VARIOUS SECURE DATA SHARING TECHNIQUES IN PUBLIC CLOUD

Neha Thakur, Er. Supreet Kaur

1Student of Department Of Computer Engineering, 2Faculty of Department Of Computer Engineering Punjabi University, Patiala, India

Abstract: This paper presents the various secure data sharing techniques in public clouds. A public cloud allows resources such as applications and storage to be accessible to the public over the internet. Due to the benefits of cloud storage, there has been a growing trend to use the public cloud for secure data sharing and storage. The public cloud storage model should solve the critical issue of data confidentiality. Shared sensitive data must be strongly secured from unauthorized users. There are many issues and challenges are associated with the public cloud storage. Public clouds improve productivity and reduce costs. We have reviewed different secure data sharing techniques in public clouds. The benefits of this study for the reader are that this study will provide information about the different methods used for secure data sharing.

Keywords: Cloud Computing, Public Cloud, Secure Data Sharing, Confidentiality.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to the shared pool of configurable computing resources (e.g., networks, storage, servers, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is consists of five essential characteristics, four deployment models and three service models. Different types of cloud are public cloud, private cloud and hybrid cloud. Private cloud is the phrase used to describe a cloud computing platform that is implemented within the firewall, under the maintenance of the IT department. A public cloud is one based on the standard cloud computing paradigm, where a cloud service provider makes numerous resources like servers and storage, available globally over the web. Public cloud services may be free or based on a pay-per-use model. A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization [1]. Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organisations hoping to gain profit. People love to share information with one another.

II. PRIVACY AND SECURITY REQUIREMENT OF DATA SHARING IN THE CLOUD

A. Data Confidentiality

Unauthorized users (including the Cloud), should not be able to access data at any given time. Data should remain confidential in transit, at rest and in backup media. Only authorized users are able to gain access to data.

B. User revocation

When a user is revoked access rights to data, that user should not be able to gain access to the data at any given time. Ideally, user revocation should not affect other authorized users from the group for efficiency purposes.

C. Scalable and Efficient

Since the number of Cloud users tends to be extremely large and at times unpredictable as users join and leave, it is imperative that the system maintain efficiency together with scalability.
D. Collusion between entities
When considering data sharing methodologies in the Cloud environment, it is vital that even if certain entities collude, they should still not be able to access any of the data without the data owner’s permission. Earlier works of literature on data sharing did not consider this problem, however collusion between entities can never be written off as an unlikely event. The public cloud storage want to solve the critical issue of data confidentiality so the common method is to encrypt the data before uploading it to the cloud it provides more security to the data [2].

III. STUDY OF EXISTING TECHNIQUES
A. Fine-grained data access control systems with user accountability in cloud computing
This paper presented the Attribute-Based Encryption (ABE), that is one effective and promising technique that may be used to provide fine-grained access control to data in the Cloud. Initially, access to data in the Cloud was provided through Access Control Lists (ACLs) however, it was not scalable and only provided coarse-grained access to data. There are two kinds of ABE which are described as follows.

Key-Policy ABE (KP-ABE)
The access control policy is stored with the user’s private key and the encrypted data additionally stores a number of attributes associated with the data. A user can only decrypt the data if the attributes of the data satisfy the access control policy in the user’s key. The access control policy is usually defined as an access tree with interior nodes representing threshold gates and leaf nodes representing attributes.

Cipher text-Policy ABE (CP-ABE)
Essentially the converse of KP-ABE. The access control policy is stored with the data and the attributes are stored in the user’s key [3].

B. Fine-grained access control and revocation
In this paper author made use of CP-ABE in the context of enterprise applications and also developed a revocation mechanism that simultaneously allows high adaptability, fine-grained access control and revocation. The department assigns users a set of attributes within their secret key and distributes the secret key to the respective users. Any user that satisfies the access control policy defined from the data collaborator can access the data. When a user is revoked access rights, the data is re-encrypted in the Cloud rendering the revoked user’s key useless. The scheme is proven to be semantically secure against chosen cipher text attacks against the CP-ABE model. However, the scheme is not elegant in the case of user revocation since the updating of cipher texts after user revocation places heavy computation overhead even if the burden is transferred to the Cloud [4].

C. Identity-Based Encryption from the Weil Pairing
Many recent research proposals have focused on developing public key systems that avoid the use of certificates altogether. The impetus for this kind of trend has largely come from the realization that the use of pairings on elliptic curves opens up many new options which are not available before. Boneh and Franklin who showed that identity-based cryptography might be practically achieved through use of pairings. Instead of using public keys and certificates, any identity string can take replace both. Anyone can encrypt a message intended for the entity described by the identity string. Identity-based cryptography does not solve the revocation problem. Indeed, in some sense it can be argued to make the situation worse since how can a person revoke his own identity? A pragmatic way to deal with this problem is to notice that the identity string can include any additional information, including a validity period. To manage revocation in identity-based cryptosystems short validity periods may be encoded into the identity string. However, this isn't going to fit an environment where immediate revocation may be required [5].

D. Certificateless public key cryptography
This paper introduced a Certificateless Public Key Cryptography (CL PKC). Since each user holds a combination of KGC produced partial private key and an additional user-chosen secret, the key escrow problem can be resolved. As the structure of CL-PKC guarantees the validity of the user’s public key without the certificate, it removes the certificate management problem. Since the advent of CL-PKC many CL-PKE schemes have been proposed based on bilinear pairings. The computational cost required for pairing is still considerably high in comparison with standard operations such as modular exponentiation in finite fields [6].

E. Security-Mediated Certificateless Cryptography
This paper introduced the notion of security-mediated Certificateless (SMC) cryptography. This allows more lightweight versions of mediated cryptography while maintaining the ability for instantaneous revocation of keys. Moreover, the solutions avoid key escrow, which has been used in all previous mediated cryptography algorithms and provide a model of security against a fully-adaptive chosen cipher text attacker, who may be a rogue key generation centre or any coalition of rogue users. This scheme also supports distributed security mediators (SEMs). A limitation of certificateless encryption this means that although there is less trust placed in the authority than for identity-based schemes (users do not reveal their private keys to the KGC), there is more trust placed in the KGC than in traditional public key schemes [7].

F. CL-PRE: a Certificateless Proxy Re-Encryption Scheme
This paper presented the CL-PRE (Certificateless Proxy Re-Encryption) scheme for secure data sharing in public cloud environments. Their scheme is based on CL-PKC to solve the key escrow problem and certificate management, it relies on pairing operations. The computational costs required for pairing are still considerably high compared to the costs of standard operations such as modular exponentiation in finite fields. Moreover, their scheme only achieves Chosen
Plaintext Attack (CPA) security. Chosen Plaintext Attack security is usually not sufficient to guarantee security in general protocol settings. For example, CPA is not sufficient for many applications such as encrypted email forwarding and secure data sharing that require security against Chosen Cipher text Attack (CCA) [8].

G. An Efficient Certificateless Encryption
In this paper author proposed a mediated certificateless encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks. In order to address the performance and security issues, in this paper, they proposed a mCL-PKE scheme without using pairing operations.

![Fig.2 CL-PKE based fine-grained encryption](image)

The cloud is employed as a secure storage as well as a key generation center. The confidentiality of the content and the keys is preserved with respect to the cloud, because the cloud cannot fully decrypt the information. Figure 2 shows CL-PKE based fine grained encryption. They implement mCL-PKE scheme and the overall cloud based system, and evaluate its security and performance [9]. Results show that schemes are efficient and practical. Further, for multiple users satisfying the same access control policies, the improved approach performs only a single encryption of each data item and reduces the overall overhead at the data owner.

IV. CONCLUSION
Public clouds are generally used in the storage and retrieval of the user’s information. Data sharing in the Cloud is still currently a strong focus of research today. The widespread adoption of cloud storage services, the public cloud storage model should solve the critical issue of data confidentiality. That is, shared sensitive data must be strongly secured from unauthorized accesses. The solution to Achieving secure data sharing in the Cloud is for the data owner to encrypt his data before storing into the Cloud, so the data remain information secure against the Cloud provider and other malicious users.

It is given as a secure way of data sharing. Thus, in this paper, we have presented a survey of different techniques used for secure data sharing in public clouds.

REFERENCES