RESEARCH ARTICLE OPEN ACCESS

Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms

Gurpreet Kaur[1], Manish Mahajan[2]
[1](Department of Information technology, Chandigarh Engineering College, Punjab-160062)
[2](Associate professor, Department of Information Technology, Chandigarh Engineering College, Punjab-160062)

ABSTRACT
Cloud computing is the next generation architecture, which focuses on IT enterprise, through which potentiality on delivery of services in an infrastructure is increased. By the means of cloud computing investing in new infrastructure, training new personnel and licensing new software descends. It offers the massive storage to the users. It moves the application databases to centralized data centers, where the data management may not be trustworthy. This paper analyze the performance of security algorithms, namely, AES, DES, BLOWFISH, RSA and MD5 on single system and cloud network for different inputs. These algorithms are compared based on two parameters, namely, Mean time and Speed-up ratio.

Keywords **-** AES, DES, BLOWFISH, Cloud computing, Google app engine, MD5, RSA.

I. INTRODUCTION

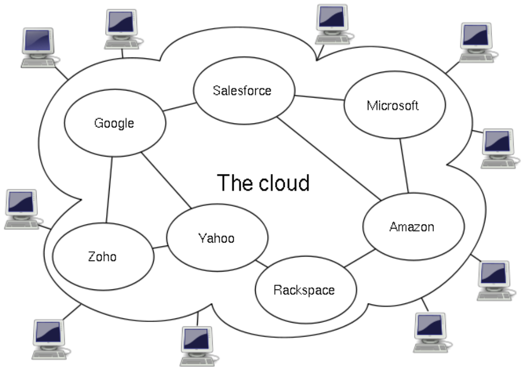
Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers to handle applications [8]**.** Cloud computing is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network. Cloud computing refers to computing with a pool of virtualized computer resources. A cloud can host different workloads, allows workloads to be deployed/scaled-out on-demand by rapid provisioning of virtual or physical machines, supports redundant, self-recovering, highly-scalable programming models and allows workloads to recover from hardware/software failures and rebalance allocations. The idea is to move desktop computing to a service-oriented platform using server clusters and huge databases at datacenters.

Let's say you're working in a company. You have the duty to make sure that all the other employees have sufficient hardware and software they need to do their jobs. When a new recruitment takes place you have to buy new hardware as well as new software for the hired person. Buying computers for everyone isn't enough -- you also have to purchase software or software licenses to give employees the tools they require. It's so stressful that you find it difficult to go to sleep on your huge pile of money every night [9].

Later, there may be an alternative for executives like you. Instead of installing a suite of software for each computer, you'd only have to load one application. That application would allow workers to log into a Web-based service which hosts all the programs the user would need for his or her job. Remote machines owned by another company would run everything from e-mail to word processing to complex data analysis programs. It's called cloud computing, and it could change the entire computer industry. In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing systems interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest [9].

Cloud computing has four essential characteristics: elasticity, scalability, provisioning, standardization, and pay-as-you-go.

This paper analysis data security model for cloud computing. We propose a data security model based on studying of cloud computing architecture. We implement software to select the suitable and highest security encryption algorithm. This software makes evaluation form five modern encryption techniques namely AES, DES, BLOWFISH, RSA, MD5.Section II states Cloud computing architecture. In section III outlines cloud computing environment. Section IV, Methodology. Section V results and section VI has conclusion.



The main attributes of cloud computing is illustrated as follows:-

1).**Elasticity and scalability:** Elasticity of the cloud means that the as per resource allocation demand the cloud can be bigger or smaller. Elasticity enables scalability, which means that the cloud can scale upward for peak demand and downward for lighter demand. Scalability also means that an application can scale when adding users and when application requirements change [7].

2).**Self-service provisioning:** Cloud customers can have an access to cloud without having a lengthy process. You request an amount of computing, storage, software, process, or more from the service provider [7].

3).**Standardization:** For the communication between the services there must be standardized API's. A standardized interface lets the customer more easily link cloud services together [7].
4) **Pay-as-you-go**: Customer have pay some amount for what resources he has used.. This pay-as-you-go model means you have to pay for what you have used.

II. CLOUD COMPUTING ARCHTECHTURE

Cloud computing service models
Infrastructure as a Service (IaaS): The IaaS layer offers storage and compute resources that developers and IT organizations can use to deliver business solutions.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations [14].

Software as a Service (SaaS): In the SaaS layer, the service provider hosts the software so you don't need to install it, manage it, or buy hardware for it. All you have to do is connect and use it. SaaS Examples include customer relationship management as a service.
Cloud computing Deployment models
1). **Public cloud**: sold to the public, very large infrastructure
2). **Private cloud**: Owned by enterprise

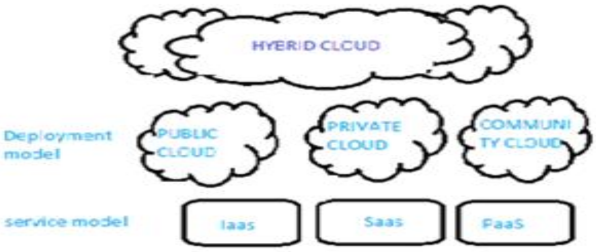


Figure 1: Deployment model

3).**Hybrid cloud**: two or more clouds composition.

4).**Community cloud**: shared infrastructure for specified community
-Cloud computing benefits
More storage, efficient Backup and Disaster Recovery, high Mobility, Cost Efficiency, Less maintenance required, Continuous availability, more scalability.
-- Cloud computing disadvantages
Less control, unreliable, unpredicted Costs for customer, more contracts and Lock-Ins, Less Security in the Cloud.

III. ALGORITHMS IMPLEMENTED

The cryptographic algorithms used are Symmetric key algorithms, Asymmetric key, algorithms and Combination key algorithms. . Encryption will make the data more secure on single system as well as on the cloud network. The algorithms will run on single system as well as on cloud network.

1).**AES**: In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively [16]

2).**MD5**: a widely used cryptographic hash function with a 128-bit hash value processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks; the message is padded so that its length is divisible by 512 [16].
In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message [16]

Table1: Keys and Key size

Key Name	Key Size
AES	256
DES	64
RSA	80
MD5	128

4).**DES**:- The DES (Data Encryption Standard) algorithm is the most widely used encryption algorithm in the world. For many years, and among many people, "secret code making" and DES have been synonymous meaning it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of the same size.

5).**RSA**:- RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. It protected user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission [16].

IV. PERFORMANCE ANALYSIS PARAMETERS

The data will be encrypted using the algorithms such as, AES, DES, BLOWFISH, RSA, Blowfish and MD5.By using these algorithms, the speed-up ratio and the mean processing time for different inputs are calculated.

4.1. Speed-Up ratio is defined as the difference between the mean processing time of single system and the cloud network. Speed-up ratio will provide tell us how fast the data have been encrypted. It will give us the idea about speed of encryption.

4.2. Mean processing time is the difference between the starting time taken to encrypt the data and the ending time. It is also evaluated both on single system and on cloud network. It is the difference between the time taken to encrypt the data. As the size of input increases the time taken to encrypt the data will increase and with the increase in time speed-up ratio decreases.

V. METHODOLOGY

The users implement their application for deploying them on the cloud. Cloud software environment provider supplies the developers with programming-level-environment with well defined set of API's. The service commonly provided by this layer is referred to as Platform as a Service (PaaS). In this category, One example is Google's App Engine, it provides a runtime environment and set of API's [16].

For interaction with Google's cloud runtime, applications are run on "sandboxed" environment. As the request increases for an application, App engine offers automatic scaling for web application. Google app handles languages such as python and java. Google App is free up to certain level of consumed resources, charges applied for the additional storage and bandwidth [16, 4]. Experimental evaluation is done on eclipse-SDK and Google App engine. The evaluation is done for different input sizes: 10KB, 13KB, 39 KB, and 56 KB.

For the data security, we have used five encryption algorithms: AES, DES, BLOWFISH, RSA and MD5.These five algorithms are implemented in the "sandboxed" environment using Eclipse .Eclipse is an integrated development environment which is used to build and run the applications. Using java on eclipse the algorithms are run on local as well as on Google app engine.

VI. RESULTS

Comparing Speed-up ratio and Mean time are used to select the highest security algorithm. Five encryption algorithms are being used namely AES, DES, BLOWFISH, RSA and MD5

Table 2: Comparison of Mean processing time of the algorithms on local system as well as on cloud network

Input	AES	AES CLOUD	DES	DES CLOUD	BLOWFISH	BLOWFISH CLOUD	RSA	RSA CLOUD	MD5	MD5 CLOUD
10 kb	11.5	1.5	7.5	2	4	2	238	274.25	1	1
13 kb	14.7	2	10	2.5	4.7	2	328.25	331.5	1	1
39 kb	21	3	31.5	6.5	8.25	2.75	358.5	351.7	1	1
56 kb	24.5	3.75	50.25	9.25	15.7	3	496.25	415.25	1	0.5

Mean processing time is calculated in milliseconds.

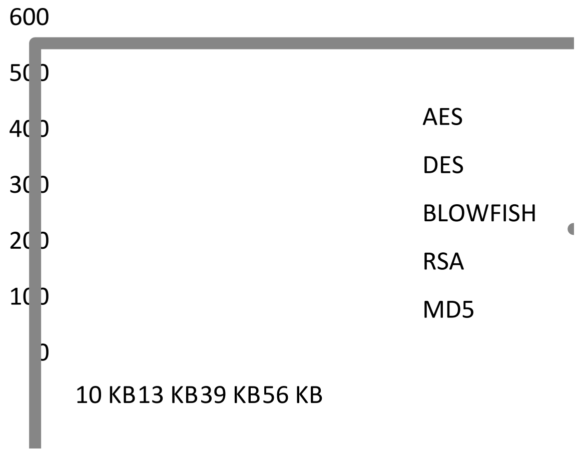


Fig 3: Comparison of Local mean time for algorithms with different input sizes.

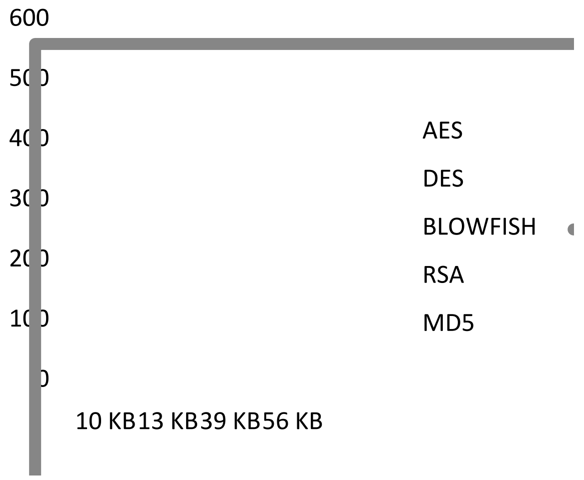


Fig 4: comparison of Cloud mean time for algorithms with different input sizes.

Table 3:Speed-up ratio of the algorithms for different input sizes

INPUT	AES	DES	BLOWFISH	RSA	MD5
10 KB	7.6	3.62	2	0.86	1
13 KB	7.2	4	2.3	0.99	1
39 KB	7	4.8	3	1.01	1
56 KB	6.6	5.43	5.25	1.19	0.5

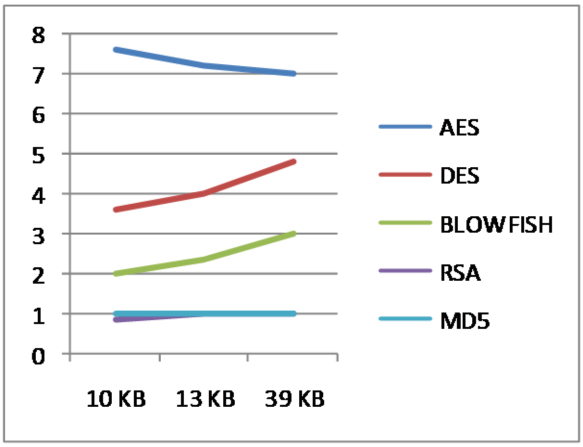


Fig 5: Comparison of speed-up ratio of the algorithms for different inputs.

From the Tabular results, the following observations can be made, using eclipse run variable input sizes on local as well as on Google App engine. Among all the algorithms RSA-an asymmetric encryption algorithm is average most time consuming and MD5 is-hashing algorithm is the least tie consuming.

AES-a symmetric encryption algorithm, the speed-up ratio falls sharply with the increase in input size.AES algorithm has the highest speed-up ratio and then is DES.

In MD5and AES algorithm the speed up ratio decreases with the increase in size. Whereas DES, RSA and BLOWFISH remains almost constant. There is a slight change in the speed-up ratio for DES, RSA and BLOWFISH.

VII. CONCLUSION

Decade's earlier algorithms are implemented on single processor system, but now encryption and decryption techniques are implemented on cloud network. Simulation for different algorithms will be done on the eclipse. The results will be obtained on basis speed-up ratio and performance parameter. All the algorithms are applied on both the cloud network and single system.

From the above results, when you are interested in performance of algorithm, go for MD5, BLOWFISH, AES and DES.

For the security of data, go for the MD5 and AES.MD5-hashing encryption algorithm is the highest security algorithm.

Finally for less time and more secure algorithm, chose MD5 followed by AES.

REFERENCES

[1] Amazon Web Services "Overview of Security Processes "http://aws.amazon.com/ August 2013

[2] Bruce Schneier. "The Blowfish Encryption Algorithm Retrieved ",October 25, 2008

[3] Center Of The Protection Of National Infrastructure CPNI by Deloitte"Information Security Briefing 0112010 Cloud Computing", p.71, Published March 2010

[4] Google App Engine. http://code.google.com/appengine/, Aug 2013

[5] http://en.wikipedia.org/wiki/Google_App _Engine. Cited Aug 2013

[6] http://www.dummies.com/how-to/content /what-is-cloud computing.html#glossary-cloud_computing, cited on Aug 21,2013

[7] http://www.dummies.com/how-to/content/ cloud-computing-cheat-sheet.html .cited on Aug 21, 2013

[8] http://www.webopedia.com/TERM/C/cloud _ computing.htmlcited on Aug 21, 2013

[9] https://bluelabelhost.com/whatisthecloud, cited on Aug 21,2013

[10] http://en.wikipedia.org/wiki/Triple_DES,cit ed on Aug 21,2013

[11] Jim zierick,"elevate cloud security with privilege delegation"http://www.ibm.com/ developerworks/cloud/library/cl-datacenter migration, Dec 2011

[12] luis m. vaquero1, luis rodero-merino1 , juan caceres1, maik lindner2 "a break in the clouds: towards a cloud.

[13] Ritika Chehal, Kuldeep Singh" Efficiency and Security of Data with Symmetric Encryption Algorithms" *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8,* August 2012

[14] Sherif El-etriby, Eman M. Mohamed, Hatem S. Abdul-kader" Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing"in *ICICT ,800-805* ,2012.Definition ", ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, 2009

[15] Priyanka Arora, Arun Singh, Himanshu Tyagi "Analysis of performance by using security algorithm on cloud network" *in international conference on Emerging trends in engineering and management (ICETM2012),* 23-24 June , 2012

[16] Priyanka Arora, Arun Singh, Himanshu Tyagi " Evaluation and Comparison of Security Issues on Cloud Computing Environment" in *World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2,* No. 5, 179-183, 2012