ISSN: 2277-5528
Impact Factor: 4.015

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

IMPLEMENTING CLOUD AS INFRASTRUCTURE-AS-A-SERVICE USING RSA ENCRYPTION-DECRYPTION ALGORITHM

[1]Fazil Akhtar, [2]Rohit Singh, [3]Shilpi Chandana
Associate Professor, Department of Computer Engineering, MAIIT, Kota, Rajasthan, India[1]
Associate professor, department of computer science engineering ,CPU kota[2]
Assistant professor, department of computer science engineering ,CPUkota[3]

ABSTRACT

Cloud computing is associate degree raising theme that has become today's highlighted analysis space as a result of it reduces the prices related to computing. In today's era, it's most attention-grabbing technology that provides the services or concepts to its users over the web. Since Cloud Computing contains the information and numerous kinds of resources within the open setting, security has become the terribly huge issue that is making several obstacles within the operating of Cloud environments.

Cloud Computing is extremely versatile and economical in nature, there square measure several challenges for knowledge security as there's no neighbourhood of the information for the Cloud user. to beat from the matter of security, we have a tendency to enforced RSA algorithmic rule.

Keywords- cloud computing, encryption, decryption, data security.

I. INTRODUCTION

Cloud Computing is largely used for knowledge storage which might be done via net computing. Time, cost, distributed advanced sourcing, quicker delivery of innovation and increasing quality area unit the essential rising options of this approach. With in the cloud computing technology, varied styles of services area unit provided by the service suppliers beside the information storage facility. During this we'll concentrate on the various problems and solutions of knowledge security connected problems.[1,3]

A Cloud shopper has component and/or laptop computer code that area unit primarily used for application delivery.[2]

There are a unit three differing kinds of service models for net computing that area unit as follows:

-Software as a Service (SaaS), these area unit the essential applications over the net.

-Platform as a Service (PaaS), this service is useful in providing platform wherever own applications will be developed by the developers.

-Infrastructure as a Service (IaaS), during this service, it primarily provides a collection of virtualized computing resources, customers deploy and own software's will be run to get services**.**

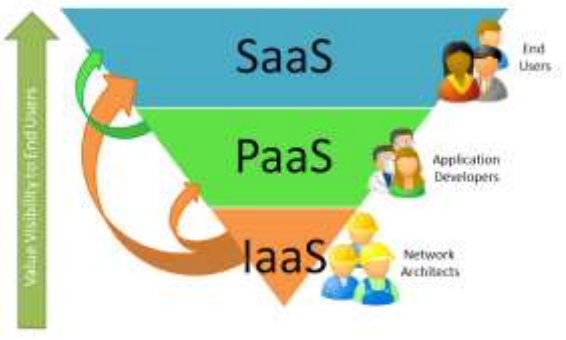


Fig. 1 Visibility value of Cloud to end user

1.1 Pproblems with knowledge security: The secured knowledge is very important for any network. Cloud Computing is principally wont to **cowl** security problems, and challenges for knowledge Security.

1.1.1 Cloud Privacy and Confidentiality:

Confidentiality suggests that the essential knowledge is protected against unauthorized access.

1.1.2 Knowledge location and Relocation:

In this, user needs to understand the precise location of information that is hold on cloud. Thus for this the client knowledge ought to be placed at explicit location. Cloud supplier should give security and authentication to customers.

1.1.3 Storage, Backup and Recovery: There should be a relevant storage system for knowledge storage. And even have backup services so it will give North American nation the info back when the hardware failure. [5,9]

1.2. Encryption and Decryption:

In cryptography, encryption is that the method of changing plain text into undecipherable format and solely approved persons will scan the messages. It's essentially wont to defend the info from unauthorized access.

Decryption is simply the vice-versa of encryption. In this, it's a method of changing cipher text into plain text, so the person will scan the message simply.[14]

1.3. RSA algorithm:

To do this	Use whose	Kind of key
Send an encrypted message	Use the receiver's	Public key
Send an encrypted message	Use the sender's	Private key
Decrypt an encrypted message	Use the receiver's	Private key
Decrypt an encrypted signature	Use the sender's	Public key

RSA rule is largely supported mathematical relation. It consists of two totally different keys one is public key and another is public key. This rule multiplies 2 massive prime numbers that consists of public key and public key. If we tend to allotted the keys then the initial prime numbers aren't abundant vital and might be discarded. In this, personal secret is primarily wont to decipher text that has been encrypted with the general public key.[14]

1.4 RSA algorithm involves 7 steps:

Step 1: Choose 2 large numbers.

Step 2: Then calculate n and multiply p and q.

Step 3: Then find encryption key by this given formula:

E=(p-1)*(q-1)

Step 4: After that find out the decryption key which satisfies the equation which is given:

d*e mod(p-1)*(q-1)=1

Step 5: find cipher text=plain text^ e mod n

Step 6: Then send the cipher text.

Step 7: Cipher text=cipher text^ d mod n.

RSA Algorithm uses two keys public and private. The public-key encryption system has mainly three phases:

Key Generation, Encryption, Decryption .

II. ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING

Many options of cloud computing, has provide adverse result thereon budget and additionally effects on security, privacy and security problems. Professionals points of cloud computing are Time, price and Innovation. There are varied security problems that are mentioned below:

i) Knowledge location

ii) Knowledge access

iii) Classification of information

ISSN: 2277-5528
Impact Factor: 4.015

iv) Service Level Agreement (SLA)
v) Security Breach
vi) Legal problems
vii) Authentication and Authorization

2.1 Issues of security occurred by Implementation of RSA:

i] Model of Security

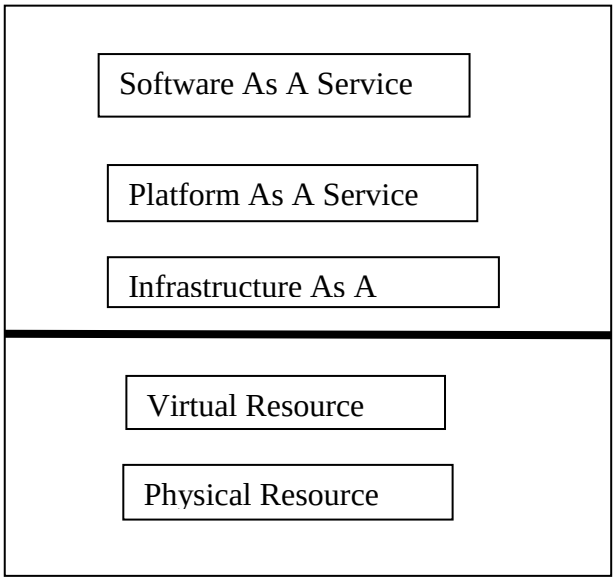


Fig 2 Model of Security on Cloud

ii] SACS Process:

It consists of varied steps that are as follows:

-Local user agent is made by the user, and safety certificate is briefly came upon. Authorization and security access to the user is complete.

- Mutual authentication between user agent and specific application takes place, once the user uses the supply on the web service layer.

- List of service resources is created by the web application consistent with user's demand so blow over it to the user agent.

iii] Simulation Tool

The experimental results are developed. This package is largely accustomed method great deal of statistics in addition as used for writing applications. it's distributed filing system. Simulating tools like CloudSim, GrimSim and Mast Sim.

iv] Experimental Analysis and Results

Distributed filing system is that the planned tool. It are often downloaded in software and may run on the windows base software. Hadoop is made, when putting in this on system that is of single node. Secure software thus attacks like - obligatory access attacks, SQL injection attack are developed to live the correct performance.

RSA is largely used for finding the issues that are generated on the Q.T. key cryptography.

III. INFRASTRUCTURE AS A SERVICE

In shaping Infrastructure as a Service we'd like to drill into specific characteristics that a cloud platform supplier should give to be thought of Infrastructure as a Service. This has been no simple task as nearly each cloud platform supplier has recently promoted options and services designed to deal with the infrastructure as a service and cloud computing market. luckily, because the technology has evolved over time, a definition of cloud computing has emerged from the National Institute of Standards and Technology (NIST) that's composed of 5 essential characteristics, 3 service models, and 4 readying models.

3.1 Essential Characteristics:

ISSN: 2277-5528
Impact Factor: 4.015

On-demand self-service-- A shopper will severally and unilaterally provision computing capabilities, like figure time, network property and storage, prore nata mechanically while not requiring human interaction with every service's supplier.[9,10]

Broad network access-- Capabilities square measure offered over the network and accessed through customary mechanisms that promote use by heterogeneous skinny or thick shopper platforms.[11,13]

Resource pooling-- The provider's computing resources square measure pooled to serve multiple customers employing a multi-tenant model, with completely different physical and virtual resources dynamically appointed and reassigned in step with shopper demand. There's a way of location independence in this the client usually has no management or data over the precise location of the provided resources, however could also be ready to specify location at a better level of abstraction (e.g., country, state, region or datacenter). Samples of computing resources embrace storage, process (compute), memory, network information measure, and virtual machines.[11]

Rapid physical property-- Capabilities will be speedily and elastically provisioned, in some cases mechanically, to quickly scale out, and speedily discharged to quickly scale in. To the buyer, the capabilities offered for provisioning usually seem to be unlimited and may be purchased in any amount at any time.[7]

Measured Service -- Cloud systems mechanically management and optimize resource use by investment a metering capability at some level of abstraction acceptable to the kind of service (e.g., storage, compute, bandwidth, active user accounts, etc.). Resource usage will be monitored, controlled, and reported, providing transparency for each the supplier and shopper of the used service.[6,9].

IV. IMPLEMENTATION AND RESULT

For implementing this feature in cloud environment we first create an infrastructure of cloud on a host machine.
This includes following steps:

Step –1 Create VM to different Data centre according to computational power of host/physical server in term of its cost processor, processing speed, memory and storage.

Step-2 Allocate cloudlet length according to Computational power.

Step -3 Vm Load Balancer maintain an index table of Vms, presently vm has zero allocation.

Step -4 Cloudlet bound according to the length and respective MIPS.

Step -5 Highest length of cloudlet get highest MIPS of virtual machine.

After the creation of infrastructure on a host machine we schedule the cloudlets to the VMs using any scheduling algorithm like FCFS or RoundRobin etc. After scheduling VMs are encrypted by applying RSA algorithm as follow:

Step-1 Create instance of Key Generator.

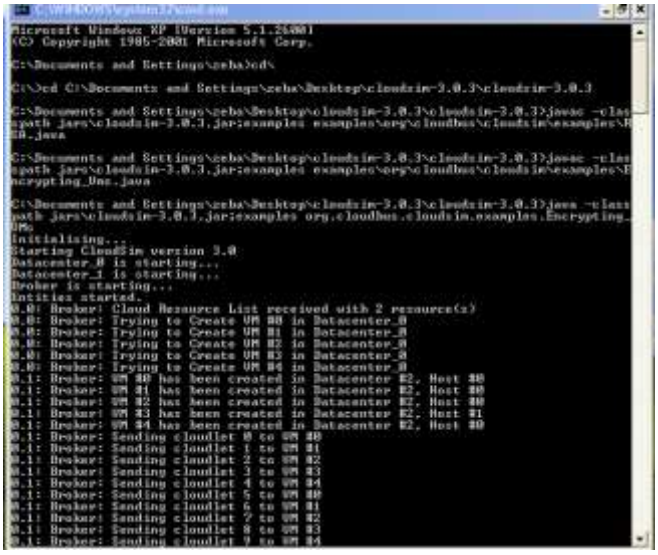
Step-2 Now generate a KEY PAIR.

Step-3 Now generate encrypted key for VMs.

Step-4 Print the cipher key.

Step-5 Finished.

It gives final output as



ISSN: 2277-5528
Impact Factor: 4.015

Fig. 3 Creation of infrastructure

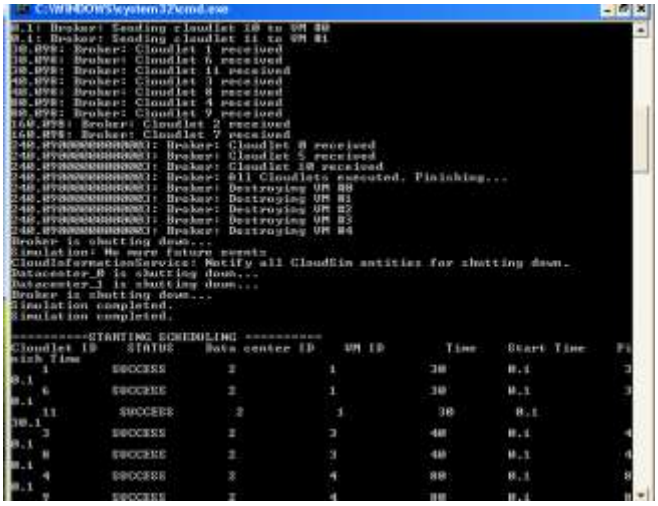


Fig.4 Scheduling

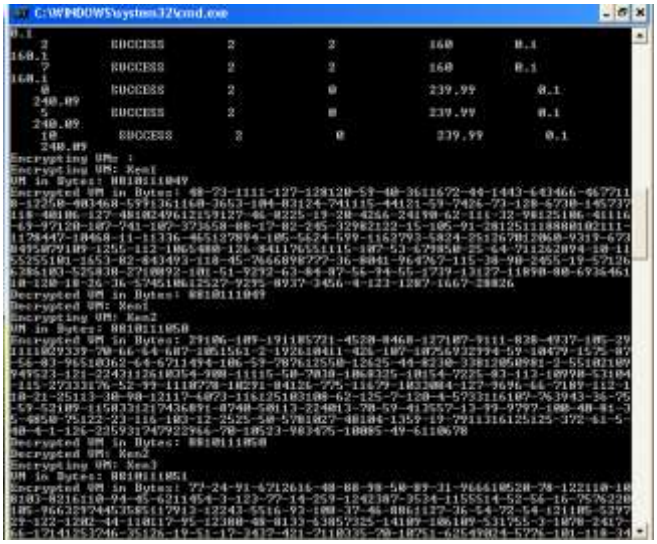
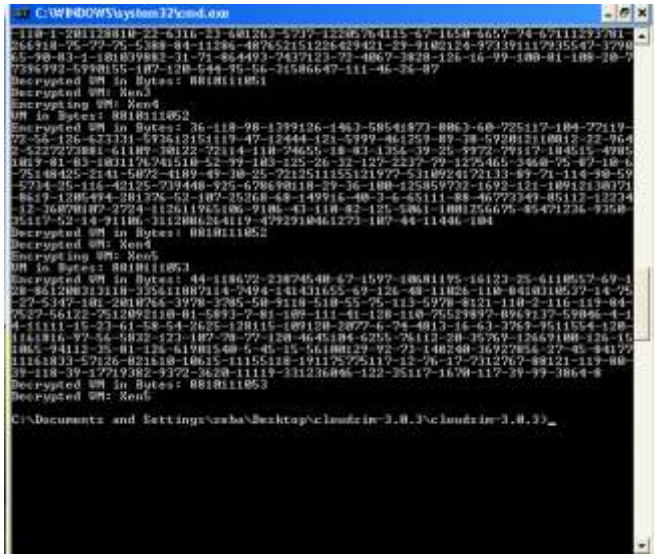


Fig. 5 Scheduling, Key Generation, Encryption and Decryption



ISSN: 2277-5528
Impact Factor: 4.015

Fig.6 Key Generation, Encryption and Decryption

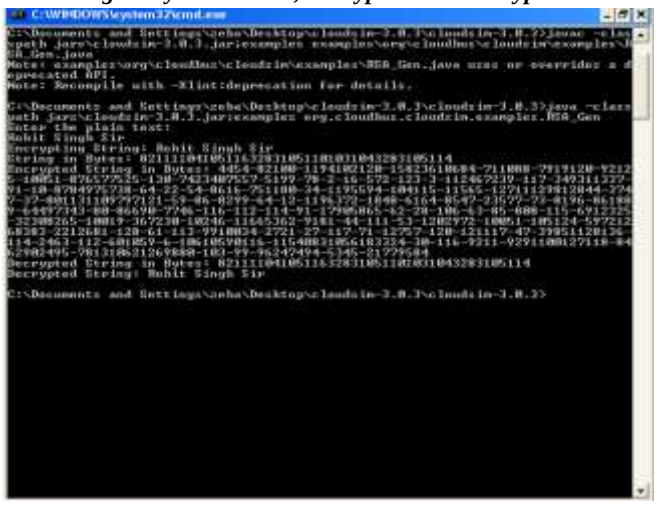


Fig.7 Generalize RSA Key Generation and Decryption(1)

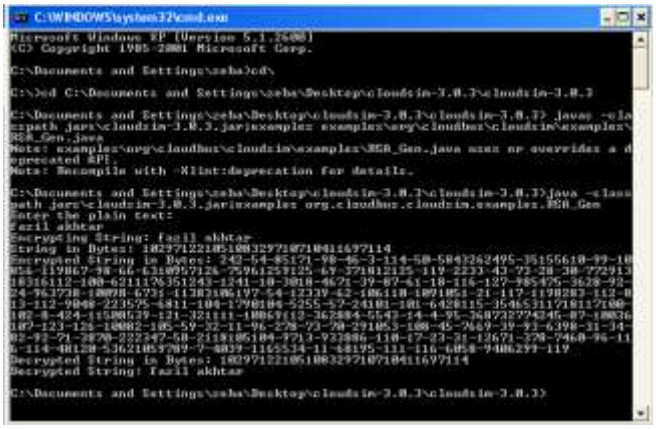


Fig.8 Generalize RSA Key Generation and Decryption(1)

V. CONCLUSION

There are some ways of making threats for cloud surroundings in such how that cloud storage or virtual machines or knowledge centres of cloud will be broken by third party attackers.

Our work creates a manual infrastructure as a service module which implies this creates VMs, data-centres, brokers, hosts and cloudlets on a selected host machine so it encrypts the VMs by mistreatment RSA algorithmic rule.

This summarizes that during this kind of service |we are able to secure VMs by secret writing therefore no threat can attack on this host machine. It's essentially double secured because it destroys all the VMs and data-centres once completion of the work.

By modifying some parameters this idea can also be utilized in cloud storage further as servers for configuring safer cloud surroundings.

VI. REFERENCES

1. R. Buyya, C. S. Yeo, and S. Venugopal. Market oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, 2008.
2. D. Chappell. Introducing the Azure services platform. White paper, Oct. 2008.

3. X. Chu et al. Aneka: Next-generation enterprise grid platform for e-science and e-business applications. Proceedings of the 3rd IEEE International Conference on e-Science and Grid Computing, 2007.
4. C. L. Dumitrescu and I. Foster. GangSim: a simulator for grid scheduling studies. Proceedings of the IEEE International Symposium on Cluster Computing and the Grid, 2005.
5. I. Foster and C. Kesselman (editors). The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, 1999.
6. F. Howell and R. Mcnab. SimJava: A discrete event simulation library for java. Proceedings of the first International Conference on Web-Based Modeling and Simulation, 1998.
7. A. Legrand, L. Marchal, and H. Casanova. Scheduling distributed applications: the SimGrid simulation framework. Proceedings of the 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, 2003.
8. J. E. Smith and R. Nair. Virtual Machines: Versatile platforms for systems and processes. Morgan Kauffmann, 2005.
9. R. Buyya and M. Murshed. GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing. Concurrency and Computation: Practice and Experience, 14(13-15), Wiley Press, Nov.-Dec., 2002.
10. A. Weiss. Computing in the clouds. NetWorker, 11(4):16–25, Dec. 2007.
11. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia. Above the Clouds: A Berkeley View of Cloud computing. Technical Report No. UCB/EECS-2009-28, University of California at Berkley, USA, Feb. 10, 2009.
12. R. Ranjan and R. Buyya. Decentralized Overlay for Federation of Enterprise Clouds. Handbook of Research on Scalable Computing Technologies, K. Li et. al. (ed), IGI Global, USA, 2009 (in press).
13. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems, 25(6): 599-616, Elsevier Science, Amsterdam, The Netherlands, June 2009.
14. Alok Tripathi, Abhinav Mishra, “cloud computing security consideration”, 2011 IEEE International Conference on signal processing, communication and computing, 27 October2011, pp. 1-5.