IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Third Party based Model for Security in Cloud Computing Environment

Pragya Pateriya[1], Mr. Anil Panwar[2]

Department of Computer Science & Engineering, IPS, Indore, India[1]

Assistant Professor, Department of Computer Science & Engineering, IPS, Indore, India[2]

Abstract: In this paper we give a survey of third party based model for security in cloud computing environment. Cloud Computing is becoming the heart or the central theme for all sort of computing. Cloud is a remote place, at which user can upload data, can download data, can do processing of data, etc. Cloud provides space, computing power, platform and many more services on rent. This paper presents a brief introduction to the concept of clouds & its services. This paper also presents the issues related to the security of data in cloud environment. A few modern attribute based encryption models for the data security have been discussed.

Keywords: cloud security, third party based model, encryption, decryption method, key generation.

I. INTRODUCTION

Cloud computing is the favorite topic to many researchers. It will become more popular in coming years as the reach of internet is increasing day by day. Cloud computing has three basic models, which are Platform as a Service (PaaS), Infrastructure or Hardware as a Service (IaaS/Haas), Software as a Service (SaaS). The Main advantages of cloud computing are: low cost, improved performance, infinite storage space etc.

Load balancing in cloud computing systems is really a challenge now. A distributed solution is required. As it is not always practically feasible or cost efficient to maintain one or more idle services just as to fulfill the required demands. All jobs can't be assigned to appropriate servers and clients individually for efficient load balancing as cloud is a very complex structure and components are present throughout a wide spread area. The cloud computing holds the promise of providing computing as the fifth utility after the other four utilities water, gas, electricity, and telephone. The major benefits of cloud computing include reduced costs and capital expenditures, the increased operational efficiencies, high scalability, flexibility and so on. There are many service-oriented cloud computing models have been proposed. It includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

II. LITERATURE SURVEY

Sahni and ater introduced the public-key cryptography attribute based encryption (ABE) for cryptographically enforced access control. In ABE both the user secret key and the ciphertext are associated with a set of attributes. A user is able to decrypt the ciphertext if and only if at least a threshold number of attributes overlap between the ciphertext and user secret key. Different from traditional publickey cryptography such as Identity-Based Encryption [3], ABE is intended for one-tomany encryption in which ciphertexts are not necessarily encrypted to one particular user.

In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. To enable more general access control, Goyal et al. [4,5] proposed a key-policy attribute-based encryption (KP-ABE) scheme – a variant of ABE.

The idea of a KP-ABE scheme is as follows: the ciphertext is associated with a set of attributes and each user secret key is embedded with an access structure which can be any monotonic tree access structure. A user is able to decrypt a ciphertext if and only if the ciphertext attributes satisfy the access structure embedded in her secret key. In the same work, Goyal et al. introduced the concept of another variant of ABE – ciphertext policy attribute-based encryption (CP-ABE). CP-ABE works in the reverse way of KP-ABE in the sense that in CP-ABE the ciphertext is associated with an access structure and each user secret key is embedded with a set of attributes.

Formally, KP-ABE and CP-ABE can be defined as follows.

Key-Policy Attribute-Based Encryption A KP-ABE scheme consists of the following four algorithms.

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

Encryption This algorithm takes a message , the public key , and a set of attributes as input. It outputs the ciphertext .

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

Decryption It takes as input the user's secret key for access structure and the ciphertext , which was encrypted under the attribute set . This algorithm outputs the message if and only if the attribute set satisfies the user's access structure .

Ciphertext-Policy Attribute-Based Encryption A CP-ABE scheme also consists of four algorithms:

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

Encrypt This algorithm takes as input the public parameter, a message , and an access structure . It outputs the cihphertext .

KeyGen This algorithm takes as input a set of attributes associated with the user and the master secret key . It outputs a secret key that enables the user to decrypt a message encrypted under an access structure if and only if matches .

Decrypt This algorithm takes as input the ciphertext and a secret key for an attributes set . It returns the message if and only if satisfies the access structure associated with the ciphertext .

In ABE, including KP-ABE and CP-ABE, the authority runs the algorithm Setup and Key Generation to generate system , , and user secret keys. Any user knowing the system public key is able to encrypt data by calling the algorithm Encryption. Only authorized users (i.e., users with intended access structures) are able to decrypt by calling the algorithm Decryption. In this dissertation, we just consider the case of one-writer-and-multiple-reader in untrusted storage for brevity. The only writer is the data owner, who also acts as the authority and is in charge of key generation. This means that the data owner takes the role of both the authority and the encryptor. In the following part of this dissertation, we will alternative call this party by "authority" or "data owner". The decryptor will be called as "data consumer", or just "user" for brevity.

III.CONCLUSION

Cloud is mostly used for storing data & processing the data. Many organizations have critical data, which is required to be kept confidential from the outside world. So the security of data is a burning issue in cloud environment. In this paper, the security issues have been discussed. A good number of existing cloud security model have also been reviewed.

REFERENCES

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25, pp. 599–616, 2009.

[2] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.

[3] D. Boneh and M. Franklin. Identity-Based Encryption from The Weil Pairing. In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.

[4] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2006.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data. In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.