Load Balancing With Efficient Identity Based Signcryption And Encryption Scheme Over Cloud Computing

Yasmeen Baqal[1], Ambreena Muneer[2]
[1, 2] Dept of CSE
[1, 2] Global Institute of Technology and Management, Gurgaon

Abstract*- Cloud computing has been a paradigm shift in the information technology domain. It offers potential benefits to users in terms of instant availability, scalability and resource sharing, while potentially posing security issues. Data is key point in cloud computing for both parties i.e. cloud service provider and application users. So to provide extra security level to data is the main duty of CSP. We have proposed a technique where data is prime issue and concept of Signcryption and Encryption (with latest algorithm) is here proposed for data security over a cloud. Finally, we explore some key research challenges of implementing new cloud-aware data security solutions, followed by conclusion where we try to entail the whole research proposal and try to formulate a security strategy which will enable the Cloud providers and customers alike to fight against ever emerging security threats.*

Keywords- Cloud Computing, Signcryption, Encryption, Public key, Data Sharing.

I. INTRODUCTION

In this era information is treated as a asset which has a value like other assets. The assets have to be secured from attacks and threats. To keep secure, information must be follow different properties like integrity, confidentiality and availability.

Integrity means information can't be changed by others. Confidentiality means only authorized people can read the information and availability means information must be available when it is needed.

Now a day in computer, internet is just a part of daily routine. The world is just like virtual network where people can communicate through internet that means information is distributed so confidentiality plays a very crucial role in distributed environment when message is transmitted from one computer to another.

The most important function of cryptography is integrity and confidentiality. Confidentiality can be achieved by encryption and integrity can be preserved by digital signature. Encryption technique is divided into two categories: Private Key Encryption technique and Public Key Encryption technique. In private key encryption there is a same secret key between sender and receiver but in public key encryption technique there are two keys (public and private key) between sender and receiver where public key is known by all the people and private key is secret. Private Key encryption is fast as compared to public key encryption. Public key encryption technique is best suited in authentication and digital signature. In public key cryptography any message that is encrypted by public key can be decrypted by matching private key. Similarly any message that is signed by private key can only be verified by matching public key. For achieving confidentiality first message is encrypted by receiver's public key and decrypted by receiver's private key. Similarly for achieving integrity message is signed by sender's private key and verified by sender's public key. In public key cryptography for ensuring integrity, confidentiality and authentication first message is signed then encrypted and send to the receiver side. In receiver side first message is decrypted then it is verified. It's the two step process called Signature-Then-Encryption technique. In this application cost is more and efficiency is less and in real time application where quick response is required signature then encryption cannot be used. To eliminate it, YullianZheng in 1997 proposed the new cryptography primitives called signcryption where signature followed by encryption can be performed on single step that increase the efficiency and reduce the cost. It has not be used in some application where only one functionality like encryption or authentication is required but after some time generalized signcryption scheme is used to eliminate it.In other words without any computation it provides confidentiality and integrity both as well as separately.

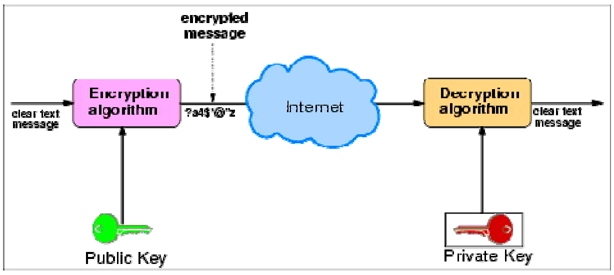


Figure 1: Public Key Encryption-Decryption Process

II. DATA SECURITY ALGORITHM

The resource will be allocated on virtual machine to data center with confidential privacy and security, so used encryption and signcryption algorithm, even the end of result we will compare between encryption and signcryption using matrices.

2.1 Encryption

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Unencrypted data is called plain text ; encrypted data is referred to as cipher text. In project, we used two types of encryption and decryption for better security

1. RSA

RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977. It is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret.

2. Blow Fish

Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use. (The U. S. government forbids the exportation of encryption software using keys larger than 40 bits except in special cases.) Blowfish was designed in 1993 by Bruce Schneier as an alternative to existing encryption algorithms. Designed with 32-bit instruction processors in mind, it is significantly faster than DES. Since its origin, it has been analyzed considerably. Blowfish is unpatented, license-free, and available free for all uses.

3. SHA-1

SHA-1 produces a 160-bit hash value or message digests from the inputted data 80 rounds of cryptographic operations to encrypt and secure a data object. Some of the protocols that use SHA-1 include:

- Transport Layer Security (TLS)
- Secure Sockets Layer (SSL)
- Pretty Good Privacy (PGP)
- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Internet Protocol Security (IPSec)

SHA-1 is commonly used in cryptographic applications and environments where the need for data integrity is high. It is also used to index hash functions and identify data corruption and checksum errors

2.2 Signcryption

Signcryption is a cryptographic primitive proposed by Yullian Zheng in 1997, which achieves integrity and confidentiality in a single logical step. Signature then encryption requires two steps but by signcryption only one step is sufficient for achieving confidentiality and integrity so signcryption reduces the communication as well as computation cost and increase the efficiency. In many application like mobile agent protocol, Key management and routing protocol and electronic transaction protocol signcryption are using. In cryptography, signcryption is a public-key primitive that simultaneously performs thefunctions of both digital signature and encryption. Encryption and digital signature are two fundamental cryptographic tools that can guarantee the confidentiality, integrity, and non-repudiation. In public key schemes, a traditional method is to digitally sign a message then followed by a signature-then-encryption that can have two problems: Low efficiency and high cost of such summation. Signcryption is a relatively new cryptographic technique that is supposed to perform the functions of digital signature and encryption in a single logical step and can effectively decrease the computational costs and communication overheads in comparison with the traditional signature-then encryption schemes.Signcryption provides the properties of both digital signatures and encryption schemes in a way that is more efficient than signing and encrypting separately.

III. RELATED WORK

3.1 CloudSim

CloudSim is a framework developed by the GRIDS laboratory of University of Melbourne whichenables seamless modelling, simulation and experimenting on designing Cloud computing infrastructures. CloudSim is a self-contained platform which can be used to model data centers, service brokers, scheduling and allocation policies of a large scaled Cloud platform. It provides a virtualization engine with extensive features for modelling the creation and life cycle management of virtual engines in a data center. CloudSim framework is built on top of Grid Sim framework also developed by the GRIDS laboratory.

The CloudAnalyst is built directly on top of CloudSim framework leveraging the features of the original framework and extending some of the capabilities of CloudSim.

3.2 Grid Sim

GridSim toolkit was developed by Buyya et al to address the problem of near impossibility of performance evaluation of real large scaled distributed environments (typically Grid systems but also P2P networks) in a repeatable and controlled manner. The GridSim toolkit is a Java based simulation toolkit that supports modelling and simulation of heterogeneous Grid resources and users spread across multiple organizations with their own policies. It supports multiple application models and provides primitives for creation of application tasks, mapping of tasks to resources and managing such tasks and resources.

3.3 Simjava

SimJava is the underlying event based simulation toolkit used in both CloudSim and GridSim.

3.4 Technologies Used

- Java – The simulator is developed 100% on Java platform, using Java SE 1.6.
- Java Swing – The GUI component is built using Swing components.
- CloudSim – CloudSim features for modelling data centers is used in Cloud Analyst.
- SimJava – Sim Java is the underlying simulation framework of CloudSim and some features of SimJava are used directly in Cloud Analyst.

IV. SETTING UP A SIMULATION

To set up a simulation you need to carry out the following steps. (Please note the screens mentioned here are explained in detail in the next section.)

1. Define user bases – Using User Base entities define the users of the application, their geographic distribution, and other properties such as the number of users, the frequency of usage and the pattern of usage such as peak hours. This is done in the Main tab of the Configure Simulation screen.
2. Define data centers – Using the Data Centers tab of the Configuration screen define the data centers you wish to use in the simulation. Define all the hardware and accounting aspects of the data centers here.
3. Allocate Virtual Machines for the application in Data Centers – Once the data centers have been created, you need to allocate virtual machines in them for the simulated application using the Main tab of the Configurations screen. A data center defined in step 2 above does not get included in the simulation unless it is allocated in this step.You can allocate multiple types of virtual machines in the same data center during this step.
4. Review and adjust the advanced parameters in the Advanced tab of the Configuration Screen.
5. Review and adjust the network latency and bandwidth matrices on the InternetCharacteristics screen.

4.1 Simulator Screens

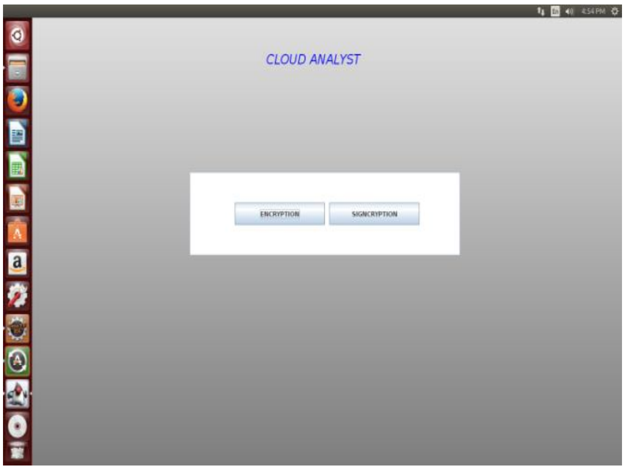


Figure 2: Cloud Analyst Encryption/Signcryption Screen

4.2.1 Main Screen with Simulation Panel

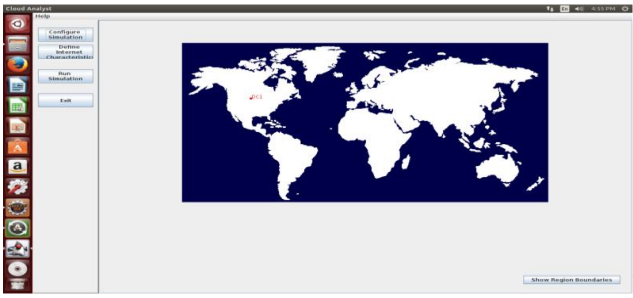


Figure 3.CloudAnalyst Main Screen

When CloudAnalyst is started the first screen displayed is the main screen. It has the simulation panel with a map of the world on the right and the main control panel on the left.

As mentioned the CloudAnalyst divides the world in to 6 regions that coincide roughly with the 6 main continents. Locations of all elements in the simulation are identified only by the region for simplicity (i.e. no x-y coordinates; all entities within are region are similar for geography specific parameters.)

Control Panel options are:

1. Configure Simulation – takes you to the Configure Simulation Screen
2. Define Internet Characteristics – takes you to the Internet Characteristics Screen
3. Run Simulation – Starts the simulation
4. Exit

At the start the simulator will be loaded with a simple default simulation.

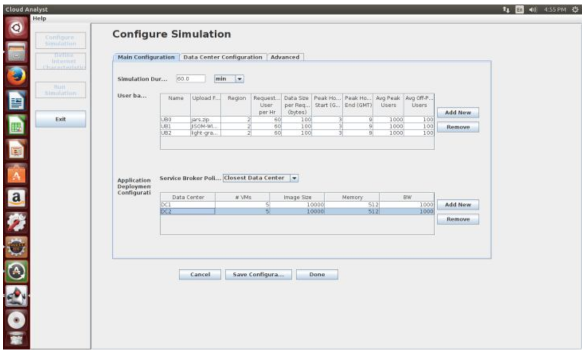
V. CONFIGURE SIMULATION SCREEN

Configure Simulation screen has three tabs.

5.1 Main Tab

The configuration options on the main tab are:

1. Simulation time – the duration of the simulation which can be given in minutes, hoursor days
2. User Bases Table – This is a table listing out all the user bases in the simulation. Each user base has following configurable fields, represented by a single row in the table.
   a. Name
   b. Region
   c. Requests per user per hour
   d. Data size per request
   e. Peak hours
   f. Average users during peak hours
   g. Average users during off-peak hours
3. The Add and Remove buttons next to the table can be used to add or remove user bases from the configuration.
4. Application Deployment Configuration – This table lists how many virtual machines are allocated for the application in each data center from the Data Centers tab, along with the details of a virtual machine. The fields are:
   a. Data Center – This is a drop down listing the names of data centers created in the Data Center tab.
   b. Number of VMs – How many VMs to be allocated to the application from the selected data center
   c. Image Size – a single VM image size in bytes
   d. Memory – amount of memory available to a single VM
   e. BW – amount of bandwidth available to a single VM



Configure Simulation

Simulation Dur... 60.0 min

User ba...

Name	Upload F...	Region	Request... User per Hr	Data Size per Req... (bytes)	Peak Ho... Start (G...	Peak Ho... End (GMT)	Avg Peak Users	Avg Off-P... Users
UB0	jars.zip	2	60	100	3	9	1000	100
UB1	JSOM-Wi...	2	60	100	3	9	1000	100
UB2	light-gra...	2	60	100	3	9	1000	100

Application Deploymen Configurati

Service Broker Poli... Closest Data Center

Data Center	# VMs	Image Size	Memory	BW
DC1	5	10000	512	1000
DC2	5	10000	512	1000

Figure 4Configure Simulation Screen - Main Tab

5. Service Broker Policy – This drop down allows you to select the brokerage policybetween data centers that decide which data center should receive traffic from whichuser base. The available policies are:
   a. Closest data center – The data center with the least network latency(disregarding network bandwidth) from a particular user base is sent all therequests from that user base.
   b. Optimize response time – This policy attempts to balance the load between datacenters when one data center gets over loaded.

5.2 Data Center Tab

The data center tab allows you to define the configuration of a data center (see Figure 8below). The table at the top lists the data centers and using the Add/Remove buttons you canadd or remove data centers to the configuration. The parameter fields are:

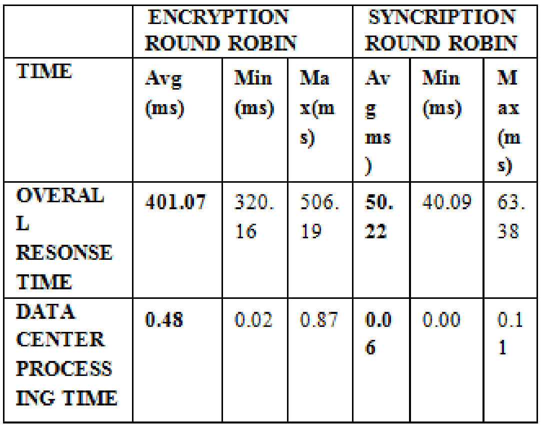
1. Name
2. Region
3. Architecture – Architecture of the servers used in the data center. e.g. X86
4. Operating System – e.g. Linux
5. Virtual Machine Monitor (VMM)
6. Cost per VM Hour
7. Cost per 1Mb Memory Hour
8. Storage cost per Gb
9. Data Transfer cost per Gb (both in and out)
10. Number of servers

When you select a data center from this table a second table will appear below it with thedetails of the server machines in the data center. The parameters for each machine can begiven according to the available fields.

1. Machine Id
2. Memory
3. Storage
4. Available network bandwidth
5. Number of processors

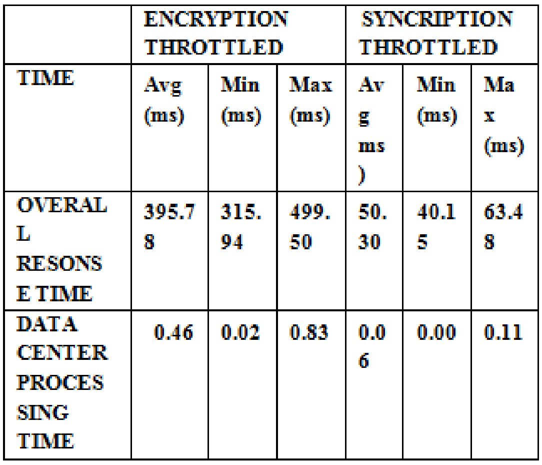
VI. RESULTS

6.1RoundRobinSchedulingAlgorithm



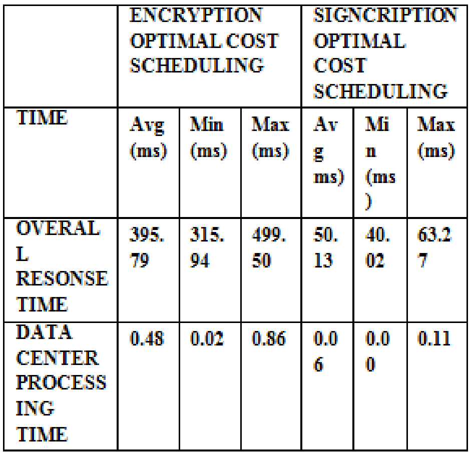
	ENCRYPTION ROUND ROBIN			SYNCRIPTION ROUND ROBIN		
TIME	Avg (ms)	Min (ms)	Max(ms)	Avg ms)	Min (ms)	Max (ms)
OVERALL RESONSE TIME	401.07	320.16	506.19	50.22	40.09	63.38
DATA CENTER PROCESSING TIME	0.48	0.02	0.87	0.06	0.00	0.11

6.2. Throttled Scheduling



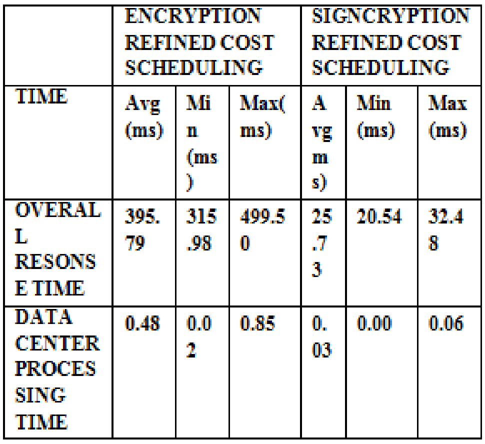
	ENCRYPTION THROTTLED			SYNCRIPTION THROTTLED		
TIME	Avg (ms)	Min (ms)	Max (ms)	Avg ms)	Min (ms)	Max (ms)
OVERALL RESONSE TIME	395.78	315.94	499.50	50.30	40.15	63.48
DATA CENTER PROCESSING TIME	0.46	0.02	0.83	0.06	0.00	0.11

6.3 Optimal Cost Scheduling Algorithm



	ENCRYPTION OPTIMAL COST SCHEDULING			SIGNCRIPTION OPTIMAL COST SCHEDULING		
TIME	Avg (ms)	Min (ms)	Max (ms)	Avg ms)	Min (ms)	Max (ms)
OVERALL RESONSE TIME	395.79	315.94	499.50	50.13	40.02	63.27
DATA CENTER PROCESSING TIME	0.48	0.02	0.86	0.06	0.00	0.11

6.4 Refined Cost Scheduling



	ENCRYPTION REFINED COST SCHEDULING			SIGNCRYPTION REFINED COST SCHEDULING		
TIME	Avg (ms)	Min (ms)	Max(ms)	Avg ms)	Min (ms)	Max (ms)
OVERALL RESONSE TIME	395.79	315.98	499.50	25.73	20.54	32.48
DATA CENTER PROCESSING TIME	0.48	0.02	0.85	0.03	0.00	0.06

The signcryption and the encryption processes are compared for the response time and the data centre processing time at the same cost (virtual machine cost and data transmission cost). The processes are compared using the four scheduling algorithms i.e. round robin, optimal cost, throttled and refined cost scheduling algorithm. Thus as shown in the above tabular results the overall response time in the signcryption process is much less than the average time in the encryption process , also the data centre processing time of the signcryption method is very less compared to the encryption process at the same cost, making signcryption optimal choice for security of data.

VII. CONCLUSION

Scheduling algorithms used in Encryption and signcryption did in this project is to provide security mechanism in the cloud computing technology. Hence we conclude that the signcryption and the encryption processes are compared for the response time and the data centre processing time at the same cost (virtual machine cost and data transmission cost). The processes are compared using the four scheduling algorithms i.e. round robin, optimal cost, throttled and refined cost scheduling algorithm. Thus as shown in the above tabular results the overall response time in the signcryption process is much less than the average time in the encryption process , also the data centre processing time of the signcryption method is very less compared to the encryption process at the same cost, making signcryption optimal choice for security of data.

REFERENCES

[1] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption) cost (signature) cost (encryption)," in Advances in Cryptology-CRYPTO'97, pp. 165{179, Springer,1997

[2] J. Baek, R. Safavi-Naini, and W. Susilo, Efficient multi-receiver identity-based encryption and its application to broadcast encryption," in Public Key Cryptography-PKC 2005, pp. 380{397, Springer, 2005

[3] B. A. Forouzan, Cryptography & Network Security. McGraw-Hill, Inc., 2007.

[4] P.-K. Encryption, \Public key encryption," Virtual Private Network (VPM).

[5] Tim Mather, "Cloud Security and Privacy", 2011.

[6] Digital Signcryption or How to AchieveCost(Signature & Encryption) <<Cost(Signature) + Cost(Encryption) *?by* Yuliang Zheng

[7] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic, Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Generation Computer Systems, Volume 25, Number 6, Pages: 599-616, ISSN: 0167-739X, Elsevier Science, Amsterdam, The Netherlands, June 2009.

[8] Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros, Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities, Proceedings of the 7th High Performance Computing and Simulation Conference (HPCS 2009, ISBN: 978-1-4244-4907-1, IEEE Press, New York, USA), Leipzig, Germany, June 21-24, 2009.