Two Factor Authentication Access Control for Web Based Cloud Computing

Chandana c[1], Vanishree M L[2], Dr. Kavitha K S[3], Dr. Kavitha C[4]

[1]*PG Student, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India*
[2]*Assistant Professor, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India*
[3]*Professor, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India*
[4]*Professor & HOD, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India*

---***---

Abstract - *In this paper, we tend to introduce a Two-factor authentication (2FA) access system for web-based cloud computing services. Specifically, in our planned 2FA access system, attribute-based access management mechanism is enforced with the need of each a user secret key and a light-weight security device. As a user cannot access the system if they are doing not hold each, the mechanism will enhance the protection of the system, particularly in those eventualities wherever several users share an equivalent laptop for web-based cloud services. additionally, attribute-based management within the system additionally allows the cloud server to limit the access to those users with an equivalent set of attributes whereas conserving user privacy, i.e., the cloud server solely is aware of that the user fulfills the desired predicate, however has no plan on the precise identity of the user.*

Key Words: two-factor, access control, web services

1. INTRODUCTION

Cloud computing could be a virtual host ADP (Automatic Data Processing)system that enables enterprises to shop, for lease, sell, or distribute software in other digital resources over the web as an on demand service. It not depends on a server or variety of machines that physically exist, because it could be a virtual system. There are several applications of cloud computing, like knowledge sharing [1],[3],[4],[6] , knowledge storage [2],[5], big knowledge management , medical system [7] etc.

As sensitive knowledge is also keep within the cloud for sharing purpose or convenient access; and eligible users may access the cloud system for numerous applications and services, user authentication has become a vital part for any cloud system. A user is needed to login before exploitation the cloud services or accessing the sensitive knowledge keep within the cloud.

There are 2 issues for the normal account/password based mostly system. First, the normal account/password-based authentication isn't privacy-preserving. However, it is well acknowledged that privacy is a necessary feature that has to be thought of in cloud computing systems. Second, it is common to share a laptop/desktop among completely different folks. It's going to be simple for hackers to put in some spyware to be told the login password from the web-browser. A recently planned access control model known as attribute-based access management could be a sensible candidate to tackle the matter. It not solely provides anonymous authentication however conjointly any defines access control policies supported completely different attributes of the requester, environment, or the info object.

In an attribute-based access control system,1 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.

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 one-time 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.

2. LITERATURE SURVEY

Cloud computing is a new technology that has unlimited potential for many application areas as well as IT, education, military, transportation, amusement, homeland defense and sensible areas. One basic advantage of mistreatment cloud computing is pay-as-you-go rating model, wherever customers pay only in keeping with their usage of the services.

Cloud security is one among the active analysis areas and in depth analysis work has been carried out in recent years. A range of effective techniques have been proposed by varied authors to give security to cloud knowledge and data.

Securing Software as a Service model of cloud that is employed to explain the safety challenges in SaaS model of cloud computing and conjointly end eavors to produce future security analysis direction.

The security problems are still in loop of solutions, due to that such a lot of organizations are waiting for adoption of cloud computing services.

This projected theme has been evaluated beneath numerous things. The new theme is thought-about as a secure theme for cloud platforms.

3. PROPOSED SYSTEM

We assume the protection device utilized in our system satisfies the subsequent necessities.

1) **Tamper-resistance: T**he content hold on within the security device isn't accessible or modifiable once it is initialized. Additionally, it'll perpetually follow the algorithm specification.

2**) Capability**: it's capable of analysis of a hash function. Additionally, it will generate random numbers and reason exponentiations of a cyclic cluster outlined over a finite field.

The architecture is split into following modules as shown in Fig-1: (a) User Key Generation Process.
(b) Access Authentication Process.

3.1 ENTITIES

Our system consists of the subsequent entities:

3.1.1 TRUSTEE: it's chargeable for generating all system parameters and initializes the protection device.

3.1.2 ATTRIBUTE-ISSUING AUTHORITY: it's accountable to get user secret key for every user per their attributes.

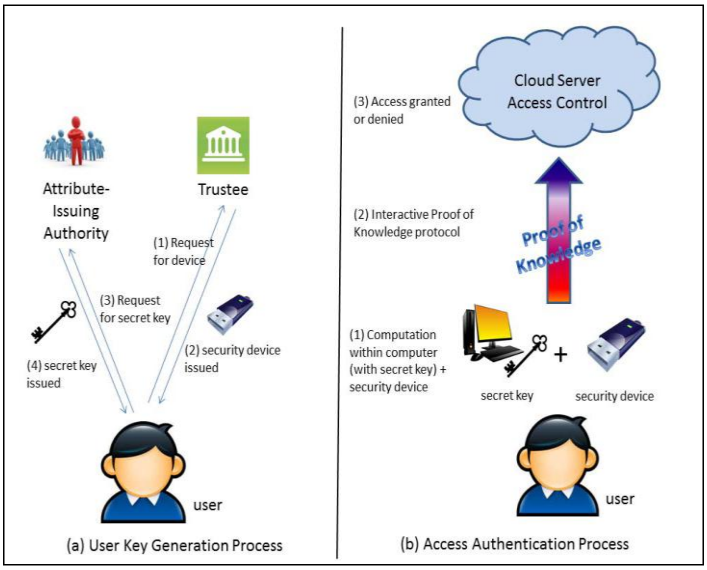
Attribute-Issuing Authority
Trustee
(1) Request for device
(3) Request for secret key
(2) security device issued
(4) secret key issued
user
(a) User Key Generation Process
Cloud Server Access Control
(3) Access granted or denied
(2) Interactive Proof of Knowledge protocol
Proof of Knowledge
(1) Computation within computer (with secret key) + security device
+
secret key
security device
user
(b) Access Authentication Process

Fig -1: Overview idea of our system.

3.1.3 USER: it's the player that creates authentication with the cloud server. Every user features a secret key issued by the attribute-issuing authority and a security device initialized by the trustee.

3.1.4 CLOUD SERVICE PROVIDER: It provides services to anonymous authorized users. It interacts with the user throughout the authentication method.

3.2 CONTRIBUTION OF THE PROJECT

A 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; and (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.

3.3 ASSUMPTIONS

The focus of this paper is on preventing private information leakage at the phase of access authentication. Thus we make some assumptions on system setup and communication channels. We assume each user communicates with the cloud service provider through an anonymous channel [8], [9] or uses IP-hiding technology. We also assume that trustee generates the security parameters according to the algorithm prescribed. Other potential attacks, such as IP hijacking, distributed denial-of-service attack, man-in-the-middle attack, etc., are out of the scope of this paper.

4. CONCLUSION

In this paper, we've given a brand new 2FA (including both user secret key and a light-weight security device) access control system for web-based cloud computing services. Based on the attribute-based access management mechanism, the projected 2FA access system has been known to not solely enable the cloud server to limit the access to those users with an equivalent set of attributes however additionally preserve user privacy. Detailed security analysis shows that the projected 2FA access control system achieves the required security needs. Through performance analysis, we have a tendency to incontestable that the construction is “feasible”. we have a tendency to leave as future work to additional improve the potency whereas keeping all nice options of the system.

REFERENCES

[1] 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

[2] 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.

[3] 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.

[4] 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.

[5] K. Liang, W. Susilo, and J. K. Liu, “Privacy-preserving ciphertext multisharing control for big data storage,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1578–1589, Aug. 2015.

[6] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan,“Secure sharing and searching for real-time video data in mobile cloud,”IEEE Netw., vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.

[7] F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, “An efficient PHR service system supporting fuzzy keyword search and fine-grained access control,” Soft Comput., vol. 18, no. 9, pp. 1795–1802, 2014.

[8] A. Juels, D. Catalano, and M. Jakobsson, “Coercion-resistant electronic elections,” in Proc. WPES, 2005, pp. 61–70.

[9] T. Okamoto, “Receipt-free electronic voting schemes for large scale elections,” in Proc. 5th Int. Workshop Secur. Protocols, 1997, pp. 25- 35.