International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Issue No. 04, April 2016
www.ijates.com
ijates
ISSN 2348 - 7550

IMPLEMENTATION OF DATA SECURITY IN CLOUD COMPUTING

Er. Nisha Yadav [1] , Dr. Amit Sharma [2]

[1] M.Tech Scholar, [2]Associate Professor, Department of Computer Science & Engineering ,
Vedant College of Engineering & Technology ,Bundi ,Rajasthan, (India)

ABSTRACT

In this research paper I am focusing on the security of data in cloud Computing. . This paper will attempt to provide a solution to protect data that is stored on the cloud. This paper is focused on the security of data/information in cloud to protect data by threats like unauthorized access, modification or miss use, denial of service attack etc. Data is a critical resource for any organization, institute or individual. The data security of cloud systems rest on the principles of confidentiality, availability, and integrity, but applied to distributed environment and dynamic architectures. Data security is very important for client in cloud computing. In cloud computing the main concern is to provide the security to client by protect files or data from unauthorized user. Security is the main intention of any technology through which unauthenticated user or intruder can't access your file or data in cloud. This model can help to encrypt and decrypt the file at the user side that provide security to data at rest as well as while moving. This model will use CHAP (Challenge-Handshake Authentication Protocol) protocol as well as RSA encryption algorithm. This will provide authentication as well as Security to the data.

Keywords- Component: Confidentiality, Cloud, CHAP(Challenge-Handshake Authentication Protocol), Decryption, Encryption, RSA(Rivest-Shamir-Adleman) Algorithm

I. INTRODUCTION

Cloud computing is a new computing technology that aims to provide reliable, customized and quality of service guaranteed, computation environments for cloud users. In cloud computing , application, software and databases are moved to the centralized large data centers, called cloud.

Cloud computing architecture is divided into two sections: **the front end** and the **back end**. They connect to each other through a network usually called the Internet. The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. On the back end of the system are the various computers, servers and the data storage systems that create the cloud of the computing services. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly.

Data protection tops the list of cloud concerns today. Vendor security capabilities are key to establishing strategic value, reports the 2012 Computerworld "Cloud Computing" study, which measured cloud computing trends among technology decision makers.

When it comes to public, private, and hybrid cloud solutions, the possibility of compromised information creates tremendous angst. Organizations expect third-party providers to manage the cloud infrastructure, but are often

uneasy about granting them visibility into sensitive data.

Derek Tumulak, vice president of product management at Vormetric, explains, "Everyone wants to use the cloud due to cost savings and new agile business models. But when it comes to cloud security, it's important to understand the different threat landscape that comes into play."

There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data

There are three service architectures of cloud:

1. Iaas (Infrastructure as a service): providers of IaaS offer computers—physical or (more often) virtual machines—and other resources. IaaS refers to online services that abstract the user from the details of infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc.

2. Paas (Platform as a service): PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform including operating system, programming-language execution environment, database, and web server.

3. Saas (Software as a service): In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs.

Data is the critical aspect in all these architectures of cloud. Data is a critical resource for any organization, institute or individual. The data security of cloud systems rest on the classical principles of confidentiality, availability, and integrity, but applied to distributed, virtualized, and dynamic architectures. data security is very important for client in cloud computing. In cloud computing the main concern is to provide the security to end user to protect files or data from unauthorized user. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. This implementation can help to encrypt and decrypt the data at the user side that provide security to data at rest as well as while moving. This model will use EAP-CHAP encryption as well as RSA encryption algorithm. This will provide authentication as well as Security to the data.

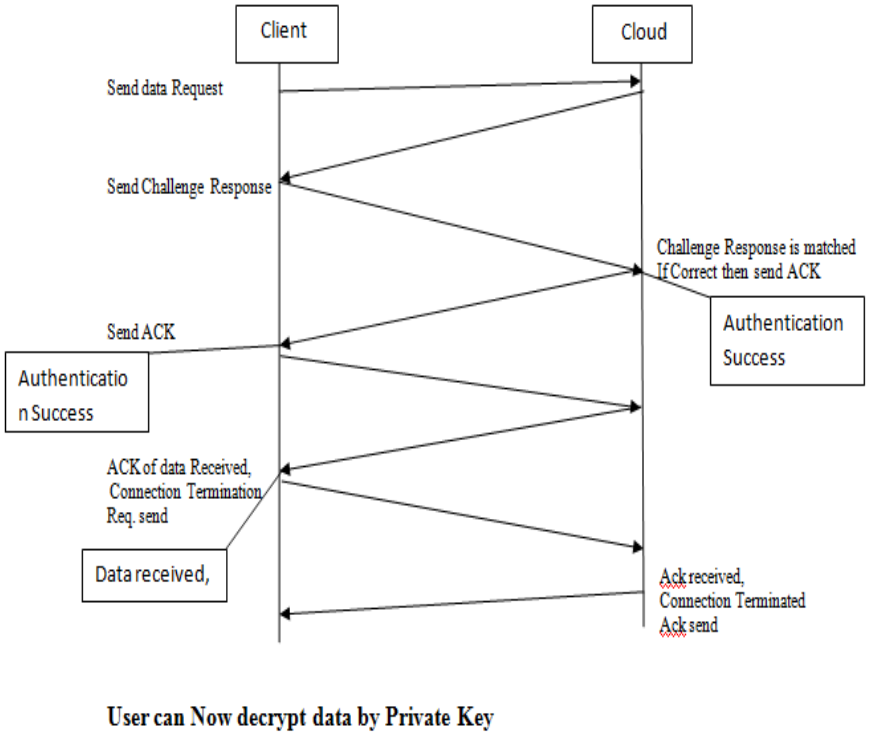

Figure1: TimeLine Diagram of Proposed Model of data security in cloud Computing

II OBJECTIVE AND PROBLEM FORMULATION

Data security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security. Cloud Computing has several major issues and concerns, such as data security, trust, expectations, regulations, and performances issues.

Some of the security concerns are listed below**:**

1. With the cloud physical security is lost because of sharing computing resources with other companies. No knowledge or control of where the resources run.
2. Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exists.
3. Customer may be able to sue cloud service providers if privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties.
4. Who controls the encryption/decryption keys? Logically it should be the customer.

Objective of this research is to provide authentication as well as authorization to the data stored in cloud. Authentication is provided by CHAP protocol by ensuring that only authorized user can download the data. It ensures that only RSA algorithm is used to provide security for data. So that data cannot be used by unauthenticated user even if he manages to access data. Since data would be in encrypted form. Data can be decrypt only after downloading by user's private key. Hence it provides security to data when downloading/moving. Hence, it prevent data leakage. Data is downloaded in encrypted form. So, this model can secure data while moving as well as when still. RSA algorithm is used as a basis to provide data-centric security for shared data. It emphasize on the integrity of data by encrypting the data. Data can only be decrypted by user who has the matching private key for data. While EAP-CHAP protocol ensure that the data can be seen and downloaded by user only who are authorized. Hence it ensures two stage securities of data.

Problem Formulation

Users who put their large data files in the cloud storage servers can relieve the burden of storage and computation. At the same time, it is critically important for users to ensure that their data are being stored correctly and safely. The major concern is the security of data at rest and while moving. So to handle this problem it is required that:

a. Data at both user and server end must be in encrypted form.
b. It should be ensured that only authenticated user can access the data.
c. Data should be in readable form if leakage persists.

III. METHODOLOGY

Methodology of proposed model includes two stages.

- First stage includes authorization through EAP-CHAP protocol to provide authorization to data.
- Stage includes encryption/decryption through RSA algorithm.

3.1 Extensible Authentication Protocol-CHAP

EAP (Extensible Authentication Protocol) will implement on Cloud environment for authentication purpose. It is used for the transport and usage of keying material and parameters generated by EAP methods. In our purposed model we use Challenge-Handshake Authentication Protocol (CHAP) for authentication.
Authentication of CHAP performs in three steps:-

1. When client demands a service, Service Provider Authentication sends a "challenge" message to client.
2. Client responds with a value that is calculated by using one way hash function on the challenge.
3. Authenticator verifies the response value against its own calculated hash value. If the values match, the Cloud provider will give service, otherwise it should terminate the connection.

3.2 RSA Encryption Algorithm

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

- Select two prime numbers.

- Calculate n = p*q.
- Calculate f(n) = (p-1)(q-1)
- Select e such that e is relatively prime to f(n) and less than f(n).
- Determine d such that de congruent modulo 1 (mod f(n)) and d<f(n).
- Public key = {e, n}, Private key = {d, n}
- Cipher text c = message e mod n
- Plain text p = cipher text d mod n

.

The steps of the methodology are given below:-

1. User sends the authentication request to the Cloud Service Provider (CSP).
2. CSP checks the authorization using EAP-CHAP and sends the acknowledgement back to the user.
3. User first encrypts his data and then outsources it to the server.
4. When the user downloads his data from CSP, it is received in the encrypted form.
5. User now decrypts the data with its own private Key.

IV. CONCLUSION

In order to fulfill the main objective of providing data security there are many research is needed since data is being uploaded to a remote location increases the ways by which data can be exploited, accessed or modified without the consent of the authorized user. This research paper proposes a method by which data can be secured while uploading/downloading as well as is only accessible to authorized user.

The investigation on confidentiality preservation and data classifications, started with a literature review. The literature view has been conducted in order to search all relevant scientific literature of top quality. The relevant academic and peer-reviewed information on the above topics is very limited at the time of writing. During the literature review, three concepts we are distilled that were related to the cloud computing paradigm in the form of dimensions. These dimensions relate to how data issued, where data is located in relation to the data owner, and how data is protected. Each of these dimensions has been answered using the Cipher Cloud framework that has been developed. Cipher Cloud encrypts the data, making its ownership exclusive to its owner and makes it independent from the facts of where the data might be stored or who manages it. Even in cases of take over and change of ownership, only the user will be able to decrypt the given data. Additionally the data is kept safe during transit using HTTPS TLS 1.0 standard making it difficult for anyone to sniff the data. Hence the objectives of the framework are fully achieved. Only technical privacy and encryption controls were analyzed and developed in this thesis paper. Such an investigation could lead to supplemental controls for limitations that might occur in cloud computing environments.

As discussed in the previous section, hybrid cloud computing is a very promising cloud deployment model that can cope with the security limitations occurring in a public cloud environment, while still being able to support many of the economic advantages of public cloud computing. Hybrid clouds depend heavily on the gateway between the private part of the hybrid cloud and the public part of the hybrid cloud. The gateway between the private and public parts of a hybrid cloud is an interesting point for further research.

REFERENCES

[1] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam,2012, An Implementation of RSA Algorithm in Google Cloud using Cloud SQL,ISSN no: 2040-7467.

[2] Rachna Arora, Anshu Parashar, 2013, Secure User Data in Cloud Computing Using Encryption Algorithms, ISSN no:2248-9622, pp.1922-1926.

[3] Koushik Akkinapalli & R. Rajeswara Rao, 2014, A Survey on Encryption and Improved Virtualization Security Techniques for Cloud Infrastructure.

[4] By Sanjoli Singla & Jasmeet Singh, 2013, Cloud Data Security using Authentication and Encryption Technique.

[5] Parsi Kalpana and Sudha Singaraju, 2012, Data Security in Cloud Computing using RSA Algorithm, ISSN 2278-5841, Vol 1, Issue 4.

[6] Dimitrios Zissis, Dimitrios Lekkas, 2010, Addressing cloud computing security issues.

[7] Anukrati Dubey & Sandeep Sahu, 2013, Challenge Token based Security for Hybrid Clouds, ISSN: 0975-4172.

[8] Mandeep Kaur, Manish Mahajan, 2013, Using encryption Algorithms to enhance the Data Security in Cloud Computing, ISSN: 2278-9723.

[9] Sonam Chugh, Sateesh Kumar Peddoju, 2012, Access Control Based Data Security in Cloud Computing.

[10] Narendra Gaurha, Dr.Manish Shrivastava, 2012, Data Security in Cloud Computing Using Linear Programming.

[11] Chandu Vaidya and Prashant Khobragade,2015, Data Security in Cloud Computing, ISSN: 2321-8169 .

[12] Andrzejak. 2010, Exploiting Non-Dedicated Resources for Cloud Computing ,In Proceedings of 12th IEEE/IFIP Network Operations & Management Symposium(NOMS 2010),Osaka Japan.

[13] Bertino, R. Ferrini 2009, Privacy- Preserving Digital Identity Management for Cloud Computing vol.32-No.2, IEEE Data Eng. Bull.

[14] D L. Ponemon 2010, Security of Cloud Computing Users, vol. 34-No. 2, International Journal of Computer Theory and Engineering.

[15] Dawson 2002, Maximizing sharing of protected information, vol.64-No.3, Journal of Computer and System Sciences.

[16] Pieters, W. 2006, Acceptance of Voting Technology: Between Confidence and Trust. In K. Stolen (Eds.), I Trust., Computer science press.

[17] Sameer Raja 2011, Cloud Computing: The Fifth Generation of Computing, International Conference on Communication Systems and Networking.

[18] Sarathy, R, dhar, K. 2006, Secure and useful data sharing Decision Support System, vol.42-No.1, Computer Science press.

[19] Xing Zhou, Xiaofei Tang 2011, Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science and Technology Harbin, china.