ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Study on Authentication and Access Control for Cloud Computing

Tejali B. Nalawade, Manohar K. Kodmelwar

Department of Computer Engineering, TSSM'S BSCOER, Narhe, Pune, India

ABSTRACT: In this paper, proposed system exhibit another fine-grained two-variable approval (2FA) get to control structure for electronic distributed Computing organizations. Specifically, in proposed system proposed 2FA get to control structure, a property based get to control framework is executed with the need of both a customer secret key and a lightweight security device. As a customer can't get to the structure in case they don't hold both, the instrument can enhance the security of the system, especially in those circumstances where various customers have a similar PC for online cloud organizations. Similarly, trademark based control in the structure too enables the cloud server to restrict the access to those customers with a similar proposed system of action of properties while saving customer insurance, i.e., the cloud server just understands that the customer fulfills the required predicate, however no piece of information has on the exact identity of the customer. Finally, proposed system moreover entire a simulation to show the practicability of proposed system proposed 2FA structure. A guileless speculation to accomplish we will probably utilize an ordinary ABS what's more, just split the client secret key into two sections. One section is kept by the client (put away in the PC) while another part is instated into the security gadget. Extraordinary consideration must be taken in the process since ordinary ABS does not ensure that the spillage of part of the Secret key does not influence the security of the plan while in two 2FA, the aggressor could have traded off one of the elements. In addition, the part should be done in a manner that the vast majority of the calculation burden ought to be with the client's PC since the security gadget shouldn't be capable.

KEYWORDS: Fine-grained, two-factor, access control, Web services, ASA, RSA.

I. INTRODUCTION

A sincere theory to fulfill proposed framework will probably utilize an ordinary ABS , simply split the customer secret key enter into two segments. One segment is kept by the customer (set away in the PC) while another part is instated into the security gadget. Uncommon thought must be taken in the process since ordinary ABS does not guarantee that the spillage of part of the Secret key does not impact the security of the arrangement while in two 2FA, the attacker could have exchanged off one of the components. Furthermore, the part should to be done in a way that by far most of the calculation load should be with the customer's PC since the security device shouldn't be able. Despite the fact that the new worldview of distributed computing gives awesome preferences, there are meanwhile also concerns about security and protection particularly for web based cloud services. As sensitive data information might be put away in the cloud for sharing reason or Convenient access; and qualified clients may likewise get to the cloud framework for different applications and administrations, client validation has turned into a basic segment for any cloud system. In particular, in proposed framework proposed 2FA get to control framework, a quality based get to control instrument is actualized with the need of both a client secret key and a lightweight security device. As a client can't get to the framework in the event that they don't hold both, the component can upgrade the security of the framework, particularly in those situations where numerous clients have a similar PC for web based cloud services. What's more, quality based control in the framework likewise enables the cloud server to restrict the access to those clients with a similar arrangement of characteristics while saving client protection, i.e., the cloud server just realizes that the client satisfies the required predicate, yet has no clue on the correct personality of the client. At long last, proposed framework additionally complete a reproduction to show the practicability of proposed framework proposed 2FA framework. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are

DOI: 10.15680/IJIRCCE.2016. 0412178

two problems for the traditional account based 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. An as of late proposed get to control model called attribute based access to control is a good candidate to handle the primary issue. It not only provides anonymous authentication but also further defines access control policies based on different attributes of the requester, environment, or the information protest. In a property based get to control system, every client has a client secret key issued by the power. Practically speaking, the client secret key is put away inside the PC.

II. REVIEW OF LITERATURE

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.

KashifMunir and Prof Dr. SellapanPalaniappan,[2] presentedframework 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 andproposed a security model and framework for secure cloud computing environment thatidentifies security requirements, attacks, threats, concerns associated to the deployment of the clouds.

Mr. AnkushKudale,Dr. Binod Kumar,[3] proposeda 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. This is a review paper for authentication and access control for cloud computing. From this Paper, we have referred a good solution authentication and access control for the cloud computing.

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. FromthisPaper, 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

Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou,[5] proposed 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.

III. SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

A. EXISTING SYSTEM APPROACH

Intervened cryptography was initially introduced as a strategy with allow immediate revocation of public keys. The essential thought of mediated cryptography is to utilize an online mediator for every transaction. This online mediator is referred to a Security Mediator since it gives a control of security capacities. If the Security Mediator does not collaborate then no exchanges with general public key are possible any more.

Disadvantages:-

1. Key-insulated cryptosystem requires all users to update their keys in every time period. The key update process requires the security device.
2. The traditional account/password-based authentication is not privacy preserving. However, it I s well acknowledged that privacy is an essential feature that must be considered in cloud Computing System.
3. Once the key has been updated, the signing or decryption algorithm does not require the device anymore within the same time period.

B.PROPOSED SYSTEM APPROACH

In this Paper, proposed system proposed a fine-grained two factor access control protocol for web based cloud computing administrations, utilizing a lightweight security gadget. The gadget has the following properties:
(1) It can process some lightweight calculations, e.g. hashing and exponentiation.
(2) it is tamper resistant, i.e., it is expected that nobody can break into it to get the secret data put away inside In this paper, proposed system a fine grained two variable access control protocol for web based cloud computing administrations, utilizing a lightweight security gadget.

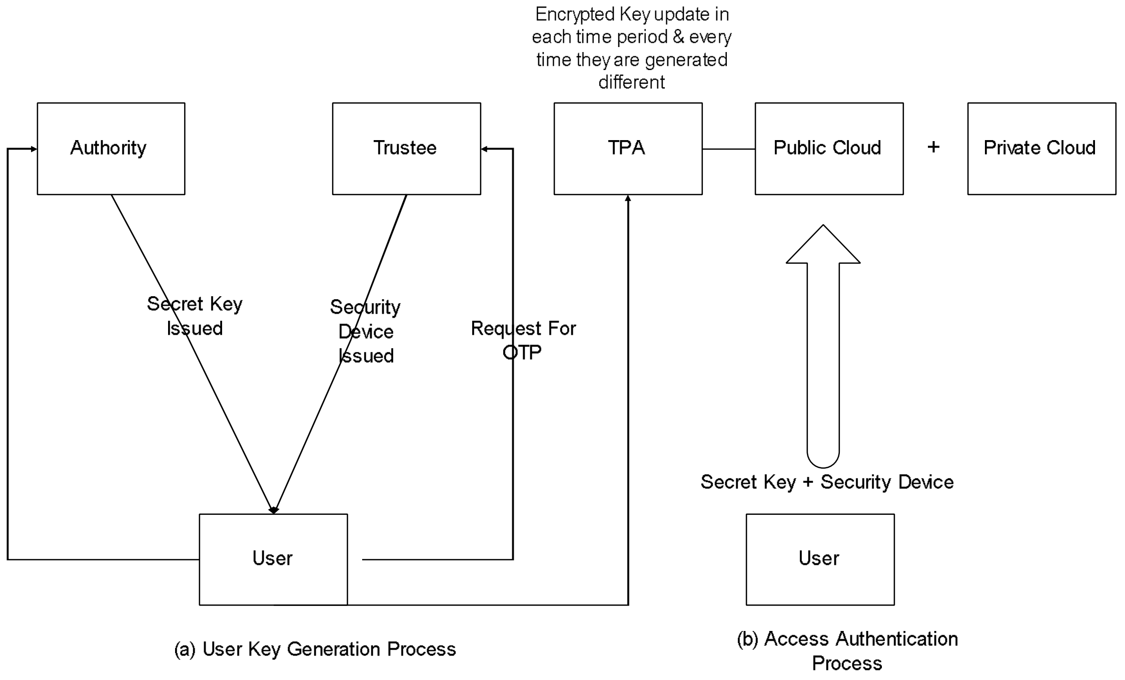
Encrypted Key update in each time period & every time they are generated different
Authority
Trustee
TPA
Public Cloud
+
Private Cloud
Secret Key Issued
Security Device Issued
Request For OTP
Secret Key + Security Device
User
User
(a) User Key Generation Process
(b) Access Authentication Process

Fig No 01 Proposed System Architecture

IV. CONCLUSION

In view of the characteristic based access control framework, the proposed 2FA access control system has been recognized to not simply give control the cloud server to restrict the path into those customers with a similar plan of properties additionally save client protection. In this paper, proposed systems have showed another 2FA get to control structure for online disseminated processing organizations. Point by point security examination shows that the proposed 2FA get to control structure finishes the coveted for security essentials. Through execution evaluation, proposed system showed that the advancement is "probably". Proposed system leave as future work to help improve the efficiency while keping each and every satisfying part of the structure.

ACKNOWLEDGEMENTS

I am profoundly grateful to Prof. Kodmelwar M.K. for his expert guidance and continuous encouragement throughout this work. I would like to express deepest appreciation towards Dr.Bilgi D.S., Principal BSCOER, Pune, Dr. G.A. Hinge, Vice-Principal and Prof. Pokale N.B.,HOD Computer Department, whose invaluable guidance supported me in completing this work.

REFERENCES

[1] Rashmi 1, Dr.G.Sahoo2, Dr.S.Mehfuz3, "Securing Software as a Service Model of CloudComputing: Issues and Solutions", IJCCSA ,Vol.3, No.4, August 2013.

[2] KashifMunir and Prof Dr. SellapanPalaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING", IJCCSA,Vol.3, No.2, April 2013.

[3] Mr. AnkushKudale,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 JianyingZhou,"k-times attribute-based anonymous access control for cloud computing", IEEE Transactions on Computers, 64 (9), 2595-2608.

[6] J. Bethencproposedsystemt, 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.