ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Comparison and Feasible Solution for Security Issues on Cloud Computing Environment

Balram Paroha[1], Prof. Prashant Kumar Koshta[2]

Research Scholar (Computer Technology and Application), Department of Computer Science Engineering,

Gyan Ganga College of Technology, India[1]

Assistant Professor, Department of Computer Science Engineering, Gyan Ganga College of Technology, India[2]

ABSTRACT: Cloud Computing is becoming a well-known buzzword nowadays. As a brand new infrastructure to offer services, Cloud Computing systems have many superiorities in comparing to those existed traditional service provisions, such as reduced upfront investment, expected performance, high availability, infinite scalability, tremendous fault-tolerance capability and so on and consequently chased by most of the IT companies, such as Google, Amazon, Microsoft, Salesforce.com. It is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS). Microsoft Azure and Google App Engine are the examples of platform as a service. The fast growth in field of “cloud computing” also increases rigorous security concerns.
This paper describes about the performance of different security algorithm on a cloud network and also on a single processor for different input sizes and advanced Encryption Standard security algorithm implemented for ensuring security framework.

KEYWORDS: Encryption; Distributed applications; Performance attributes; Analysis of security algorithms.

I. INTRODUCTION

Cloud computing is a technology that keep up data and its application by using internet and central remote servers [1]. Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers [4]. It allows consumers and businesses to use applications without installation and access their personal files. It provides much more efficient computing by centralizing storage, memory, processing and bandwidth. Google Apps [11, 12] is the paramount example of Cloud computing, it enables to access services via the browser and deployed on millions of machines over the Internet. Resources are accessible from the cloud at any time and from any place across the globe using the internet .Cloud users only pay for the resources allocated to them [2,11,12].It is the development of distributed computing, parallel computing and grid computing, in other words it is the business realization of all these concept[3].Now PC to do work such as handles documents, store material, sends Email or share files through U-disk. If PC doesn’t work, data will lose. But in cloud computing, cloud will do all these things for us. In the Grid computing as it requires the use of software that can divide and frame out pieces of a program as one large system image to a great number of computers. One concern about grid is that if one piece of the software on a node fails, other pieces of the software on other nodes may fail. This is alleviated if that component has a fail over component on another node, but, if components rely on other pieces of software to accomplish one or more grid computing tasks create problem. As grid computing, it will make a huge resource pool through grouping all the resources. The resources provided by cloud are to complete a special task [14]. For example, a user may apply resource from the resource pool to deploy its application, not submit its task to grid

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

and let grid complete it. The cloud providers have Infrastructure as a Service (IaaS), Platform as a Service (PaaS) [13], and Software as a Service (SaaS) and many more services to offer[5][12][13] Where SaaS means the service provided to client is the applications running on the cloud computing infrastructure provided by the service providers. It can access by thin client interfaces such as bowser etc. PaaS refers to deploy the applications created by the development language and tool say Java, python, .net etc. which is provided by the service providers to the cloud infrastructure [13]. IaaS refers to the services provided to the users is to lease the processing power, storage, network and other basic computing resources, with which users can deploy and run any software including operating systems and applications.

To all these services, there is no need for users to manage or control the cloud infrastructure, including network, server, operating system, storage and even the functions of applications. Various benefit for cloud computing adoption are: - Better Speed and Flexibility of Implementing Business Changes, Lower Cost/Risk/Time in Starting a New Business Model [6].

This paper aims to find in quantitative terms like speed- up ratio that benefits of using cloud resources for implementing security algorithms. Such algorithms are commonly used by businesses to encrypt large volumes of data. Section II outlines the Cloud Software Environment used for carrying out the concerned observations (Google's AppEngine). In section III, proposed work by experimental results and observations are reported. In Section IV we have explained the inferences obtained from the results and Section V describes the future prospects of our research.

II. CLOUD SOFTWARE ENVIRONMENT

The users of this layer are cloud applications' developers, implementing their applications for and deploying them on the cloud. The providers of the cloud software environments supply the developers with a programming-language-level environment with a set of well-defined APIs to facilitate the interaction between the environments and the cloud applications, as well as to accelerate the deployment and support the scalability needed of those cloud applications[7] [12]. The service provided by cloud systems in this layer is commonly referred to as Platform as a Service (PaaS). One example of systems in this category is Google's App Engine [5], which provides a runtime environment and APIs

For applications to interact with Google's cloud runtime environment. [26]. Applications are sand boxed and run across multiple servers. App Engine offers automatic scaling for web applications as the number of requests increases for an application, App Engine automatically allocates more resources for the web application to handle the additional demand. Google App Engine [11] [12] [14] is free up to a certain level of consumed resources. Fees are charged for additional storage, bandwidth, or instance hours required by the application. It was first released as a preview version in April 2008, and came out of preview in September 2011. Currently, the supported programming languages are Python, Java Google handles deploying code to a cluster, monitoring, failover, and launching. Google App Engine ,SLA based on its programming language API that does not allow users to directly control the infrastructure [8], Google would likely manage all causes of failures except or those made by the cloud user in developing the software running on the cloud [14].

RSA is an algorithm for public-key cryptography, involves a public key and a private key. [17, 25]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.

MD5 (Message-Digest algorithm 5), 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 (sixteen 32-bit little endian integers); the message is padded so that its length is divisible by 512 [16, 25].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

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 [21].

Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plain text [15][16,25].

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plain text [15, 18]. The AES ciphers have been analyzed extensively and are now used worldwide [21].

III. PROPOSED WORK

This paper presents the overcome of running these algorithm locally. So to increase speed-up ratio and mean processing time for different inputs, the following approach has been proposed. Each of there-mentioned algorithms was run locally as well as on cloud. Experimental evaluation done on eclipse-SDK-3.6.1Also, each one was run on different input sizes: 2kb, 5kb, 10kb, 20kb and 50kb. The comparison (uniprocessor) running time and running time on the cloud was done by calculating the Speed-Up Ratio.

Speed-Up Ratio is defined as the ratio of mean processing time on a single processor to the mean processing time on the cloud.

Each algorithm was run multiple times with each input size and the mean value was used for calculations in each case.

TABLE 1. A COMPARISON OF MEAN PROCESSING TIME OF THE THREE ALGORITHMS ON THE CLOUD (APPENGINE) AND ON A SINGLE PROCESSOR (LOCAL) FOR DIFFERENT INPUT SIZES

Input Size	RSA (local)	RSA (Cloud)	MD5 (local)	MD5 (cloud)	AES (local)	AES (cloud)
2kb	678.4	380.2	15.6	0.7	425	2.3
5kb	747.3	390.2	15.9	0.9	445.7	8.2
10kb	796.8	400.9	15.9	1	454.2	15.5
20kb	853.4	429	16	1.4	487.4	24.8

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

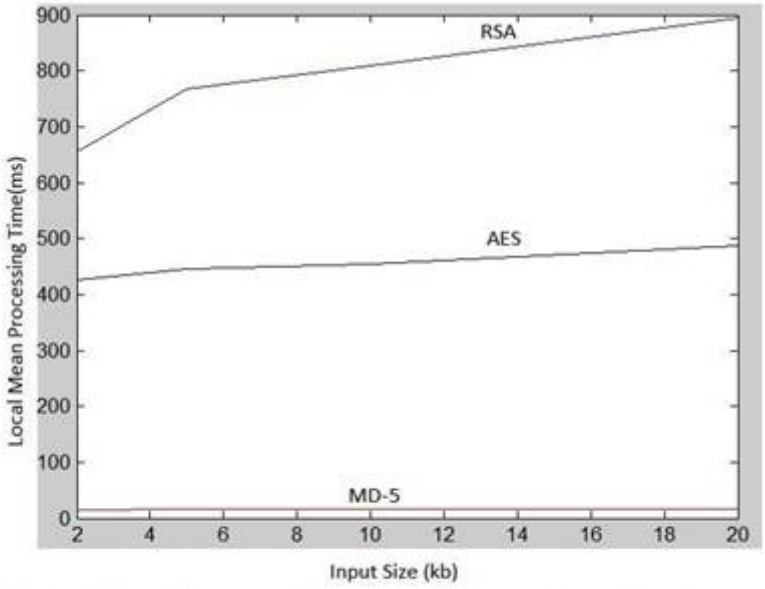

Figure. 1 Comparsion of Local Mean processing time for three algorithms with different input.

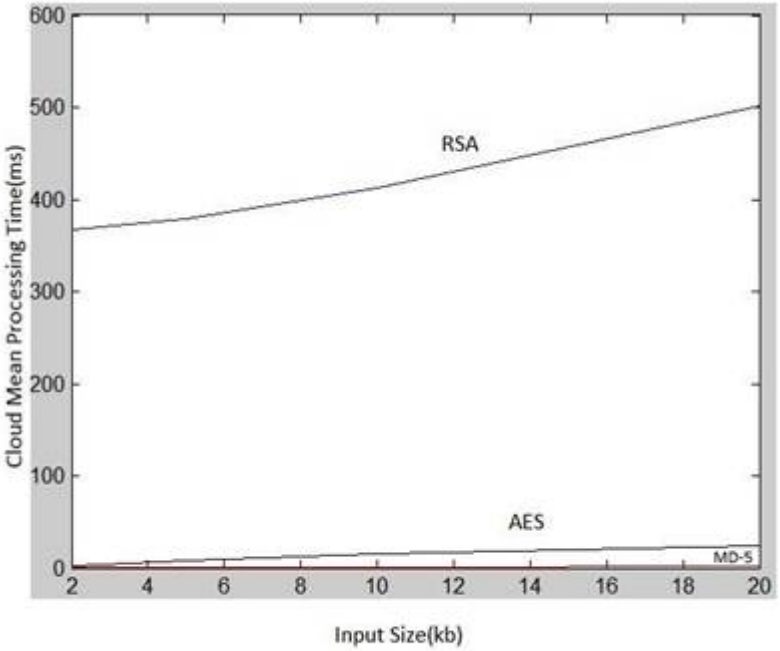

Figure. 2 Comparsion of Cloud Mean processing time for three algorithms with different input.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

TABLE II. SPEED-UP RATIO OF THE THREE ALGORITHMS FOR DIFFERENT INPUT SIZES

Input Size	RSA	MD5	AES
2kb	1.784324	22.28571	184.7826
5kb	1.915172	17.66667	54.35366
10kb	1.987528	15.90000	29.30323
20kb	1.989277	11.42857	19.65323
50kb	2.046099	9.588235	9.16934

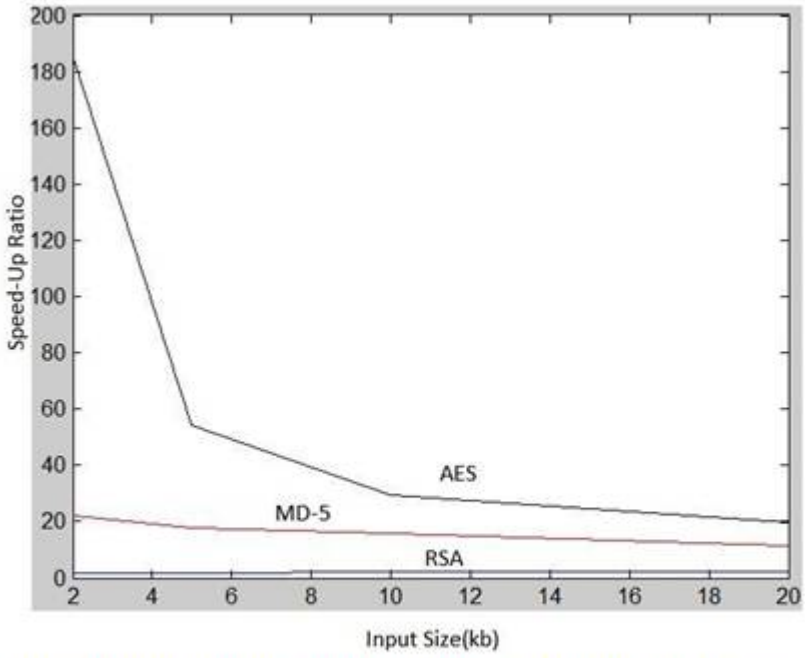

Figure. 3 Comparison of Speed-up ratio for three algorithms with different input.

From the tabular results above, the following observations and inferences can be made using eclipse run it as local as well as on Google App engine. Also with the help of simulator, comparison of graph is shown for three algorithms with different input. Amongst the algorithms RSA- an asymmetric encryption algorithm, is on an average the most time consuming and MD5- a hashing algorithm, the least. This is true in a uni-processor (local) as well as cloud (Appengine) environment.

The highest Speed-Up is obtained in AES- a symmetric encryption algorithm for low input sizes, the Speed-Up falls sharply as the input size is increased.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

For each input size, the speed up achieved is highest for AES- a symmetric encryption algorithm, followed by MD5- a hashing algorithm and the least for RSA- an asymmetric encryption algorithm.

For both MD5- a hashing algorithm and AES- a symmetric encryption algorithm, the speed up ratio decreases with increase in input size whereas for RSA- an asymmetric encryption algorithm, it remains almost constant (showing a minute decrease) with increase in input size.

IV. CONCLUSION

In earlier system these algorithms are implemented on the single processor system but because of the availability of the fast and parallel computing resources, the better encryption and decryption techniques can be implemented by using these security algorithms in cloud network. All the observations after simulation show that cloud network can be used for better performance. We have implemented various cryptographic algorithms on a cloud network which concludes that the algorithms implemented are more efficient than using them on single system. The simulation was done on the eclipse and the graphical results were shown by using mat lab. We observed that performance of an algorithm on a cloud network varies according to the type of the algorithm such as symmetric, asymmetric or hashing and also varies with the size of the input.

We have many more algorithms to be evaluated and their results can be analyzed with one another to produce the best implemented security algorithm in cloud environment for future use.

REFERENCES

[1] 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
[2] Farhan Bashir Shaikh, Sajjad Haider , "Security Threats in Cloud Computing," in 6th international conference internet technology and secured transtion,11-14 december,2011,Abu Dhabi,United Areb Emirates
[3] Shuai Zhang, Xuebin Chen , "The Comparison Between Cloud Computing and Grid Computing," 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)
[4] Joshi Ashay Mukundrao , Galande Prakash Vikram "Enhancing Security in Cloud Computing" in Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online), Vol 1, No.1, 2011
[5] Junjie Peng, Xuejun Zhang, Zhou Lei, Bofeng Zhang, Wu Zhang, Qing Li, "Comparison of Several Cloud Computing Platforms," in Second International Symposium on Information Science and Engineering,2009 I
[6] Murat Kantarcioglu, Alain Bensoussan, SingRu(Celine) Hoe, "Impact of security risks on cloud computing adoption," in forty-ninth annual allerton conference allerton house, uiuc, illinois, USA ,september 28 -30, 2011
[7] Lamia Youseff, Maria Butrico, Dilma Da Silva, "Toward a Unified Ontology of Cloud Computing, in 2008 ,http://www.cs.ucsb
[8] Kunwadee, sripanidkulchai, sambit sahu, yaoping ruan, anees shaikh, and chitra dorai, "Are clouds ready for large distributed applications?," in IBM T.J. Watson Research Center.[9] Microsoft, "Comparing Web Service Performance: WS Test 1.1 Benchmark Results for.NET 2.0, .NET1.1, Sun One/ JWSDP 1.5 and IBM WebSphere6.0" http://www.theserverside.net/tt/articles/content/NET2Benchmarks,2006.
[10] http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Pre sensations/MD5.pdf.
[11] Google App Engine. http://code.google.com/appengine/, July 2008.
[12] 3tera,http://www.3tera.com, April 2009, "Cloud Computing For Web Applications."
[13] http://www.sales.com, April 2009, "Platform as a Service (Paas) - Powering On-Demand SaaS Development."
[14] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., "Above the Clouds: A Berkeley View of Cloud Computing."
[15] G. Jai Arul Jose1, C. Sajeev2 , "Implementation of Data Security in Cloud ," in International Journal of P2P Network Trends and Technology- July to Aug Issue 2011.
[16] D.Kesavaraja1 , R.Balasubramanian2 and D.Sasireka3 "Implementation of cloud data server (cds)for providing secure service in E-business" , in international journal of database mangement system(IJDBMS),Vol2,No2,May 2010
[17] Joshi Ashay Mukundrao, Galande Prakash ,Vikram "Enhancing Security in Cloud Computing," in Information and Knowledge Management cwww.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 1, No.1, 2011.
[18] M.Sudha1 , M.Monica2 "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography," in Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012 Copyright ©World Science Publisher ,United States www.worldsciencepublisher.org.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

[19] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences 2011.
[20] R. La Quata Sumter, "Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford," USA.
[21] M. Sudha , Dr.Bandaru Rama Krishna Rao , M. Monica "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment," in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.
[22] John Harauz, Lori M. Kaufman and Bruce Potter, "Data security in the world of cloud computing," 2009 IEEE CO Published by the IEEE Computer and Reliability Societies.
[23] Guy Bunker, Farnam Jahanian, Aad van Moorsel and Joseph Weinman, " Dependability in the cloud: Challenges and opportunities," ‖IEEE 2009.
[24] www.infoworld.com/.../cloud-computing/what-cloud-computing- real...
[25] William Stallings, "Cryptography and Network Security Principles and Practices," Prentice Hall, New Delhi.
[26] http://en.wikipedia.org/wiki/Google_App_Engine