iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3689

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Secured Access Control Using Secret key and OTP for Cloud Computing Services.

Miss. Harnoor Sodhi[1], Miss. Tejaswini Kashid[2], Miss. Shriyanka Khade[3], Miss. Supriya Pingale[4], Prof. Jameer Kotwal[5]
[1, 2, 3, 4] *Department of Computer Engineering, Pimpri Chinchwad College of Engineering and Research, Ravet, Pune.*

Abstract: ***Cloud computing is an internet based computing which enables sharing of services. The advantage of cloud is cost saving. The prime disadvantage is security. We consider another Secured access Control Using secret key and OTP for cloud computing services to achieve security in distributed cloud storage. In particular, in our proposed access control framework, a property based access control system is executed with the need of both a client secret key and a lightweight security device. As a client can't access the data on the off chance that they don't hold both secrete key and OTP. Moreover, we use Identity Based Encryption (IBE) algorithm to encrypt user data or file. IBE is an important primitive of ID-based cryptography. The public key encryption is a type in which the public key of user contains some unique information above the identity of user(e.g. user's mail address). We also apply Cauchy approach for data storage on cloud. With the help of our system we can achieve maximum security of data in distributed cloud.***

Keywords: Access control, ASA, Cauchy Approach, Delfi Hellman, Fine-grained, Identity Based Encryption, RSA, Two-factor, Web services.

I. INTRODUCTION

Cloud computing is an internet based computing which enables sharing of services. With cloud computing, users can remotely store their data into the cloud and use on-demand high-quality applications. In cloud computing 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 which has become a critical component for any cloud system. Cloud allows users to use applications without installation any application and access their personal files and application at any computer with internet or intranet access. The advantage of cloud is cost savings. The prime disadvantage is security. We present another Secured Access Control Using Secret Key and OTP Cloud Computing Services to achieving security in distributed cloud storage. In particular, in our proposed access control framework, a property based access control system is
executed with the need of both a client secret key and a lightweight security device. As a client can't access the data on the off chance that they don't hold both secrete key and OTP. Moreover, we use Identity Based Encryption (IBE) algorithm to encrypt user data or file. IBE is an important primitive of ID-based cryptography. The public key encryption is a type in which the public key of user contains some unique information above the identity of user (e.g. user's mail address). We also apply Cauchy approach for data storage on cloud. In this approach first we divide (fragment) our file and then store each fragments on nodes. When user wants to upload another file then system checks is any fragment is similar to previous fragments. If any similar fragment is found then Cauchy approach assign pointer to new similar fragment instead of storing that fragment..

II. EXISTING SYSTEM

As sensitive data may be stored in the cloud for allocation 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 existing 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. Therefore such systems are not fully secured. In the existing system each user has a user secret key issued by the authority but the user's secret key is stored inside the personal computer. Even though the computer may be protected by a password, it can still be probably guessed or stolen by undetected malwares.

A. Existing System Disadvantages

1) The traditional account/password-based authentication is not privacy-preserving.

2) 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) Existing system is not fully secured.

III. PROPOSED SYSTEM

In our system we use two important parameter for downloading the file i.e. OTP and secret key. Client can't access the data on the off chance that they don't hold both secrete key and OTP. Moreover, we use Identity Based Encryption (IBE) algorithm to encrypt user data or file. IBE is an important primitive of ID-based cryptography. We also apply Cauchy approach for data storage on cloud. In this approach first we divide (fragment) our file and then store each fragments on nodes. When user wants to upload another file then system checks is any fragment is similar to previous fragments. If any similar fragment is found then Cauchy approach give pointer to new similar fragment instead of storing that fragment.

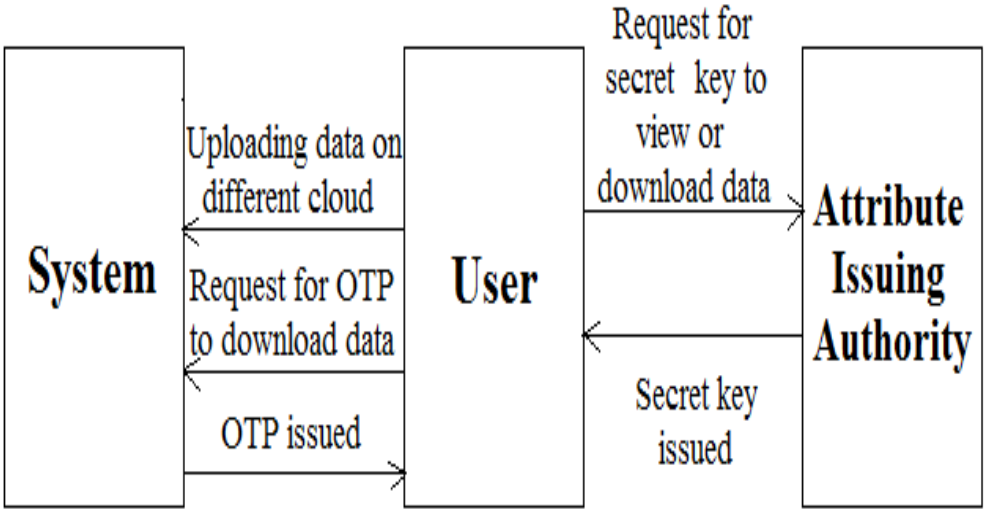


Fig 1. Architecture

The above diagram represents our system architecture. User has choice to select any cloud i.e. public cloud or private cloud for data uploading (storing). At the time of uploading we encrypt file by using Identity Based Encryption (IBE) algorithm and then we fragment file. Then we use Cauchy approach for checking same fragment is already stored or not to reduce storage space on cloud. When user wants to view data then he/she must need to get a secrete key and when user wants to download data from cloud then he/she must need to get a secrete key and OTP.

A. Advantage

1) At the same time, the privacy of the user is also preserved.

2) The cloud system only knows that the user processes some required attribute, but not the real identity of the user.

IV. LITERATURE SURVEY

A. Paper1: Rashmi 1, Dr.G.Sahoo2, Dr.S.Mehfuz3,[1] presented securing software as a service model of cloud which is used to describe the security challenges in Software as a Service (SaaS) model of cloud computing and also end eavors to provide future security research directions. From this paper we have referred the solution On Cloud Computing Security.

B. Paper2: KashifMunir and Prof Dr. Sellapan Palaniappan,[2] presented framework for secure cloud computing. A cloud security model and security framework that identifies security challenges in cloud computing. From this paper we have referred the solution for security challenges in cloud computing and proposed a security model and framework for secure cloud computing environment that identifies security requirements, attacks, threats, concerns associated to the deployment of the clouds.

C. Paper3: Mr. AnkushKudale, Dr. Binod Kumar,[3] proposed a study on authentication and access control for cloud computing. The security issues are still in loop of solutions, because of that so many organizations are waiting for adoption of cloud computing services. From this Paper, we have referred a good solution authentication and access control for the cloud computing.

D. Paper4: Harvinder Singh1, Amandeep Kaur2,[4] presented access control model for cloud platforms using multi-tier graphical authentication. This proposed scheme has been evaluated under various situations. Both of the graphical password schemes have been evaluated individually with various password combinations. The new multi-level graphical password scheme can be considered as a secure scheme for cloud platforms**.** From this Paper , we have referred the model will be enhanced with more functionality and higher level of authentication security; it would be implemented by using security questions, image based security for the login protection and at the last level User Identification Number (UIN) would be used to access or view the data in cloud platforms on mobile devices and software systems for computers

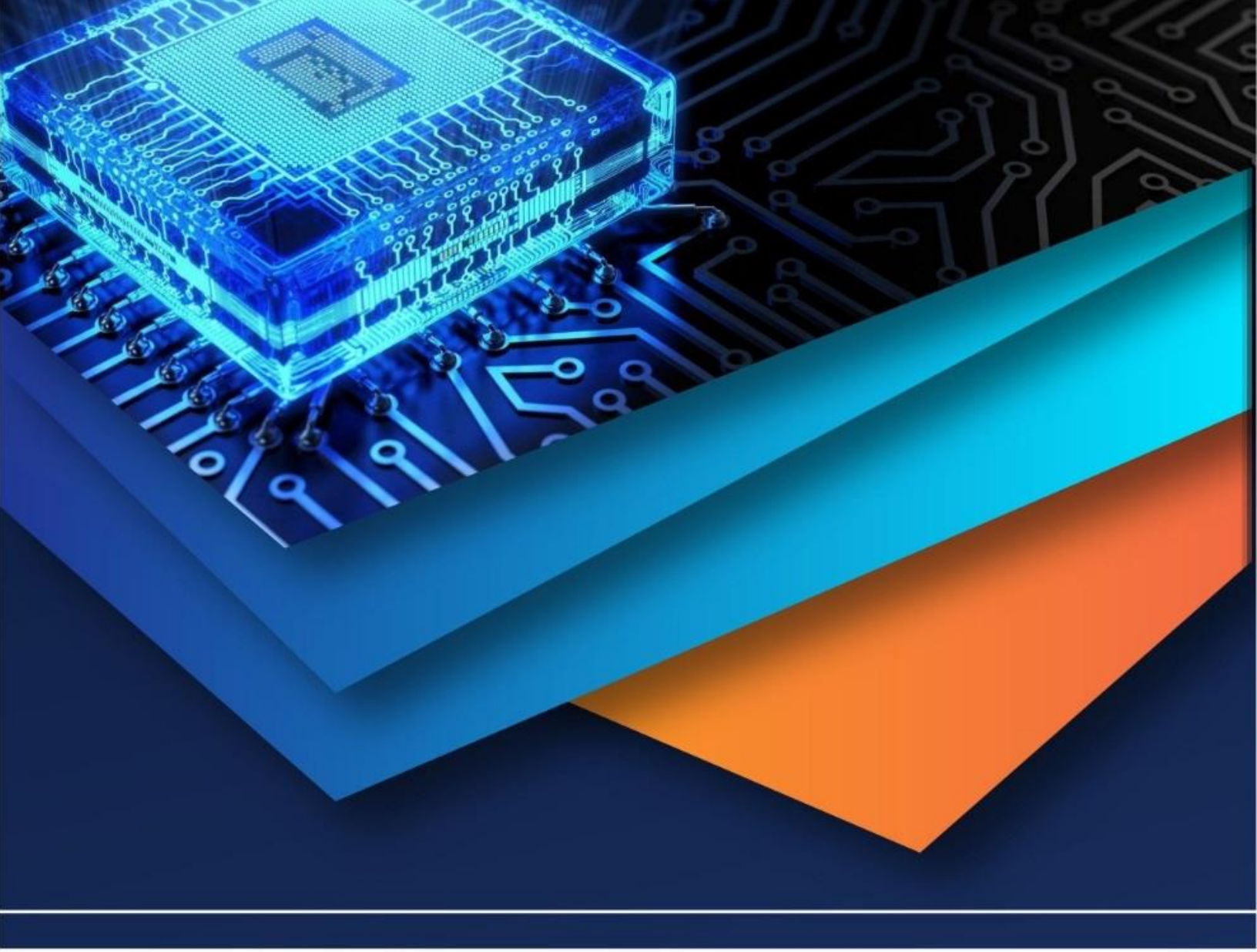
E. Paper5: Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou,[5] projected k-times attribute-based anonymous access control for cloud computing which is particularly designed for supporting cloud computing environment. From this Paper , We have referred an attribute-based access control mechanism which can be regarded as the interactive form of Attribute Based Signature.

V. CONCLUSION

This paper proposed the Secured Access Control Using Secret key and OTP for Cloud Computing Services. to achieving security in distributed cloud storage. Based on the characteristic based access control system, the proposed two-way access control framework has been recognized to not just give power the cloud server to limit the way-in to those clients with the same arrangement of properties additionally save client protection. Moreover, we use Identity Based Encryption (IBE) algorithm to encrypt user data or file. IBE is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). We also apply Cauchy approach for data storage on cloud. With the help of Cauchy approach we save storage (memory) space. Point by point security examination demonstrates that the proposed access control framework accomplishes the coveted security prerequisites. We leave as future work to assist enhances the productivity while keeping every single pleasing part of the framework.

REFERENCES

[1] Rashmi 1, Dr.G.Sahoo2, Dr.S.Mehfuz3, “Securing Software as a Service Model of Cloud Computing: Issues and Solutions”, IJCCSA, Vol.3, No.4, August 2013.
[2] Kashif Munir and Prof Dr. Sellapan Palaniappan, “Framework for Secure Cloud Computing”, IJCCSA, Vol.3, No.2, April 2013.
[3] Mr. Ankush Kudale, Dr. Binod Kumar, “A Study on Authentication and Access Control for Cloud Computing”, Vol. 1(2), July 2014 (ISSN: 2321-8088).
[4] Harvinder Singh1, Amandeep Kaur2, “Access Control Model for Cloud Platforms Using Multi-Tier Graphical Authentication”, Volume 4 Issue 11, November 2015.
[5] Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou, “k-times attribute-based anonymous access control for cloud computing”, IEEE Transactions on Computers, 64 (9), 2595-2608.
[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based 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. 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.
[12] K. Liang, W. Susilo, and J. K. Liu, “Privacy-preserving ciphertext multisharing control for big data storage,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1578–1589, Aug. 2015.
[13] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, “Secure sharing and searching for real-time video data in mobile cloud,” IEEE Netw., vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.
[14] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.
[15] Y. Wu, Z. Wei, and R. H. Deng, “Attribute-based access to scalable media in cloud-assisted content sharing networks,” IEEE Trans Multimedia, vol. 15, no. 4, pp. 778–788, Jun. 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY