Volume 5, Issue 2, April 2018 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

An Attribute-Based Access Control Web Based Mechanism in Cloud Computing Services

D Srilakshmi
PG Scholar,
DNR College of Engineering & Technology
Bhimavaram (A.P.) [INDIA]
Email: siridenduluri44@gmail.com

M C S Varma
Assistant Professor
Department of Computer Science and Engineering
DNR College of Engineering & Technology
Bhimavaram (A.P.) [INDIA]
Email: mcsvarma@gmail.com

DDD Suribabu
Head & Associate Professor
Department of Computer Science and Engineering
DNR College of Engineering &Technology
Bhimavaram (A.P.) [INDIA]
Email: dnr.csehod@gmail.com

ABSTRACT

In this paper, we introduce a new fine-grained two factor authentication (2FA) access control system for web based cloud computing services Specifically, in our proposed 2FA access control system, an attribute based access control mechanism is implemented with the necessity of both a user secret key and alight weight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

Keywords:—*Fine-grained, two-factor, access control, Web services.*

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private First, the traditional account/password based authentication is not privacy preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems. Second, it is common to share a computer among different people. It may be easy for hackers to install some spy ware to learn the login password from the web browser. A recently proposed access control model called *attribute-based access control* is a good candidate to tackle the first problem. It not only provides anonymous authentication but also further defines access control policies based on different attributes of the requester, environment, or the data object. In an attribute-based access control system, each user has a user secret key issued by the authority. In practice, the user secret key is stored inside the personal computer. When we consider the above mentioned second problem on web-based services, it is common that computers may be shared by many users especially in some large enterprises or

organizations. For example, let us consider the following two scenarios:

In a hospital, computers are shared by different staff. Dr. Alice uses the computer in room A when she is on duty in the daytime, while Dr. Bob uses the same computer in the same room when he is on duty at night.

In a university, computers in the undergraduate lab are usually shared by different students. In these cases, user secret keys could be easily stolen or used by an unauthorized party. Even though the computer may be locked by a password, it can still be possibly guessed or stolen by un detected malwares.

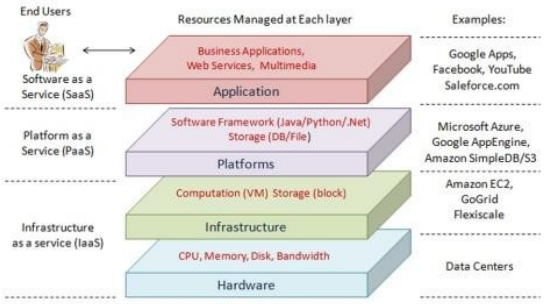

Figure 1: Cloud Architecture.

A more secure way is to use two-factor authentica-tion(2FA). 2FA is very common among web-based-banking services. In addition to a username/password, the user is also required to have a device to display a one-time password. Some systems may require the user to have a mobile phone while the onetime password will be sent to the mobile phone through SMS during the log in process. By using 2FA, users will have more confidence to use shared computers to login for web based banking services. For the same reason, it will be better to have a 2FA system for users in the web based cloud services in order to increase the security level in the system.

II. OBJECTIVE

In this paper, we propose a fine-grained two-factor access control protocol for web based cloud computing services, using a light weight security device. The device has the following properties: (1) it can compute some light weight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is assumed that no one can break in to it to get the secret information stored inside.

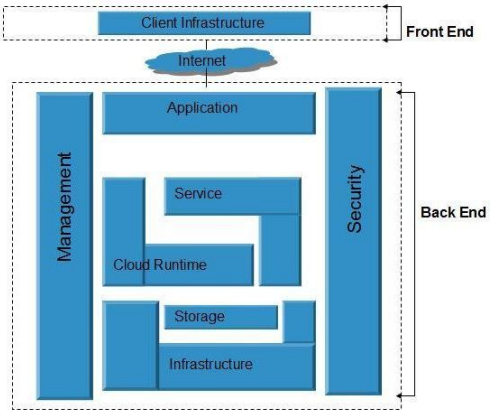

Figure 2: Security Views and Management

With this device, our protocol provides a 2FA security. First the user secret key (which is usually stored inside the computer) is required. In addition, the security device should be also connected to the computer (e.g. through USB) in order to authenticate the user for accessing the cloud. The user can be granted access only if he has both items. Further more, the user cannot use his secret key with another device belonging to others for the access.

Our protocol supports fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user. To show the practicality of our system, we simulate the prototype of the protocol.

III. PROPOSAL

Attribute. Based encryption (ABE) is the corner stone of attribute-based cryptosystem. ABE enables fine-grained access control over encrypted data using access policies and

associates attributes with private keys and cipher texts. With in this context, cipher text-policy ABE(CP-ABE) allows as cal able way of data encryption such that the encrypt or defines the access policy that the decryptor (and his/heart tributes set) needs to satisfy to decrypt

The cipher text. Thus, different users are allowed to decrypt different pieces of data with respect to the pre defined policy. This can eliminate the trust on the storage server to prevent unauthorized data access.

Besides dealing with authenticated access on encrypted data in cloud storage service, ABE can also be used for access control to cloud computing service, in a similar way as an encryption scheme can be used for authentication purpose: The cloud server may encrypt a random message using the access policy and ask the user to decrypt. If the user can successfully decrypt the ciphertext (which means the user's attributes set satisfies the prescribed policy), then it is allowed to access the cloud computing service.

In addition to ABE, another cryptographic primitive in attribute-based cryptosystem is attribute-based signature (ABS). An ABS scheme enables a user to signames sage with fine grained control over identifying information. Specifically, in an ABS scheme, users obtain their attribute private keys from an attribute authority. Then they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that the signer's attributes satisfy the signing predicate if the signature is valid. At the same time, the identity of signer remains hidden. Thus it can achieve anonymous attribute-based access control efficiently. Recently, Yuen*etal.* proposed an attribute based access control mechanism which can be regarded as the interactive form of ABS.

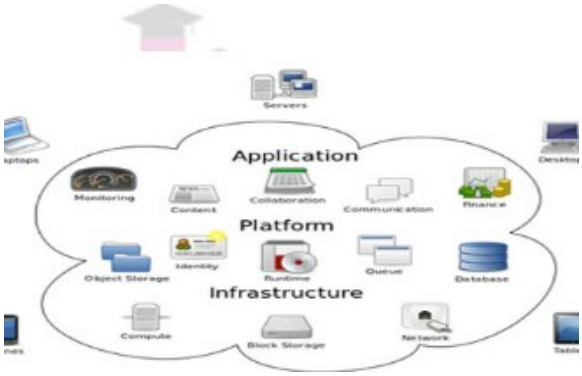

Figure 3: Fine Grained Mechanism

B. Access Control With Security Device

1. ***Security Mediated Crypto System:*** Mediated cryptography was first introduced in a same thod to allow immediate revocation of public keys. The basic idea of mediated cryptography is to use a non line media tor for every transaction. This online mediator is referred to a SEM (Security Mediator) since it provides a control of security capabilities. If the SEM does not cooperate then no transactions with the public key are possible any longer. Recently, an attribute-based version of SEM was proposed in The notion of SEM cryptography was further modified as security mediated certificate less (SMC) cryptography. In a SMC system, a user has a secret key, public key and an identity. In the signing or decryption algorithm, it requires the secret key and the SEM together. In the signature verification or encryption algorithm, it requires the user public key and the corresponding identity. Since the SEM is controlled by an authority which is used to handle user revocation, the authority refuses to provide any cooperation for any revoked user. Thus revoked users cannot generate signature or decrypt cipher text.

   Note that SMC is different from our concept. The main purpose of SMC is to

solve there vocation problem. Thus the SME is controlled by the authority. In other words, the authority needs to be *online* for every signature signing and ciphertext decryption. The user is not anonymous in SMC. While in our system, the security device is controlled by the user. Anonymity is also preserved.

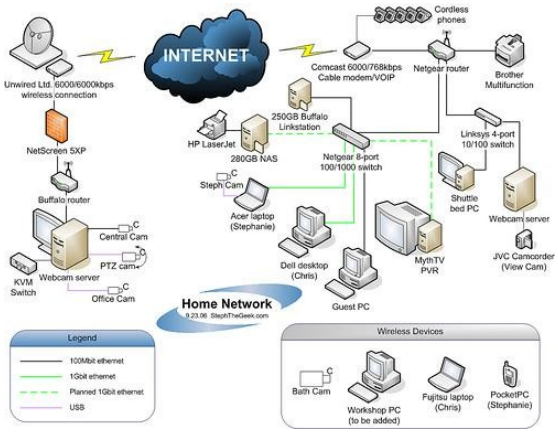

Figure 4:General idea of key and information transmission in cloud.

2. ***Key-Insulated Crypto system:*** The paradigm of key-insulated cryptography was introduced in the general idea of key -insulated security was to store long term keys in a physically secure but computationally limited device. Short-term secret keys are kept by users on a powerful but insecure device where cryptographic computations take place. Short term secrets are then refreshed at discrete time periods via interaction between the user and the base while the public key remains unchanged through out the lifetime of the system. At the beginning of each time period, the user obtains a partial secret key from the device. By combining this partial secret key with the secret key for the previous period, the user renews the secret key for the current time period.

IV. CONCLUSIONS

In this paper we present the fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a light weight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web based cloud services. In addition, attribute based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

REFERENCES:

[1] M. H. Au and A. Kapadia, "PERM: Practical reputation-based blacklisting without TTPS," in Proc. ACM Conference Computer Communication Security (CCS), Raleigh, NC, USA, Oct. 2012, pp.929 –940.

[2] M. H. Au, A. Kapadia, and W. Susilo, "BLACR : TTP-free blacklist able an onymouscredentials with reputation," in Proc. 19th NDSS, 2012, pp.1–17.

[3] M. H. Au, W. Susilo, and Y. Mu, "Constant-sized ynamick- TAA," in Proc. 5th International Conference. SCN, 2006, pp.111–125.

[4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based frame work for big data in formation management of smart grid," IEEE Trans. Cloud Computing., vol.3, no. 2, pp.233–244, Apr./Jun.2015.

[5] M. Bellare and O. Goldreich, "On defining proofs of knowledge," in Proc. 12th Annu. Int. CRYPTO, 1992, pp.390–420.

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

[7] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology. Berlin, Germany: Springer- Verlag, 2004, pp.41–55.

[8] 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.

[9] J. Camenisch, "Group signature scheme sand payment systems based on the discrete logarithm problem," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1998.

[10] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in Proc. 16th ACM Conference Computer Communication Security (CCS), Chicago, IL, USA, Nov.2009, pp.131–140.

[11] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in Proc. 3rd International Conference Security Communication. Network (SCN), Amalfi, Italy, Sep. 2002, pp.268–289.

[12] J.Camenisch and A. Lysyanskaya, "Signature schemes and anonymouscredentials from bilinear maps," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 56–72.

[13] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator," in Proc. ICICS, 2014, pp. 274–289.

[14] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security-mediated certificate less cryptography," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp.508–524.

[15] C.- K. Chu, W.- T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concern sin popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

* * * * *