Journal of Engineering Sciences
Vol 11, Issue 1, JAN/2020
ISSN NO:0377-9254

CONSISTING CONTROL ORGANIZE THE EXACT COMPONENTS OF CLOUD COMPUTING WEB SERVICES

A.Navya[1], Dr.Ch.Srihari[2], Dr.A Satyanarayana[3]

[1]M.Tech Student, Dept of CSE, Siddhartha Institute of Technology & Sciences, Hyderabad, T.S, India

[2] Associate Professor, Dept of CSE, Siddhartha Institute of Technology & Sciences, Hyderabad, T.S, India

[3] Assistant Professor, Dept of CSE HOD, Siddhartha Institute of Technology & Sciences, Hyderabad, T.S, India

ABSTRACT:

Introducing a new system to monitor access to two-factor authentication for web-based cloud computing services. Specifically, in our proposed access control system, the attribute-based access control mechanism is implemented with the user's secret key and a lightweight security device is required. Since the user cannot access the system if not maintained, the mechanism can improve system security, especially in those scenarios in which many users share the same computer for web-based cloud services. In addition, the function-based system control also allows the cloud server to also restrict access to those users with the same set of functions while maintaining user privacy, that is, the cloud server only knows that the user meets the required prediction, but has no idea of the exact user identity. Finally, we are also simulating to show the applicability of the proposed system.

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

1. INTRODUCTION:

Cloud Computing is a virtual host computer system that allows organizations to buy, rent, sell or distribute software and other digital resources through the Internet as an on-demand service. It no longer depends on a server or a number of physically present devices, since it is a virtual system. There are many cloud computing applications, such as data exchange [3], [5], [6], data storage [2], [4], big data management [1], the system of medical information. End users access cloud-based applications through a web browser, a thin application or a mobile application, while commercial programs and user data are stored on servers in a remote location. The benefits of web-based cloud computing services are enormous, including ease of access, reduced costs and capital expenditures, greater operational efficiency, scalability, flexibility and immediate marketing time. Although the new cloud computing model offers great benefits, there are also security and privacy issues, especially for web-based cloud services. Confidential data can also be stored in the cloud for exchange or convenient access purposes; Qualified users can also access the system in the cloud for many applications and services, user authentication has become an important component of any system in the cloud. The user must log in before using the services in the cloud or access confidential data stored in the cloud. There are two problems with the traditional account / password system. First, traditional authentication based on the account / password does not depend on privacy. However, it is recognized that privacy is an essential feature that should be considered in cloud computing systems. Second, it is common to share a computer between different people. It can be easy for hackers to install some spyware to discover the login password from a web browser. A recently proposed access control model called Attribute-based Access Control is a good candidate to address the first problem. Not only does it provide anonymous authentication, but it also defines access control policies based on different attributes of the request, the environment or the data object. In the attribute-based access control system, 1 per user has a secret user key issued by the authority. In practice, the user's secret key is stored inside the personal

computer. When we look at the second problem mentioned above in web-based services, it is common for many users to share computers, especially in some large companies or organizations. For example, consider the following two scenarios:

• In the hospital, computers are shared by different employees. Dr. Alice uses the computer in room A when on call during the day, while Dr. Bob uses the same computer in the same room when on call at night.

• In college, computers in the university lab are generally shared by different students. In these cases, the user's secret keys can be easily stolen or used by an unauthorized party. Although the computer may be protected with a password, it is likely to be mistreated or estimated by undiscovered malware. A more secure method is to use two-factor authentication (2FA). 2FA is very common among online electronic banking services. In addition to the username / password, the user must also have a device to view the one-time password. Some systems may require the user to have a mobile phone, while the unique password will be sent to the mobile phone via SMS during the login process. With 2FA, users will have more confidence to use shared computers to log in to their web-based online banking services. For the same reason, it would be better to have a 2FA system for users in web-based cloud services to increase the level of system security. Precise two-factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the following characteristics: (1) It can calculate some lightweight algorithms, such as hash and exponentiation. (2) It is tamper proof, that is, it is assumed that no one can assault it to obtain the confidential information stored inside. With this device, our protocol provides 2FA security. First, the s key is required

2. TERMINOLOGY AND PROBLEM STATEMENT

Broker encryption was first introduced as a way to allow the immediate abolition of public keys. The basic idea of mediated encryption is to use an online medium for each transaction. The online agent refers to SEM (Security Broker) because it provides control over security capabilities. If SEM does not cooperate, public key transactions can no longer be performed. The general idea of isolated password security is to store long-term keys on a physically secure but algorithmically limited device. Users keep short-term secret keys in a powerful but insecure device where encryption calculations are performed. Short-term secrets are updated in separate periods of time by interaction between users, while the public key remains intact throughout the life of the system. An isolated key encryption system requires that all users update their passwords in each period of time. The main update requires a security device. Once the key is updated, the signature or decryption algorithm no longer requires the device for the same period of time. Authentication based on a conventional account / password is not privacy. However, it is recognized that privacy is an essential feature that should be considered in cloud computing systems. It is common to share a computer between different people. It can be easy for hackers to install some spyware to find out the password of a web browser. The opponent acts as a role for the cloud server and tries to find out who the user is interacting with. Access without secret key: the opponent tries to access the system (within his privileges) without any secret key. You could have your own security device.

3. IMPLEMENTING DYNAMIC FACETED SEARCH

Our protocol supports function-based access with precision, which provides great flexibility to the system to define different access policies according to different scenarios. At the same time, user privacy is preserved. The cloud only knows that the user has some required features, but not the true identity of the user. To demonstrate the practical application of our system, we simulate the protocol prototype. Tamper Resistance The content stored within this security device cannot be accessed and is not configured once adjustable. In addition, it will always follow the algorithm specifications. The possibility is able to evaluate the malfunction. In addition, you can generate random numbers and calculate the basis for a specific periodic set with a limited field. It introduced a new 2FA access system (which includes a user secret key and a lightweight security device) for web-based cloud computing services. The 2FA access control system has been defined so that the cloud server can not only limit access to these users with the same set of functions, but also maintain user privacy. In addition, the user cannot use their secret

key with another device belonging to others to access it. Our protocol supports function-based access with precision, which provides great flexibility to the system to define different access policies according to different scenarios. At the same time, user privacy is preserved. The cloud only knows that the user has some required features, but not the true identity of the user. To demonstrate the practical application of our system, we simulate the protocol prototype.

To be the required universe of features. For simplicity, we assume A = [1, n] for some natural numbers n. We will use the vector x ∈ {0, 1} n to represent the set of user attributes. Let x = (x1, ..., xn) ∈ {0, 1} n. If the user has the attribute i, xi = 1. Otherwise, xi = 0.

1) System preparation: the system preparation process consists of two parts. The first part of TSetup is executed by an administrator to create general parameters. The second part of ASetup is operated by the authority issuing attributes to create the master secret key and the public key. TSetup: We are going to λ a security parameter. Manages Guardian G (1λ) (described in

A) to create param = (G, GT, p, eˆ) and random selection for the generators g, gˆ, h, h0, h1, ..., hn ∈ G. Also choose a hash-resistant hash function H: {0, 1} ∗ → Zp. Also, leave tpk = ˆe (g, h0) tsk for the randomly generated tsk ∈R Zp. Publish TPK = (param, g, gˆ, h, h0, h1, ..., hn, H, tpk). ASetup: Attribute issuing authority randomly selects Zp and calculates w = hγ. Publish APK = (w) and set ASK = (γ).

2) Creation of a user key: the process of creating a user key consists of three parts. First, the user creates his public secret key in USetup. The trustee configures the security device to configure the device. Finally, the Attribute Generation Authority creates the secret key for the user attribute according to the Attr Gen user attribute.

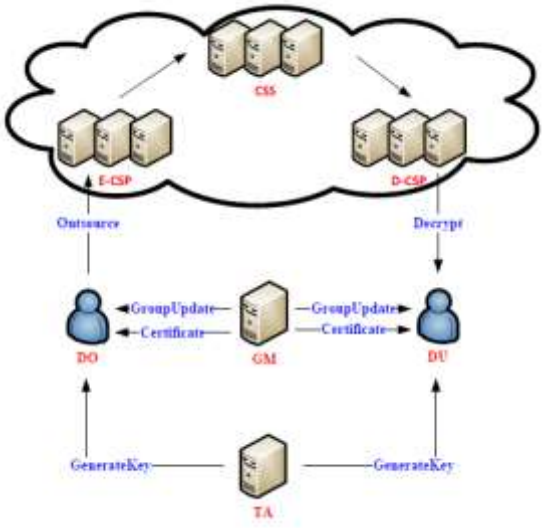

Figure 1: System Architecture

4. CONCLUSION:

We introduced a new 2FA access control system (which includes a user secret key and a lightweight security device) for web-based cloud computing services. Based on the theme-based access control mechanism, the proposed 2FA access control system was identified not only to allow the cloud server to restrict access to these users with the same set of features, but also to maintain the user privacy. The detailed security analysis shows that the proposed access control system 2A meets the required security requirements. When evaluating performance, we have shown that building is "possible." We leave future work to improve efficiency while maintaining all the nice features of the system.

REFERENCES:

[1] 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 Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015

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

[3] X. Huang et al., "Cost-effective authentic and anonymous data sharing with forward security,"

IEEE Trans. Comput., vol. 64, no. 4, pp. 971–983, Apr. 2015.
[4] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in Proc. 10th Int. Conf. ISPEC, 2014, pp. 346–358.
[5] K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.
[6] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th ESORICS, 2014, pp. 257–272.