ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

Two-Factor Data Access Control with Efficient Revocation for Multi-Authority Cloud Storage Systems

Asif Akram .R[a] and R. Banumathi[b] M.Phil. , M.Tech.(CSE)
[a] Research Scholar, Department of Computer Science, PRIST University, Thanjavur.
[b] Research Supervisor, Department of Computer Science, PRIST University, Thanjavur.

Abstract: Our project 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.

Keywords: Attributes, Data Access, Security system, 2FA

I. 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 [30], [31], [33], [22], data storage [15], [45], [25], [32], big data management [4], medical information system [44] 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 pro-vides great advantages, there are meanwhile also con-cerns 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.

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.

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 assumed that no one can break into it to get the secret information stored inside.

II. SYSTEM ANALYSIS

A. Existing System

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

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

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.

Disadvantages of Existing System

1. 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.
2. 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.
3. In existing, Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares.

B. Proposed System

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 assumed that no one can break into it to get the secret information stored inside.

Advantages of Proposed System

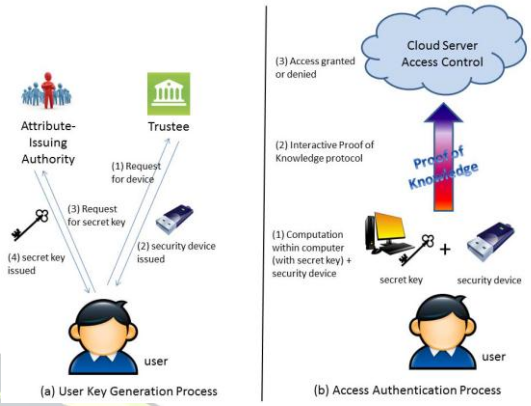
1. Our protocol provides a 2FA security
2. Our protocol supports fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved.

C. Implementation

In this implementation we have 4 Modules,

1. Trustee Module
2. Attribute-Issuing Authority Module
3. User Module
4. Cloud Service Provider Module

System Architecture



D. Problem Definition

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 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. A recently proposed access control model called attribute-based access control is a good candidate to tackle the first problem. 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.

Factor Authentication

If you are walking down the street and you ask for my name, how would you know I am telling you the truth? Well, since you would have no real reason to doubt me, you may just take my word on the matter. But if you were not a trusting sole, you may ask to see some identification. At that point, burden of proof would be on me. I could either decline the offer to prove my identity to you and just walk away, or I could reach for my driver's license. Upon seeing the driver's license, you could either proceed with the conversation believing that my driver's license is real, or, you could just walk away or even report me to the authorities.

Single-Factor Authentication

The most prevalent authentication type in use today is single-factor authentication. In short, single-factor authentication is your basic username/ password combination. The single factor in this case is something you know; your password. Most business networks and most

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

internet sites use basic username/password combination to allow access to secured or private resources.

Problems with Single-Factor Authentication.

How often are usernames and passwords utilized in the daily course of life? At the workplace, employees have to log into their corporate network at least once a day. Some companies still utilize multiple networks. Multiple networks add additional username/password combinations to remember and use. Still many other companies with mainframe capabilities require an additional login credentials. All of the different networks and mainframe's then have different password standards and different lengths of time until the password will need to be changed.

The second 50% of the combination, the password, is the main component of the phrase that is often miss-understood, miss-managed and too often taken for granted. Studies have shown that many users write down their password, choose easily guessed passwords, constantly re-use old passwords and sometimes share their passwords with other people. Technicians often report finding users password on sticky notes under the keyboard, or just stuck on the side of their monitor (Bigler 32).

The Microsoft Corporation has attempted to mitigate one of the inherit problems with the username/password combination. Microsoft has been a proponent of the idea of using "Strong Passwords." Instead of having people use common names for password, Microsoft has detailed the use of using a combination of letters, numbers, and special characters for passwords. While guessing someone's password will be more difficult if the password is "#$#rU78!", the use of strong passwords will still not deter individuals from writing their passwords down. In fact, the use of "strong passwords" will likely increase the number of times someone jots down their password, just so they do not forget it.

The common username/password combination is a form of single-factor authentication; the single factor being the password. Another form of authentication, two-factor authentication, is again starting to get noticed in the workplace. The increased use of two-factor authentication is helping to mitigate most of the problems of the basic username/ password system.

Two-Factor Authentication

Two-factor authentication provides a significant increase in security over the traditional username/password combination. The two factors of two factor authentication are: something you know and something you have. In the single-factor world of authentication, the password was the "something you know" part. The additional factor, "something you have", is the key component.

The something you have component can either be tokens, smart cards, pin/tan's, and biometrics (to be discussed later).

Tokens display a set of numbers on a small screen. Usually, the set of numbers changes every minute. This number then is joined with the user's password, or pin number to create a passcode. A correct passcode then authenticates the user to access the secure resources.

Smart Cards are used in combination with a Smart Card reader. The user will insert the card and the card sends an encrypted message to the website or, the reader displays a unique code that the user will enter.

E. Design Implementation

Two mode of operation are accessible for the users focused around their inclination and imperatives. The first approach is a stand-alone approach that is not difficult to utilize, secure, and cheap which is the traditional mode of authentication known as Alphanumeric Password. The second approach is an approach that is also easy to use and secure which is a Graphical Password such as Pass faces, click points, image and picture based.

III. CONCLUSIONS

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. Through performance evaluation, we demonstrated that the construction is "feasible". We leave as future work to further improve the efficiency while keeping all nice features of the system.

REFERENCES

[1]. M. H. Au and A. Kapadia. PERM: practical reputation-based blacklisting without TTPS. In T. Yu, G. Danezis, and V. D. Gligor, editors, the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012, pages 929– 940. ACM, 2012.

[2]. M. H. Au, A. Kapadia, and W. Susilo. Blacr: Ttp-free blacklistable anonymous credentials with reputation. In NDSS. The Internet Society, 2012.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

[3]. M. H. Au, W. Susilo, and Y. Mu. Constant-Size Dynamic k-TAA. In SCN, volume 4116 of Lecture Notes in Computer Science, pages 111–125. Springer, 2006.

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

[5]. M. Bellare and O. Goldreich. On defining proofs of knowledge. In CRYPTO, volume 740 of Lecture Notes in Computer Science, pages 390–420. Springer, 1992.

[6]. 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.

[7]. D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In Franklin [19], pages 41–55.

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

[9]. J. Camenisch. Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem. PhD thesis, ETH Zurich, 1998. Reprint as vol. 2 of ETH Series in Information Security and Cryptog-raphy, ISBN 3-89649-286-1, Hartung-GorreVerlag, Konstanz, 1998.

[10]. J. Camenisch, M. Dubovitskaya, and G. Neven. Oblivious transfer with access control. In E. Al-Shaer, S. Jha, and A. D. Keromytis, editors, Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, Novem-ber 9-13, 2009, pages 131–140. ACM, 2009.

[11]. J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In S. Cimato, C. Galdi, and G. Persiano, editors, Security in Communication Networks, Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers, volume 2576 of Lecture Notes in Computer Science, pages 268–289. Springer, 2002.

[12]. J. Camenisch and A. Lysyanskaya. Signature Schemes and Anony-mous Credentials from Bilinear Maps. In Franklin [19], pages 56–72.

[13]. 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.

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