International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services

P.Jaipal Reddy, M.Venkateswara Rao, V. Sridhar Reddy

jaipalreddypadakanti@gmail.com , venkat2m2@gmail.com , vsridharreddy@vbithyd.ac.in

[1] PG Scholar, Dept of CSE, VBIT College of engineering, Aushapur (v), Ghatkasar (m), Medchal Dist, Telangana, India,

[2] Associate Professor, Dept of CSE, VBIT College of engineering, Aushapur (v), Ghatkasar (m), Medchal Dist, Telangana, India,

[3]Associate Professor, Dept of CSE, VBIT College of engineering, Aushapur (v), Ghatkasar (m), Medchal Dist, Telangana, India,

ABSTRACT: *In several distributed systems a user should only be able 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 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.*

By using our techniques encrypted data can be kept confidential even if the storage server is un trusted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. In addition, we provide an implementation of our system and give performance measurements

1.INTRODUCTION

The cloud is not simply the latest fashionable term for the Internet. Though the Internet is a necessary foundation for the cloud, the cloud is something more than the Internet. The cloud is where you go to use technology when you need it, for as long as you need it, and not a minute more. You do not install anything on your desktop, and you do not pay for the technology when you are not using it. Cloud computing, where applications and files are hosted on a "cloud" consisting of thousands of computers and servers, all linked to gether and accessible via the Internet. Hence, you can access all your programs and documents from any computer that's connected to the Internet. It enables cloud customers to remotely store their data into the cloud so as to enjoy the on - demand high quality applications and services from a shared pool of configurable computing resources . Successful examples of Cloud Storage Service Providers are Drop box ,Amazon's EC2 and S3 , iCloud , Nirvanix etc. which provide data storage service in the pay - as - you use fashion at relatively low prices. For example, Amazon's S3 data storage service just charges $0 . 12 to $0 . 15 per gigabyte month. As compared to building their own infrastructures, users are able to save their investments significantly by migrating businesses into the cloud. The benefits brought by this new computing model include but are not limited to: relief of the burden for storage management, universal data access with independent geographical locations , and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc . With the prevalence of cloud services, more and more sensitive information are being centralized into the cloud servers, such as emails, private videos and photos, company finance data, government documents, etc. On the surface, cloud storage has several advantages over traditional data storage. For example, if you store your data on a cloud storage system, you'll be able to get

to that data from any location that has Internet access. You wouldn't need to carry around a physical storage device or use the same computer to save and retrieve your information. As data owners store their data on external servers, there have been increasing demands and concerns for data confidentiality, authentication and access control . Data is biggest asset to an organization & how confidentiality, authentication and access control can be outsourced. There is a threat to data owner that if CSP is malicious or CSP has some vulnerability. Hence data owner must have some way of ensuring the data is confidential from CSP. I propose a framework that solves thi s problem – maintaining confidentiality of Data from CSP, using concepts of Cryptography (Encryption/ decryption, Symmetric & Asymmetric encryption), Hybrid Cloud, Existing organizational resources (Active directory). The remainder of the paper is organize d as follows. presents proposed framework. Section gives results. concludes the paper and also suggests further extensions.

Attribute-Based Cryptosystem

There is a trend for sensitive user data to be stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Google and Yahoo. The attack correlation center, dshield.org , presents aggregated views of attacks on the Internet, but stores intrusion reports individually submitted by users. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that personal data will be compromised. This worry is escalated by the surge in recent attacks and legal pressure faced by such services. One method for alleviating some of these problems is to store data in encrypted form. Thus, if the storage is compromised the amount of information loss will be limited. One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data. Suppose a particular user wants to grant decryption access to a party to all of its Internet traffic logs for all entries on a particular range of dates that had a source IP address from a particular subnet. The user either needs

Some Naive Approaches

Double encryption: A security device (with an additional public key or serial number) is still required. The encryption process is executed twice. First encrypt the plaintext corresponding to the public key or identity of the user. Then encrypt it again corresponding to the public key or serial number of the security device. For the decryption stage, the security device first decrypts once. The partially decrypted ciphertext is then passed to the computer which uses the user secret key to further decrypt it. Without either part (user secret key or security device) one cannot decrypt the ciphertext. It seems that this naive approach can achieve our goal. However, there exist many practical issues that it cannot solve. For example,

If the user has lost his security device, then his/ her corresponding ciphertext in the cloud cannot be decrypted forever! That is, the approach cannot support security device update/revocability.

The sender needs to know the serial number/ public key of the security device, in additional to the user's identity/public key. That makes the encryption process more complicated. In the case of identity-based encryption, the concept of identity-based" has been totally lost as the sender needs to know not only the identitybut another serial number!

2) Split the secret key into two parts: Another naive way to think of is to simply split the secret key into two parts. The first part is stored in the computer while the second part is embedded into a security device. Similar to the above approach, without either part one cannot decrypt the ciphertext. Again it seems that this approach can achieve our goal. However, note that the security of a normal encryption scheme cannot be guaranteed if part of the secret key has been exposed. The security is only guaranteed if the whole secret key has not been exposed to the adversary. In other words, if we simply split the secret key into two parts, the adversary with either part may have non-negligible chance to decrypt (or at least to know some information about the plaintext). This is not the case that we expect. There exists another cryptographic primitive called "leakage-resilient encryption". The security of the scheme is still guaranteed if the leakage of the secret key is up to certain bits such that the knowledge of these bits does not help to recover the whole secret key. However, though using leakage resilient primitive can safeguard the leakage of certain bits, there exists another practical limitation. Suppose we put part of the secret key into the security device.

Unfortunately the device is stolen. The user needs to obtain a replacement device so that he can continue to decrypt his corresponding secret key. The trivial way is to copy the same bits (as in the stolen device) to the new device by the private key generator (PKG). This approach can be easily achieved. Nevertheless, there exists security risk. If the adversary (who has stolen the security device) can also break into the computer where the other part of secret key is stored, then it can decrypt all ciphertext corresponding to the victim user. The most secure way is to cease the validity of the stolen security device. The same analogy is the online banking. A user needs to have a security device (together with the knowledge of his/her password) in order to login the e-banking service. If the security device is reported as lost, the user can no longer use the old device to login. Thus using leakage resilient primitive cannot provide this security feature which is considered as the most important criterion of twofactor security protection.

3) Other methods: Some real-world systems, such as AT&T and druva, also leverage two-factor encryption techniques to protect message from being leaked to malicious users. However, their techniques suffer from a potential practical risk. Below we take druva system as an example. In a druva system, a message is first encrypted under a user key k1, and next uploaded to a cloud server. The user key k1 is further encrypted by another user key k2, and stored in the server as well. The key k2 is held by the user. When retrieving the message, the user needs to use k2 to

2.LITERATURE SURVEY

M. H. Au and A. Kapadia explained 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. The major drawback of BLACR 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. PERM thus supports millions of user sessions and makes reputation-based blacklisting practical for large-scale deployments.

M. H. Au, A. Kapadia, and W. Susilo, studded 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 BLAC 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. Despite being the state of the art in anonymous revocation, these schemes 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 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.

M. H. Au, W. Susilo, and Y. Mu Explained 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. Dynamic k-TAA allows application providers to independently grant or revoke users from their own access group so as to provide better control over their clients. In terms of time and space complexity, existing dynamic k-TAA schemes are of complexities O(k), where k is the allowed number of authentication. In this paper, we construct a dynamic k-TAA scheme with space and time complexities of O(log(k)). We also outline how to construct dynamic k-TAA scheme with a constant proving effort. Public key size of this variant, however, is O(k). We then describe a trade-off between efficiency and setup freeness of AP, in which AP does not need to hold any secret while maintaining control over their clients. To build our system, we modify the short group signature scheme into a signature scheme and provide efficient protocols that allow one to prove in zero-knowledge the knowledge of a signature and to obtain a signature on a committed block of messages. We prove that the signature scheme is secure in the standard model under the q-SDH assumption. Finally, we show that our dynamic k-TAA scheme, constructed from bilinear pairing, is secure in the random oracle model.

We constructed a constant-size dynamic k-TAA scheme and proved its security. We also analyzed the efficiency of our system and compare it with existing (dynamic) k-TAA schemes. Our scheme outperforms any existing dynamic k-TAA schemes in the literature. Finally, the BBS+ signature we analyze could be useful for other cryptographic systems.

J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, survey on A smart grid is an electricity network that uses digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end-users It possesses demand response capacity to help balance electrical consumption with supply. It is pointed out that there are tenacious economic as well as environmental urgings for the refurbishment of the conventional power systems, and its replacement with a Smart Electrical Power Grid or simply Smart Grid. 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. Smart grid is an electric grid which includes a variety of operational and energy measures including smart meters, smart appliances which are used to measure the power consumption of those devices, and it consists of renewable energy resources, and energy efficiency resources which can be used by those devices. In this paper, we propose a cloud computing based framework for big data information and a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework.

We have introduced a hierarchical structure framework called as a Smart-Frame for the information management and it also provides us with the security approaches to secure the data being stored in this vast network. We focussed on the Identity Based Cryptography and the Identity Based Proxy Re-Encryption schemes for providing the security to the Smart Grid. From this proposal we identified the few limitations while increasing the number of user. If top level data centre handled all the device information & user data, the performance will be weaken. So we built the regional and zone level data centre for maintaining the data. The top cloud level provides a global view of the framework and other will provide the information to parent cloud. From the above 3DES algorithm, we provided

a solution based on "identity-based cryptography and identity-based proxy re-encryption" which provides secure communication services with the Smart-Frame. This will achieve not only scalability and flexibility but also security features.

The notion of a "proof of knowledge," suggested by Goldwasser, Micali and Rackoff, has been used in many works as a tool for the construction of cryptographic protocols and other schemes. Yet the commonly cited formalizations of this notion are unsatisfactory and in particular inadequate for some of the applications in which they are used. Consequently, new researchers keep getting misled by existing literature. The purpose of this paper is to indicate the source of these problems and suggest a definition which resolves them.

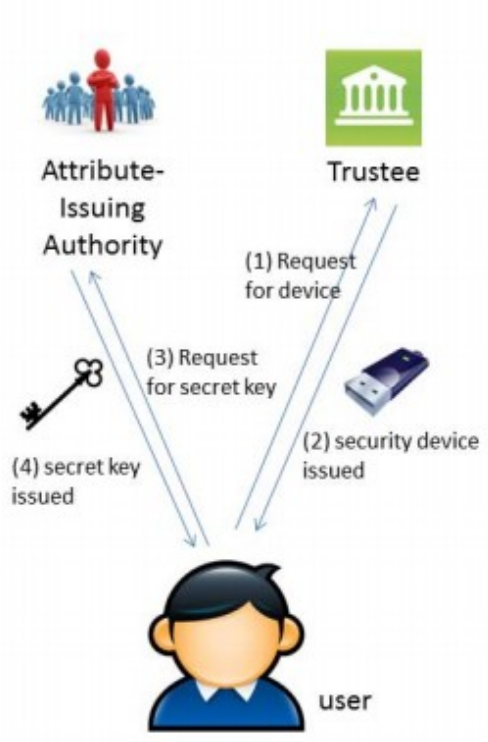


Fig 1: user key generation process

3. FRAMEWORK

3.1 SYSTEM MODEL Figure1 shows the user key generation process,firstly the user has to request for device fro m the trustee if the attributes matches the requirements then the trustee will issue the security device it will be the first level of access to download a file in the cloud and next user has to request for secret key from the attribute issuing authority,i f the attributes matches with the requirements then the attribute issuing authority will issue the secret key it will be the second level of access.

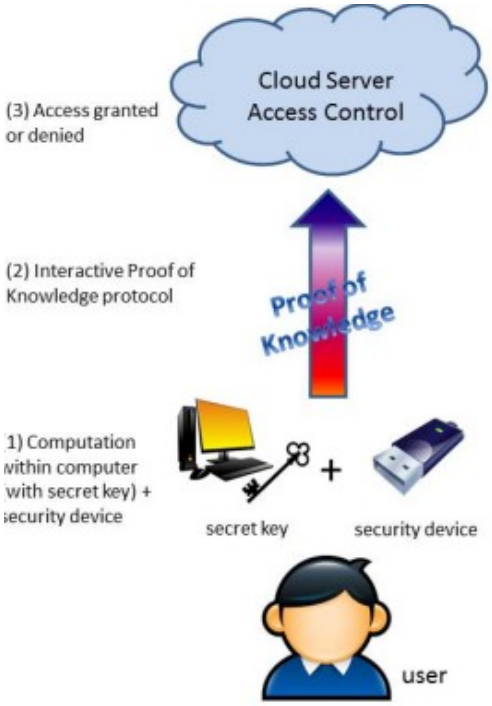
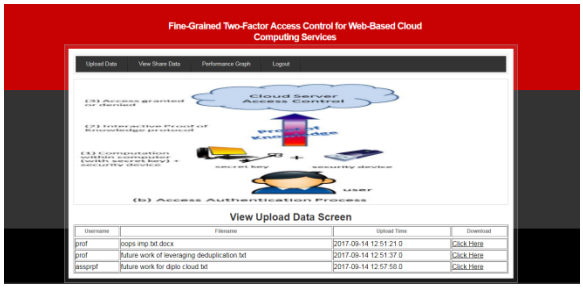


Fig 2: Access authentication process

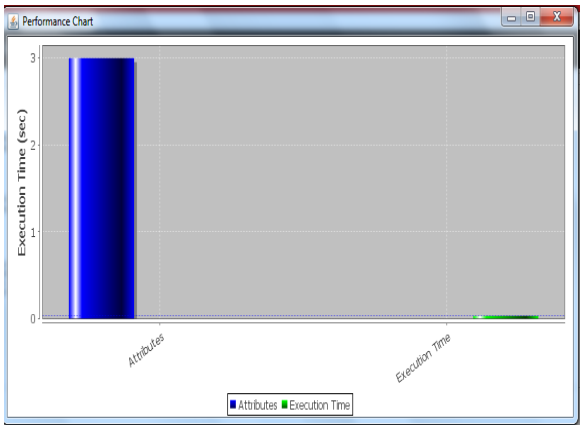
International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

A naive thinking to achieve our 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 a ffect the security of the schemewhile in two 2FA, the attacker could have compromised one of the factors. 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

EXPERIMENTAL RESULTS



It shows no.of attributes and total execution time.



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 restric t 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

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.

[13] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator," in Proc. ICICS, 2014, pp. 274–289.

[14] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security-mediated certificateless cryptography," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 508–524. [15] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[16] R. Cramer, I. Damgård, and P. D. MacKenzie, "Efficient zero-knowledge proofs of knowledge without intractability assumptions," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 1751, H. Imai and Y. Zheng, Eds. Berlin, Germany: Springer-Verlag, 2000, pp. 354–373.

[17] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in Proc. EUROCRYPT, 2002, pp. 65–82.

[18] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416–431.

[19] M. K. Franklin, in Proc. 24th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 2004.

[20] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.