Data Security Mechanism for Cloud

Mr. G. A. Patil.[1st]
[1st] Asst. Prof. & HOD. CSE Dept.
DYPCET, Kolhapur.

Mr. S. B. Patil.[2nd]
[2nd] Asst. Prof. CSE. Dept.
K. I. T. COEK, Kolhapur.

ABSTRACT

Cloud computing is a means by which highly scalable services can be consumed over Internet and network on rental basis. Various cloud service providers are offering different services over cloud environment. Many big investors like Amazon S3, EC2, Microsoft Azure, IBM Blue, are providing cloud environments. When data is stored over cloud, vendors hold a limitless possibility to access this data. Social engineering done by cloud vendors or their employees would lead to information leak or even substantial loss of data. Commonly used authentication mechanism guarantee that authenticated users can access their data, but they do not guarantee security of data from the cloud vendor. This paper emphasizes on improving existing authentication mechanism & implementing data security schemes to secure data from the cloud vendor and other users of cloud.

GENERAL TERMS*:* Cloud Security.

Keywords: Authentication by Characteristics (AC), Authentication by Knowledge (AK), Authentication by Ownership (AO), Cloud Service Provider (CSP), Public Key Infrastructure (PKI) and One Time Password (OTP).

1. INTRODUCTION

The Cloud Computing is a technology which has been in use by small, medium and large scale companies. Many end users are using cloud services. We can simply categorize users of cloud in two generalized groups. First group involving small, medium and large scale companies and second group containing end users. Depending on the size of business and requirements of infrastructure support for day to day operations, every company needs different services from Cloud Service Providers. Also, individuals will demand services as per their requirements. Here, the common issue for both categories of users is security of their data [1]. There are security concerns that prevent companies from taking advantages of the cloud [3]. Traditional mechanisms of security are not adequate for cloud environment [3]. Every single client of CSP will have different security requirements. Users will demand different levels of security. Different policies need to be decided for security provisioning [4]. The commonly used security mechanism for data access is Username and Password pair. As username password pair is concerned with authentication of user, it guarantees that only valid user will get access to data, but at the same time it is not concerned about securing data when it is stored in cloud & when it flows through network from user end to cloud and vice versa[1]. Data stored in plain text format over the cloud is a security threat.

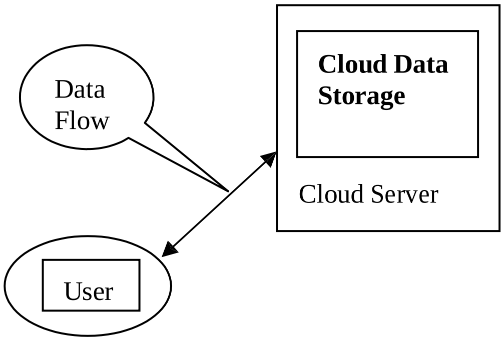

Figure1: Data Flow & Data Storage over Cloud Environment

Security Issues in the scenario shown in figure 1 are as under -

1. Data Stored over cloud is in plain text format.
2. Data flow through network is in plain text format.
3. In case encryption service is provided by cloud vendor, it cannot be trusted as CSP will have access to encryption algorithm and the key used.

The schemes explained in this paper will deal with tackling such security issues in several levels. Clients of cloud have to select appropriate registration and authentication levels. Accordingly the CSP will provide different registration levels for clients of cloud & further cloud clients use data security mechanism to secure data from cloud vendor [5].

The authentication module will address the issues by categorizing clients by their requirements of security. Categorizing of clients will be done first by registration process and then by authentication mechanism selected by clients. For registering to the cloud, user has to select one of the registration levels. In registration level-0, no documents are required for creating and accessing user account over cloud. Users will be asked to submit documents to Cloud Service Providers during level-1 of registration. While in registration level-2 documents as well as physical presence of user is required during registration. Client should register with cloud by selecting one of these registration levels.

After registration is complete Cloud Service Provider can check which level is adopted by client for registration. Higher level of registration means the access is of more importance. After registration, authentication mechanism needs to be selected, this is also provided in different ways. In authentication level-0(AK), the user is authenticated by username & password pair. Authentication Level-1(AO) needs authentication by electronic cards and pass-keys whereas Authentication Level-2(AC) is used for biometric operations.

2. Registration Mechanism

2.1 Registration Level0

In level0 registration mechanism, new users are not asked to submit any documents to open an account. They can submit on-line registration form and start using cloud service, just as we do it while opening an email account. This level is appropriate if data stored and processed over cloud is non sensitive and leak of information does not cause financial loss. (This level is appropriate for end users).

2.2 Registration Level1

Submission of documents is required for activating cloud user account. This level is recommended to avoid financial or business loss due to loss of data stored over cloud. Even a minor problem in accessing data may result in loss. In these cases client should register with cloud by submitting documents. Physical presence of user while submitting the documents is not required in this level. (This level is appropriate for small and medium scale companies).

2.3 Registration Level2

User should register to cloud by physically approaching & submitting documents to Cloud Service Provider. This is required if client has a very confidential information. Physically submitting the document verifies the users' authenticity. (This registration level is appropriate for medium and large scale companies).

3. AUTHENTICATION MECHANISMS

After completing registration procedure, users should be authenticated to cloud. Username & Password pair is a commonly used standard. This section will highlight on different levels of authentication mechanisms.

3.1 Authentication Level0

This level is known as Authentication by Knowledge-AK. After registration user should select authentication level. In Level 0 authentication, user has to select a pair of username & password. This pair will be used by user and Cloud Service Provider for authenticating user over the cloud.

Cloud Service Provider should store the user name and password. When user need to access the cloud he will be allowed by verifying his username & password.

3.2 Authentication Level1

In Authentication by Ownership – AO, user of cloud will get a swap card or other physical device, which will help him for authentication. This device should be used while accessing service from cloud. As we do with ATM cards where we swap and then enter valid pass key, the same procedure can be applied to level1 authentication service.

3.3 Authentication Level2

Authentication Level 2 is called as Authentication by Characteristics-AC, where user will be asked to submit biometric entry, e.g. thumb impression or retina image or both. In this case user has to be physically present when he wants to access a cloud service. No one else can get access to his account.

4. PASSWORD MANAGEMENT

Different levels of authentication will come with different needs of password management. Password Management can be done in the ways mentioned in table 1, depending on which authentication level has been selected by user. Password management has to be done by user himself for Authentication level0. Common practice is users should memorize the username & password. User can maintain a soft copy of username & password. In authentication level1, user gets ownership of swap cards and/or electronic gadgets. If only swap cards are available then, after successful swap he should be asked to enter valid password, based on which the access is granted or denied.

If swap cards with electronic gadget is available, then swap card will play role of username & electronic gadget will generate a OTP for that session. When user swaps card, electronic gadget will receive a password from cloud for that session. Every swap of card will get a new password from cloud. This is called as One Time Password (OTP). Table-1 below lists password type & authentication level in first column and second column describes how to manage password or carry necessary things to manage it. Second column also elaborates how user will provide password token while accessing service based on the type of password tokens that he is provided with.

Table-1: Password Management

Password Token	Description
Password or PIN token (Authentication Level 1)	A secret character string that a client memorizes and uses to authenticate his or her identity.
Password List (Authentication Level 1)	The personal soft file containing list of all passwords. List may contain PIN used for authentication.
One-time Device Password Token (Authentication Level 2)	The personal hardware device that generates the OTP - One Time Password. It should be generated and sent in decrypted form.
Soft Cryptographic token	A key that is typically stored on a USB stick or media which should be provided at the time of new session establishment.

5. PROPOSED IMPLEMENTATION SCHEMES

This section will focus on implementation of schemes to tackle three security issues as stated in the introduction part. To address these issues cloud vendor should have a private & public compartment. When user wants to store private data it should be stored in private compartment of the respective user. This compartment is accessible to particular user only. When user needs to share some data with trusted users it can be stored in his public compartment over the cloud. Public compartment will be accessible to trusted users of the owner of data. Scheme No.1 ensures privacy & security of data stored in private compartment, and Scheme No. 2 ensures that data stored in public compartment is accessible to owner & its trusted users only. Other users cannot access private & public compartment of the owner of the data.

5.1 Scheme No. 1:

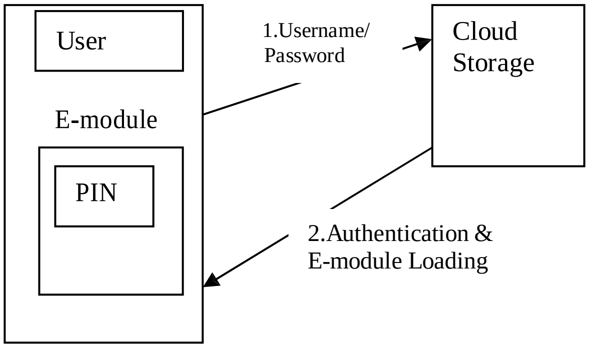

Figure 2: Authentication & Cryptographic

To access service from cloud, user should be authenticated. Depending upon authentication level selected by user, CSP should first check authenticity of user. If he is authorized, then cloud will load a E-module to client end. This E-module is a cryptographic module which will perform encryption and decryption of data when required.

When user will upload file to cloud server, E-module will encrypt data on client's end and then it will send it to storage server over the cloud. On user requests to download data stored in cloud, server will send the data in encrypted format. After arrival of the data at client end, E-module will decrypt it and original file is available to the client.

This encryption and decryption of data will be done at client side by making use of a secret key. This key will be generated on client side by E-module. To generate secret key E-module will ask user to enter a PIN no. Server does not have any idea about secret key used for encryption and PIN used to generate secret key. These both things are done at client side. So, even if the data stored is in encrypted format and the algorithm used to encrypt it is available to cloud, it is difficult to decrypt it. User is assured about security of data stored in cloud. The scheme no.1 ensures data privacy of private compartment. However this scheme does not provide public data compartment to share data among trusted users, which can be overcome by scheme No.2.

5.2 Scheme No. 2:

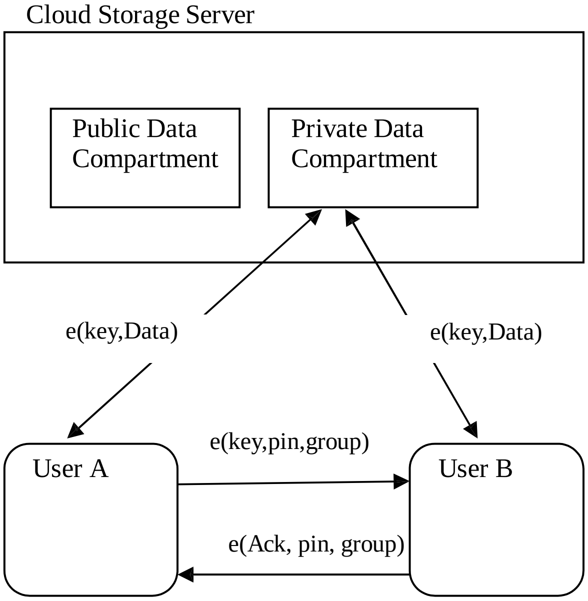

Figure 3: Group Cryptographic Module

is accessible to trusted users. So, user can create a group, and the data stored in group compartment is accessible to all members of the group. One would like to make some data public to trusted users so that it can be accessed by them. But it should be accessible to only those users who are members of group and not accessible to other users of cloud. To achieve this scheme no.2 can be implemented as shown in figure 3.

In this scheme a private area of user will be accessed in same way as explained in scheme no. 1, but for public data, group users A and B have to exchange first the PIN which will be helpful for cryptographic operations. Diffie Hellman like key exchange algorithm can be applied to implement this key exchange. After exchanging the PIN, users A and B can use this PIN to store data on public part. As both users know the PIN, they can access all the data stored in public compartment. Since the key used to store data in private compartment is known to particular user only, his private data block is secured. This scheme even can be expanded to achieve group policies like one to many, many to one and many to many group communication mechanisms.

5.3 Experimental Environment

To test these schemes we have setup a Ubuntu enterprise cloud with several nodes. The scheme no.1 is developed using java web technology, MySql and tomcat server. As scheme no.1 is based on secret key cryptography, it was implemented using RSA algorithm making use of private key to encrypt the private compartment data. However, extension can be done to encrypt public compartment using the public key of RSA. Also any other secret key algorithm can be used to implement scheme no.1. Test results of scheme no.1 show satisfactory results for providing data security over cloud environment as stated above. Because of java technology used for implementation these schemes also can be tested on live cloud of Google app engine.

6. CONCLUSION & FURTHER WORK

Data security is major issue for Cloud Computing. Data security has many aspects like integrity, availability and accessibility. This paper has highlighted on accessibility issues of cloud computing. Registration levels and Authentication Mechanism will assure data security and only authenticated person will get access to data over cloud. Data is stored in encrypted format, so only authenticated user will get access to data, who can only decrypt it. Successful implementation will give assurance to all users of cloud about their data privacy. Also, private & public compartment will make data sharing easy and secure. The efforts are undergoing for devising the stable mechanism for implementation of scheme no. 2.

7. REFERENCES

[1] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, "Data Security Model for Cloud Computing", ISBN 978-952-5726-06-0, Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009), Qingdao, China, November 21-22, 2009.

[2] Cong Wang, Qian Wang, and Kui Ren, "Ensuring Data Storage Security in Cloud Computing".

[3] Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina Elaine Shi, Jessica Staddon "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control" PARC Fujitsu Laboratories of America.

[4] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen, "Secure Provenance: The Essential of Bread and Butter of *Data Forensics in Cloud Computing"*, ACM digital library.

[5] SIMENCE, time.lex "Multilevel authentication policy mapping".

[6] ScottYilekUC, SanDiego Rescorla, Hovav Shacham Brandon Enright, UC San Diego "When Private Keys are Public:Results from the 2008 Debian OpenSSL Vulnerability", ACM digital library.

[7] Benjamin Aziz, Alvaro Arenas, "A Secure and Scalable Grid-based Content Management System", 2010 International Conference on Availability, Reliability and Security.

[8] Asoke K Talukder "Security & Scalability Architecture for Next Generation Internet Services" Geschickten Solutions Bangalore, India.

[9] Wassim Itani Ayman Kayssi Ali Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", 2009 Eighth IEEE International Conference on Dependable.

[10] Junaid Arshad, Paul Townend, Jie Xu, "Quantification of Security for Compute Intensive Workloads in Clouds", 2009 15th International Conference on Parallel and Distributed Systems.