Fine Grained Multi-Factor Access Control for Web based Cloud Computing Services

Syeda Asra[1] Preeti Math[2]
[1]Professor [2]PG Student
[1,2]Department of Computer Science
[1,2]Appa IET College of Engineering, Kalaburgi, Karnataka, India

Abstract— 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 is cloud computing. Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy for web based cloud services. A multi-factor authentication and access control system for web-based cloud computing services is developed. In the proposed authenticated access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a trusted security key response. The login of the user is secured by one time key password system (OTP) and each login is secured with session keys i.e. The user is allowed to work only for a permitted time period. A user cannot access the system if she /he does not hold all the three factors: the OTP, secret key, secret key response, the mechanism enhances the security of the system, especially in those cases 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, the user .The cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user the cloud holds the user with attributes and the polices. The cloud servers cant access the files of the user i.e. the files stored are in an encrypted format the encryption key is given by only the user.

Key words: Access Control, Key Response, Encryption, Encryption Key, Cloud Storage, OTP, Session Keys

I. INTRODUCTION

Cloud computing completely virtual system, i.e. it doesn't exist in real. It no longer depends on a server or a number of machines that physically exist User authentication and identity has become a critical component for any cloud system. A user has to login before using the sensitive data stored in cloud storage. There are two problems here, the traditional account with simple username and password is not privacy preserving. Second is its common to share the same computers among different people. In this paper we propose multi factor authentication and access control system for web based cloud computing services. In the process the login of the user is secured by both session keys and the OTP login. The user requests the trustee key response and the authority secret key for accessing the file, even after logging in the user cannot access the files from cloud storage if he/she didn't possess both the trustee key response and the authority secret key which enhances the security of the system.

In this paper, it is intended to develop a high end security system for providing authentication and access control mechanism which is very fast and accurate in computation as well as limited usage of storage server.

II. PROPOSED WORK

Multi factor access control

A. Login

1) Session Keys

Session keys are sometimes called symmetric keys, because the same key is used for both encryption and decryption. A session key may be derived from a hash value, using the CryptDeriveKey function (this method is called a session-key derivation scheme). Throughout each session, the key is transmitted along with each message and is encrypted with the recipient's public key. Because much of their security relies upon the brevity of their use, session keys are changed frequently. A different session key may be used for each message .every session key is unique and assigns an session ID for each login and logs out automatically when the time period is complete .

2) OTP

A one-time password (OTP) is an automatically randomly generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. The OTP is sent to users personal cell phone number. It is valid for a very short time and can be used only once by the user.

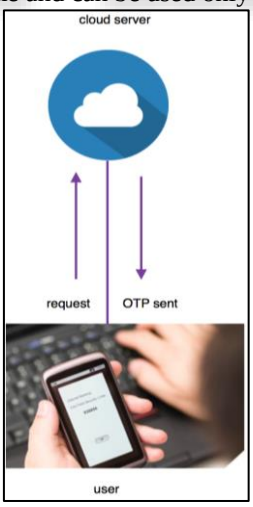

Fig. 1: One Time Password (OTP)

B. Generation of user key

It consists of the three 1) requests 2) trustee response 3) issuing authority secret key.

- Requests: The user has to request the trustee for the trustee key response, the trustee verifies the user about his registration and the login for that particular time and issues the response from the user which is valid for a certain period of time for the logged in user. Next step, the user has to request the authority for the secret key,

the authority verifies the user twice here once though the trustee and other by logged in time.

- Trustee response: The trustee has the user request who verifies him and issues the response key for a particular file he has requested for ,the same file request has to be done for the secret key
- Authority secret key: The authority has the user request who sends the secret key to the user which is randomly generated, user can access his files on logging in with both the secret key and the trustee response, if the user misses any of the key he couldn't access the file and the login is valid for a particular session if the user couldn't complete his work within this time, he must login again with the same mechanisms.

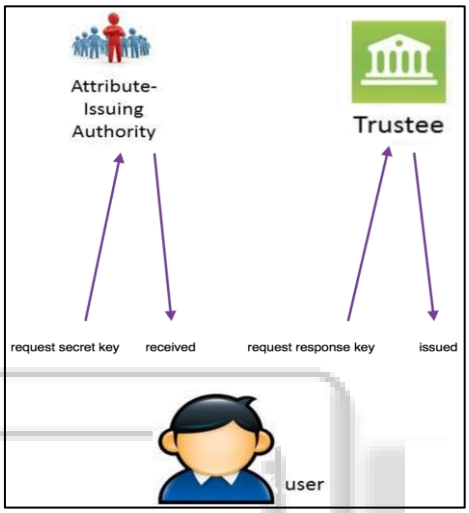

Fig. 2: Generation of User Key

C. *Access Authentication Process*

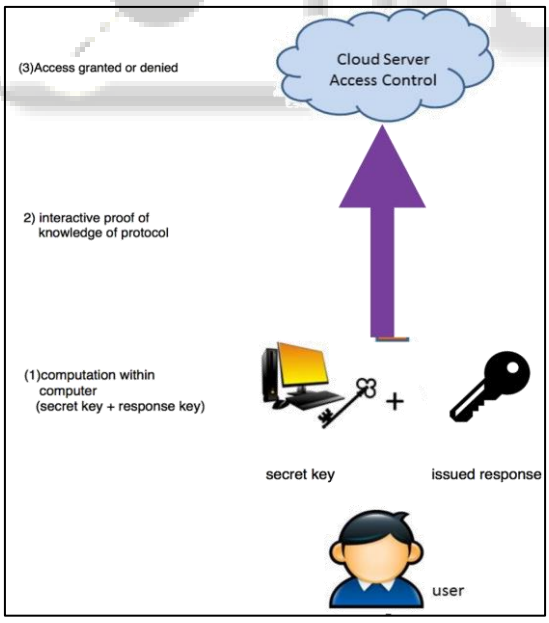

Fig. 3: Access Authentication Process

At the second phase user has the both trustee key response and the authority secret key, the user can't miss any one of those keys, user can access his files by both the keys stored in cloud. The clouds server has no exact knowledge of the identity of the user .the server knows the user only through the attributes and the policies in the process .the files stored in the cloud are encrypted files and the encryption key is known only by the user which makes the mechanism temper resistance i. e, even if in the rare cases the cloud server were hacked the third party cant access the file or read them as they are encrypted.

III. IMPLEMENTATION

The usage of this work is executed in the most extreme famous apparatus of java that is Eclipse Luna by interfacing it to MySQL Workbench 5.2 CE. Obscure Luna is a joined progression condition (IDE) for making applications utilizing institutionalized java programming dialect.

We create a web based dynamic project using eclipse, the CSP used in work is DriveHQ which is It cloud service provider and some unique feature like DriveHQ file manager, DriveHQ online backup, and cloud sharing facility. The files uploaded are saved in DriveHQ in an encrypted format, making it more secure.

We make an electronic dynamic venture utilizing shroud, the CSP utilized as a part of work is DriveHQ which is It cloud specialist organization and some one of a kind element like DriveHQ document administrator, DriveHQ online backup, and cloud sharing facility. The records transferred are spared in DriveHQ in an encoded design, making it more secure. The exploratory outcomes figure that this work accomplishes high proficiency by giving security thrice i.e., login by utilizing session keys, by trustee security reaction and the authority secret key. the work additionally shows the cloud server knows the clients just by the properties yet not the correct character of the client .the records put away in the cloud server are in scrambled arrangement .the encryption key is known just by the client. Moreover, the outsider assault is counteracted by the utilization of the encryption to records transferred in the cloud server

IV. CONCLUSION AND FUTURE WORK

A. *Conclusion*

A multi factor authentication and access control system for web based cloud computing has been introduced , in the proposed multi factor 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 is privacy preserving. The detailed security analysis is as follows:

The mechanism uses OTP services and session keys for login of the user.

Accessing of files by the user is secured twice in the system by trustee response and the secret key.

Files stored in cloud server are encrypted making it more secure and non-accessible by the third party authorities.

The encryption key is known only by the user.

V. FUTURE WORK

This paper has a vast future scope of work. It is highly extensible. The security issues are increasing day by day. Since the technologies and its secure use is an important concern we use different and secure access control and authentication mechanism. The major concern is more user friendly and highly secure measures must be developed and implemented. So the future work has a scope on this area where more user friendly security measures has to be concentrated.

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.

[3] M. H. Au, W. Susilo, and Y. Mu. Constant-Size Dynamic k-TAA.In SCN, volume 4116 of Lecture Notes in Computer Science, pages111–125. 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 management 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, pages390–420. Springer, 1992.

[6] J. Bethencourt, A. Sahai, and B. Waters. Cipher text-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 Cryptography, ISBN 3-89649-286-1, Hartung-Gorre Verlag, 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, November 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 Anonymous 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.

[15] C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou. Security concerns in popular cloud storage services. IEEE Pervasive Computing, 12(4):50–57, 2013.

[16] R. Cramer, I. Damg°ard, and P. D. MacKenzie. Efficient zero knowledge proofs of knowledge without intractability assumptions.In H. Imai and Y. Zheng, editors, Public Key Cryptography, volume 1751 of Lecture Notes in Computer Science, pages 354–373.Springer, 2000.

[17] Y. Dodis, J. Katz, S. Xu, and M. Yung. Key-insulated public key cryptosystems. In EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 65–82. Springer, 2002.

[18] Y. Dodis and A. Yampolskiy. A verifiable random function with short proofs and keys. In S. Vaudenay, editor, Public Key Cryptography, volume 3386 of Lecture Notes in Computer Science, pages 416–431. Springer, 2005.

