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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Evaluation and Review of Security Algorithm on Cloud Computing Environment

Sunil Yadav, Kanishk Bahadur Singh

MTech (CS&E), School of Computing Science and engineering, Galgotias University, Greater Noida, U.P, India.

ABSTRACT: Cloud computing basically comes to focus on IT, a way to increase scope or add potentiality on the fly without spending in new infrastructure, training new personnel, or licensing new software. It encircle any subscription-based or pay-per-use service that, in real time over the Internet, extends its existing capabilities. It is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (Pass), 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 because of its broadband Internet, shared pool of resources, flexible configuration, On-demand services and by service charges and other unique advantages, and in various industrial applications Rapid rise. For business users, can significantly reduce the computational and storage. Maintenance costs; for individual users and the calculation information stored by the discharge. In the cloud, reducing the number of their limited storage and computing resources arising Constraints. Cloud computing providers with their strong economic and technological strength; Guarantee a high degree of reliability of the cloud under law and regulations. In cloud computing, the user is placed in the cloud server data and meter Considered out of control, the data are protected, whether computing tasks Cannot determine the correct execution. Hence the need to design appropriate security protection mechanisms Protect user data confidentiality, integrity, availability, and the need to make cloud services.

The method of execution is credible, or can occur through accountability Attack quickly determines where the problem lies. In a public cloud, a large number of users You can lease the resources in the cloud, and can lease the infrastructure to other use. Households to provide services, or inevitable to communicate between the number of these users according sharing. So between the cloud and more secure access to user needs and design. Control mechanisms [3]. Because of the open nature of cloud computing and resource sharing special, emerged, as based on a common side channel attack based physical machines and a total denial of service attacks in the subnet and so on.

To design new defensive measures to resist these attacks. In addition, it is more research [4] proposed to carry out the security services in the cloud, one can enough to enhance the capacity and processing power to update the security services, on the other hand can Reduce the computational cost of the customer. This new security product is called "security that service "(SecurityasaService). Mobile phone as a client of the situation because of its computing and storage capacity Very limited. At present, research include anti-virus service [4], the certification, Safety testing and Digital Rights Management and so on.

Security Requirements of Cloud Computing

A. Confidentiality

In order to protect data privacy, data in the cloud should cipher text form, type storage, but the encryption

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

method has brought on the overhead operation, and therefore to calculate the cost to as little as possible to bring reliable data confidentiality; To protect the privacy of user behavior, cloud servers to ensure that users Anonymous use of cloud resources and safety record data origin. Furthermore, in Some applications, the server needs to be transported in a user data above count, and operation results are returned to the user in plain text format, thus enabling service is able to operate directly on top of the cipher text is an important demand side to. In the best case, the server any operation on the cipher text can be directly mapped to corresponding operations on the plaintext, this encryption method called fully homomorphism encryption [6]. If fully homomorphism encryption efficiently. The realization of security, not only to protect the user's privacy, but also efficiency does not decrease. In the case of fully homomorphism encryption cannot be efficiently implemented, Lee with the same characteristics as a function of state protection of privacy, the cipher text based operation, but also is very important. In cloud computing, information retrieval is a very common operation make, and therefore supports the search cloud security encryption is an important requirement. Already some support for the search of encryption supports only single keyword search, and search results do not support the sorting and fuzzy search. Features for cloud computing, mesh studies include fuzzy search before, supporting the sort of search and multi-keyword search [7] and so on. If the operation cannot be performed on the cipher text, then any action by the user to be related to the data to be sent back to the user cipher text
After the party decryption then, it will seriously reduce efficiency.

B. data integrity

In a cloud-based storage services, such as Amazon Simple Storage Service S3, Amazon Elastic Block Store EBS, and Nirvana cloud storage Service, the need to ensure the integrity of the stored data. Several cloud-based According stream processing, the main consideration is the complete data processing results Detection and malicious service providers. In data storage, since users can not fully trust the cloud server will protect the integrity of their own data, so users need them Integrity of the data for validation. Remote data integrity verification is a good way to solve this problem, it cannot download user data under the circumstances, based solely on the data to identify the challenges and server response code shall be able to verify the integrity of the data. The main source of data stream processing, the integrity verification requirements to user data processing service provider cloud mistrust. In this under the case, ensuring the integrity of the data processing results is essential.

C. Access Control

Cloud computing resources to stop illegal users and other users Access to data or the like, fine-grained control access to legitimate users, because This cloud server needs access to the user's behavior for effective verification. Its access control requirements include the following two aspects:
(1) Network Access Control: refers to a cloud infrastructure between hosts Each other access control.
(2) Data access control: refers to the user data stored in the cloud Access control data to ensure that the operation of the user revocation.
For the, the user dynamically join and user can audit and other requirements Support.

D. authentications

Existing authentication technologies include three categories: (1) based on the user Holding secret certification; (2) hardware-based user holds (such as smart Card, U Shield, etc.) certification; (3) based on user biometric (eg fingerprint) Certification. Currently password authentication and X. 509 Certificate is a cloud Products used widely considered authentication methods. In addition, the level of Based Authentication can achieve levels of between multiple cloud Identity management. Multi-factor authentication can from the multiple features of the Client authentication, it is possible to provide enhanced security.

E. Credibility

In order to enhance the credibility of cloud computing and cloud storage services can Starting from two aspects. On the one hand is to provide accountability function of cloud computing, communication had achieved record operating information tracking and accountability malicious actions, such as [9] Propose a

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

cloud environment based on trust and fuzzy comprehensive evaluation unit trust management cloud System, based on credible mode service calls and feedback cloud services Type; the other is to build a trusted cloud computing platform, through credible account Count, secure boot, cloud gateways [8] and other technical means to be cloud computing.

F. Firewall Configuration security

Infrastructure cloud, such as Amazon Elastic Compute Cloud [8], the cloud the virtual machine need to communicate, these communication between virtual machines are divided into Communication and virtual machines and external communication. Control communication via Firewall to achieve, and therefore the security of the firewall configuration is very important. If the firewall configuration problems, then the attacker is likely to use a Port is not properly configured for a virtual machine to attack. Therefore, in the cloud Calculations necessary to design the virtual machine firewall configurations safety of trial Search algorithm.

G. virtual machine security

Virtual machine technology to build cloud services architecture a large-scale user Request and network resource allocation efficiency is widely used, but with this same When the virtual machine is also facing two aspects of security, on the one hand is a virtual machine Safety oversight program, on the other hand is a secure virtual machine images Resistance . In a virtual infrastructure supporting technology into the cloud, virtual machines Supervision software program is the highest authority on each physical machine, so its safe There is no doubt of the importance of the whole. In addition, the use of third-party virtual released The case of machine images, virtual machine images whether to include malware.

II. 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.

Input Size	RSA (local)	RSA (Cloud)	MD5 (local)	MD5 (cloud)	AES (local)	AES (cloud)
2kb	678.2	380	15.5	0.9	426	2.5
5kb	747.1	390.1	15.7	1	445	8.5
10kb	796.5	400	15.6	1.2	454.4	15.7
20kb	853.2	431	16.2	1.5	487.6	24.9

TABLE1.COMPARISON OF MEAN PROCESSING TIME OF THE THREE ALGORITHMS ON THE CLOUD (APP ENGINE) AND ON A SINGLE PROCESSOR (LOCAL) FOR DIFFERENT INPUT SIZES.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Input Size	RSA	MD5	AES
2kb	1.784736	17.22222	170.4
5Kb	1.9151499	15.7	52.3529
10kb	1.99125	13	28.94267
20kb	1.979582	10.8	19.582329

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

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. 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.

III. 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 also analyzed the Mean Processing Time of the three algorithms on the Cloud (Appengine) and on a Single Processor (Local) for different input sizes and we observed the variation in speedup ratio and mean processing time of different type of security algorithms in both cases.

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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

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.
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.