International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

An Efficient Two - Factor Access Control For Web-Based Cloud Computing Services Using Jar File

V. Arulsakthi , K. Sudha

Muthayammal Engineering College, Rasipuram, Rasipuram, Tamil Nadu, India

ABSTRACT

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the internet. This computing paradigm also conveys many new challenges for data security and access control. The users are outsourcing sensitive data for sharing on cloud servers, which are not within the same trusted domain as original data. To keep sensitive user data confidential against entrusted servers. Existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorize users. However, in this performance these solutions unoriginally introduce a heavy computation overhead on the sensitive data for key distribution and data management. These problems are not simultaneously achieving the data confidentiality of access control actually still remains unresolved. Analyzed how the existing schemes secure against the key-logger, shoulder-surfing attacks, and multiple attacks. The proposed system illuminates to implement the secret key using JAR file application instead device for web based access control protocol. Main purpose of the existing system to proposed system is complications in carrying the device to everywhere, to avoid non- accessibility through the physical damage and loss of the device. In the proposed system secret key is developed using JAR file application developed with blowfish algorithm scheme for encryption and decryption.

Keywords : Web-Based Cloud Computing, Factor Access Control , Cloud Computing, Authentication

I. INTRODUCTION

1.1 CLOUD COMPUTING

Cloud computing is 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. It no longer depends on a server or a number of machines that physically exist, as it is a virtual system. There are many applications of cloud computing, such as data sharing data storage big data management, medical information system etc.

1.2 WEB BASED END USERS IN CLOUD SERVICE

End users access cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. The benefits of web-based cloud computing services are huge, which include the ease of accessibility, reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility and immediate time to market. Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy especially for web based cloud services. As sensitive 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.

1.3 AUTHENTICATION

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 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. A recently proposed access control model called attribute-based access control is a good candidate to tackle the first problem. It not only provides anonymous authentication but also further defines access control policies based on different attributes of the requester, environment, or the data object. In an attribute-based access control system, each user has a user secret key issued by the authority. In practice, the user secret key is stored inside the personal computer. When consider the above mentioned second problem on web-based services, it is common that computers may be shared by many users especially in some large enterprises or organizations.
For example, let us consider the following two scenarios:In a hospital, computers are shared by different staff. Dr. Alice uses the computer in room A when she is on duty in the daytime, while Dr. Bob uses the same computer in the same room when he is on duty at night. Inuniversities, computers in the undergraduate lab are usually shared by different students. In these cases, user secret keys could be easily stolen or used by an unauthorized party. Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares.

II. LITERATURE SURVEY

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

AND Y.XIANG 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 centreto 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.

Disadvantages

1. To manage different types of front-end intelligent devices such as power assets and smart meters efficiently;
2. To process a huge amount of data received from these devices.

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 deter-mines 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.

Disadvantages

1. It is increasingly difficult to guarantee the security of data using traditional methods
2. Creating multi-authority ABE is to prevent collusion attacks between users that obtain key components from different authorities.

III. SYSTEM INFORMATION

3.1 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.

DISADVANTAGES

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.

3.2 PROPOSED SYSTEM:

In this project, the proposed system as the effective two-factor access control protocol for web-based cloud computing services, using JAR file. In the JAR 11 module the jar will be built with different expression calculation. First the random key will be segregated in 3 variables as per the 3 variable the code value will be assigned and set into the expression. For each JAR the expression calculation will vary.

ADVANTAGES OF PROPOSED SYSTEM:

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. 3. Identify the real identity of the user

3.3 SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

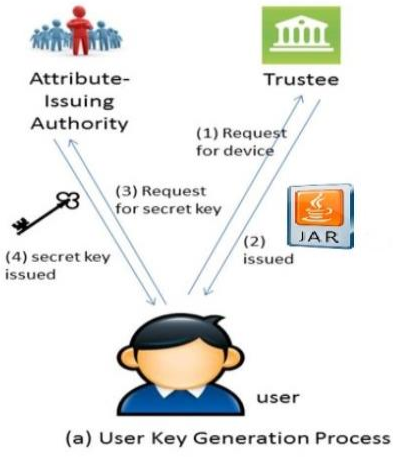
System	:	Pentium IV 2.4 GHz.
Hard Disk	:	40 GB.
Floppy Drive	:	1.44 Mb.
Monitor	:	14’ Colour Monitor.
Mouse	:	Optical Mouse.
Ram	:	512 Mb.

SOFTWARE REQUIREMENTS:

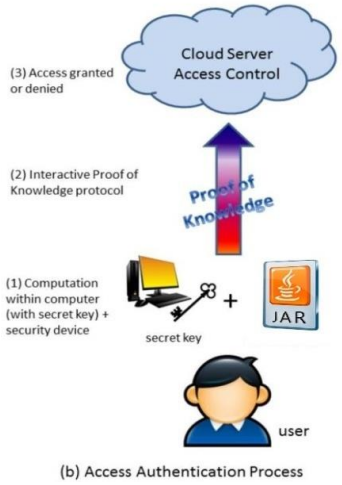
Operating system	:	Windows 8.
Coding Language	:	J2EE and Servlet.
Data Base	:	MYSQL Server.
Tools	:	Net beans 7.4.

IV. SYSTEM ORGANIZATION

4.1 SYSTEM ARCHITECTURE



(a) User Key Generation Process



(b) Access Authentication Process

Figure 4.1 (A) User Key Generation Process(B)Access Authentication Process

V. PROBLEM DEFINITION

In the Existing system the access code will be sent to the mobile using that user login to the website. Access code security is not there.it present a password protection scheme. That involves a small amount of human computing in an Internet-based environment, which will be resistant to phishing scams, Trojan horses, and shoulder surfing attacks. As sensitive 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 has become a critical component for any cloud system. A user is required to login before using the cloud services or access ing the sensitive data stored in the cloud.

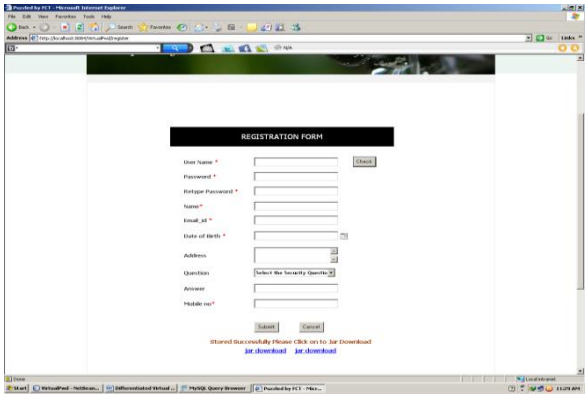


Figure 4.2.1 Registration Form

4.2 MODULE DESCRIPTION:

4.2.1 REGISTRATION MODULE

In the Registration Module, the users have to make registration here. As per the registration JAR will be downloaded as per the random value. User has to install the JAR in the java supporting mobile. Using the JAR only we will do the login form. In the JAR there will be expression calculation. Expression varies for each JAR. Expression will be stored in the database.

4.2.2 LOGIN MODULE

In the login form the user will give the user name and password first. If the username and password is same means a random key will be sent to the access page. User has to install the JAR and enter the random key contain in access page. As per the user expression calculation will be done and viewed in the access code text field. Please enter the value in the website if the value is correct means enter to the user's page.

Figure 4.2.2 Login

4.2.3 UPLOAD MODULE

In the Upload Module the user can login and upload the document. While uploading the document the user can set either two options. One is Private and another is public .If the private is set means only the user who upload it can download the document. If the public is set means all the user has given access right to download it.

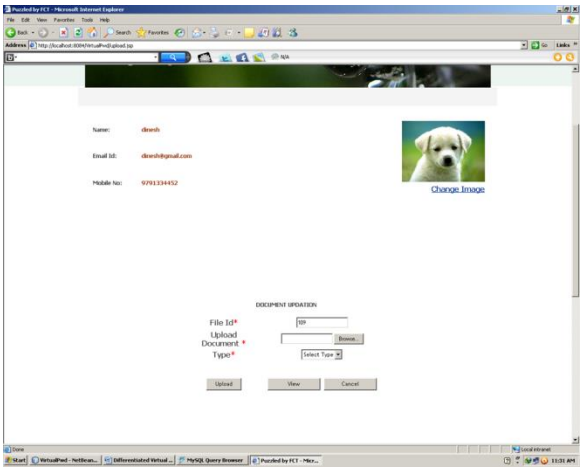


Figure 4.2.3 Upload

4.2.4 JAR MODULE

In the Jar module the 11 jar will be build with different expression calculation. First the random key will be fragmented in 3 variables as per the 3 variable the code value will be assigned and set into the expression. For each jar the expression calculation will vary. If the user doesn't have the java supporting mobile means using emulator he/she can run the jar.

4.2.5 DOWNLOAD MODULE

In the Upload Module the user can login and download the document. While uploading the document the user can set either two options. One is Private and another is public .If the private is set means only the user who upload it can download the document. If the public is set means all the user has given access right to download it. Search of Document using document name or using user name is applicable here. If the private option is there for the document means user can make request to concern user to give access right too.

VI. CONCLUSION

The idea to present the new 2FA (including both user secret key and jar file) 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 those users with the same set of attributes but also preserve user privacy. The proposed system illuminates to implement the secret key using JAR file application instead of using the light weight device for web based access control protocol. The secret key is developed using JAR file application, is going implemented with blowfish algorithm scheme for encryption and decryption. The proposed system illuminated into 5 five modules and start up with the module as Registration, login module and upload module. Detailed security analysis shows that the proposed 2FA access control system according to the desired security requirements in future work. To improve the efficiency of the 2FA factor, using the JAR module and downloadmodule developed, while keeping all the features of the securitysystem to identify the real identity user.

VII. 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.