storage capacity from the providers to store end user,organization, or application data. Cloud storage has several advantages over traditional data storage: relief from the burden for storage management, universal data access with location independence and avoidance of capital expenditure on hardware, software and personnel maintenances. It also allows sharing of data with others in a flexible manner Moving the data to an off-site storage system, maintained by a third party(cloud service provider), on which data owner does not have any control posses many data security challenges of privacy - the risks of unauthorized disclosure of the users' sensitive data by the service providers, data integrity-validity of outsourced data due to its internet-based data storage and management

etc. In cloud environment data confidentiality is not the only data security requirement. Since cloud allows data sharing, a great attention to be given to fine- grained access control to the stored data.

The traditional method to provide confidentiality to such sensitive data is to encrypt them before uploading to the cloud. In traditional public key infrastructure, each user encrypts his file and stores it in the server and the decryption key is disclosed only to the particular authorized user. Regarding confidentiality, this scheme is secure, but this solution requires efficient key management and distribution which is proven to be difficult. Also, as the number of users in the system becomes large this method will not be efficient. These limitations and the need for fine- grained access control for data sharing, lead to the introduction of new access control schemes based on attribute based encryption(ABE)[3].Unlike in traditional cryptography where the intended recipient identity is clearly known, in an attribute based systems one only needs to specify the attributes or credentials of the recipient(s).Here cipher texts are not encrypted to one particular user as in traditional public key cryptography.It enables to handle unknown users also. Different types of ABE schemes are proposed to provide fine-grained access control to data stored in cloud. But they could not satisfy the requirements such as scalability- ability to handle increasing number of system users without degrading efficiency, flexibility-should support complex access control policies with great easiness and easy user revocation -should avoid re-encryption of data and re-distribution of new access keys during the revocation of each user. These limitations of ABE schemes are covered by Hierarchical Attribute Set Based Encryption (HASBE)[1].It is an extension of Attribute Set Based Encryption(ASBE).HASBE achieves scalability due to its hierarchical structure and also inherits fine-grained access control and flexibility in supporting compound attributes from ASBE[7].Another highlighting feature of HASBE is its easy user revocation method. In addition to these access control needs, the data owners want to know the integrity of the data which they uploaded to the cloud. HASBE does not include integrity checking facility and it is the major drawback of this scheme. This paper integrates integrity checking module based on privacy preserving public auditing with HASBE scheme and thus provides more security to the system.

RELATED WORKS

This section reviews the concept of attribute based encryptions and provide a brief overview of Attribute Set Based Encryption(ASBE) and Hierarchical Attribute Set Based Encryption(HASBE).All these schemes are proposed as access control mechanisms to cloud storage.

Sahai and Waters proposed Attribute based encryption to provide better solution for access control. It used user identities as attributes and these attributes play important role in encryption and decryption. The primary ABE used a threshold policy for access control, but it lacks expressibility. ABE schemes are further classified into key-policy attribute based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE), in which concept of access policies are introduced. In KP-ABE[4] access policies are asscociated with users private key while in CP-ABE[5] it is in the ciphertext. In the ABE scheme, ciphertexts are not encrypted to one particular user as in traditional public key cryptography.Rather, both ciphertexts and users' decryption keys are associated with a set of attributes or a policy over attributes. A user is able to decrypt a ciphertext only if there is a match between attributes in the decryption key and the ciphertext.

In KP-ABE since the access policy is built in to the users private key, the data owner who encrypt the data can't choose who can decrypt the data. He has to trust the key issuer. But in CP-ABE since users' decryption keys are associated with a set of attributes, it is more natural to apply. These scheme provided fine grained access control to the sensitive data in the cloud but it failed in the case of handling complex access control policies. It lacks scalability and in case a previously legitimate user needs to be revoked, related data has to be re-encrypted. Here data owners need to be online all the time so as to encrypt or re-encrypt data .

In CP-ABE scheme decryption keys only support user attributes that are organized logically as a single set. So users can only use all possible combinations of attributes in a single set issued in their key to satisfy a policy. To solve this problem, Bobba [7]

introduced ciphertext-policy attribute-set-based encryption (CP-ASBE or ASBE for short). ASBE is an extended form of CP-ABE which organizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. It groups user attributes into sets such that those belonging to a single set have no restrictions on how they can be combined. Similarly, multiple numerical assignments for a given attribute can be supported by placing each assignment in a separate set.

To achieve scalability, flexibility and fine grained access control and efficient user revocation, Hierarchical attribute set based encryption [HASBE] by extending cipher-text-policy attribute set based encryption [CP-ASBE or ASBE] scheme is proposed[1]. HASBE extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE. HASBE supports compound attributes due to flexible attribute set combinations as well as achieves efficient user revocation without requiring re-encryption because of attributes assigned multiple values.

HASBE system consists of five types of parties: a cloud service provider, data owners, data consumers, a number of domain authorities, and a trusted authority. The trusted authority is the root authority and responsible for managing top-level domain authorities. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. Data consumers download and decrypt the file stored in cloud. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner and keys are delegated through this hierarchy.

PROBLEM STATEMENT

Even though HASBE scheme achieves scalability, flexibility and fine grained access control, there is no method called integrity scheme in HASBE to ensure that the data will be remained correctly in the cloud. Hence it is the major drawback of HASBE scheme. The data owners are facing a serious risk of corrupting or missing their data because of lack of physical control over their outsourced data. In order to overcome this security risk, privacy preserving public auditing concept could be proposed, which integrates data integrity proof with HASBE scheme.

OBJECTIVES

The data owners want to prevent the server and unauthorized users from learning the contents of their sensitive files. Each of them owns a privacy policy. In particular, the proposed scheme has the following objectives:

- Fine grained access control : Different users can be authorized to read different sets of files.
- User revocation: Whenever it is necessary, a user's access privileges should be revoked from future access in an efficient and easy way.
- Flexible policy specification: The complex data access policies can be specified in a flexible manner.
- Scalability: To support a large and unpredictable number of users, the system should be highly scalable, in terms of complexity in key management, user management, and computation and storage.
- Enable users to ensure the integrity of data they are outsourced.
    - Public audit ability: to allow a Third Part Auditor (TPA) to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.
    - Storage correctness: to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users data intact.
    - Privacy-preserving: to ensure that the TPA cannot derive users data content from the information collected during the auditing process.

METHODOLOGY

The entire system applies to Personal Health Record (PHR), which is an electronic record of an individual's health information. Online PHR service [8-9] allows an individual to create, store, manage and share his personal health data in a centralized way. Since

cloud computing provides infinite computing resources and elastic storage, PHR service providers shift the data and applications in order to lower their operational cost.

The overall methodology of this work can be divided into two parts - Secure PHR Sharing using HASBE and Secure data auditing. The architecture of Secure PHR sharing is given in figure 1 and secure data auditing in figure 2.

B. Secure PHR Sharing

For secure PHR sharing, HASBE has a hierarchical structure of system users. Hierarchy enables the system to handle increasing number of users without degrading the efficiency. PHR owners can upload their encrypted PHR files to cloud storage and data consumers can download and decrypt the required file from the cloud. In this system, the PHR owners need not be online all the time since they are not responsible for issuing decryption keys to data consumers. It is the responsibility of a domain authority to issue decryption keys to users under its domain. The system can be extended to any depth and in the same level there can be more than one domain authorities so that no authority should become a bottleneck to handle large number of system users.Here, the system under consideration uses a depth 2 hierarchy and there are five modules for secure PHR sharing.

1. Trusted Authority Module
2. Domain Authority Module
3. Data Owner Module
4. Data Consumer Module
5. PHR Cloud Service Module

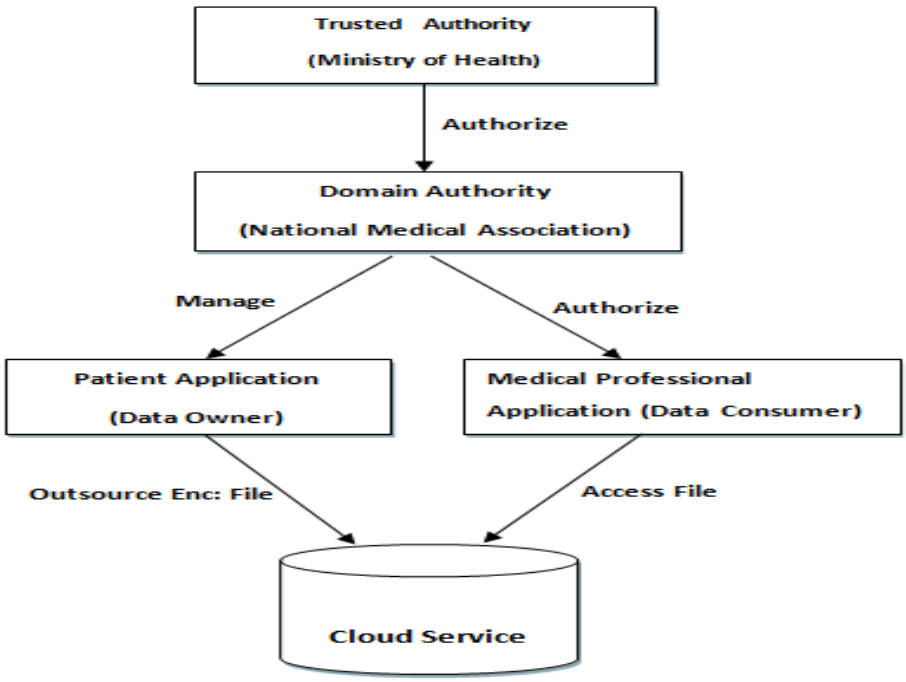

Fig 1:HASBE Architecture

1. Trusted Authority Module

The trusted authority is the root or parent authority. It is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. In our system the Ministry of Health is the trusted authority.

The major functions of Ministry of Health are,

- Admin can login from the home page and can perform domain authority registration.
- To set up the system by generating master secret key MK_0 and a public key based on universal set of system attributes .
- Generate master key for domain authority using public key PK, master key MK_0 and set of attributes corresponding to domain authority.

2. Domain Authority Module

Domain Authority (DA) is responsible for managing PHR owners and authorizing data consumers. In our system a single domain authority called National Medical Association(NMA) comes under Ministry of Health.

- NMA first registers to the trusted authority. During the registration the attributes corresponding to the DA is specified. Also a request for domain key is send to trusted authority through web services. Only after receiving domain key- public key and domain master key, DA can authorize users in it's domain.
- Major functions of NMA are,
    - To provide public key for the patients to perform attribute based encryption.
    - Log in and View the details of medical professionals.
    - To provide attribute based private key for the medical professionals for decrypting the medical records.
    - Perform user revocation.

3. Data Owner Module

In our system patients are the data owners. A patient application is there which allows the patient to interact with PHR service provider. The main functions of these module are,

- Patients first register to the system and then log in.
- Patients can set the access privilege as who can view the files and upload encrypted files to cloud.
- Patient application performs encryption in two stages. First the file is encrypted with AES, then AES key is encrypted with patient specified policy and public key provided by NMA. Second stage corresponds to attribute set based encryption.
- Encrypted file along with encrypted AES key is uploaded to the cloud.

4. Data Consumer Module

Medical professionals act as data consumers. Through the medical professional application doctors interact with PHR service provider.

- Each hospital administrator log in and creates employees by entering their details. Registration details are also given to NMA through web services.
- Doctors can later log in to the application using their username and password.
- The application allows doctors to view required patient details and download their files by interacting with PHR service provider in cloud through web services.
- Medical professional application performs decryption of files for each employee by requesting corresponding private key based on attributes of the employee from NMA.

5. PHR Cloud Service Module

Responsible for storing encrypted files. It preprocess the file for generating metadata for auditing purpose.

A. Secure Data Auditing

Data auditing is performed by a third party Auditor (TPA) on behalf of the PHR service provider. For the cloud PHR service provideris the data owner. On the other hand PHR service provider is the client of TPA. It first registers to TPA. The initial

verification details about uploaded files are given to TPA through proper communication channels. Upon getting data auditing delegation from PHR service provider, TPA interact with cloud and performs a privacy preserving public auditing. Homomorphic Linear Authenticator is used to allow TPA to perform integrity checking without retrieving the original data content. It issues challenges to cloud which indicates random file blocks to be checked. Cloud generates data correctness proof and TPA verifies it and indicates the result.

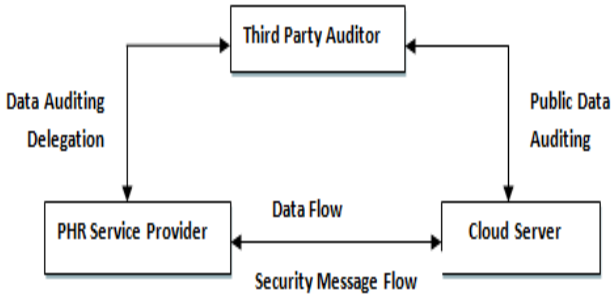

Fig 2: Auditing Architecture

CONCLUSION

In this paper, we proposed the privacy preserving public auditing concept for HASBE scheme, to overcome the drawback of, absence of integrity assurance method in HASBE. Even though HASBE scheme achieves scalability, flexibility and fine- grained access control, it fails to prove data integrity in the cloud. Since, the data owner has no physical control over his outsourced data, such an auditing is necessary to prevent cloud service provider from hiding data loss or corruption information from the owner. Audit result from TPA would also be beneficial for the cloud service providers to improve their cloud based service platform, and users can give their data to the cloud and be worry free about the data integrity.The proposed system preserves all advantages of HASBE and also adds an additional quality of integrity proof to this system.

REFERENCES:

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, *Senior Member, IEEE,"* HASBE: A Hierarchical Attribute set-Based Solution for Flexible and Scalable Access Control in Cloud Computing", ieee transactions on information forensics and security, vol. 7, no. 2, april 2012

[2] Kangchan Lee," Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications ,Vol. 6, No. 4, October, 2012.

[3] Cheng-Chi Lee1, Pei-Shan Chung2, and Min-Shiang *Hwang ,"*A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", *International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013*

[4] Vipul Goyal *Omkant Pandeyy Amit Sahaiz Brent Waters,"* Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data"

[5] John Bethencourt, Amit Sahai, Brent Waters **"**Ciphertext-Policy Attribute-Based Encryption ", in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[6] Guojun Wanga, Qin Liu a,b, Jie Wub, Minyi Guo, Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, www.elsevier.com locate / /cose

[7] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran," Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption" University of Illinois at Urbana-Champaign, July 27, 2009

[8] Ming Li, Shucheng Yu, ,Yao Zheng, Kui Ren, and Wenjing Lou," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" in IEEE Transactions On Parallel And Distributed Systems ,2012

[9] Chunxia Leng1, Huiqun Yu, Jingming Wang, Jianhua Huang," Securing Personal Health Records in Clouds by Enforcing Sticky Policies" in TELKOMNIKA, Vol. 11, No. 4, April 2013, pp. 2200 ~ 2208 e-ISSN: 2087-278X.

[10] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou (2010), "Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing".

[11] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,"Homomorphic Authentication with Random MaskingTechnique Ensuring Privacy & Security in CloudComputing", Bioinfo Security Informatics, vol. 2, no. 2,pp. 49-52, ISSN. 2249-9423, 12 April 2012

[12] Devi D," Scalable and Flexible Access Control with Secure Data Auditing in Cloud Computing", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4118-4123,ISSN:0975-9646