Fine-grained Two-factor Access Control for Web-based Cloud Computing Services

Kishore R[1] , Dr. G T Raju[2]

[1]Department of Computer Science, 4th Semester MTech, RNS Institute of Technology, Bengaluru, India
Professor, [2]Department of Computer Science, RNS Institute of Technology, Bengaluru, India

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 user secret key and a lightweight security device. As a user cannot access the system if s/he does 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.

Key Words: *Fine-grained, Two-Factor, Access Control, Web Services.*

1. INTRODUCTION

Cloud computing is a virtual host computer system that enables enterprises to buy, lease, sell, or distribute software and other digital resources over the internet as an on-demand service. It no longer depends on a server or a number of machines that physically exist, as it is a virtual system. There are many applications of cloud computing, such as data sharing data storage[1], big data management[2] medical information system etc. End users access cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. The benefits of web-based cloud computing services are huge, which include the ease of accessibility, reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility and immediate time to market.

Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy especially for web based cloud services. As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may also access the cloud system for various applications and services, user authentication has become a critical component for any cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are two problems for the traditional account/password based system. First, the traditional account/password based authentication is not privacy-preserving. However, it is well acknowledged that privacy is an essential feature and that must be considered here in the cloud computing systems. Second, it is common to share a computer among different people. It may be easy for hackers to install some spyware 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 system1, 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 undetected malwares.

A more secure way is to use two-factor authentication (2FA). 2FA is very common among web-based e-banking services. In addition to a username/password, the user is also required to have a device to display a onetime password. Some systems may require the user to have a mobile phone while the one-time password will be sent to the mobile phone through SMS during the login process. By using 2FA, users will have more confidence to use shared computers to login for web based e-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.

1.1 Our Contribution

In this paper, we propose a fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the following properties:

(1) it can compute some lightweight algorithms, e.g. hashing and exponentiation

(2) it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside. 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. Furthermore, 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. In the next section, we will review some related works that are related to our concept.

2. RELATED WORK

We review some related works including attribute-based cryptosystems and access control with security device in this section.

2.1 Attribute-Based Cryptosystem

Attribute-based encryption (ABE) is the cornerstone of attribute-based cryptosystem. ABE enables fine grained access control over encrypted data using access policies and associates attributes with private keys and ciphertexts.

Within this context, cipher text-policy ABE (CP-ABE)[2]allows a scalable way of data encryption such that the encryptor defines the access policy that the decryptor (and his/her attributes 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 [4][5],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 cipher text (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 sign a message 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 et al. [6] proposed an attribute-based access control mechanism which can be regarded as the interactive form of ABS.

2.2 Access Control with Security Device

Security Mediated Cryptosystem

Mediated cryptography was first introduced in [7] as a method to allow immediate revocation of public keys. The basic idea of mediated cryptography is to use an on-line mediator for every transaction. This on-line 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[8].

The notion of SEM cryptography was further modified as security mediated certificateless (SMC) cryptography[9],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 the revocation problem. Thus the SME is controlled by the authority. In other words, the authority needs to be online for every signature signing and cipher text decryption. The user is not anonymous in SMC. While in our system, the security device is controlled by the user. Anonymity is also preserved.

Key-Insulated Cryptosystem

The paradigm of key-insulated cryptography was introduced in [10]. 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 throughout 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. Different from our concept, key-insulated cryptosystem requires all users to update their keys in every time period. The key update process requires the security device. Once the key has been updated, the signing or decryption algorithm does not require the device any more within the same time period. While our concept does require the security device every time the user tries to access the system. Furthermore, there is no key updating required in our system.

3. PROPOSED SYSTEM

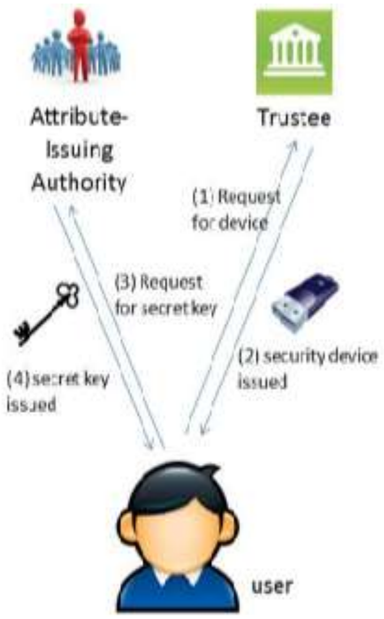
Attribute-Issuing Authority
Trustee
(1) Request for device
(3) Request for secret key
(2) security device issued
(4) secret key issued
user

Figure 1 User Key Generation Process

Figure1 shows the user key generation process,firstly the user has to request for device from the trustee if the attributes matches the requirements then the trustee will issue the security device it will be the first level of access to download a file in the cloud and next user has to request for secret key from the attribute issuing authority,if the attributes matches with the requirements then the attribute issuing authority will issue the secret key it will be the second level of access.

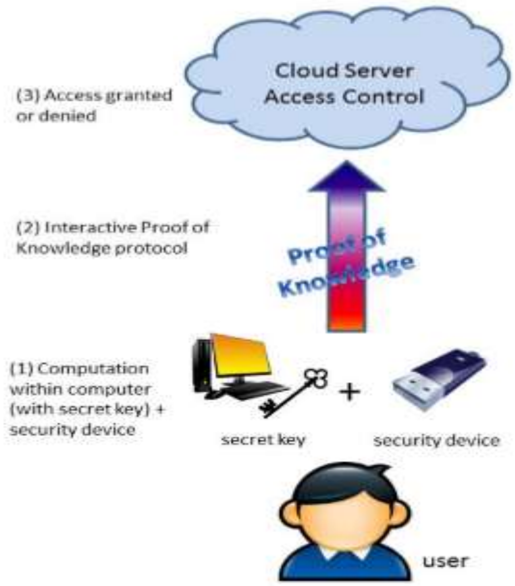

Figure 2 User Access Authentication Process

A naive thinking to achieve our goal is to use a normal ABS and simply split the user secret key into two parts. One part is kept by the user (stored in the computer) while another part is initialized into the security device. Special care must be taken in the process since normal ABS does not guarantee that the leakage of part of the secret key does not affect the security of the schemewhile in two 2FA, the attacker could have compromised one of the factors. Besides, the splitting should be done in such a way that most of the computation load should be with the user's computer since the security device is not supposed to be powerful.We specifically design our system in another manner. We do not split the secret key into two parts. Instead, we introduce some additional unique information stored in the security device. The authentication process requires this piece of information together with the user secret key.

3.1 Entities

Our system consists of the following entities:

- **Trustee**: It is responsible for generating all system parameters and initializes the security device.

- **Attribute-issuing Authority**: It is responsible to generate user secret key for each user according to their attributes.

- **User**: It is the player that makes authentication with the cloud server. Each user has a secret key issued by the attribute-issuing authority and a security device initialized by the trustee.

- **Cloud Service Provider**: It provides services to anonymous authorized users. It interacts with the user during the authentication process.

4. CONCLUSION

In this paper, we have presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements

5. ACKNOWLEDGMENT

I would like to thank my parents for their constant support and motivation and my internal guide Prof. G T Raju, Department of Computer Science at RNS Institute of Technology for their guidance in successfully undertaking the project. I would also like to thank our beloved Dr. G T Raju, who is the professor, dean and HOD of Department of Computer Science for the encouragement and support. Finally I would also like to thank my teaching and non-teaching staff for providing us wonderful teaching and all the necessary support.

6. REFERENCES

[1] C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J.zhour Security concerns in popular cloud storage services. IEEE Pervasive Computing, 12(4):50–57, 2013.

[2] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A Secure cloud computing based framework for big data information management of smart grid. IEEE T. Cloud Computing, 3(2):233–244, 2015.

[3] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.

[4] J Han, W. Susilo, Y. Mu, and J. Yan. Privacy-preserving decentralized key-policy attribute-based encryption. IEEE Trans. Parallel Distrib. Syst., 23(11):2150–2162, 2012.

[5] [5] JHur. Attribute-based secure data sharing with hidden Policies in smart grid.IEEE Trans. Parallel Distrib. Syst., 24(11):2171–2180, 2013.

[6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, J. Zhou. k-times attribute-based anonymous access control for cloud computing. IEEE Trans. Computers, 64(9):2595–2608, 2015.

[7] D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techno., 4(1):60–82, 2004.

[8] Y. Chen, Z. L. Jiang, S. Yiu, J. K. Liu, M. H. Au, and X. wang. Fully secure ciphertext-policy attribute based encryption with security mediator. In ICICS ‘14, volume 8958 of Lecture Notes in Computer Science, pages 274–289. Springer, 2014.

[9] S. S. M. Chow, C. Boyd, and J. M. G. Nieto. Security-mediatedcertificateless cryptography. In Public Key Cryptography, volume 3958 of Lecture Notes in Computer Science, pages 508–524. Springer, 2006.

[10] Y. Dodis, J. Katz, S. Xu, and M. Yung. Key-insulated public key cryptosystem.In EUROCRYPT,vol:2332 of Lecture Notes in CSE, pages65–82.Springer,2002.