International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Cloud Computing Services For Two-Factor Access Control

Y.Madhusekhar & S.Padma

1. Associative Professor, mallareddy institute of technology, mail id: madhuyms@gmail.com
2. M. Tech Student, mallareddyinstitute of technology, mail id: padmas1309@gmail.com

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 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.

Keyword: Authority***, cloud computing, 2FA, data user, encryption***

1. INTRODUCTION

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 atnight. Ina university, computers in the undergraduate lab is usually shared bydifferent 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 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

2.1.Practical reputation-based blacklisting without TTPS: Some users may misbehave under the cover of anonymity by, e.g., defacing WebPages on Wikipedia or posting vulgar comments on YouTube. To prevent such abuse, a few anonymous credential schemes have been proposed that revoke access for misbehaving users while maintaining their anonymity such that no trusted third party (TTP) is involved in the revocation process. Recently we proposed BLACR, a TTP-free scheme that supports `reputation-based blacklisting' --- the service provider can score users' anonymous sessions (e.g., good vs. inappropriate comments) and users with insufficient reputation are denied access

2.2.TTP-free black list able anonymous credentials withreputation: Anonymous authentication can give users the license to misbehave since there is no fear of retribution. As a deterrent, or means to revocation, various schemes for accountable anonymity feature some kind of

(possibly distributed) trusted third party (TTP) with the power to identify or link misbehaving users. Recently, schemes such as BLACR and PEREA showed how anonymous revocation can be achieved without such TTPs—anonymous users can be revoked if they misbehave, and yet nobody can identify or link such users cryptographically. We present BLACR, which significantly advances anonymous revocation in three ways: 1) It constitutes a first attempt to generalize reputation-based anonymous revocation, where negative or positive scores can be assigned to anonymous sessions across multiple categories. Servers can block users based on policies, which specify a boolean combination of reputations in these categories; 2) We present a weighted extension, which allows the total severity score to ramp up for multiple misbehaviors by the same user; and, 3) We make a significant improvement in authentication times through a technique we call express lane authentication, which makes reputation-based anonymous revocation practical.

2.3.Constant-size dynamic *k*-TAA:Dynamic k-times anonymous authentication (k-TAA) schemes allow members of a group to be authenticated anonymously by application providers for a bounded number of times, where application providers can independently and dynamically grant or revoke access right to members in their own group. In this paper, we construct a dynamic k-TAA scheme with space and time complexities of O(log(k)) and a variant, in which the authentication protocol only requires constant time and space complexities at the cost of O(k) -sized public key. We also describe some tradeoff issues between different system characteristics. We detail all the zero-knowledge proof-of-knowledge protocols involved and show that our construction is secure in the random oracle model under the q-strong Diffie–Hellman assumption and q-decisional Diffie–Hellman inversion assumption. We provide aproof-of-concept implementation, experiment on its performance, and show that our scheme is practical.

2.4. A secure cloud computing based framework for big data information management of smart grid: Smart grid is a technological innovation that improves efficiency, reliability, economics, and sustainability of electricity services. It plays a crucial role in modern energy infrastructure. The main challenges of smart grids, however, are how to manage different types of front-end intelligent devices such as power assets and smart meters efficiently; and how to process a huge amount of data received from these devices. Cloud computing, a technology that provides computational resources on demands, is a good candidate to address these challenges since it has several good properties such as energy saving, cost saving, agility, scalability, and flexibility. In this paper, we propose a secure cloud computing based framework for big data information management in smart grids, which we call “Smart-Frame.” The main idea of our framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. In addition to this structural framework, we present a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework.

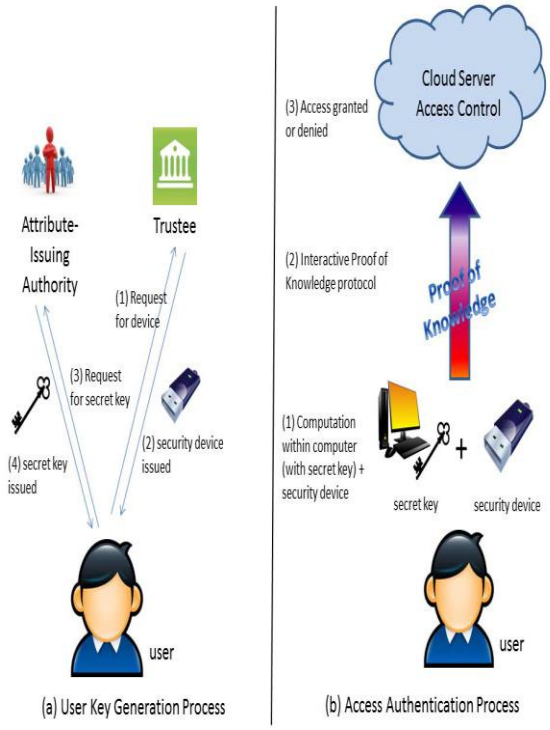
2.5.Ciphertext-policy attribute based encryption: In several distributed systems a user should only beable to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for

realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted moreover, our methods are secure against collusion attacks

3 PROPOSED METHODOLOGY

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.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. It can compute some lightweight algorithms, e.g. hashing and exponentiation; and 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.

4. SCHEME DESCRIPTION:



a)Data User Module: Every user need to register while accessing to cloud. After user registered, at the time of user login then user need to provide one time key to access user home. One time key will be provided by cloud. key will be corresponding user mail id.After user access the user home, User can view the all files upload in cloud.User need to send the file request for both trustee and authority.After user have the two factor access control, user can download the corresponding file.

b)Two Factor Access Control: If user need to access file in cloud. They need to get the two factor access control. Trustee: Need to get security response from trustee for corresponding file.Authority: Need to get secret key from authority for corresponding file.

c) Authority: Authority will upload the file in cloud. And uploaded file will store in drive HQ in encrypted format. Authority will give secret key for all files whenuser request

for any file and the secret key will be send to corresponding user mail Id.

d)Trustee Module: It acts as admin for cloud server. Trustee will give request for all files security response when user request for any file.

e) Cloud Server Module: Cloud view uploaded files in cloud. Cloud view Downloaded files by user in cloud.

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. 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 *Proc. ACM Conf. Comput. Commun.Secur.(CCS)*, Raleigh, NC, USA, Oct. 2012, pp. 929–940.

[2] M. H. Au, A. Kapadia, and W. Susilo, "BLACR: TTP-free blacklistable anonymous credentials with reputation," in *Proc. 19th NDSS*, 2012, pp. 1–17.

[3] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic *k*-TAA," in *Proc. 5th Int. Conf. SCN*, 2006, pp. 111–125.

[4] 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.

[5] M. Bellare and O. Goldreich, "On defining proofs of knowledge," in *Proc. 12th Annu. Int. CRYPTO*, 1992, pp. 390–420.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp.Secur. Privacy*, May 2007, pp. 321–334.

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

[8] 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.

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

[10] 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.

[11] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *Proc. 3rd Int. Conf. Secur.Commun.Netw. (SCN)*, Amalfi, Italy, Sep. 2002, pp. 268–289.

[12] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2004, pp. 56–72.