International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Superior-Grained Dual-Factor Access Control Designed for Web-Based Cloud Computing Services

Gaddipathi Bharathi[*1], Shaik Akbarul Riyaz[2]
[*1]Associate Professor , Department of MCA , St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India
[2]PG Student, Department of MCA , St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

In this paper, we present another fine-grained two-variable validation (2FA) access control framework for electronic distributed computing administrations. In particular, in our proposed 2FA access control framework, a property based access control system is executed with the need of both a client secret key and a lightweight security device. As a client can't access the framework on the off chance that they do not hold both, the instrument can improve the security of the framework, particularly in those situations where numerous clients have the same PC for online cloud administrations. Likewise, characteristic based control in the framework too enables the cloud server to restrict the access to those clients with the same arrangement of properties while preserving client protection, i.e., the cloud server just realizes that the client satisfies the required predicate, however no clue has on the precise personality of the client. Finally, we likewise complete a simulation to exhibit the practicability of our proposed 2FA framework.

Keywords: Fine-grained, two-factor, access control, Web services, ASA, RSA, DelfiHellman

I. INTRODUCTION

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 a lightweight 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. A guileless speculation to accomplish we will probably utilize an ordinary ABS what's more, just split the client secret key into two sections. One section is kept by the client (put away in the PC) while another part is instated into the security gadget. Extraordinary consideration must be taken in the process since ordinary ABS does not ensure that the spillage of part of the Secret key does not influence the security of the plan while in two 2FA, the aggressor could have traded off one of the elements. In addition, the part should be done in a manner that the vast majority of the calculation burden ought to be with the client's PC since the security gadget should not be capable.

II. LITERATURE SURVEY

Rashmi 1, Dr.G.Sahoo2, Dr.S.Mehfuz3,[1] presented securing software as a service model of cloud which is used to describe the security challenges in Software as a Service (SaaS) model of cloud computing and also end eavors to provide future security research directions.From this paper we have referred the solution On Cloud Computing Security.

KashifMunir and Prof Dr. SellapanPalaniappan, [2] presented framework for secure cloud computing. A cloud security model and security framework that identifies security challenges in cloud computing. From this paper, we have referred the solution for security challenges in cloud computing and proposed a security

model and framework for secure cloud computing environment that identifies security requirements, attacks, threats, concerns associated to the deployment of the clouds.

Mr. AnkushKudale,Dr. Binod Kumar,[3] proposed study on authentication and access control for cloud computing. The security issues are still in loop of solutions, because of that so many organizations are waiting for adoption of cloud computing services. This is a review paper for authentication and access control for cloud computing. From this Paper, we have referred a good solution authentication and access control for the cloud computing.

Harbinger Singh1, Amandeep Kaur2, [4] presented access control model for cloud platforms using multi-tier graphical authentication. This proposed scheme has been evaluated under various situations. Both of the graphical password schemes have been evaluated individually with various password combinations. The new multi-level graphical password scheme can be considered as a secure scheme for cloud platforms**.** From this Paper, we have referred the model will be enhanced with more functionality and higher level of authentication security; it would be implemented by using security questions, image based security for the login protection and at the last level User Identification Number (UIN) would be used to access or view the data in cloud platforms on mobile devices and software systems for computers

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 which is particularly designed for supporting cloud computing environment. From this Paper , We have referred an attribute-based access control mechanism which can be regarded as the interactive form of Attribute Based Signature.

III. EXISTING SYSTEM APPROACH

As sensitive data may be stored in the cloud for sharing purpose or convenient access and eligible users may 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 existing system. 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 spyware to learn the login password from the web-browser. Therefore, such systems are not fully secured.

Disadvantage:

- The traditional account/password-based authentication is not privacy preserving.
- 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.

Existing system is not fully secured.

IV. PROPOSED SYSTEM APPROACH

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 and (2) it is tamper resistant, i.e., it is presume 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 attached to the computer (e.g. through USB) in order to authenticate the user for accessing the cloud. The user can be permitted access only if he has both items. However, the user cannot use his secret key with another device belonging to others for the access.

Advantage:

1. 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.
2. At the same time, the privacy of the user is also preserved.
3. The cloud system only knows that the user processes some required attribute, but not the real identity of the user.

4. To show the practicality of our system, we simulate the prototype of the protocol.

V. PROPOSED ARCHITECTURE

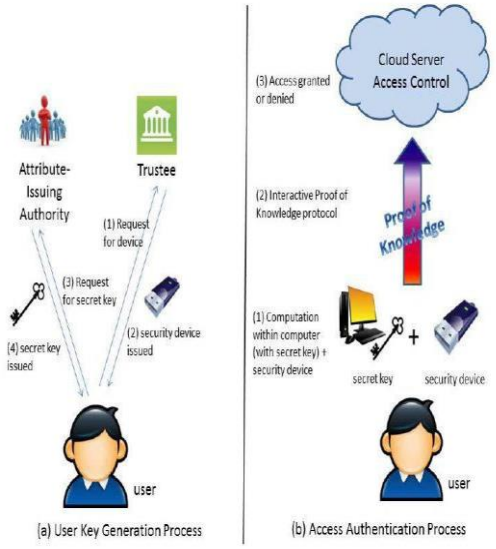

Figure 1. Proposed System Architecture

VI. MODULES

1) Trustee:

It is responsible for creating all system parameters and initializes the security device.

2) Attribute-issuing Authority:

It is accountable to generate user secret key for each user according to their attributes.

3) User:

The player 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.

4) Cloud Service Provider:

It provides services to anonymous authorized users. It interacts with the user during the authentication process.

VII. CONCLUSION

In this paper, we have exhibited another 2FA access control framework for online-distributed computing administrations. Based on the characteristic based access control system, the proposed 2FA access control framework has been recognized to not just give power the cloud server to limit the way in to those clients with the same arrangement of properties additionally save client protection. Point by point security examination demonstrates that the proposed 2FA access control framework accomplishes the coveted security prerequisites. Through execution assessment, we showed that the development is "probable". We leave as future work to assist enhances the productivity while keeping every single pleasing part of the framework.

VI.REFERENCES

[1]. Kashif Munir and Prof Dr. Sellapan Palaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING", IJCCSA,Vol.3, No.2, April 2013.

[2]. Mr. AnkushKudale, Dr. Binod Kumar," A STUDY ON AUTHENTICATION AND ACCESS CONTROL FOR CLOUD COMPUTING", Vol. 1(2), July 2014 (ISSN: 2321-8088).

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

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

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

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

[7]. 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.

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

[9]. J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in Proc. 16th ACM Conf. Comput.Commun.Secur.(CCS), Chicago, IL, USA, Nov. 2009, pp. 131-140.