

Quality Grained Two-Component Access Manage for Web-Primarily Based Cloud Computing Services

Dr. Mohammed Abdul Waheed¹ Asha Rani.H.P²

¹Associate Professor ²M.Tech Student

^{1,2}Department of Computer Science & Engineering

^{1,2}Visvesvaraya Technological University CPGS, Kalaburagi, Karnataka (India)

Abstract— The Quality Grained Two-Component Access Manage for Web-Primarily Based Cloud Computing Services is proposed to over come the problem of authentication. Specifically, in our proposed system 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 system.

Key words: Cloud Computing Services, Two-Component Access Manage

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, data storage big data management, medical information system. 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.

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.

In a university, computers in the undergraduate lab are usually shared by different 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.

II. LITERATURE SURVEY

A. *PERM: Practical reputation-based blacklisting without TTPS*

AUTHORS: M. H. Au and A. Kapadia

In [1] Some of the 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 have proposed a BLACR, a TTP-free scheme which carry 'reputation-based blacklisting' --- the service provider can score users' unknown sessions (e.g., good vs. inappropriate comments) and users with inadequate reputation are denied access.

The major drawback of the BLACR system is the linear computational overhead in the size of the reputation list, which allows it to support reputation for only a few thousand user sessions in practical settings. We propose PERM, a revocation-window-based scheme (misbehaviors must be caught within a window of time), which makes computation independent of the size of the reputation list.

B. *BLACR: TTP-free blacklistable anonymous credentials with reputation*

AUTHORS: M. H. Au, A. Kapadia, and W. Susilo

In [2] Anonymous authentication can provide 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, many schemes such as the BLAC and the PEREA proved how undesigned revocation can be obtained without such TTPs—anonymous users can be revoked if they misbehave, and yet nobody can identify or link such users cryptographically. Despite being the state of the art in anonymous revocation, these methods allow only a basic form of revocation amounting to 'revoke anybody with d or more misbehaviors' or 'revoke anybody whose combined misbehavior score is too high' (where misbehaviors are assigned a 'severity' score). We represent BLACR, with significantly advances anonymous revocation in three ways: 1) It leads to a first attempt to generalization of reputation-based anonymous revocation, where negative or positive scores can be designated to anonymous sessions across

various categories. Servers can block the users based on policies, which informs a boolean combination of reputations in these categories; 2) We present a weighted extension, which allows the total rigorous result to ramp up for multiple misbehaviors by the same user; and, 3) We make a enormous improvement in authentication times through a technique we call express lane authentication, which allows reputation-based anonymous revocation practical.

C. Constant-size dynamic k-TAA

AUTHORS: M. H. Au, W. Susilo, and Y. Mu

In [3] Dynamic k-times unnamed authentication (k-TAA) systems allow the members of a group to be secured anonymously by the application providers for a bounded number of times. Here we construct an energetic k-TAA scheme with space along with 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 initialize 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 a proof-of-concept implementation, experiment on its performance, and show that our scheme is practical.

D. A secure cloud computing based framework for big data information management of smart grid

AUTHORS: J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang

In [4] 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 problems of smart grids, however, are how to handle various 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 offers computational resources on demands, is a good candidate to address these problems since it has several good properties such as energy saving, cost saving, agility, scalability, and flexibility. We propose a secure cloud computing based infra structure for big data management in smart grids, which we call "Smart-Frame." The main goal of our system is to build a hierarchical structure of cloud computing centers to provide variety of computing services for information management and big data analysis. In addition to this substructural framework, we have present a secure way based on identity-based encryption, signature and proxy re-encryption to inscription critical security problems of the proposed framework.

E. Ciphertext-policy attribute based encryption

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters

In [5] for several distributed systems a user should only be able to access data if a user owns a set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store so that the data and mediate access control. However, if any server storing the data is compromised, then the integrity of the data will

be compromised. Here we present an alternate for realizing complicated access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. Existing systems utilized Attribute Based Encryption systems to describe the encrypted data and built approaches into user's keys; while in the proposed system attributes are used to specify a user's identity, and a party encrypting data that determines a way for who can decrypt. Thus, our methods are hypothetical closer to existing access control methods such as Role-Based Access Control (RBAC). In addition, we provide an execution of our system and give performance measurements.

III. SYSTEM ARCHITECTURE

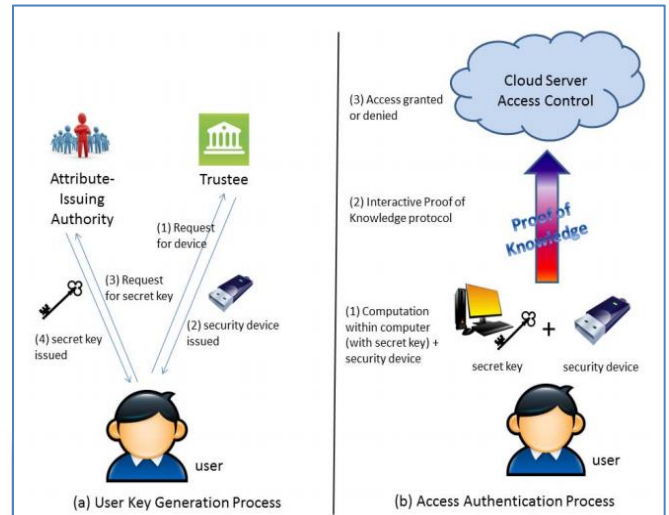


Fig. 1: Architecture

Trustee is responsible for generating all system parameters and initialize the security device. Attribute-issuing Authority is responsible to generate user secret key for each user according to their attributes. User is the player that makes authentication with the cloud server. Each user has been assigned a secret key by the attribute-issuing authority and a security device initialized by the trustee. Cloud Service Provider provides services to anonymous authorized users. It interacts with the user during the authentication process.

IV. METHODOLOGY

A naive thinking to achieve the goal is to use a normal ABS and simply split the user secret key into two parts. One part is kept by the user (stored in the computer) while another part is initialized into the security device. Special care must be taken in the process since normal ABS does not guarantee that the leakage of part of the secret key does not affect the security of the scheme while in proposed system, the attacker could have compromised one of the actors. Besides, the splitting should be done in such a way that most of the computation load should be with the user's computer since the security device is not supposed to be powerful.

We specifically design our system in another manner. We do not split the secret key into two parts. Instead, we introduce some additional unique information stored in the security device. The authentication process requires this piece of information together with the user

secret key. It is guaranteed that missing either part cannot let the authentication pass. There is also a linking relationship between the user's device and the secret key so that the user cannot use another user's device for the authentication. The communication overhead is minimal and the computation required in the device is just some lightweight algorithms such as hashing or exponentiation.

V. RESULTS

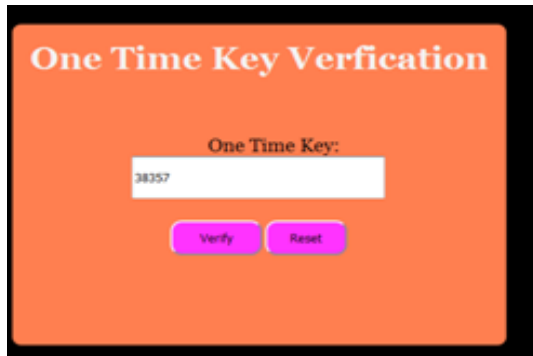


Fig. 2: One time verification key

Figure shows one time verification key which is only to the authorized user. Even the user's id is hacked, without one time key the user personal documents cannot be hacked.



Fig. 3: Two way security

Figure shows the two way security for more safety of the user data. The user can access the required data only if both the trustee and authority has given the permission for data access. This two way access protection is the new proposed system for data protection.

VI. CONCLUSION

The new Quality Grained Two-Component Access Manage For Web-Primarily Based Cloud Computing Services (including both user secret key and a lightweight security device) access control system for web-based cloud computing services has been proposed for authentication. Based on the attribute-based access control mechanism, the proposed Quality Grained Two-Component Access Manage For Web-Primarily Based Cloud Computing Services 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 Quality Grained Two-Component Access Manage for Web-Primarily Based Cloud Computing Services access control system achieves the desired security requirements. Through performance evaluation, the construction is "feasible".

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, sssno. 2, pp. 233–244, Apr./Jun. 2015.
- [5] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.