IJCSC 0973-7391 Volume 6 • Number 1 Sep - Mar 2015 pp.79-82 available online at www.csjournalss.com

A Framework in Cloud Computing Security of User Data using Bidirectional Authentication and Encryption

[1]Ramandeep Kaur Bhinder, [2]Dr. Dheerendra Singh and [3]Er.Gurjot Singh Sodhi
[1]Student, M.Tech CSE, SUSCET, Tangori, Mohali, Punjab, India
[2]Professor & Head, Dept. of CSE, SUSCET, Tangori, Mohali, Punjab, India
[3]Assistant Professor, Dept. of CSE, SUSCET, Tangori, Mohali, Punjab, India
ramandeep.bhinder91@gmail.com, professordsingh@gmail.com, gurjotsinghcse@sus.edu.in

Abstract- Cloud computing is a technology that provides services over the internet. Cloud act as Data Centre. A customer utilizes clouds resources and services and is charged accordingly. Security is the most important concern in cloud computing. There are many security issues of cloud computing which are related to trust, data confidentiality, authentication, access control etc. The impact of data security and the extent of loss that is suffered due to unauthorized access to cloud data motivates to take the problem as a challenge and come up with feasible solutions that can protect the data from theft, mishandling.In this paper a security technique is proposed for cloud computing environment that provides Bidirectional Authentication between client and server. In the proposed technique, the Hybrid Encryption Algorithm involving RSA and AES with chaotic theory is used. The proposed technique involves two steps: Authentication and Encryption. Client provides a new password for each new file to be saved in cloud storage. This will create basis of chaos theory - Randomness. The proposed technique provides improved level of security to the cloud computing framework.
Index Terms- Cloud Computing, authentication, encryption.

I. Introduction

Cloud Computing nowadays is the essential part of the computing world with every day increases in its usages and popularity. Large number of users is now dependent on Cloud Computing application for their day to day work of professional and personal life. Cloud Computing is a technology to provide services over the internet. Cloud act as data Centre. A customer utilizes clouds resources, storage and other services and is charged accordingly. Subscription to cloud is based on the type of services requires by users Iaas (Infrastructure as a service), Paas (Platform as service) and Saas (Software as a service). Therefore Cloud Computing has emerged as a means by which computational power storage, resources and application as provided to users as 'Utility' for meeting their demands. This cloud model promotes availability. It is composed of five essential characteristics, three service models and four deployment models.

1.1 Essential Characteristics:

On-demand self-service: Cloud Computing environment provides end user a simple, efficient and flexible way to carry on the provisioned storage, services, resources and computing power. This all is an immediate action taken place by users without interaction with third party or Cloud Service Provider (CSP).

Broad network access: Resources hosted by cloud computing environment are available at broader network range of devices (e.g., mobile phones, laptops, and PDAs). The resources can be accessed by user from any location and any network device.

Resource pooling: Cloud services provider serves many clients with same set of provisioned scalable services and resources. Cloud Service Provider (CSP) creates a perception of infinite resources available by controlling and managing resources at meta-level. According to clients demand, resources are allocated and de-allocated. Aim is to separate client response from actual handling of management of resources regardless of their location.

Rapid elasticity: Cloud computing framework provides user the seamless service allocation and de-allocation. Elasticity of resources is rapid that is scale up and scale down for the users for the effective and efficient functioning of cloud environment.

Measured Service: In a cloud computing framework, cloud service provider (CSP) controls and monitors aspects of cloud services (e.g., storage, processing, bandwidth, and active user accounts). These aspects are needed for billing according to which particular user is charged by some billing

mechanism. This also helps in effective use of resources, overall predictive planning, access control, capacitive planning and other tasks.

1.2 Service Models:

Cloud Infrastructure as a Service (IaaS): This cloud service model deals with cloud infrastructure services. These are self-service model for managing, accessing and monitoring data storages. The remote datacenter infrastructure includes virtualized computation, storage, networking and networking services (e.g: firewalls). IaaS user manages application, runtime, data, middleware, etc. Service provider also manages user services usage. In IaaS model, a third party provider provides hardware, software, storage and other components of infrastructure and manages them according to user needs.

Cloud Software as a Service (SaaS): This is also known as cloud application services. This model is a software distribution model where software are hosted and managed by cloud providers, for the clients over the network. By the Software as a Service model client are not required to purchase and install software on their devices (personal computers, laptops, etc.) but can directly access from the cloud. SaaS provides several benefits: wider accessibility, easy collaboration, compatibility, easy and effective administration, automatic updates and management.

Cloud Platform as a Service (PaaS): These services are also known as cloud platform services. In this model Cloud Service Provider (CSP) provides cloud component to software for application and other developments to the users. Users can use PaaS framework for development, testing, running, customizing and deployment of applications. All of these features can be carried out by user in a quick, simple and cost effective manner. Users or developers of applications manages application, remaining management of services, storage, networking, Operating systems and others are done by service providers.

1.3 Deployment Models:

Public cloud: Public cloud is basically the normal cloud computing environment. A large number of clients are provided resources, applications and services by the cloud service provider (CSP) using same shared framework over the internet. Public cloud model can be faster deployed with much more scalability and accessibility. Public cloud uses same set of resources and provides them to multiple users, therefore it is cost effective

Private cloud: This is also called an inside or internal cloud of an organization, or the corporate cloud. It is implemented within the organization firewall and is controlled by the IT department. In private cloud, only the specified client can operate. Private clouds can be seen as traditional local access networks (LAN) with benefits of virtualization.

Hybrid cloud: Hybrid cloud is a cloud computing environment which is a combination of both public cloud and private cloud. Organization can perpetuate control of their internally managed private cloud while count on public cloud when needed. Hybrid cloud environment allows workload to move between private cloud and public cloud when computation needed and cost changes. It gives organization more data deployment methods and options. Hybrid clouds are important for dynamic workloads or workloads which are highly changeable. This type of cloud helps organization in recovering data in case of emergency or disaster and gets the business back online quickly without any loss.

Community cloud: Community cloud is multi-user infrastructure that is shared by number of organizations to carry out common computing objectives. Objectives can be related to performance requirements such as host applications or related to regulatory compliance such as audit. Community cloud is the combination of public cloud and private cloud. Community cloud realizes features and benefits of public cloud-multi-tenancy and pay-as-per-usage, and private cloud- security and privacy. Community cloud can be implemented on-premises, off-premises or by third party managed service providers.

II. Proposed Technique

The proposed algorithm includes two steps:

Authentication: It is the process of identifying a user. Authentication will be done from both the sides-server and client side which makes the communication more secure and results in secured cloud services. After a successful authentication from both sides users will be allowed to access their data stored on the cloud and can store data over authenticated cloud. While authentication of users and server the whole communication will be done using RSA. Figure below shows the two way authentication from client and server. K_{PC}, K_{RC}arethe pair of public and private key of client side and $K_{PS}, K_{RS}$are the pair of public and private key of server side. During the connection between server and client both will share their public key K_{PX}, (X is

either server or client) with each other so that the further communication between the two will be secured, both will now communicate with each other after encrypting data with the each other's public key and decrypt their own private key, K_{RX}. At the client end usernameU, password P will be send along with the message R_{1c} which will be used to authenticate server. Rest of the steps is explained in the figure below.

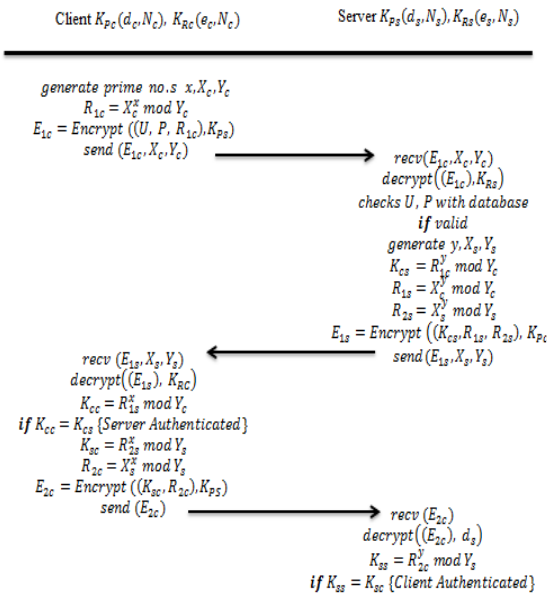

Figure 1 Working of Bidirectional Authentication

Encryption: The encryption is done by cryptographic agent using Advance Encryption Standard algorithm. Whenever data is stored over cloud it will be encrypted using secret key asked at the time of uploading by the user. Different secret key can be given for different file and hence chaos of decrypting any file will increase. Since this key is known to client only, so while accessing its own file, only client can decrypt it. This approach makes the data more secure from attacks. The client accesses the services of cloud by login through a web application. The database used at the back end for storing the details of the client is MySQL. Figure below shows the steps after successful authentication of server and client.

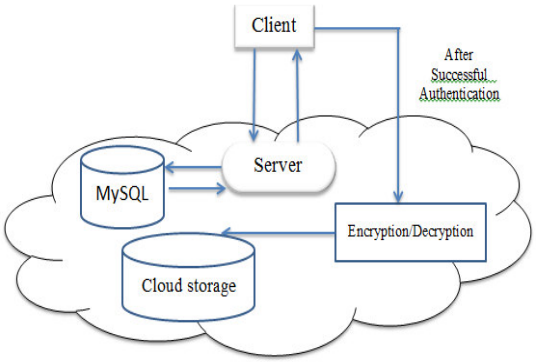

Figure2 Basic Diagram of Proposed Method

III. Conclusion and Future work

Cloud Computing is a technology to provide services over the internet.There are many security issues of cloud computing which are related to trust, data confidentiality, authentication, access control etc. The impact of data security and the extent of loss that is suffered due to unauthorized access to cloud data motivates to take the problem as a challenge and come up with feasible solutions that can protect the data from theft, mishandling. In this paper a security technique proposed for cloud computing environment that provides Bidirectional Authentication between clients and server. The Hybrid Encryption Algorithm involving RSA and AES with chaotic theory is developed. The proposed technique involves two steps: Authentication and Encryption. Client provides a new password for each new file to be saved in cloud storage. This will create basis of chaos theory - Randomness. The proposed technique provides improved level of security to the cloud computing framework. In the future work, confirmation can be provided to the particular user about passwords. Also, different key values can be taken and checked against encryption decryption variations and possible attacks.

REFERENCES

[1] Cao, Ning, et al. "Privacy-preserving multi-keyword ranked search over encrypted cloud data." Parallel and Distributed Systems, IEEE Transactions on25.1 (2014): 222-233.

[2] Prajapati, Ashish, and AmitRathod. "Enhancing Security in Cloud Computing Using Bi-directional DNA Encryption Algorithm." Intelligent Computing, Communication and Devices.Springer India, 2015.349-356.

[3] Li, Ming, et al. "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption." Parallel and Distributed

Systems, IEEE Transactions on 24.1 (2013): 131-143.
[4] Mishra, Neha. "A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues." RIET-IJSET: International Journal of Science, Engineering and Technology 2.1 (2015): 59-68.
[5] Suryadi, M. T., and Eva Nurpeti. "Performance of Chaos-Based Encryption Algorithm for Digital Image." TELKOMNIKA (Telecommunication Computing Electronics and Control) 12.3 (2014): 675-682.
[6] Sajid, Mohammad, and ZahidRaza. "Cloud Computing: Issues &Challenges."International Conference on Cloud, Big Data and Trust, Madhya Pradesh, India. 2013.
[7] Nagaraj, Srinivasan, et al. "A Bio-Crypto Protocol for Password Protection Using ECC." Bulletin of Electrical Engineering and Informatics 4.1 (2015): 67-72.
[8] Saparudin, Saparudin, GhazaliSulong, and Muhammed Ahmed Saleh. "Multi Facial Blurring using Improved Henon Map." TELKOMNIKA (Telecommunication Computing Electronics and Control) 12.4 (2014).
[9] Madan, Mamta, and MohitMathur. "Cloud Network Management Model A Novel Approach to Manage Cloud Traffic." arXiv preprint arXiv:1411.2084 (2014).
[10] Ahmad, Tauseef, et al. "Development of Cloud Computing and Security Issues." Information and Knowledge Management.Vol. 3.No. 1. 2013
[11] Kumar, Mohit, AkshatAggarwal, and AnkitGarg. "A Review on Various Digital Image Encryption Techniques and Security Criteria." International Journal of Computer Applications 96.13 (2014): 19-26.
[12] Mahajan, Prerna, and AbhishekSachdeva. "A study of Encryption Algorithms AES, DES and RSA for Security." Global Journal of Computer Science and Technology 13.15 (2013).
[13] Singh, Gurpreet, and A. Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security." International Journal of Computer Applications 67.19 (2013): 33-38.
[14] Sivasakthi, T., and N. Prabakaran. "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing."International Journal of Innovative Research in Computer and Communication Engineering 2.2 (2014): 456-459.
[15] Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." INFOCOM, 2010 Proceedings IEEE.Ieee, 2010.
[16] Ercolani, Giuseppe. "Cloud Computing Services Potential Analysis.An integrated model for evaluating Software as a Service." Cloud Computing(2013): 77-80.
[17] Sidhu, Aparjita, and Rajiv Mahajan. "RESEARCH ARTICLE ENHANCING SECURITY IN CLOUD COMPUTING STRUCTURE BY HYBRID ENCRYPTION." International Journal of Recent Scientific Research 5 (2014): 128-132.
[18] Ferretti, Luca, Michele Colajanni, and MircoMarchetti. "Distributed, concurrent, and independent access to encrypted cloud databases." Parallel and Distributed Systems, IEEE Transactions on 25.2 (2014): 437-446.
[19] Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." System Sciences (HICSS), 2011 44th Hawaii International Conference on.IEEE, 2011.
[20] Horváth, Máté. "Attribute-Based Encryption Optimized for Cloud Computing."SOFSEM 2015: Theory and Practice of Computer Science. Springer Berlin Heidelberg, 2015.566-577.