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. 5, Issue 9, September 2017

Granulated Efficient Access Control for Tracery-Based Using Two-Factor Authentication in Cloud Computing

Kasa Deepa[1], J.Raghunath[2], T.Ramamohan[3]

M.Tech Student, Dept. of CSE, GATES Engineering College, Affiliated to JNTUA, Andhra Pradesh, India[1]

Assistant Professor, Dept. of CSE, GATES Engineering College, Affiliated to JNTUA, Andhra Pradesh, India[2]

Assistant Professor, Dept. of CSE, GATES Engineering College, Affiliated to JNTUA, Andhra Pradesh, India[3]

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. 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.

I. INTRODUCTION

Cloud computing may be a virtual host system that enables enterprises to purchase for, lease, sell, or distribute software associated different digital resources over the web as an on demand service. It now not depends on a server or variety of machines that physically exist, because it may be a virtual system. There are a unit several applications of cloud computing, like information sharing information storage big information management , medical data system etc. Endusers access cloud-based applications through a wb browser, skinny consumer or mobile app whereas the business package code and user's information area unit keep on servers at an overseas location A recently planned access control model known as attribute based access management may be a smart candidate to tackle the primary drawback. It not solely provides anonymous authentication however conjointly additional defines access control policies supported completely different attributes of the requester, environment, or the information object. In associate attribute-based access control system,1 every user includes a user secret key issued by the authority. In apply, the user secret secret is keep within the personal laptop. after we contemplate the higher than mentioned second drawback on web-based services, it's common that computers is also shared by several users particularly in some large enterprises or organizations.

Consider an organization – industrial, government, or military – wherever all staff (referred to as users) have bound authorizations. we tend to assume that a Public Key Infrastructure (PKI) is offered and every one users have digital signature, as well as en/de-cryption, capabilities. within the course of performing arts routine everyday tasks, users cash in of secure applications, like email, file transfer, remote log-in and internet browsing. Now suppose that a trusty user (Alice) will one thing that warrants immediate revocation of her security privileges. for instance, Alice could be dismissed, or she may suspect that her personal key has been compromised. Ideally, straightaway following revocation, the key holder, either Alice herself or associate degree assailant, ought to be unable to perform any security operations and use any secure applications. Specifically, this might mean:

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. 5, Issue 9, September 2017

The key holder cannot scan any secure email. This includes encrypted email that already resides on Alice's email server (or native host) and potential future email erroneously encrypted for Alice. though encrypted email could also be delivered to Alice's email server, the key holder ought to be unable to rewrite it.
The key holder cannot generate valid digital signatures on any longer messages. However, signatures generated by Alice before revocation might have to stay valid.

II. LITERATURE SURVEY

1) A Secure Cloud Computing Based Framework For Big Data Information Management Of Smart Grid Author: J.Baek, Q.H Vu, J.K.Liu, X.Huang
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 challenges of smart grids are how to manage different types of front-end intelligent devices such as power assets and smart meters efficiently and also how to process a huge amount of data received from these devices. Cloud computing, a technology that provides computational resources on demands, is a good candidate to address these challenges since it has several good properties such as energy saving, cost saving, agility, scalability and flexibility. The proposed system illustrate about a secure cloud computing based on the framework for big data information management in smart grids, which it called as "Smart-Frame." The main idea of our framework is to build a hierarchical structure of cloud computing centre to provide different types of computing services for information management and big data analysis. In addition to this structural framework, and also articulate about a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework

2) Cipher Text-Policy Attribute-Based Encryption Author: J. Bethencourt.A. Sahai And B. Waters
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. The present is a system for realizing complex access control on encrypted data that is called as "Cipher text-Policy Attribute-Based Encryption". By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, these 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 this system attributes are used to describe a user‟s credentials, and a party encrypting data determines a policy for who can decrypt. Thus, this method is conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, it provides an implementation of system and gives performance measurements.

III. EXISTING SYSTEM

Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about web based cloud services only. As a data may be stored in the database for sharing purpose or convenient access and eligible users may also access the online system for various applications and services, user authentication has become a critical component for any system. A user is required to login before using the cloud services or accessing the sensitive data stored in the database.
1. 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.
2. 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.
3. In existing, Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares.

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. 5, Issue 9, September 2017

IV. PROPOSED SYSTEM

In my project, I propose a granulated efficient access control protocol for tracery-based cloud computing services, using a lightweight security device. The device has the following properties: (1) it can compute some lightweight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside.

In this project, I propose a Granulated Efficient Access Control For Tracery-Based Using Two-Factor Authentication in Cloud Computing Services.. The device has the following properties. It can compute some lightweight algorithms, e.g. hashing and exponentiation; and it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside.

With this device, access control protocol provides a security. First the user secret key (which is usually stored inside the computer) is required. In addition, the security device should be also connected to the computer (e.g. through USB) in order to authenticate the user for accessing the cloud. The user can be granted access only if he has both items.

1. Protocol provides a 2FA security

2 Protocols support fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved.

V. MODULE DESCRIPTION

Data User Module

- Every user need to register while accessing to cloud.
- After user registered, at the time of user login then user need to provide one time key to access user home.
- One time key will be provided by cloud. key will be corresponding user mail id.
- After user access the user home, User can view the all files upload in cloud.
- User need to send the file request for both trustee and authority.
- After user have the two factor access control, user can download the corresponding file.

Two Factor Access Control:

- If user need to access file in cloud. They need to get the two factor access control.
- Trustee: Need to get security response from trustee for corresponding file.
- Authority: Need to get secret key from authority for corresponding file.

Authority:

- Authority will upload the file in cloud. And uploaded file will store in drive HQ in encrypted format.
- Authority will give secret key for all files when user request for any file and the secret key will be send to corresponding user mail Id.

Trustee Module

- It acts as admin for cloud server.
- Trustee will give request for all files security response when user request for any file.

Cloud Server Module

- Cloud view uploaded files in cloud.
- Cloud view Downloaded files by user in cloud.

VI. CONCLUSION

In this project, I 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 restrict the access to

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. 5, Issue 9, September 2017

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]. 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.
[2]. J. Bethencourt.A. Sahai, and B. Waters.
Ciphertext-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.
[3]. D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techn., 4(1):60–82, 2004.
[4]. K. Joseph, Liu, Man Ho Au, Xinyi Huang, Rongxing Lu, Jin Li. Fine –grained two- factor access control for web based cloud computing services. journal 1556-6013(C).IEEE 2016.
[5]. 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.
[6]. R. Cramer, I. Damgard, and P. D. MacKenzie. Efficient zeroknowledge 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.