Secure Data Sharing in Cloud

Rajesh Ranjan
M.Tech Scholar In Computer Science & Engineering
Mr Anoop Singh ,Associate Professor Sarvepalli
Radhakrishnan University,Bhopal
Madhya Pradesh ,India

***Abstract*–Cloud storage is widely used for sharing data due to low cost maintenance. But, it is also necessary to secure data on cloud. Secure Data Sharing in Cloud focuses mainly on: a) privacy and confidentiality, b) key management and encryption, c) secure data sharing without re-encryption and d) forward and backward access control. When user wants to share data, it sends request to trusted party that generates a symmetric key which is used to encrypt the data for sharing. This key is used to compute two key shares for trusted party and user. The key is deleted using secure overwriting. Its working was formally verified using High Level Petri Nets, SMT Library, and Z3 solver. It was implemented in Visual Studio and its performance was evaluated based on time consumption for various operations which revealed that it has the potential to be effectively used for secure data sharing in cloud.**

Keywords–Cloud computing; data confidentiality; fine-grained access control.

I. INTRODUCTION

The inspiration for the name cloud computing is from the symbol which represents internet in flow chart diagram. 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).

Cloud computing offers significant innovations in virtualization and distributed computing, improves access to high-speed Internet as well and accelerated interest to a weak economy. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the different service-oriented cloud computing models. [1]

A cloud can be private or public. In public, cloud service can be sold to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) In private, cloud act as a proprietary network or hosted services are supplied to limited people through Data Centre. It may be Private or public, the ultimate goal of cloud computing is to provide easy, scalable access to computing resources and IT services. The security requirements in service-oriented cloud computing model are as follows:

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. [9]

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. [9]

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. [8][10]

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. [11]

The effective implementation for the above mentioned security issues would be encrypting data by using certain encryption techniques, which allows flexibility in specifying differential access rights of individual users in a feasible way.

II. KEY-POLICY ATTRIBUTE–BASED ENCRYPTION

In Key-Policy Attribute-Based Encryption (KP-ABE), each ciphertext is labeled by the encryptor with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of ciphertexts the key can decrypt. The scheme is named as Key-Policy Attribute-Based Encryption, since the access structure is specified in the private key, while the ciphertexts are simply labeled with a set of descriptive attributes [12].

An important application of KP-ABE mainly deals with secure forensic analysis. One of the most important needs for electronic forensic analysis is an audit log containing a detailed account of all activity on the system or network to be protected. Such audit logs, however, raise significant security concerns such as a comprehensive audit log would become a prized target for enemy capture. KP-ABE system provides an attractive solution to the audit log problem.

Audit log entries could be annotated with attributes such as, for instance, the name of the user, the date and time of the user action, and the type of data modified or accessed by the user action. Then, a forensic analyst charged with some investigation would be issued a secret key associated with a particular access structure which would correspond to the key allowing for a particular kind of encrypted search; such a key, would only open audit log records whose attributes satisfied certain condition [2]. The drawback in this scheme is the encryptor exerts no control over who has access to the data she encrypts, except by her choice of descriptive attributes for the data [3].

III. CIPHERTEXT-POLICY ATTRIBUTE BASED ENCRYPTION

In CP-ABE schemes attribute policies are associated with data and attributes are associated with keys. Decryption is enabled only those keys which are associated with attributes satisfy the policy associated with the data. The encryptor must be able to smartly decide who should or should not have access to the data that she/he encrypts. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).

The 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, they specify an associated access structure over attributes. A user will only be able to decrypt a ciphertext if that user's attributes pass through the ciphertext's access structure. [3].

CP-ABE [13] users can use all possible combinations of attributes issued in their keys to satisfy policies. This scheme can only support user attributes that are organized logically as a single set. First, this makes it both cumbersome and tedious to capture naturally occurring "compound attributes", i.e., attributes build intuitively from other attributes, and specifying policies using those attributes. The Best and only way to prevent users from combining such attributes in undesirable ways when using current CP-ABE schemes is by appending the attributes as strings. Since the approach has an undesirable consequence, this is a challenging task support policies that involve other combinations of singleton attributes used to build the compound attribute.

CP-ABE schemes that support numerical attributes are limited to assigning only one value to any given numerical attribute within a key. But there are many real world systems where multiple numerical value assignments for a given attribute are common. [4]

IV. CIPHERTEXT-POLICY ATTRIBUTE SET BASED ENCRYPTION

The new form of CP-ABE is Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) which organizes user attributes into a recursive set based structure and allows users to impose dynamic

constraints on how those attributes may be combined to satisfy a policy that can selectively restrict decrypting users to use attributes from within a single set or allow them to combine attributes from multiple sets.

Thus, by grouping user attributes into sets such that those belonging to a single set have no restrictions on how they can be combined, CP-ASBE can support compound attributes without sacrificing the flexibility to easily specify policies involving the underlying singleton attributes. Similarly, multiple numerical assignments for a given attribute can be supported by placing each assignment in a separate set. [4]

V. FUZZY IDENTITY-BASED ENCRYPTION

The Fuzzy Identity-Based Encryption views an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity a, to decrypt a ciphertext encrypted with an identity a', if and only if the identities a and a' are close to each other as measured by the set overlap distance metric. Therefore, the 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. 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 ciphertext encrypted with a slightly different measurement of the same biometric.[14]

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 a simple untrusted storage server instead of relying on trusted server to perform authentication checks before delivering a document. [5]

VI. HIERARCHICAL IDENTITY-BASED ENCRYPTION

IBE sys is a public key system where the public key can be an arbitrary string such as email address. A master key is used by a central authority to issue private keys to identify that request them. HIBE is a generalization of IBE [14] that mirrors an organizational hierarchy. An identity at level k of the hierarchy tree can issue private key to its descendant identifies but cannot decrypt message. It allows a root public key generator to distribute the workload by delegating public key generation and identity authentication to lower-level public key generators. [6]

VII. HIERARCHICAL ATTRIBUTE-BASED ENCRYPTION

Hierarchical attribute-based encryption (HABE) model is the combination of Hierarchical Identity- Based Encryption system (HIBE) and a Ciphertext Policy-Attribute Based Encryption (CP-ABE) system. HASBE focus is to provide fine-grained access control, full delegation and to efficiently share confidential data on cloud servers. The HABE scheme eliminates the on-line inquiry for authenticated attribute public keys [7] .This scheme also includes the drawbacks mentioned in Ciphertext- Policy Attribute Based Encryption. [4]

VIII. HIERARCHICAL ATTRIBUTE-SET-BASED ENCRYPTION

Hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute- set-based encryption (ASBE) with a hierarchical structure of users. It is scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. [8]

The drawback in this scheme is that it applies cryptographic methods by disclosing data decryption keys only to authorize users. 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.

IX. CONCLUSION

This paper contains several encryption schemes for secure sharing of outsourced data in cloud server. From the survey we understand that some amount of work has been done in the field of cloud computing for several security issues. It can be applied to achieve scalable, flexible, security, privacy, data confidentiality and fine-grained access control of outsourced data in cloud computing. The study concludes that the Hierarchical attribute-set-

based encryption is the advanced encryption scheme for outsourcing data in the cloud service provider. On the other hand the techniques and strategies of encryption in cloud computing have to be improved with its distinct characteristics in mind. There is more scope for future research in the field of secure data sharing in the cloud

REFERENCES

[1] M. Nelson, "Building an Open Cloud," Science. vol. 34 no. 5935 pp. 1656–1657, Jun2009.

[2] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[4] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[5] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[6] Yanli Ren and Dawu Gu,"Efficient Hierarchical Identity Based Encryption Scheme in the Standard Model"in Proc. Informatica 32 (2008),pp 207–211.

[7] G.Wang, Q. Liu, and J.Wu, "Hierachical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

[8] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing"in Proc.IEEE Transactions on Information Forensics and Security, vol.7, No.2, April 2012.

[9] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance, O'Reilly Media, Inc., 2009.

[10] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. Communications of the ACM, Volume 53 Issue 4, pages 50-58. April 2010.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.

[12] Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology, Technion , Haifa, Israel, 1996.

[13] L. Cheung and C. Newport. Provably secure ciphertext policy abe. In CCS '07:Proceedings of the 14th ACM conference on Computer and communications security, pages 456–465, New York, NY, USA, 2007. ACM.

[14] 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.