ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

An Analysis of Cloud Computing And Multi-Level Security Using RSA Algorithm

S.NAGASUNDARAM
Assistant Professor/MCA, SakthiMariamman Engineering College, Thandalam, Chennai-602 105.
Research Scholar, SCSVMV University, Kanchipuram.

Dr.S.K.SRIVATSA
Professor (Retd), Anna University-MIT Campus, Chennai.Guide,SCSVMV University, Kanchipuram.

Abstract*—Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

***Keywords* :SaaS,PaaS,IaaS, Cloud computing, Security and control.**

I. Introduction of Security Issues Associated with the Cloud

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers.[i] Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community).[ii]Cloud security controls: Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture, they can usually be found in one of the following categories:[iii] Deterrent controls: These controls are intended to reduce attackson a cloud system. Preventive controls: Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Detective controls: Detective controls are intended to detect and react appropriately to any incidents that occur. Corrective controls: Corrective controls reduce the consequences of an incident, normally by limiting the damage.

II. Security and Privacy

1. Identity management:

Every enterprise will have its own identity management system to control access to information and computing resources.

2. Physical security:

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc.

3. Personnel security:

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities.

4. Privacy:

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety.

5. Data security:

There are a number of security threats associated with cloud data services, not only covering traditional security threats.

6. Data Confidentiality:

Data confidentiality is the property that data contents are not made available or disclosed to illegal users.

7. Data Access Controllability:

Access controllability means that a data owner can perform the selective restriction of access to his data outsourced to cloud.

8. Data Integrity:

Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that his data in a cloud can be stored correctly and trustworthily.

9. Effective encryption:
Attribute-Based Encryption Algorithm.

10. Ciphertext-policy ABE (CP-ABE):

In the CP-ABE, the encryptor controls access strategy, as the strategy gets more complex, the design of system public key becomes more complex, and the security of the system is proved to be more difficult.

11. Key-policy ABE (KP-ABE):

In the KP-ABE, attribute sets are used to explain the encrypted texts and the private keys with the specified encrypted texts that users will have the left to decrypt.[iv]

12. Fully homomorphic encryption (FHE):

Fully Homomorphic encryption allows straightforward computations on encrypted information, and also allows computing sum and product for the encrypted data without decryption.

13. Searchable Encryption (SE):

Searchable Encryption is a cryptographic primitive which offers secure search functions over encrypted data. Compliance:Numerous laws and regulations pertain to the storage and use of data.

III. Data Security using RSA Algorithm

In order to determine the data security, the data is encrypted using RSA algorithm before uploading and decrypted before downloading. Bob wants to send Alice an encrypted message M so he obtains her RSA public key (n,e) which in this example is (143, 7).

$$M^e \bmod n = 9^7 \bmod 143 = 48 = C$$

When Alice receives Bob's message she decrypts it by using her RSA private key (*d*, *n*) as follows:

$$C^d \bmod n = 48^{103} \bmod 143 = 9 = M$$

To use RSA keys to digitally sign a message, Alice would create a hash or message digest of her message to Bob, encrypt the hash value with her RSA private key and add it to the message. Bob can then verify that the message has been sent by Alice and has not been altered bydecrypting the hash value with her public key. If this value matches the hash of the original message, then only Alice could have sent it (authentication and non-repudiation) and the message is exactly as she wrote it (integrity). Alice could, of course, encrypt her message with Bob's RSA public key (confidentiality) before sending it to Bob. A digital certificate contains information that identifies the certificate's owner and also contains the owner's public key. Certificates are signed by the certificate authority that issues them, and can simplify the process of obtaining public keys and verifying the owner.

Numerical Example:

Choose p = 3 and q = 11
Compute n = p * q = 3 * 11 = 33
Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
Choose e such that 1 < e <φ(n) and e and n are co-prime.
Let e = 7

Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1] Public key is (e, n) => (7, 33)
Private key is (d, n) => (3, 33)
The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

The above RSA algorithm and numerical example shows the data encryption and decryption happening without any data loss. Similarly the above algorithm is used to do encryption anddecryption on data to be uploaded anddownloaded in the cloud.

```
    Algorithm_MSSP ( )
    {
Initialization:
    CS - Cloud Server
    CAM          -  Cloud Authentication Manager
    $U_i$  -         $i^{th}$ User wheri= 1 to n
    fori = 1 to N
    $U_i$ – join (cloud); // User do registration
    and join CS -> (usrNm, Pwd)
    endi
    fori = 1 to N
    Ui ->entry(CS)
    if (Ui.valid == true) then CS -> (usrNm,
    Pwd) end i
    fori = 1 to N
    Ui ->open(folder)
    if (Ui.valid == true) then Ui.permission=grant
    if (action==upload) then data=RSA_encryption(data)
    else if (action == download) then data =
    RSA_decryption(data) elseUi.permission=denial
    endi
    }
```

The above algorithm illustrates the entire functionality of the MSSP approach. All the new users have to get registration and an authentication password from the cloud server. While login to the cloud, the user has to get permission from the CS to do cloud activities like uploading and downloading data in their respective folder. Before uploading the data it will be encrypted using RSA algorithm and the data will be decrypted by the same RSA algorithm before uploading and downloading in the cloud. The above MSSP algorithm is written in the form of pseudo code in order to implement and verify in any computer programming language.[v]

Proposed Approach:

Three levels of security of Data Level, User Level and Data Storage Level are provided here. First one is user level security where verifies the user as a valid trustable user or not. A Dynamic Multi-Stage Password Generation (DMSPG) method is used to provide user level security. The data security is obtained by encrypting the data using RSA algorithm and finally the data maintenance security is provided by authenticating right users to access the data folder. It is well known and available is, whenever a user enters into cloud computing, the user should pass certain credentials such as username and password. If the user submitted username and the password are valid then the user can enter into cloud and can access all cloud functionalities. The password can be altered and changed by the user at any time in his account. The account of a user consists of all the information about the users. Since cloud is a multi-tenantenvironment, each user is validated by providing a password while entering into the cloud environment in the earlier studies. In this paper, the old password is regenerated by a new password and replaces the old one. Each time the password generated dynamically and automatically to improve the security.

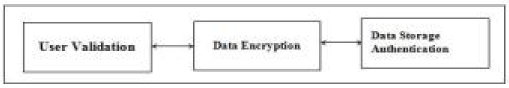

Fig.1. Security Level

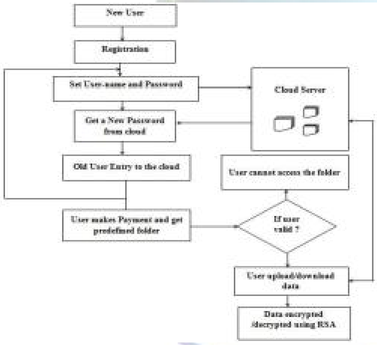
New User
Registration
Set User-name and Password
Get a New Password from cloud
Old User Entry to the cloud
User makes Payment and get predefined folder
Cloud Server
User cannot access the folder
If user valid ?
User upload/download data
Data encrypted /decrypted using RSA

Fig.2. Flow of the Proposed Approach

Whenever the user enters into the cloud he permits by verifying the old password, while authentication the Cloud Authentication Manager (CAM) provides a new password to the user for next entry to the cloud and this functionality is illustrated in Figure-2. The user password is changed dynamically and given to the user by the CAM at every entry into the cloud. Second, after receiving authentication from the CAM, the user has to make some payment in order to obtain the services in terms of software, platform or infrastructure. For any kind of services, according to the duration the user has to make a payment for utilizing the services. In this paper it is assumed that the user request for infrastructure as a service. Due to the size of the infrastructure and duration of using the infrastructure the payment will be charged. After successful payment the user will be assigned by an infrastructure (folder/web-space) with a name, where the name is given to the user. Each time the user password and the name of the folder are compared for data integrity. If and only if the CAM finds valid, the customer can upload and download their data from the folder. Else it rejects the user activity and complaint registered.[vi]

REFERENCES

[1] https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-cloudid-1

[2] https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Srinavasin-2

[3] https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Krutz.2C. Ronald.L. 2010.8.

[4] https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-16.

[5] S.Nagasundaram and S. K. Srivatsa., “A Multi-Stage security provision for cloud computing”, 2016/ Advances in Natural and Applied Sciences.10(8)June 2016, Pp 123-126.

[6] Nagasundaram.S, and Dr.S. K. Srivatsa. “A Multi-Stage security provision for cloud computing”, 2016/ Advances in Natural and Applied Sciences.10(8) June 2016, Pp 123-126.