ISSN:0975-9646

A Bi-level Security Mechanism with Encryption and User Authentication through Hardware Token for Cloud Computing Based Web Application

Shrinivas Kathale[#1], Shraddha Phansalkar[*2]

*[#1,*2]Department of Computer Science, Symbiosis International University*
Pune India

***Abstract*— In contrast to traditional solutions, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. Although commercial CSP provides secured data storage to the client data, it is a research challenge to satisfy the user's requirement of confidentiality and authentication. Cloud security solutions typically have single security architecture but have many customers with different demands. Even multi-tenancy feature of cloud gives rise to security issue related to data and also the authentication of users. Though cloud service provider solves this problem by strong encryption algorithms for data security, the security achieved, works at single level. We propose a system with bi-level security mechanism which uses encryption at cloud service level along with application controller level security and system level security which provides transient user authentication with a small hardware token. This token continuously monitors the user's presence over a wireless connection link to the machine through which user is accessing cloud. The system enforces the security guarantees, although at a cost of performance.**

***Keywords*— Encryption, Decryption, Cloud storage, Hardware Token, Authenticity**

I. Introduction

Cloud computing is defined as the service in which multi-tenancy enables sharing of software resources and infrastructures from different locations with lowest costs [1].

Cloud security is the most important factor in cloud computing because both data and software are fully not contained on the user's computer [2]. Cloud services stores user's data on cloud and provide access to them through APIs. The storage of the user data, which is confidential, private arises the need of high level security and privacy. There are many security issues and challenges in cloud computing explained in [3]. CSP provide a general level of security guarantee which may be insufficient to the user's need of high end security. We know encryption is the commonly offered cloud security mechanism to protect client's data. Data is stored in encrypted format on the cloud and accessible only to the authenticated users. Different kinds of symmetric and asymmetric encryption algorithms are used to enhance security of cloud by converting plaint text to cipher and vice versa explained in [4]. Two Belgian cryptographers, Daeman and Rijmen developed AES symmetric key algorithm meaning same key is used for encryption and decryption based on Rijndael cipher [5]. The encryption-decryption techniques works at the cloud-application interface and the user –application level is secured only through conventional username-password mechanism. It is this level which can enhance the security guarantee through some mechanism which vouches for the user authentication. Use of hardware token is a stronger way to enhance the security mechanism. Hardware token is peripheral device of system which is used for communicating with other device over short range of wireless link [6]. We may consider hardware token as Bluetooth device which is having unique id which is used for uniquely identification of particular device. As bluetooth has its short range of wireless link for communicating with other devices there are limited chances of getting communicated by wrong devices [7] or intruders. Cloud security mechanisms leveraged at one level is impractical solution hence we propose leveled security architecture which makes the system more robust and secure.

II. Related Work

In the literature, several techniques have been developed for enhancing data security on cloud data stores. Prominent techniques include algorithms for encryption decryption with application to formal verification techniques for increasing security of system [8], [9], [10]. Some of the researcher have provided username-password with time bound access but, it leads to complexity [11]. Daeman and Rijmen developed AES algorithm based on Rijndael cipher with different key and block sizes [5].

Encryption algorithm guarantees the protection of data over cloud against accidental/ malicious change. However the authentication techniques are used [12] such as user name and passwords are preferred for their simplicity and less overhead. As application server needs to shoulder the responsibility of the authentication and authorization problem, it is a programmer's overhead. To answer this security issue, we propose integrated working of application which operates at:

a. Application Controller level security
b. System level security

Hence the contribution is proposing a design model for bi-level security mechanism which can provide good security solution to critical web based cloud applications albeit at the cost of performance.

III. DESIGN MODEL

Design model for bi-level security mechanism with levelled security is as follows:

A. *Architecture Design*

Fig. 1 shows clear idea of how the architecture of bi-level security mechanism provides two levels of security. First level of security is at application controller level security and other is at system level security.

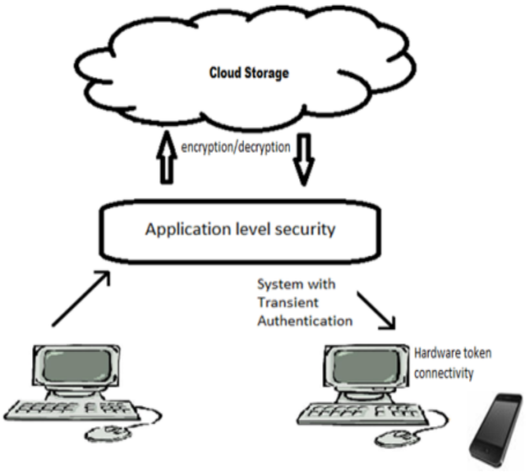

Fig. 1 Architecture of proposed system

At the top level we have cloud storage which is MySql data storage which could be a private/public cloud infrastructure.

Middle level is an application server/web server which could be implemented by any application development software.

Lower level is the client level. The client could be implemented as a thin client with interface to the application.

IV. IMPLEMENTATION

This section includes implementation details and flow of proposed architecture in levelled security and information about encryption upload, decryption download its working and explanation of database.

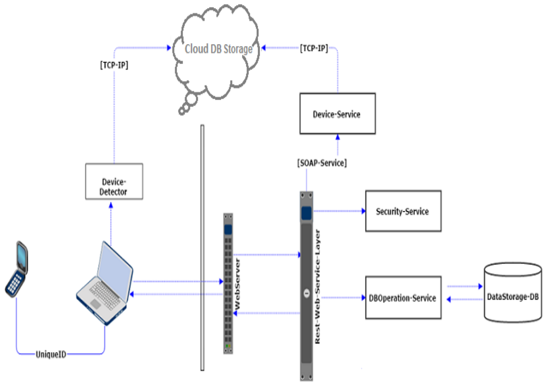

Fig. 2 Integrated structure of bi-level security

Above diagram (fig.2) explains how the system is distributed in three modules and working of these modules in terms of confidentiality and authentication is as follows.

Here, we used Amazon’s EC2 [13] platform which provides reliable, secure and inexpensive environment. This proven environment will ensure complete control of our resources. We have installed Mysql server on it.

A. *Data Server*

1. *Cloud Database Storage:*

Cloud DB storage stores data contents in encrypted format in table named data_storage in database named file_storage. This table includes attributes such as User_name, Content, Content_name.

2. *User Information Storage:*

It stores user’s information and consists of attributes such as User_Name, passwd, device_name, device_id.

3. *Server Operating Log:*

It stores user’s information and consists of attributes such as Operation_name, User_Name, Attribute (fsize).

Following table contains detailed information of data storage in tabular form.

TABLE I

DATA MODEL

DB Table Name	Data Storage Attributes
Data_Storage	User_Name, Content, Content_Name,
User_Info_Storage	User_Name, passwd, device_name, device_id
Server_Operating_log	Operation_Name, User_Name, Attribute (fsize)

B. *Application Server*

Here, we used Java Platform to implement system as standard API of java helps us to write Bluetooth application that works across many hardware platforms and java API enables application to run on different types of hardware, operating systems etc.We have implemented this system with apache tomcat server. As apache tomcat is open source software which provides HTTP web server environment for java code to run on it. To provide high level of security we have used AES symmetric key Algorithm for encrypt upload on the cloud and decrypt download from cloud storage as it is fast and effective by federal government standards.

As we used java platform which enables us to use java library named Bluecove 2.1.1[14] to communicate system O.S. with hardware device. It simply works as interface between hardware device and system O.S.

Client is implemented as a thin client with interface to the application.

C. *Security Levels*

1) *Level-1 Application Controller Level Security:*

Application controller level security is implemented at application server which is intermediate between cloud database storage and application server. This security is tied with AES algorithm which is having 128bit block size. AES algorithm is very popular for security and has been adopted by U. S. Government and now used worldwide. In this level we have provided tight bonding of security from application server to cloud storage.

2) Level-2 System Level Security:

A system level security is equipped with hardware token provided by smart phone for authenticating users and verifying who is accessing cloud service. We are communicating hardware token (Bluetooth) with system O.S. for authenticating users availability over machine through which user is accessing cloud storage system.

V. Conclusion and Future Work

We proposed a bi-level security mechanism for authenticating users which works to reduce security risks associated with client server applications on cloud to secure more sensitive data. Our mechanism deals with leveled security because it is two-fold with encryption algorithms like AES, and username-password with hardware token authentication to reduce security risks individually at different levels.

The system guarantees enhanced security at the cost of performance issues like response time, hardware connectivity, token storage. Also as the hardware devices need to be registered there is an inherent limitation to the number of users that can register the system. This can be further improvised by third party authentication or outsourcing.

Acknowledgment

I would like to take this opportunity to express my profound gratitude and deep regard to my Project Guide *Shraddha Phansalkar* for her exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. Her valuable suggestions were of immense help throughout my project work. I would also like to give my sincere gratitude to all the friends who filled in the survey, without which this research would be incomplete.

References

[1] Saini Pearson “Privacy, security and trust in cloud computing” HP Laboratories HP- 2012.

[2] Hwang, Chuang, Yi-Chang Hsu, Chien-Hsing Wu “A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service” IEEE 2011.

[3] Kuyoro S. O., Ibikunle F. & Awodele O. “Cloud Computing Security Issues and Challenges” (IJCN), Volume 3, Issue 5, 2011.

[4] Rashmi Nigoti et al “A survey of cryptographic algorithms for cloud computing” (IJETCAS) 2013.

[5] Advanced Encryption Standard - Wikipedia, the free encyclopedia.htm

[6] Hardayal Shekhawat “Mobile cloud computing security using Transient authentication system” JIKRIT 2012.

[7] Minar , Tarique, Kema Banani “A Secured Bluetooth Based Social Network” IJCA Volume 26– No.1, July 2011.

[8] http://en.wikipedia.org/wiki/Encryption

[9] Richard A.Kemmerer “Analytical encryption protocols using formal verification techniques” IEEE1989.

[10] Majdi Al-qdah, Lin Yi Hui “Simple encryption decryption application” IJCSS Volume.1.

[11] Yu-Li Lin, Tzong-Chen Wu and Chien-Lung Hsu “Secure and efficient time bound key assignment scheme for access control in hierarchical structure ” IJICIC feb. 2010.

[12] Levente el. al. “Extensions to an authentication technique proposed for the global mobility network” IEEE 2000.

[13] http://aws.amazon.com /ec2/

[14] http://bluecove.org/