ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 6, April 2017

A Survey on Data Access Control Mechanisms in Cloud

Arya Prasad
PG Scholar
Department of Information Technology
Govt.Engineering college
Bartonhill, Trivandrum
aryaprasad2992@gmail.com

Sreedivya R S
Assistant Professor
Department of Information Technology
Govt.Engineering college
Bartonhill, Trivandrum
rssreedivya@gmail.com

Abstract—Cloud computing is one of the emerging technologies that benefits from the processing power and the computing resources of many connected geographically distanced computers via the Internet. It confides remote services with a user's data and software, it enables a user to do a large amount of storage and computations. Due to which data security in the cloud becomes a big issue. To protect the data and privacy of users the access control methods are used, which ensures authorized users to access the data and the system. Suitable security protections are provided for cloud services to avoid higher costs and loss of business due to unauthorized access and threats. This paper describes some of the access control mechanisms used in the cloud.

KEYWORDS— Cloud, security, threats, access mechanisms

I. INTRODUCTION

Cloud computing is the delivery of computing resources such as servers, storage, databases, networking, software etc. over the Internet [1]. It is the result of an evolution of the widespread adoption of virtualization, service-oriented archi-tecture, autonomic, and utility computing. Cloud computing is rapidly becoming the most popular mode of internet applica-tion. More and more enterprises and individuals resort their need of data storage and computing to the clouds. The critical issues met in cloud computing are privacy, trust and access control. Since users are able to access various cloud resources, access control mechanisms are of significant importance in a cloud computing environment. Before outsourcing sensitive data to the cloud for storage a user must enforce any of the data access control mechanisms.

II. THREATS TO DATA SECURITY

In a cloud computing environment, data is stored in the clouds, so the user is no longer in full control of their own private data.

A. The External Threats

The cloud computing users have put a large number of sensitive information into the clouds. The quantity of data processing in the cloud increases every day. Attackers from the network may interact with the cloud system through the Cloud Service Provides to the users. Attackers can make an incursion by using the hardware and software leaks of the cloud computing system. Attackers also may eavesdrop and analyse the users data transmitted through the network.

B. The Internal Attacks

Internal threats are from Cloud service providers (CSP), Customer or Third party organizations supporting the oper-ation of cloud service. They use existing privileges to gain further access or support third parties in executing attacks against confidentiality,integrity and availability of information within cloud service. In public cloud mode, the controls of security technology adopting, implementation of security policy and security system operation are done by CSP. The CSP of public cloud is not trusted for users. They may bypass the user application, view sensitive users' data which stored in the clouds directly, reveal and sell users' privacy. Some of the attackers know some security vulnerabilities exist within the cloud computing system. By using the vulnerabilities they can get the privilege and control of the system and then access to the user data. In addition, human error also may lead to leakage of users' data.

III. EXISTING ACESS CONTROL MECHANISMS

Cloud computing environment is widely distributed and highly dynamic. Static policies will not be efficient for cloud access models. We require access models with dynamic poli-cies. Before uploading to the cloud, the data must be encrypted by using some cryptographic algorithms for protecting the confidentiality.

A. Identity Based Encryption

ID-based encryption was proposed by Adi Shamir in 1984. It is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). A trusted third party, called the Private Key Generator (PKG), generates the private keys. Private Key generator generates a master public key and master private key, where master public key is created by user unique information. The user can decrypt the file by getting the private key with his identity from a private key generator, by using that he can decrypt the file [2]. Private Key generator not only generates the private keys, but also verify the user identities. The main drawback in Identity based encryption is needed to trust the private key generator since it holds all private keys and must remain online.

Advantages:

Reduces the complexity of the encryption process.
No certificates needed.

No pre-enrollment required.

Keys expire, so they don’t need to be revoked. In a traditional public-key system, keys must be revoked if compromised.

Disadvantages:

A secure channel between user and private key generator is required.

PKG need high level of assurance, since it holds all private keys and must remain online.

Encrypted data is decrypted only by one known user, so this lacks advance data sharing.

B. Attribute Based Encryption

An Attribute Based Encryption (ABE) is a public-key based one to many encryptions scheme introduced by Sahai et al.. In this scheme, set of attributes are treated as user identity and its used for encryption and decryption techniques. Trusted agent generates keys for data owner and user. It generates key according to the attributes of the user. In which the secret key of a user and the ciphertext are dependent upon attributes. The decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. Collusion-resistance is crucial security fea-ture 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 [3]. Problem behind in this technique, the data owner need to use the authorized user public key for encryption.Attribute based encryption access policy is classified into two types key policy attributes based encryption and ciphertext policy attributes based encryption.

Advantages:

Reduce the communication overhead.

Provide a fine-grained access control. No pre-enrollment required.

Collusion-resistance is crucial security feature of Attribute Based Encryption

Disadvantages:

The data owner needs to use each authorized user’s public key to encrypt data.

C. Key Policy Based Encryption

It is the modified form of basic ABE model. Users are assigned with an access tree structure over the data attributes. Nodes of the access tree are threshold gates and leaf nodes are the attributes. To reflect the access tree structure the secret key of the user is defined. Ciphertexts are labeled with sets of attributes and private keys are associated with monotonic access structures that control which ciphertexts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is for one-to-many communications. In a key-policy attribute-based encryption (KP-ABE) system, a set of descriptive attributes are used by the sender to label ciphertexts [4]. The trusted attribute authority issues user’s private key, and captures a policy (also called the access structure) that determines which key can decrypt the ciphertexts [4].

Advantages:

Easy to deal with user revocation Key.

Its designed for one-to-many communications. Achieve fine-grained access control.

More flexible to control users than ABE Scheme.

Disadvantages:

The data owner cannot decide who can decrypt the encrypted data. It is not suitable for some applications because data owner has to trust the key issuer.

D. 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 users private key is associated with a set of attributes. A user can decrypt the ciphertext if and only if the attributes in the private key is satisfied the access tree specified in the cipher text. 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 [6]. The encryptor who specifies the threshold access structure for his interested attributes while encrypting a message. Messages are encrypted based on this access structure. Users whose attributes satisfy this access structure are only able to decrypt it. In CP-ABE scheme, attribute management and key distribution are managed by the authority (For example, authority may be registration office in university , Human Resources in company, etc.). The data owner defines the access policy and encrypts the data with access policies. [5] discussed about a method, Sensor network consists of low cost battery powered nodes which is limited in power. Hence power efficient methods are needed for data gathering and aggregation in order to achieve prolonged network life. However, there are several energy efficient routing protocols in the literature; quiet of them are centralized approaches, that is low energy conservation.

Advantages:

The disadvantage of KP-ABE is over come in CP-ABE and it support the access control in the real environment.

Disadvantages:

The user combine all attributes in a single set issued in their keys to satisfy policies.

E. Role Based Encryption

Data owner before storing the data in cloud, first they encrypt the data in local system and then store the encrypted data in the cloud. Data users cannot directly access the data from cloud. All users are assigned with roles and responsi-bility. The roles are assigned based on the responsibilities and qualification. The authenticate users have privileges to access the data with specific roles. The users are assigned with different roles and each of them are having a set of permissions. A role manager responsibility is to assign a role to the user, and if the user is going out, then revoke a role from the user. Cloud Provider, users and others are not able to see the data if they are not assigned with proper roles. Data owner can revoke the role if they found as unauthorized user.

F. Hierarchical Attribute Based Encryption

Hierarchical attribute based encryption is combination of hierarchical identity based encryption (HIBE) and ciphertext policy attribute based encryption (CP-ABE). It supports one-to-many encryption. Encrypted file can be decrypted by a user and all his family members, using their own secret keys. HABE hold the property of hierarchical generation of keys in the HIBE system, and the property of flexible access control in the CP-ABE system. Data owner encrypt the data and send the encrypted data to the cloud. The policy of the data files can be changed by the owner by updating the expiration time. Domain authority provides with the privileges and data owners are controlled by domain authority [7].

Advantages:

Less initial capital investment.

Shorter start-up time for new services.

Lower maintenance cost and operation costs.
Easier disaster recovery.

G. Multi-authority Attribute Based Encryption

V Bozovic et al. introduce Multi-authority Attribute Based Encryption. In this scheme it uses multiple parties to dis-tribute attributes for users. A Multi-authority ABE system is composed of K attribute authorities and one central authority. Multi-authority CP-ABE is more suitable for data access control, multiple authorities issued the attributes to users and using access policy the data owner share the data defined over attributes from different authorities. In this technique, users attributes can be changed dynamically. A user may be designate with new attributes or revoked some current attributes, then data access should be changed accordingly. Each data owner before encrypting the data, they divide the data into different parts and each parts is encrypt with contents keys by using symmetric encryption techniques. Then, from multiple attribute authorities the owner defines the access policies and content keys are encrypted using these policies. Once data are encrypted and its send to cloud server with the ciphertext [8]. The server do have an option to access the data, and the user can decrypt the data if and only if user attributes satisfy the access policy defined in the ciphertext.

Advantages:

Different attribute domains are managed by different authorities.

Expressiveness, efficiency and security are not weaker than that of the single authority.

No authority can independently decrypt any ciphertext. The advantage of the system is that the system provides collusion resistance, the system is more efficient, more robust and provides scalability.

The authorities are working independently of each other. Therefore, the failure or malfunctioning of one authority will not affect the working of other authorities. This improves the robustness of the system.

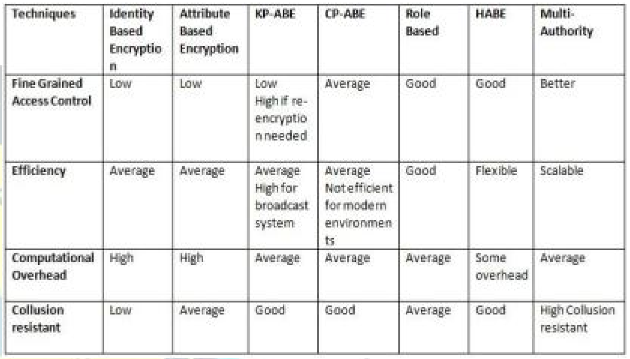
Disadvantages:

The CA can decrypt every ciphertext so that the user privacy and confidentiality of the data is less in this system.

There is overhead involved in managing the distributed authorities.

IV. RESULTS AND COMPARISON

In the bellow table we compare different access control mechanism



Techniques	Identity Based Encryptio n	Attribute Based Encryption	KP-ABE	CP-ABE	Role Based	HABE	Multi-Authority
Fine Grained Access Control	Low	Low	Low High if re-encryptio n needed	Average	Good	Good	Better
Efficiency	Average	Average	Average High for broadcast system	Average Not efficient for modern environmen ts	Good	Flexible	Scalable
Computational Overhead	High	High	Average	Average	Average	Some overhead	Average
Collusion resistant	Low	Average	Good	Good	Average	Good	High Collusion resistant

Fig. 1. Comparison of different mechanism

V. CONCLUSION

The security issue is the biggest barrier when promote and apply the cloud computing technologies on a large scale. In cloud computing the users' data are stored in the clouds, the confidentiality of the data is facing great challenge. Access control is an important mechanism for privacy protection in cloud computing, and it is also an important approach to avoid the data in the clouds being illegally accessed, distorted and used. In this paper we discussed about the survey on access controls Security issues in cloud computing. The existing solutions are role based access control, identification based access control, attribute based access control and hierarchical based access control.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, 2011.

[2] Hongwei Li, Yuanshun Dai1, Ling Tian, "Identity based authentication for cloud computing", Springer-Verlag Berlin Heidelberg, pp 157- 166, 2009.

[3] Bobba, R., Khurana, H., Prabhakarn, M.: Attribute sets a practically Motivated Enhancement to attribute based Encryption, 2009.

[4] Christo Ananth, S.Mathu Muhila, N.Priyadharshini, G.Sudha, P.Venkateswari, H.Vishali, "A New Energy Efficient Routing Scheme for Data Gathering ",International Journal Of Advanced Research Trends In Engineering And Technology (IJARTET), Vol. 2, Issue 10, October 2015), pp: 1-4

[5] Changji wang, Xuan Liu,Wentao Li,"Implementing a Personal Health Record Cloud Platform using Ciphertext-Policy Attribute Based Encryp-tion,International Conferenc e on Intelleigent Networking and Collabo-rative Systems,2012.

[6] Betten Court, J.: Ciphertext-policy attribute based encryption. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 321334, 2007.

[7] Deepthi Adulapuram, ”Hierarchical Attribute Set-Based Encryption”, International Journal of Computer Science and Information Technology and Security IJCSITS, ISSN: 2249-9555,Vol. 3, No.4, August 2013.

[8] Kan Yang, Xiaohua Jia, ”Expressive, Efficient, and Revocable Data Access Control for Multi-Authority cloud Storage”, IEEE Transactions on Parallel and Distributed Systems,Vol,25,No 7, July 2014.