Cyber Times International Journal of Technology & Management

Vol. 11 Issue 2, April 2018 – September 2018

TABLE OF CONTENTS

PRIVACY ENCRYPTION TECHNIQUES FOR CLOUD DATABASE SERVICE: A SURVEY

Shruti Shishir Gosavi
Asst. Prof., Department of Computer Science,
Tilak Maharashtra Vidyapeeth, Pune,
gosavishruti09@gmail.com

ABSTRACT

A user should be able to access data if user possesses a set of credentials or attributes. However if any server is storing the data is being compromised, and then the confidentiality of data will also be compromised. Outsourcing data on cloud may lose access control over users and confidentiality control data. In this paper, we discuss various approaches to address the challenges, existing solutions, and future work needed to provide a truthful cloud computing milieu. This paper presents a survey on privacy preserving schemes and techniques used so far to secure the data when outsourced to the cloud server.

KEYWORDS: *Privacy, Cloud Computing, Database, Attribute based Encryption, Challenges.*

I. INTRODUCTION

Cloud computing has been defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be hastily provisioned and released with least management effort or service provider interaction. This raises privacy and confidentiality concerns because the service providers necessarily has all the data and could accidently or deliberately discloses it or use it for unauthorized purpose. However various privacy issues arise when sore data is outsourced to cloud. The cloud computing paradigm changes the way in which information is handled, especially where personal data processing is concerned.

In recent years cryptographic technique is treated as one of the key technique to solve privacy and security issues related to cloud computing environment.

II. PROBLEM STATEMENT

Preserving privacy of end user and its data is very much important now-a-days. Today there are much more privacy issues when data stored on cloud. Issues such as insufficient user control, disclosure of confidential information, unauthorized secondary storage and many more. The techniques discussed below will solve the issues to a high extent. Below are some security issues discussed from user's as well as from owner's perspective which were stated as challenges in [1][10] while deploying a cloud service.

USER'S PERSPECTIVE

- **How to query the cloud server without revealing query details?**

In this case, by knowing the users sensitive search interest we know the user's query

details & by this we can gradually learn the encrypted database.

- **How to hide the query contents from database owner?**

This happens when a high level executive is qualified to search any value without revealing query to anyone.

- **How to hide query contents while assuring database owner hidden contents are authorized by some certificate authority?**

If the user is FBI, who does not want to reveal the person it is wants to get some confidence by making sure FBI is authorized by court to do this investigation.

DATABASE OWNER'S PERSPECTIVE

- **How to protect outsourced data from theft by hackers?**

Use encryption technique & authenticated access by users.

- **How to protect outsourced data from abuse?**

Before outsourcing, owner should encrypt the database. Those users who have decryption key can download the database & encrypt it & perform querying in situ.

- **How to realize content-level fine grained access control for users?**

In this case, the second challenge does not solve this challenge as it requires variable decryption capabilities for different users.

Ideal solution would be the database owner should issue a given user a key that allows the user to search & decrypt certain records.

III. RESEARCH METHODOLOGY

To confront the above challenges mentioned, we have prepared a survey beneath in which we have discussed diverse types of privacy encryption schemes and algorithms.

Private information retrieval

The PIR [5] allows a user to retrieve a record from database while hiding the identity of the record from a database server. Formally, private information retrieval is a general problem of private retrieving the ith bit out of an n-bit string stored at server. Private means that the server does not know about 'i' i.e. the server does not learn which bit the client is interested.

Private Information Retrieval protocols allow a user to protect his privacy by hiding the identity of database items being retrieved by the user.

Search on Encrypted data

SoE [14] is also known as keyword based retrieval on encrypted data and was introduced by D. Song, etal. They developed a scheme which allowed the ***U*** to store the encrypted data on an untrusted server and then later on server will search for a specific keyword or a plaintext.

Predicate Encryption

This encryption [8][9][12] scheme can be considered as ABE technique that supports attribute hiding. In predicate encryption systems, one can evaluate one or more predicates on encrypted data while all other data about plaintext remains hidden.

In predicate encryption the private key owner can compute a capability that allows one to evaluate predicates on encrypted data.

Identity Based Encryption

In IBE [7], Adi Shamir introduced a new cryptographic scheme by using which users can communicate securely & without using three things:

a) Private or public keys
b) Key directories
c) Services of third party.

It just offers the U with a personalized smart card as he joins the network. The information is stored in the card securely. The Ucan just sign in using the embedded information to encrypt the messages he sends & decrypt the messages he receives independently.

Fuzzy Identity Based Encryption

In this [11] scheme, we can view an identity as set of descriptive attributes. A user with the secret key ω for an identity is able to decrypt a cipher text encrypted with public key ω if an only if ω and ω are within certain distance as judged by some metrics such as "set overlap" distance metrics.

Hierarchical Identity based encryption

This scheme [13] precisely gives security definitions using 2-level HIBE schemes contains private key generation (PKG), domain PKG & users. These are associated with primitive IDs called as PIDs and they are arbitrary strings. It is a concrete two level HIBE scheme and is collusion resistant. In previous IBE[1-IBE], it uses only one private key generator that distributes private keys to user. In 2-HIBE, users retrieve their domain PKG. Domain PKG can compute their private key of any user in their domain as they have previously requested their domain secret key from the root PKG (who possesses master secret).

Attribute Based Encryption

In this [2] system allows user's private key to be expressed in terms of any access formula over attributes. In these systems, encryptor will associate encrypted data with a set of attributes. An authority with access to master keys will issue users different private keys, where a user's private key is associated with an access structure over attributes & reflects the access policy assigned by user. The decryption algorithm allows user to decrypt data using their assigned private keys as long as access policy specified by their private key permits it. The original ABE is somewhat limited in that it only permits an authority to issue private keys that express threshold access policies in which certain number of specified attributes need to be present in the cipher text in order for a user to decrypt it.

ABE was greatly increased by Goyal, etal. By creating ABE in which user's private keys can express any monotone access formula consisting AND, OR or threshold gates.

Ostrovsky, etal. proved this same scheme based on Decisional Bilinear Deffie-Hellman(BDH)assumption.

Key Policy Attribute based Encryption

In this [6] system, cipher text are labeled with set of attributes & private keys are associated with access structures that control which cipher text the user is able to decrypt. This is a new technique to implement fine grained access control. Data stored is stored on the server in an encrypted form while different users are still allowed to decrypt different pieces of data per security policy.

Cipher text Policy Attribute based encryption

In this [3] the system realizes complex access control on encrypted data. By using the technique one can keep confidential encrypted data on an untrusted server. These systems are secured against collusion attacks. In this system, attributes are used to describe user's credentials & a party

encrypting data determines a policy for can decrypt it.

These methods are somewhat similar to the methods used in Role Based Access Policy (RBAC). This is exactly reverse possibility to have user keys are associated with set of attributes, whereas cipher text are associated with policy.

Bounded Cipher text Policy Attribute based Encryption

As compared to original CPABE scheme, the user's private key is associated with set of attributes & encrypted cipher text will specify an access policy over attributes. The user will be able to decrypt if an only if his attributes satisfy the cipher text policy.

Previous CPABE systems supported limited access structure & proof of security was only in generic group model. Whereas in BCPABE [4], the system can support access structure in which they can represent bounded size access tree with threshold gates as its nodes. The bound on the size of access trees is chosen at the time of system setup.

IV. CONCLUSION

Ever-increasing use of handheld devices, cloud system give rise to data confidentiality and data security as critical issues and Attribute Based Encryption is the foremost solution for real world requirements. Attribute Based Encryption schemes are useful in situations where list of users are unknown during the set up. Attribute based encryption scheme started groundwork for encryption and access control issues. Attribute based encryption ensures a fine grained control over decryptors. The benefit of attribute based encryption is its key strength, enabling users to have a stronger encryption, as compared to other encryption schemes. Furthermore, attribute based encryption scheme offers security against collusion attacks.

V. FUTURE SCOPE

Each and every encryption schemes discussed above are different and strong in their field. There are two important concepts required i.e. secret key and cipher text. Both the concepts provide high level security. As a future scope, we can design such a scheme which provides us most secure, scalable and efficient algorithm to increase security and privacy in maintaining data on to the cloud.

REFERENCES

[1] Lu, Yanbin, and Gene Tsudik. "Privacy-preserving cloud database querying." *Journal of Internet Services and Information Security (JISIS)* 1.4 (2011): 5-25.

[2] Ostrovsky, Rafail, Amit Sahai, and Brent Waters. "Attribute-based encryption with non-monotonic access structures." *Proceedings of the 14th ACM conference on Computer and communications security*. 195-203 ACM, 2007.

[3] J. Bethencourt, A. Sahai, and B. Waters. Cipher text-policy attribute-based encryption. *In Proc. of the 2007IEEE Symposium on Security and Privacy (S&P'07), Berkeley, California, USA*, pages 321–334. IEEE, May 2007.

[4] Goyal, Vipul, et al. "Bounded ciphertext policy attribute based encryption."*Automata, Languages and Programming*. Springer Berlin Heidelberg, 2008. 579-591.

[5] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan. Private information retrieval. *Journal of the ACM (JACM)*, 45:965–981, November 1998.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of the 13th ACM Conference on Computer and Communications Security (CCS'06) Alexandria, Virginia, USA*, pages 89–98. ACM, October 2006.

[7] M. Green and S. Hohenberger. Blind Identity-based encryption and simulatable oblivious transfer. In *Proc.of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT'07), Kuching, Malaysia, LNCS*, volume 4833, pages 265–282. Springer-Verlag, December 2007.

[8] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Proc. of the 27th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'08), Istanbul, Turkey, LNCS,*

volume 4965, pages 146–162. Springer-Verlag, 2008.

[9] Shi, Elaine, and Brent Waters. "Delegating capabilities in predicate encryption systems." *Automata, Languages and Programming*. Springer Berlin Heidelberg, 2008. 560-578.

[10] Y. Lu and G. Tsudik. Enhancing data privacy in the cloud. In *Proc. of the 5th IFIP WG 11.11 International Conference on Trust Management (IFIPTM'11), Copenhagen, Denmark, LNCS*, volume 358, pages 117–132.Springer-Verlag, 2011.

[11] Sahai and B. Waters. Fuzzy Identity-based encryption. In *Proc. of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark, LNCS* volume 3494, pages 557–557. Springer-Verlag, May 2005.

[12] E. Shen, E. Shi, and B. Waters. Predicate privacy in encryption systems. In *Proc. of the 6th Conference on Theory of Cryptography (TCC'09), San Francisco, California, USA, LNCS*, volume 5444, pages 457–473.Springer-Verlag, March 2009.

[13] Horwitz, Jeremy, and Ben Lynn. "Toward hierarchical identity-based encryption." *Advances in Cryptology—EUROCRYPT 2002*. Springer Berlin Heidelberg, 2002.