Review Study of Cloud Computing – Benefits, Risk, Challenges and Security

MOHD DANISH[1], PRACHI SHARMA[2]
[1,2] *Department of Computer Engineering, Poornima College of Engineering, , Jaipur, Rajasthan. India*

Abstract- ***Cloud Computing is define as a mode, for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources like networks, servers, storage, application, services etc. Cloud Computing is a term to delivering any and all Information Technology from computing power to computing infrastructure, application, business process, storage and personal from collaboration to an end-user as a service. Cloud Computing is a set of sophisticated and on-demand computing services initially offered by commercial providers, such as Amazon, Google and Microsoft etc.***

Index Terms- Cloud Computing, Benefits, Risk, Security, Challenges, Security issues.

I. INTRODUCTION

Cloud computing appeared in 2006, when Amazon Elastic Computing Cloud (EC2) introduced into the world. Many information Enterprises develop their platform for cloud computing. In 2007, Dell releases his solution of cloud computing, at the same time IBM Blue Cloud comes in. Such as Google Map-reduce, Microsoft Windows Azure According to an estimation, by 2012, the Cloud computing market reached $420 billion. All this has shown the coming of the era of cloud computing.

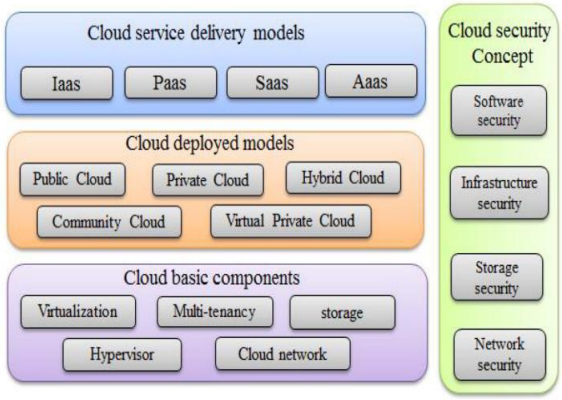

Figure-1 Software Services[9]

Table 1.1 – Cloud Services provider

Company	Products/Services
Amazon	Elastic Compute Cloud(EC2) Simple Storage Service(S3)
Google	Google App Engine Google Drive Google Maps
Microsoft	Windows Azure Microsoft SQL services

There are Four type of services provide by cloud computing-

A. Software as a Service (SaaS)

In a Cloud Computing SaaS provide a on Demand Network. In A cloud Computing Main Access Tool is Web browser.

Example-Billing Software,Image and Vidio editor.

B. Platform as a Service (PaaS)

In Cloud Computing PaaS Provide a Software Application without to install the software tool in his computer. In A cloud Computing Main Access Tool is cloud development Environment.

Example-Operating System, Software Tresting Tools.

C. Infrastructure as a Service (IaaS)

In Cloud Computing IaaS Provide a infra structure which are Physically suituated at remote location from a consumer. In A cloud Computing Main Access Tool is Virtual infrastructure manager.

Example-Computer server, processing power.

II. PROBLEM DOMAIN

1.1 Importance of the Research Problem

1.1.1 Problem in cloud security

The three issues of cloud computing security are: confidentiality, integrity and availability.

A. Availability

Availability is reliable and timly access to cloud data. In security service cloud Computing system are working order.

B. Integrity

Integrity means data are not modified unauthorised user.But unothorised data are not change othorised person.

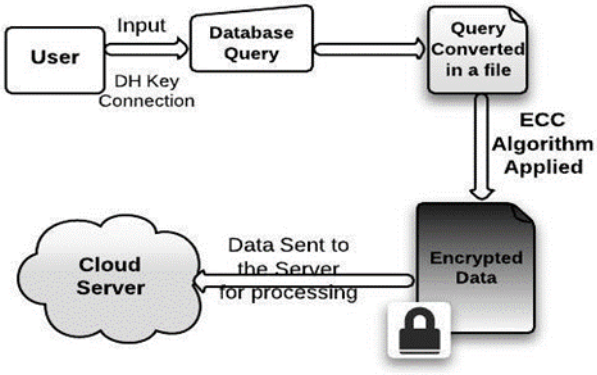

Figure 2- Data Processing view of Client[3]

C. Confidentiality

Confidentiality means internal information are secure. But to not access and changed unauthorized user.

III. OBJECTIVE

In Cloud Computing Protect Internet browsers from attacks to secure end-user security. In Cloud Computing to protect Internet-connected personal computing devices by applying security software, personal firewalls and patches on a regular maintenance schedule.

In Cloud Computing main Objective is to secure a data combing RSA and SHA1 for the better security.

IV. LITERATURE REVIEW

There are some important definitions and review on Cloud computing: National Institute of Standards and Technology (NIST)- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [1]

Aaron Ricadela -

"Today's combination of high speed networks, sophisticated PC graphics processors, and fast, inexpensive servers and disk storage has tilted engineers toward housing more computing in data centers. In the earlier part of this decade, researchers espoused a similar, centralized approach called "grid computing." But cloud computing projects are more powerful and crash-proof than grid systems developed even in recent years." [2]

Kirill Sheynkman

"The 'cloud' model initially has focused on making the hardware layer consumable as on-demand compute and storage capacity. This is an important first step, but for companies to harness the power of the cloud, complete application infrastructure needs to be easily configured, deployed, dynamically-scaled and managed in these virtualized hardware environments." [3]

V. BASE PAPER METHODOLOGY AND DESCRIPTION

We are combing RSA and SHA1 for the better security. RSA is for the encryption and decryption of the data and SHA1 is for generating hash value. It helps to provide security which only the authorized user can access it.

In this algorithm we are taking a string and we will generate the public key and private key and encrypt the string using the RSA algorithm and finally generating the hash value of the same message using SHA1.

VI. LIMITATIONS OF THE BASE PAPER

In a cloud computing there are various Limitation security issues, Confidentially, Integrity, Availability, Authentication, Authorization, Auditing, Accountability face during cloud engineering.

VII. DESCRIPTION OF THE PROPOSED RESEARCH WORK

RSA Algorithm

The RSA algorithm is cryptographic algorithm. RSA stands for (Ron Rivest, Adi Shamir and Len Adleman).RSA includes of Public-Key and Private-Key. In Cloud computing Data is Encryption by Public–Key and Dcryption by Private-Key.

It is a three step process-

1. Generation Key
2. Encryption Key
3. Decryption Key

1. Key Generation-

The first step in the RSA algorithm is key generation. It should be done before the encryption process.

2. Encryption:

Encryption is the process of converting original message/Readable (Plain Text) into (cipher Text) Unreadable message.

3. Decryption:

Decryption is the process of converting Unredable message (Cipher Text) into (plain Text) readable message.

SHA1 (Secure Hash Algorithm)-

1. SHA1 is a cryptographic algorithm for creating hash function.
2. A hash algorithm is the algorithm which convert the string of any length into a unique length string (Input).
3. The converted string (output) is comparatively smaller than the input data.
4. It is generally used to ensure data integrity, passwords authentication and message integrity.
5. One way encryption is the result of a special mathematical function known as hash function.
6. SHA-l processes input data in 512-bit blocks.

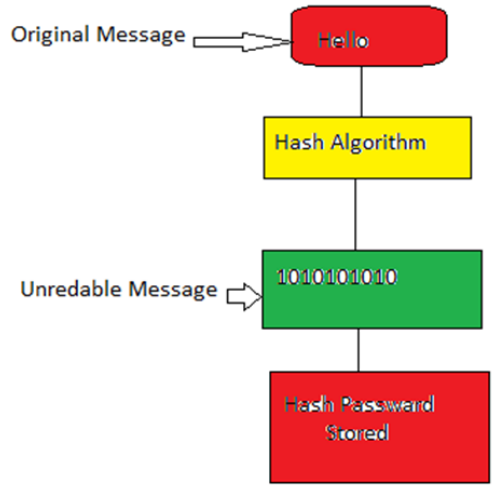

Figure 3.1- SHA1 Algorithm [8]

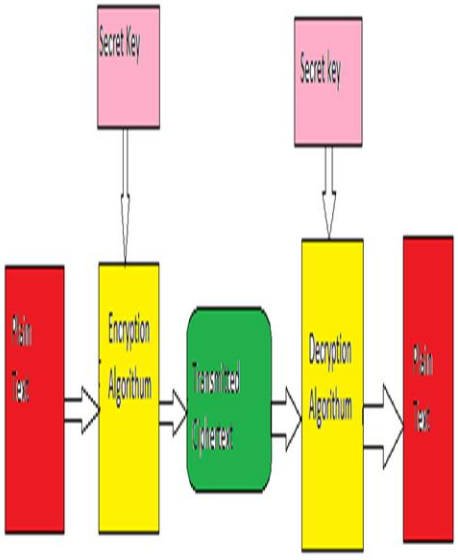

Figure 3.2- Encryption Message

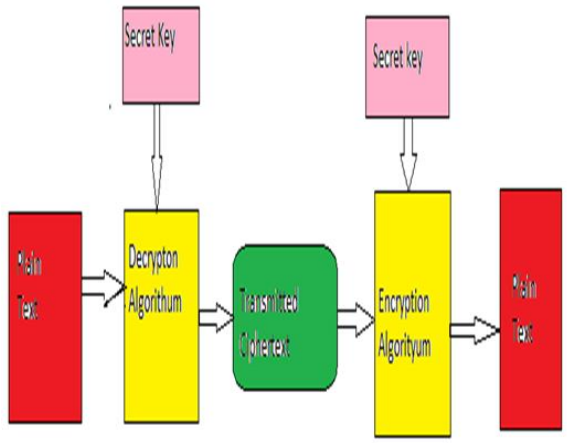

Figure 3.3- Decryption Message

REFERENCES

[1] Sudhansu Ranjan Lenka , Biswaranjan NayakEnhancing "Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm".

[2] Burt Kaliski, The Mathematics of the RSA Public-Key Cryptosystem, RSA Laboratories , February, 2003.

[3] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Laboratory for Computer Science,Massachusetts Institute of Technology, Cam-bridge, November, 1977.

[4] William Stallings, "Network Security Essentials Applications and Standards"Third Edition, Pearson Education, 2007.

[5] Atul Kahate "Cryptography and Network Security".Chetan S. Kadu, Abhay A. Jadhav, Prashant L. Mandale "Improving Security of Cloud Environment in Dynamic Cloud Network" (IJCSIT) International

[6] Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1681-1684.

[7] Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol.2(3), 242-249, 2012

[8] Shweta Singh1 M. Tech Scholar, Department of CSE, Jamia Hamdrad University, Delhi, India. International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 6 (2017), pp. 1419-1429

[9] Tabrez Nafis2 Assistant Professor , Department of CSE, Jamia Hamdrad University, Delhi, India. International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 6 (2017), pp. 1419-1429

[10] Ankita Sethi3 Assistant Professor, Department of CSE, IPEM group of institutions, India. International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 6 (2017), pp. 1419-1429