International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

SURVEY ON CONTROLLED ACCESS USING ATTRIBUTE BASED ENCRYPTION IN CLOUD COMPUTING

Shubha G L, Sunil G L

PG student, Dept. of CSE, Acharya Institute of technology, Karnataka, India
Professor, Dept. of CSE, Acharya Institute of technology, Karnataka, India

---

Abstract - *For distributed computing the access control framework is presented which is called as fine grained two-variable validation framework (2FA). In particular, one needs both secret key and lightweight security device to execute the access control system. To access the security of the framework the user must hold both of them. In case where client could not access the framework in the absence of both secret key and security device, the instrument will improve the framework security only in situations where multiple clients have single PC for cloud administration online. Similarly framework enables cloud server to restrict those clients with same set of properties for client protection i.e., it satisfies client predicate where there is no clue for personality of the client.*

Key Words*: *validation, fine grained, access control (AC), framework

1. INTRODUCTION

For web based services, new fined-grained [9] (2FA) access control has been introduced here. Both secret key and security devices is implemented by the mechanism of attribute-based system (ABS) in 2FA [6]. As a client do not hold both of them he cannot access the system, for this the security is required to those where many clients will share the computer for cloud service. To maintain the privacy of the client the attribute-based control also enables the cloud to restrict the access to the client with similar set of attributes, which means that only the user fulfillment for predicates is known to cloud server without knowing users exact identity.

The attribute based encryption (ABE) is a public key where user's secret key and its ciphertext are attribute dependent. The ciphertext decryption is possible where the set of secret key attributes is being matched with the set of ciphertext attributes. A crucial security of ABE is the collision resistance where many number of keys unable to access the data with single key to grant the access.

To split the user secret key the user will accomplish the ordinary ABS. Here one section is inserted into security gadget and another section is given in the hands of client. Extraordinary consideration are made in process, as ABS [10] will not ensure the part that is spillage of the secret key where security of the plan is not influenced.

The cloud uses multiple encryption techniques here we use two of them they are a) ABE is a kind of public key wherein user's secret key and ciphertext are attribute dependent. In ABE the client has the unique set of identity attributes. b) CP-ABE is support AND gate to negative and positive attributes as the policy for access and it also proved under standard model as secure.

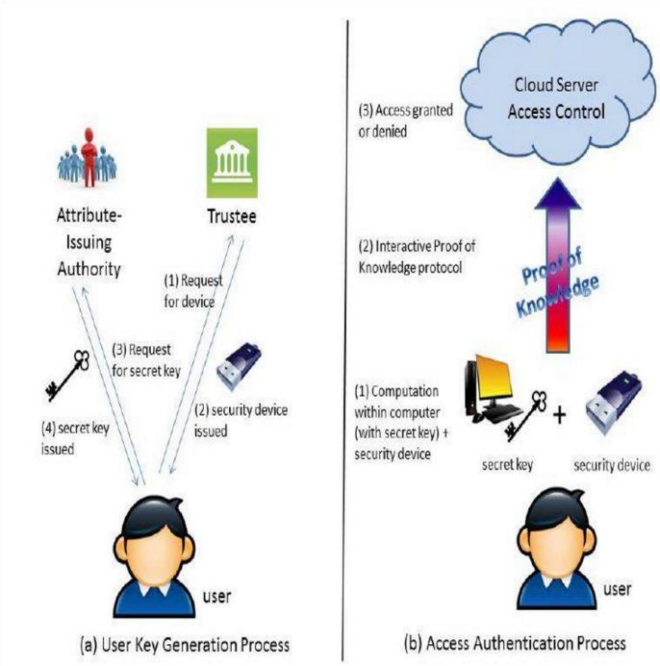

Figure 1.1: Overview of system architecture

In this architecture it has two process a) User-key generation has two models known has trustee n attribute issuing authority. In this process trustee receives the request from client for a device, where the device is verified by trustee and issues the device to the client. Later on client request for secret key to the attribute authority, authority will verify and issue secret key to the client.

b) Access authentication is used to authenticate the process where the user has both the security device and secret key by using which the client will access the information from the cloud server.

2. RELATED WORK

Rashmi, Dr.G.Sahoo2, Dr.S.Mehfuz3, [1] "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", this paper mainly refers to the security solution on cloud computing using Software as a service model for describing security challenges on cloud.

KashifMunir and Prof Dr. SellapanPalaniappan, [2] presented framework for secure cloud computing. In this paper a framework being designed that identifies cloud computing security challenges from which a solution is referred for security challenges. This also proposed a framework and a model for secure cloud computing environment which identifies attacks, security requirements, threats, concerns for cloud deployment.

Mr. AnkushKudale, Dr. Binod Kumar, [3] proposed a study on authentication and access control for cloud computing. In this paper, security issues has the solutions because many of the organization has adopted in cloud computing services. It also referred solution for authentication and access control and also it tells about solution for security issues.

Harvinder Singh1, Amandeep Kaur2, [4] presented access control model for cloud platforms using multi-tier graphical authentication. In the paper, scheme has been examined under different situations. Graphical password has assessed with different combination of password. Multi-level graphical password has taken a secure outline platform for cloud. Here the model has greater enhancement with number of functionalities and advance level of security validation, it is implemented by using security for login, questions are made for security and last User identification number can be access the data in cloud services on computers and mobile plans.

Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo , and Jianying Zhou,[5] proposed k-times attribute-based anonymous access control for cloud computing ,this paper supports the cloud environment. The notation permits client to validate him /her anonymously for cloud server. Here k-times provides the anonymous access for the cloud i.e., it means server restrict precise set of client to access the maximum k-times for a event. For new notation it provides a security model and concrete instantiation and also gives security proof. The attribute-based mechanism can be observed in the form of attribute based signature.

3. ENCRYPTION MECHANISMS

Attribute based encryption (ABE): It is a kind of public-key, enables client to encrypt and attributes to decrypt the data. In ABE application the encrypted data is kept in cloud, using ciphertext access policies and key attributes.

The advantages of ABE is operation involves costly pairings and high complexity of policies to be accessed. In this paper, the informally, verification, validation are check by the user and the user also viewed the transformation of the system.

There are two types of ABE schemes they are a) KP-ABE

b) CP-ABE

In KP-ABE, the private key attribute is linked with access policy. The encryptor does not know who will decrypt the data. To trust the issuer of the key there is only choice to choose descriptive data of attributes. For certain application the KP-ABE [8] is not suitable but it support the secret key in encryption scheme.

The KP-ABE gives access to fine grained but it not suitable for scalability and flexibility .To overcome this problem we use CP-ABE scheme

In this paper CP-ABE [7] where the attribute of the cyphertext is associated with access policy and the private key of the user is allied with attribute set.

The decryption of cyphertext is possible only if attribute set is allied with private key which fulfills the policy that is linked with cyphertext. CP-ABE is support AND gate to negative and positive attributes as the policy for access and it also proved under standard model as secure.

In CP-ABE the user is allied with the attribute set where the secret key is also dependent on it. For encrypting a data, the attributes will identifies the encryptor threshold structure. Where the attribute fulfill the structure so that the data can be decrypt.

CP-ABE technique, the encrypted data is retained secure and stable against attacks

Summary of Comparative Analysis

PARAMETERS	KP-ABE	CP-ABE
Fine-Grained AC	Low, sometimes high	Average
Efficiency	Average	Average
Overhead	High	Average
Collision Resistance	Good	Good

4. CONCLUSION

In this paper, for distributed computing the access control framework is presented which is called as fine grained two-variable validation framework (2FA). This framework enables cloud server to restrict those clients with same set of properties for client protection, moreover to give power

cloud server have same arrangement which is been recognized by 2FA access control system. Examining security precisely demonstrates that 2FA framework for access control accomplishes security prerequisites. This paper also surveys on attribute based encryption and about the control of access using security devices. Two schemes detailed for attribute based encryption named KP-ABE and CP-ABE where CP-ABE proved to be more effective .The development made more "probable" along with the execution assessment, however much of future work could be done on its enhancement.

REFERENCES

[1] Rashmi , Dr.G.Sahoo2, Dr.S.Mehfuz3, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", IJCCSA , Vol.3, No.4, August 2013.

[2] KashifMunir and Prof Dr.SellapanPalaniappan," Framework For Secure Cloud Computing", IJCCSA, Vol.3, No.2, April 2013.

[3] Mr. AnkushKudale, Dr. Binod Kumar," A Study On Authentication And Access Control For Cloud Computing", Vol. 1(2), July 2014 (ISSN: 2321-8088).

[4] Harvinder Singh1, Amandeep Kaur2," Access Control Model for Cloud Platforms Using Multi-Tier Graphical Authentication", Volume 4 Issue 11, November 2015.

[5] Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou," k-times attribute-based anonymous access control for cloud computing", IEEE Transactions on Computers, 64 (9), 2595-2608.

[6] Joseph K. Liu, Man Ho Au*, Xinyi Huang, Rongxing Lu, Jin Li," Fine-grained Two-factor Access Control for Web-based Cloud Computing Services", IEEE Transaction on forensic and security,TIFS.2015

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp.Secur. Privacy, May 2007, pp. 321–334.

[8] Parmar Vipul Kumar J[a]. RajaniKanth Aluvalu[b] ," Key Policy Attribute Based Encryption (KP-ABE): A Review", volume2,issue2,2015

[9] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, 2004

[10] Yongdong Wu, Zhuo Wei, and Robert H. Deng," Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks", IEEE Transaction, Volume 15,no 4,2013