International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 4 (April'2016)

SURVEY ON SECURITY OF BIG DATA OUTSOURCING IN CLOUD

Saurabh Kumar,
B.E Student,
Department of Information Science and Engineering,
New Horizon College of Engineering,
Bangalore, India.

Shahan Sayeed,
B.E Student,
Department of Information Science and Engineering,
New Horizon College of Engineering,
Bangalore, India.

Shariq Hussain,
B.E Student,
Department of Information Science and Engineering,
New Horizon College of Engineering,
Bangalore, India.

Shubham Saraf,
B.E Student,
Department of Information Science and Engineering,
New Horizon College of Engineering,
Bangalore, India.

Divya K V,
Assistant Professor,
Department of Information Science and Engineering,
New Horizon College of Engineering,
Bangalore,India

Abstract: Now a days the number of users in cloud computing are increasing enormously due to its advantage of providing flexible storage requirement. Due to the high volume and velocity of big data, it is an effective option to store big data in the cloud Attribute-Based Encryption (ABE) is a capable technique to ensure the end-to-end security of big data in the cloud. However, the policy updating has always been a challenging issue when ABE is used to construct access control schemes. A trivial implementation is to let data owners retrieve the data and re-encrypt it under the new access policy, and then send it back to the cloud. This method, however, incurs a high communication overhead and heavy computation burden on data owners.

Keywords: Access control, Attribute Based Encryption (ABE), Policy Updating, Outsourcing, Big Data, Cloud

I. INTRODUCTION

Cloud computing is one of the evolving technologies. The cloud computing contains huge open distributed system. It is important to protect the data and privacy of users. Access Control methods ensure that authorized users access the data and the system. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. When hosting big data into the cloud, the data security becomes a major concern as cloud servers cannot be fully trusted by data owners.

Attribute-Based Encryption (ABE) allows end-to-end data security in cloud storage system. It allows data owners to define access policies and allows data encryption under those policies, such that only users whose attributes satisfying these access policies can decrypt the data. When more and more organizations and enterprises outsource data into the cloud, the policy updating becomes a vital issue as data access policies may be changed dynamically and frequently by data owners. However, this policy updating issue has not been considered in existing attribute-based access control schemes.

Major challenges of outsourcing policy updating to the cloud is to guarantee the following requirements:

1) Correctness: Users who owns sufficient attributes should still be able to decrypt the data encrypted under new access policy by running the original decryption algorithm.

2) Completeness: The policy updating method should be able to update any type of access policy.

3) Security: The policy updating should not break the security of the access control system or introduce any new security problems.

Instead of retrieving and re-encrypting the data, data owners only send policy updating query to cloud server, and let cloud server update the policies of encrypted data directly.

The contributions of this survey include:

1) Policy updating problem in ABE systems and develop a new method to outsource the policy updating to the server.

2) Data access control scheme for big data, which enables efficient dynamic policy updating.

3) Policy updating algorithms for different types of access policies, e.g., Boolean Formulas, LSSS Structure and Access Tree.

We surveyed from the base paper that proposes an efficient and secure policy checking method that enables data owners to check whether the ciphertexts have been updated correctly by cloud server. In this method, we do not require any help of data users, and data owners can check the correctness of the ciphertext updating by their own secret keys and checking keys issued by each authority. Our method can also guarantee data owners cannot use their secret keys.

II. LITERATURE SURVEY

Cloud computing, is a kind of Internet-based computing that provides on demand access to shared resources and data to remote computers and other devices. It is a structure for enabling everywhere, on-demand access to a shared group of configurable computing resources (e.g., networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centre. It relies on sharing of resources to achieve consistency and economic of scale, similar to a utility over a network.

A. CLOUD COMPUTNG SECURITY ISSUES

[1] Cloud Computing Security Issues in Infrastructure as a Service, Volume 2, Issue 1, January 2012, IEEE.

1. Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored.

2. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

3. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

4. Legal Issues

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones". On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.

B.ATTRIBUTE BASED ENCRYPTION (ABE)

[2] Attribute-based encryption for fine grained access control of encrypted data, in CCS'06. ACM, 2006.

An attribute based encryption scheme introduced by Sahai and Waters in 2005 and the goal is to provide security and access control. Attribute-based encryption (ABE) is a public-key based one to many encryptions that allows users to encrypt and decrypt data based on user attributes. In which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. Decryption is only possible when the number of matching is at least a threshold value d. Collusion-resistance is crucial security feature of Attribute-Based Encryption. An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system.

1. Key Policy Attribute Based Encryption(KP-ABE)

It is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reflect the access tree Structure, the secret key of the user is defined. Ciphertexts are labelled with sets of attributes and private keys are associated

with monotonic access structures that control which ciphertexts a user is able to decrypt.

Setup: Algorithm takes input K as a security parameter and returns PK as public key and a system master secret key MK.PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

Techniques/ parameter	ABE	KP-ABE	CP-ABE
Fine Grained Access Control	Low	Low, High If There Is Re-encryption Technique	Average Realization Of Complex Access Control
Efficiency	Average	Average, High For Broadcast Type System	Average, Not Efficient For Modern Enterprise Environment
Computational Overhead	High	Most Of Computational Overheads	Average Computational Overheads
Collusion Resistant	Average	Good	Good

Table 1. Comparison of ABE Schemes

Encryption: Algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the ciphertext E.

Key Generation: Algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under a set of attributes if and only if matches T.

Decryption: It takes as input the user's secret key SK for access structure T and the ciphertext E, which was encrypted under the attribute set. This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme. The problem with KP-ABE scheme is the encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, it is unsuitable in some application because a data owner has to trust the key issuer.

2) Cipher Text Policy Attribute Based Encryption

Another modified form of ABE called CP-ABE introduced by Sahai. In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. CP-ABE works in the reverse way of KP-ABE.

The access structure of this scheme or algorithm, it inherits the same method which was used in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data, it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is similar to the traditional access control schemes. The encryptor who specifies the threshold access structure for his interested attributes while encrypting a message. Based on this access structure message is then encrypted such that only those whose attributes satisfy the access structure can decrypt the most existing ABE schemes are derived from the CPABE scheme.

CP-ABE scheme consists of following four algorithms:

Setup: This algorithm takes as input a security parameter K and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

Encrypt: This algorithm takes as input the public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.

Key-Gen: This algorithm takes as input a set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

Decrypt: This algorithm takes as input the ciphertext CT and a secret key SK for an attributes set. It returns the message M if and only if satisfies the access structure associated with the ciphertext CT. It improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt.

III. CONCLUSION

The advancement of cloud computing is dramatically changing the horizon of information technology and ultimately turns the utility computing into a reality. Firstly, this paper presents an introduction to cloud computing and discusses about characteristics of a cloud computing. Secondly focused on the different types of access control such as Discretionary Access control, Mandatory Access Control, Role-Based Access Control and Attribute Based Access Control and also detailed view about the Attribute based encryption. This paper analysed about the policy updating problem in big data access control systems and formulated the challenging requirements like data overload and time consumption of this

IV. REFERENCES

[1] Cloud Computing Security Issues in Infrastructure as a Service, Volume 2, Issue 1, January 2012, IEEE

[2] Kan Yang, XiaohuaJia, KuiRen, "Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud," in IEEE Transactions on Parallel and Distributed Systems, 2014.

[3] V.Goyal, O. Pandey, A.Sahai, and B. Waters, "Attribute-based encryption for fine grained access control of encrypted data," in CCS'06. ACM, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in S&P'07. IEEE, 2007, pp. 321–334.

[5] B.Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in PKC'11. Springer, 2011, pp. 53–70.

[6] A. Beimel, "Secure schemes for secret sharing and key distribution," DSc dissertation, 1996.