International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 08 | Nov-2015 www.irjet.net p-ISSN: 2395-0072

Review on Secure Data Sharing on Cloud

Miss. Sushma D. Borkar

Lecturer, Computer engineering Department, V.P.M's Polytechnic, Thane, Maharashtra, India.

Abstract - ***Cloud computing is a huge area which basically provides many services on the basis of pay as you go. One of the fundamental services provided by cloud is data storage. Cloud provides cost efficiency and an efficient solution for sharing resource among cloud users. A secure and efficient data sharing scheme for groups in cloud is not an easy task. It needs to provide identity privacy, multiple owner and dynamic data sharing without getting effected by the number of cloud users revoked. A 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. We have reviewed different secure data sharing techniques in clouds. This paper present information about the different methods used for secure data sharing.***

Key Words: *Cloud Computing, Secure Data Sharing, Confidentiality, Access Control.*

1. INTRODUCTION

Cloud computing has become a widely accepted paradigm for providing services over the internet. There are three distinct characteristic in cloud service which differs from traditional hosting. First is sold on demand, typically by the minute or the hour; Elasticity , a user can have as much or as little of a service as they want at any given time; and The service management which will be taken care by provider (The requirement of the consumer is just a computer and Internet access). With the increasing popularity of cloud storage, the risks for security, data integration, confidentiality of data are implicitly increasing. Therefore, the cloud provider must consider the security and confidentiality as the challenging factors for data sharing functionality. The care has to be taken to protect data, as cloud storage is storing of the data remotely which is regulated by third party. The third party takes the responsibility for keeping data accessible and available to users all the time. Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organizations hoping to gain profit. People love to share information with one another. Along with the fast growing internet, users can access and utilize all their files and mails from any place in the world. Instead of storing the data into the hard drive, user can save the data on the cloud which makes him avail all the data accessible for him from any corner of the world using internet. But considering the privacy of data, the traditional techniques for authentication are not reliable, because the unavoidable privilege escalation will disclose the confidentiality of data. For protecting the confidentiality of the data stored in cloud storage, the care has to be taken for encrypting those data before uploading them on to the cloud by using some or the other cryptographic algorithms. The users are encouraged to encrypt their data before uploading them on the cloud by their own keys whenever the user is not satisfied with trusting the security of the Virtual Machines or the technical team. In modern cryptography, encryption keys obtained are of two categories, symmetric and asymmetric (public) key. The public key encryption tends to be much more secured as it involves combination of two different keys, public and private key respectively. This gives more flexibility for various applications.

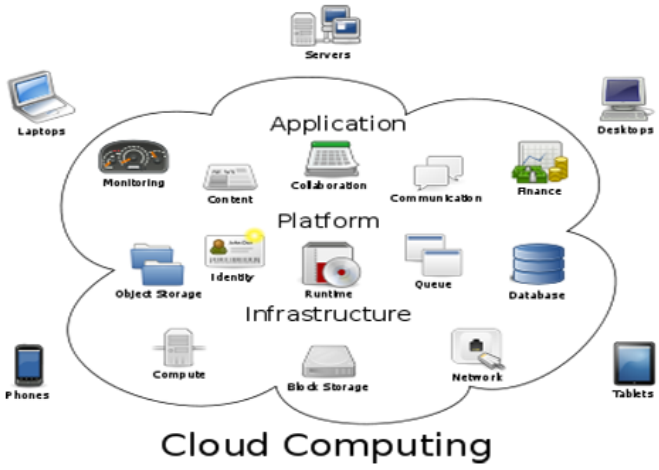

Figure 1: Architecture of cloud computing

1.1. SECURE DATA SHARING IN THE CLOUD

Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organizations aiming to gain profit. However, in recent times, it has been welcomed by a huge number of people as it has become significantly social. It is thus not surprising that more and more people are demanding data sharing capability on their phones, computers and even recently Smart TVs. People love to share information with one another. Whether it is with friends, family, colleagues or the world, many people benefit greatly through sharing data. Some of the benefits include:

• **Higher productivity**:

Businesses get more work done as well as making collaboration with peers much more efficient and hence is key to satisfying their business goals. Hospitals also benefit from data sharing and this has led to the lowering of healthcare costs . Students also benefit when working on group projects, as they are better able to collaborate with members and get work done more efficiently.

• **More enjoyment**:

Many people of any age, gender or ethnicity can connect with friends, family and colleagues to share their experiences in life as well as catch up with others via social networking sites such as Facebook or MySpace.

However, the main problem with data sharing in the Cloud is the privacy and security issues. The Cloud is open to many privacy and security attacks, which make many users wary of adopting Cloud technology for data sharing purposes.

Requirements of Data sharing in the Cloud: To enable data sharing in the Cloud, it is imperative that only authorized users are able to get right to use to data stored in the Cloud. We were reviewing the perfect constraints of data sharing in the Cloud below

- The data owner should be proficient to identify a group of clients that are permitted to view his/her information
- Any component of the group is supposed to gain access to the data anytime exclusive of the information owner's intrusion.
- No other client, other than the data owner and the components of the collection, should gain right of entry to the information, as well as the Cloud Service Provider.
- No member of the group should be allowed to revoke rights of other members of the group or join new users to the group.
- The data owner should be capable to withdraw right of entry to information for any component of the collection.
- The data owner should be proficient to append components to the collection.
- No component of the collection should be permitted to withdraw accurate of other elements of the collection or link new clients to the collection.
- The data owner should be intelligent to indicate who has read/write authorizations on the data owner's files.

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

A. Data security

The provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

B. Privacy

The providers should ensure that all critical data are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

C. Data confidentiality

The cloud users want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors.

D. Fine-grained access control

The provider should facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control.

2. DATA BREACHES, LEAKS & HACKS:

Due to Multitenancy environment in cloud breaching the data will become a potential threat. Data breach effects two security properties of data confidentiality, integrity & authenticity. Confidentiality -refers that only authorized parties or systems can access the data and integrity refers that data is not deleted, manipulated or fabricated by some third party who is not authenticated to perform such task. Data breach may occur internally by some data manager who has direct access to the data or from outside by some malicious hacker. However confidentiality and integrity issues are addressed by strong cryptographic mechanism like DES and AES with common PKI infrastructure. In this data and key management become an issue for data owner which can be addressed by combining techniques of attribute based encryption, proxy re-encryption and lazy re encryption.

3. CRYPTOGRAPHIC TECHNIQUES IN THE CLOUD

In general, when user wants to store data securely on an un-trusted storage, he needs a way to encrypt the data and then store keys on secure key store as presented in figure 2. Further, there are a wide range of the encryption schemes and key management approaches that are applicable to a cloud environment. This section provides an overview about the main approaches that can be used to share data securely in the cloud.

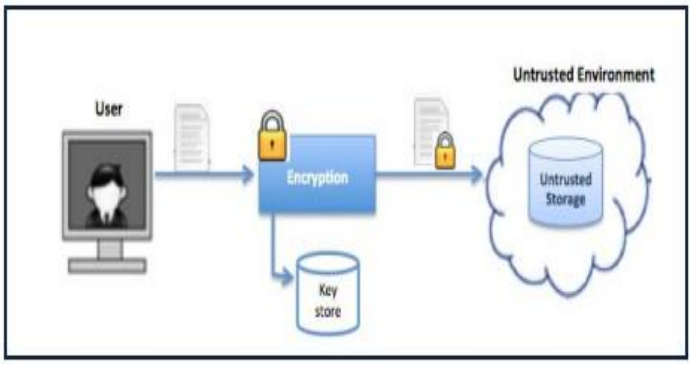

Figure 2: Architecture of secure cloud storage

3.1. IDENTITY-BASED ENCRYPTION

(IBE) helps in public key and certificate management for Public Key Infrastructure (PKI). Outsourcing computation was put into IBE and an IBE scheme in the server-aided setting was proposed. The key generation operations are given to a Key Update Cloud Service Provider and thus only simple operations are left. An analysis of the various encryption techniques used such as homomorphic encryption, searchable and structured encryption, identity-based encryption and signature based encryption yielded the following. IBE is a form of public key cryptography in which a third party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages. This kind of encryption reduces the complexity of the encryption process for both users and administrators. In the Linear Search algorithm, a symmetric encryption algorithm is used to encrypt the plain text. An identity based signature scheme is deterministic if the signature on a message by the same user is always the same. Homomorphic encryption alludes to encryption where plain texts and cipher texts both are treated with an equivalent algebraic function. 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 [2]. 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. A public key encryption with keyword search (PEKS) scheme contains four polynomial time algorithms. In ABE, the attributes and policies of the message and the user decides which user can decrypt a cipher text. A central authority will create secret keys for the users based on attributes/policies for each user.

3.2. ATTRIBUTE-BASED ENCRYPTION

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. Attribute based encryption are of many types. The most common of them being, key attribute-based and cipher text attribute based. A new encryption technique, multi authority hierarchical attribute based encryption [1] is suggested. 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 encrypt 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.

The main difference between these two types of attribute based encryption techniques is that one is dependent on the access policy. In Key policy attribute based encryption, the cipher text is connected with set of attributes and provides data owner with key and policy pair. The message is decrypted if the attribute in the cipher text complies with the key access policy. Cipher text is connected with access policy and is decrypted on satisfaction of the attributes. The suggested technique was tested using NIST Statistical test and it was found that the multi authority hierarchical attribute based encryption ensured most security in data.

3.3. FULLY HOMOMORPHIC ENCRYPTION

Homomorphic encryption ensures privacy of data in communication, storage or in use with tools similar to conventional cryptography, but with extra features of computing over encrypted data, searching an encrypted data, etc. The main disadvantage of traditional encryption techniques is that to manipulate the data, it has to be decoded first. Fully homomorphic encryption (FHE) performs computation with the encrypted data and this is sent. A scheme was devised wherein the calculations can be performed securely in the cloud without the server knowing the content of the data sent or what function needs to be performed. The design used symmetric homomorphic encryption [2] to enhance data security which allowed performing computations on encrypted data without using secret key of client. The encryption used is also symmetric thereby reducing the MIPS rate as well.

Another study on Fully Homomorphic Encryption implemented symmetric key encryption scheme with fully homomorphic evaluation capabilities. A fully homomorphic scheme with symmetric keys [3] was incorporated into an application. Majority of the schemes proposed so far only involved a single party, whereas their scheme ensured multiparty computation.

3.4. CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY

This paper introduced a Certificate less 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 CLPKC 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

3.5. PROXY RE-ENCRYPTION

In this scheme a semi-trusted proxy is used to replace a cipher text that can be decrypted by user A into another cipher text that can be decrypted by user B, without recognizing the original information and user secret keys Therefore, this approach enables the data owner delegates a third party to perform some computational intensive tasks, such as, re- encryption while leaking little part of the information.

4. CONCLUSIONS

Cryptographic techniques in the cloud must enable data protection, availability of the data and sharing of data. Symmetric or asymmetric encryption methods are not alone sufficient for the needs of cloud computing environment. A combination of two or more of the cryptographic techniques will aid in the security of data. This paper has aimed at giving a general overview of the various cryptographic techniques that are being employed for use in the cloud computing environment. The mapping of the threats under the security domains gives an insight onto the domains that need to be made most secure. Securing the domains that are most often used with a strong cryptographic technique, can enable optimized security in the cloud. Future work in this area will include an analysis of these techniques on a cloud computing environment to find the most optimized algorithm which will ensure data security in the cloud.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing (2011).

[2] Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.

[3] R. Manjusha and R.Ramachandran, "Comparative study of attribute based encryption techniques in cloud computing," Embedded Systems (ICES), 2014 International Conference on, pp. 116-120.