ISSN: 2321-7782 (Online)
Volume 1, Issue 7, December 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

A Review: Data Security Approach in Cloud computing by using RSA Algorithm

Anjana Chaudhary[1]
M.Tech Scholars
Computer Science and Engineering
L.R. Institute of Engineering and Technology
Solan - India

Ravinder Thakur[2]
Assistant Professor
Department of CSE
L.R. Institute of Engineering and Technology
Solan - India

Manish Mann[3]
Assistant Professor
Department of CSE
L.R. Institute of Engineering and Technology
Solan - India

Abstract: ***Cloud computing is becoming very popular computing paradigm for network applications. Cloud computing is basically an on-demand utility. Cloud computing provides different types of services and applications in the internet cloud. In cloud computing, Data Storage as a service (DaaS) allows users to store their data on remote servers and also have instant access to their data from any location using the internet connection. The data communication on the internet or over any networks is at risk to the attackers attack. So in order to secure the data some encryption scheme is used. In this project, we study the architecture of the cloud and also secure our network so that only authorized persons can access the data. For this, we propose a method for data storage and securing data in cloud computing environment by using the encryption method.***

Keywords: Cloud computing, Security, Data Storage, Data Encryption, Data Decryption.

I. INTRODUCTION

1.1 Cloud Computing

Cloud computing is a model of information processing, storage, and delivery in which physical resources are provided to clients on demand. Instead of purchasing actual physical devices servers, storage, or any networking equipment, clients lease these resources from a cloud service provider as an outsourced service. It can also be defined as "management of resources, applications and information as services over the cloud (internet) on demand" [3]. In order to define cloud computing, it is first necessary to explain what is referenced by the phrase "The Cloud". The first reference to "The Cloud" originated from the telephone industry in the early 1990s, when Virtual Private Network (VPN) service was first offered [5]. In cloud computing, data and programs are stored centrally and accessed anytime from anywhere by different users. To prevent our sensitive information, data owners may have to encrypt their data before sending. In this way, only the authorized users with the decryption keys can recover the data.

1.2 Abstraction Layers of Cloud Computing

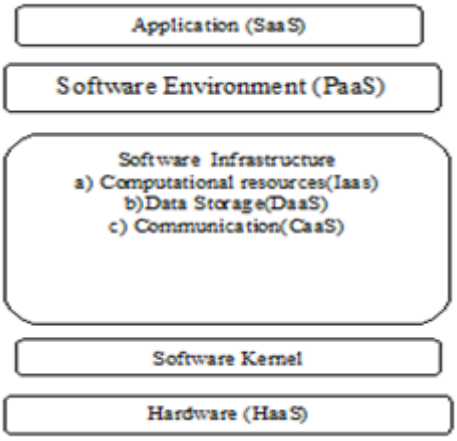

Fig 1. Shows five abstraction layers of cloud computing

1.2.1 Abstract Layers

A) The bottom layer is the physical hardware known as Hardware as a service (HaaS) in which the cloud-provider owned servers and switches that serve as the cloud's backbone.

B) The next layer consists of the cloud's software kernel which acts as a bridge between the data processing performed in the cloud's hardware layer and the software infrastructure layer which operates the hardware. Its main job is to manage the server's hardware resources while at the same time allowing other programs to run and utilize these same resources.

C) The abstraction layer above the software kernel is called software infrastructure. This layer renders basic network resources to the two layers above it in order to facilitate new cloud software environments and applications that can be delivered to end-users in the form of IT services. The software infrastructure layer provides different types of services that can be separated into three different subcategories: computational resources, data storage, and communication.

D) The next layer is called the software environment, or platform layer commonly referred to as Platform as a Service (PaaS). The primary users of this abstract layer are the cloud application developers that distribute their programs using the cloud.

E) The top layer of cloud computing above the software environment is the application layer known as Software as a Service (SaaS). This layer acts as an interface between cloud applications and end-users to offer them on-demand and many times fee-based access to web-based software through their web browsers [5].

1.3 Security issues in Cloud Computing

In cloud computing, data owners can store their data in the cloud remotely in order to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. The Cloud Service Providers (CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data. Cloud computing provides access to data, but the challenge is to ensure that only authorized entities can gain access to it. When we use cloud environments, we rely on third parties to make decisions about our data and platforms in ways never seen before in computing [7].

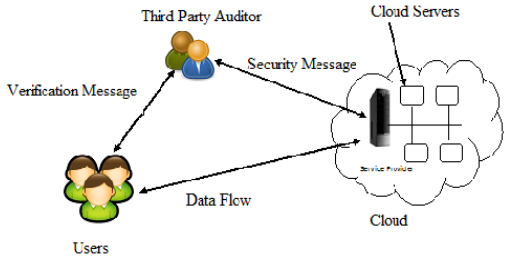

Fig 2. Shows the architecture for cloud computing storage

The advantage of cloud is cost savings. The prime disadvantage is security. Since the data placed in the cloud is accessible to everyone, security is not guarantee. I propose a method for Cloud Computing system by providing data storage and securing Cloud Computing system using RSA algorithm. In this method some important security services including key generation, encryption and decryption are provided in Cloud Computing system [4].

The architecture consists of four different entities: data owner, user, cloud server (CS), and Third party Auditor (TPA).

Here the TPA is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request. In this, the data owner may represent either the individual or the enterprise customer, who relies on the cloud server for remote data storage and maintenance, and thus is relieved of the burden of building and maintaining local storage infrastructure.

Cloud computing is a model for information and services by using existing technologies. It uses the internet infrastructure to allow communication between client side and server side services/applications. In cloud computing, Cloud service providers (CSP's) exist between clients that offer cloud platforms for their customers to use and create their own web services. The major security challenge is that the owner of the data has no control on their data processing. Due to involvement of many technologies including networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management, various security issues arises in cloud computing.

Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders.
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile [3]. The main objectives of this research are to secure the users data so that only authorized users can access the data.

II. LITERATURE REVIEW

2.1 CLOUD COMPUTING

Cloud computing is an internet based computing where users can share their data, resources, software and it can also provide information to computers and many other devices on demand. Cloud computing is a new technology that delivers many types of resources on the internet. So, cloud computing uses internet as a communication medium to deliver its services. Cloud computing can be offered within enterprises through LANs but in reality, it does not operate globally without internet. Many

enterprises and other organizations need to store and operate on a huge amount of data. Cloud computing aims at renting such resources on demand [10].

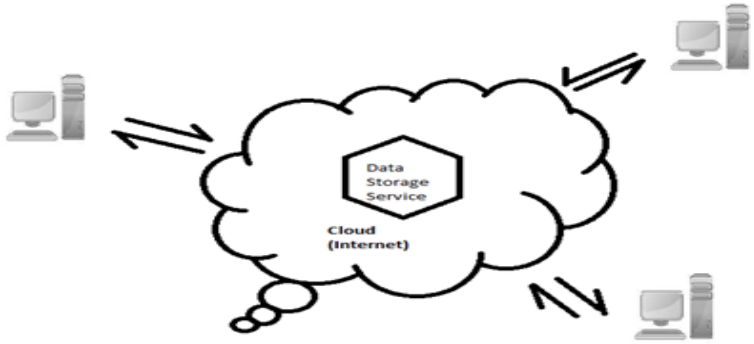

Fig 3. Cloud Computing

The National Institute of Standards and Technology (NIST) defines cloud computing as a model for convenient, on-demand network access to computing resources such as networks, servers, storage, applications etc. The word "cloud" refers to the Internet, clouds can be public, private, or hybrid (a combination of both public and private clouds)[4].

2.2 CLOUD DEPLOYMENT MODELS

A) Public Cloud: In public cloud, the cloud infrastructure is available to the general public.

B) Private Cloud: In private cloud, the cloud is available solely for a single organization.

C) *Community Cloud:* In this type of cloud deployment model, the infrastructure of the cloud is shared by several organizations and supports a specific community with shared concerns [6].

2.3 ARCHITECTURAL LAYERS of CLOUD COMPUTING

A) Software as a service (SaaS) Software as a Service features a complete application offered as a service on demand. A single instance of the software runs on the cloud and services multiple end users or client organizations.

B) Platform as a service (PaaS) This service encapsulates a layer of software and provides it as a service that can be used to build higher-level services.

C) Infrastructure as a service (IaaS) Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network [9].

2.4 CLOUD COMPUTING EVOLUTION

There has always been a debate about the evolution of Cloud Computing and Grid Computing. Some people think that both work on same phenomena while others call Cloud Computing as an extension of Grid computing. The table below shows that Cloud Computing is different from Grid computing. Cloud Computing use the concept of virtualization to maximize the computing power. Virtualization, by separating the logical from the physical, resolves some of the challenges faced by grid computing".

	Grid Computing	**Cloud Computing**
Means of utilization	Allocation of multiple servers onto a single task or job	Virtualization of servers; one server to compute several tasks concurrently

Typical usage pattern	Typically used for job execution, i.e. the execution of a program for a limited time	More frequently used to support long-running services
Level of abstraction	Expose high level of detail	Provide higher-level Abstractions

Table 2. Difference between Grid Computing and Cloud Computing

Grid Computing is the starting point and basis for Cloud Computing. Cloud Computing basically represents the increasing trend towards the external deployment of IT resources, such as computational power, storage or business applications, and obtaining them as services [6]. Cloud computing is a fast growing area in computing research and industry today. It has the potential to make the not so new idea of 'computing as a utility' a reality in the near future.[8]

2.5 CHARACTERISTICS [4]

Characteristics	Description
Manageability	The ability to manage a system with minimal resources
Access Method	Protocol through which cloud storage is exposed
Performance	It is measured by using bandwidth and latency
Scalability	Ability to scale in order to meet higher demands or load in better way
Data availability	Measure of a system's uptime
Control	Ability to control a system, to configure for cost, performance etc.
Storage	Measure of how efficiently the raw storage is used.
Cost	Measure of the cost of the storage.

Table. 3 Characteristics of Cloud Computing

2.6 Various Attacks in Cloud Environment

Cloud computing is becoming one of the most enticing technologies, because of its cost-efficiency and flexibility. Various security issues in the cloud are impeding the vision of cloud computing as a new IT procurement model. Existing cryptographic techniques can be utilized for data security, but privacy protection and outsourced computation need significant attention—both are relatively new research directions [8]. Many of the companies encrypt your files while they are en-route to the cloud *and* guard your files while in storage. Cloud computing provides access to data, but the challenge is to ensure that only authorized entities can gain access to it[2]. Data as a Service (DaaS) is emerging as an important service model in which data stored in the cloud is made available to customers based on their access criteria (decided by the data owner).On one hand, the legal implications of the data (especially in cloud computing data location matters as the laws governing the data differ across geographic boundaries) and applications being held by a third party are complex and are not well understood [1]. Our research focus is to provide a solution for the threats that are the major issue for anyone when they want to adopt cloud services for their work. For this purpose, a framework should be designed for execution of data and information securely in cloud environment. It will protect users' data, messages, information against various attacks. Some of the most common attacks are described in Table 4.

Name of the attack	Description
Tampering	Attacker may alter the information stored in the database
Eavesdropping	Attacker gains access over the data path
Viruses and Worms	These are piece of code that decrease the performance of hardware and application

Table 4. Shows different security attack

III. Security Architecture for Cloud Computing by using Third Party Auditor

3.1 Security Architecture of Cloud Computing

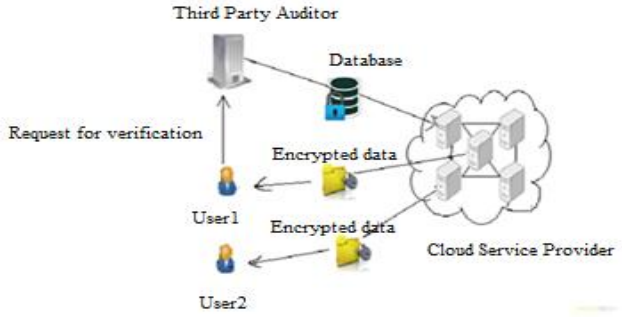

Fig 4. Security model for cloud computing

Our research focus is to provide a solution for various threats that becomes major issue for anyone when they want to adopt cloud services for their work. For this purpose, a framework should be designed for execution of data and information securely in cloud environment. It will protect users' data, messages, information against various attacks. The main objectives of this research are to secure the users data so that only authorized users can access the data.

The fig 4 above shows various components in the security model for cloud computing: Cloud controller, users and cloud storage. Here Third Party Auditor is used to ensure the security in the cloud data storage. The following steps are performed before the data transfer i.e.

1. The user sends a message for data authentication to the Third Party Auditor.
2. The Third Party Auditor checks the user's request for data authentication.
3. If the user is an authorized person then data has been transfer to the user in encrypted form.
4. The Third Party Auditor sends denied message to the user if he/she is not authorized.

IV. Conclusion

In this report, we give the overview of data storage as well as security in cloud system. The main idea behind this report is to provide integrity to the cloud storage area. In order to provide security in cloud computing we use RSA algorithm. In this method some important security services including key generation, encryption and decryption are provided in Cloud Computing system. Here the TPA is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request. The main goal is to securely store and manage the data so that only authorized users can have access over the data.

Acknowledgement

It gives me immense pleasure to express my deepest sense of gratitude and sincere thanks to my highly respected and esteemed guide Er. Ravinder Thakur, Asst. Professor CSE Deptt., LRIET, SOLAN for their valuable guidance, encouragement and help for completing this work. Their useful suggestions for this whole work and co-operative behavior are sincerely acknowledged. I also wish to express my gratitude to (Dr. Manish Mann) for his kind hearted support and guidance.

References

1. Bharath K.Samanthula,Yousef Elmehdwi, Gerry Howser, Sanjay Madrian,"A secure data sharing and query processing framework via federation of cloud computing", Department of Computer Science, Missouri University of Science and Technology, 500 West 15th Street, Rolla, MO65401, United States, 2013
2. Mark D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions", The Journal of Systems and Software 86 (2013) 2263–2268

3. Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO. 3, March 2012
4. Rupali Sachin Vairagade1, Nitin Ashokrao Vairagade 2,"Cloud Computing Data Storage and Security Enhancement", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 6, August 2012
5. Fei Hu1, Meikang Qiu2, Jiayin Li2, Travis Grant1, Draw Tylor1, Seth McCaleb1, Lee Butler1 and Richard Hamner 1,"A Review on Cloud Computing: Design Challenges in Architecture and Security",Journal of Computing and Information Technology - CIT 19, 2011, 1, 25–55 doi:10.2498/cit.1001864
6. Rehan Saleem (831015-T132),"“CLOUD COMPUTING’S EFFECT ON ENTERPRISES” “…in terms of Cost and Security”, January, 2011
7. Hassan Takabi and James B.D.Joshi University of Pittsburgh Gail-Joon Ahn Arizona State University,"Security and Privacy Challenges in Cloud Computing Environments",COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES NOVEMBER/DECEMBER 2010
8. Bhathiya Wickremasinghe,"CloudAnalyst: A CloudSim-based Tool for Modelling and Analysis of Large Scale Cloud Computing EnvironmentsT,"433-659 DISTRIBUTED COMPUTING PROJECT, CSSE DEPT., UNIVERSITY OF MELBOURNE,2009
9. Sun microsystem,”Introduction to Cloud Computing architecture”, White Paper 1st Edition, June 2009
10. Sven Bugiel1, Stefan Nurnberger1,Ahmad-Reza Sadeghi1,Thomas Schneider2,”TwinClouds:An Architecture for Secure Cloud Computing”, Center for Advanced Security Research Darmstadt, Technische University at Darmstadt, Germany.

AUTHOR(S) PROFILE

Anjana Chaudhary, received the Diploma in Computer Science from Himachal Pradesh Takniki Shiskha Board, Dharamshala in 2009 and B.Tech. in Computer Science from Kurukshetra University,Kurukshetra in 2012. She is currently a M. Tech. candidate in the Department of Computer Science at the Himachal Pradesh Technical University, Hamirpur. Her current research interests include cloud computing and its security.

