ISSN No. 0976-5697

Volume 5, No. 5, May-June 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secure Cloud Network using Partial Homomorphic Algorithms

Vineet Kumar Singh
M.E. Student
Department of Computer Science NITTTR
Chandigarh (U.T.), India
vineetnitr@gmail.com

Dr. Maitreyee Dutta
Associate Professor
Department of Computer Science, NITTTR
Chandigarh (U.T.), India
d_maitreyee@yahoo.co.in

Abstract-- Cloud computing has proved its worth in different technological domains by various means. With its IAAS, PAAS and SAAS, it has adopted the concept of pay as-per-use which is very trustworthy for all types of service consumers. Cloud computing is the demand of changing time and everyday more and more service consumers of cloud services are increasing. With the continuously increasing number of consumers, cloud security is now a much big concern than ever. In spite of many advantages of the cloud computing, many organizations are still reluctant towards the adoption of this technological advancement, and unfortunately the reason is genuine. The security concerns of cloud network are even increasing along with today's growing cloud network. These security concerns can be addressed if users encrypt the data while transmitting to the cloud with strong security algorithms. In this paper we have analyzed the performance of such strong semantically secure algorithms, namely Homomorphic Algorithms, for cloud network. As Homomorphic algorithms are very strong in terms of zero knowledge proof, these algorithms will be having wide application in near future, especially in the untrusted environment like cloud computing. We have analyzed the performance of Paillier and Benaloh Partial homomorphic Algorithms for the cloud network. The algorithms are tested on the single system and on the cloud environment as well.

Index Terms— Cloud computing, cloud security, homomorphic algorithms, Benaloh Homomorphic Algorithm, Paillier Homomorphic Algorithm.

I. INTRODUCTION

Cloud computing offers a technological shift in which consumer need not worry about infrastructure or software, instead they get all of these requirements readily available on pay as-per-use basis by the service provider, which in turn results in less expense than owning all these requirements[2].According to US National Institute of Standards and Technology (NIST) the key characteristics of cloud are on-demand self-service, rapid elasticity and pay as per the usage of business models[1]. NIST has defined four deployment versions for cloud computing: public, private, hybrid, and community clouds. Interested readers may refer to the NIST definition of cloud computing for their detailed description [1].Cloud computing has proved to be a great technology for the organizations those who need large computing power, without investing large capital in setting up the IT infrastructure. [3]. Among many benefits of cloud computing, some most enticing are i)Less hardware and maintenance cost, ii) Round the world accessibility , and iii) Flexible and highly automated processes, for example client need not bother about maintenance or software updates [4,5].

Cloud Computing is a successive technological approach of the technologies like grid computing, distributed computing, parallel computing, virtualization technology and utility computing [6].Virtualization & its associated software's play an important role in cloud computing, which is usually known as Virtual Machine Monitor (VMM) or Hypervisor [7]. Virtualization allows one single physical server to host many guest virtual machines (VM), operating systems and applications without the increased cost and complexity of running multiple machines[8]. According to Amarnath Jasti et al.[9], virtualization optimizes the application efficiency in a cost effective fashion, but it may also project some security risks. Security is a major consideration in cloud as the control of owners data lies in service providers hand which is already some-what risky than owning the data at the owners end itself [10]. According to the Cloud Computing Services Survey, done by IDC IT group in 2009, over 87% of the people said that security is the number one issue which prevents the adoption of the cloud computing [11].Thus there is a need to understand the cloud specific risks, & various ways to detect & prevent from those risks which are associated towards successful adoption of the cloud.

II. ASSOSIATED RISKS

As cloud computing is a new enhanced version of the technology, it has also created some new challenges, which are quite different from traditional security challenges. Based on the survey of Cloud Security Alliance (CSA),"The Notorious Nine: Cloud Computing Top Threats in

2013"[12], which they performed with the industry experts on greatest vulnerabilities of cloud computing, there are nine critical threats to cloud security (ranked in order of severity)-

a. Data Breaches

b. Data Loss

c. Account Hijacking

d. Insure Application Programming Interfaces

e. DOS (Denial of Service)

f. Malicious Insiders

g. Abuse of Cloud Services

h. Insufficient Due Diligence

i. Shared Technology Issues

These threats are found most vulnerable for cloud computing in the latest report of CSA [12].Better understanding of the cloud threats will lead to better adoption towards cloud technology. Among all these threats data breaches is most traditional and still most dangerous too. Let's discuss what researchers conclude about data breaches and why it still persists.

Data breaches are ranked as number one threat for the cloud computing. Since the inception of cloud computing technology, this threat is still present in the system. Multi-tenancy is one of the most important reasons among several, for data breaches. Since data from various organizations lie together in a multi-tenant cloud environment, breaching into the cloud will ultimately attack the data of all the users. Thus, the cloud of such huge information becomes an attractive target for attackers [15].

Data remanence is also one of the reasons of security breach, & generally it is unintentional. Data remanence is the vestigial of data that have been nominally removed or migrated. As several virtual machines running on one physical machine lack of separation between multiple users, may lead to the unwilling disclosure of private data in case of data remanence. This may cause higher risk to the cloud users than with dedicated resources [13, 22].

Trusted third Party services within the cloud, establishes the necessary trust level and provides ideal solutions to preserve the confidentiality, integrity and authenticity of data and Communications [13, 14].

Breach notifications are also important as Poor breach notification may lead to privacy breach [16]. Unfortunately, the breach notifications could not really protect a customer's data. A recent survey shows that service consumers who received data breach notifications within the past years are at a higher security risk than the typical service consumers [17].

Daniel J. Abadi concluded [18] that it is a great risk in storing transactional data on an un-trusted host. Transactional databases contain the complete set of operational data needed to power overall business processes. This data includes detail at the lowest granularity, and often includes important information such as credit card numbers of the customers. Thus, any increase in potential security breaches is typically unacceptable. Facebook user data breach is a recent example of the questionable user data safety on cloud systems [20].

After discussing views of several researchers it can be concluded that there are so many reasons why still client feel reluctant in accepting this technology. Cloud is a very huge information repository and no client would like to take risk on his/her information. If we consider that cloud end security is up to the mark, then also there is question about unsecure client data while transition to the cloud end. Our next section is an attempt to find out some efficient solutions, which can be helpful in real time environment.

III. OVERVIEW OF HOMOMORPHIC ENCRYPTION

Cloud computing involves frequent uploading and downloading of data along with nasty computation on servers which are managed by third party. Since the client does not control the cloud environment, always there is a probability of losing the confidentiality and integrity of data either by intentional or unintentional means. These privacy concerns may be addressed by sending the encrypted data to the cloud by the client [21, 22]. Homomorphic encryption permits specific computations on cipher text, which produces an encrypted result which is also in cipher text and this outcome is the result of computations as if it were performed on the plaintext. [23]

Homomorphic encryption is classified into three categories. Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE), and Fully Homomorphic Encryption (FHE).In Partially Homomorphic Encryption, it is possible to perform one operation on encrypted data, such as multiplication or addition but not both. Somewhat homomorphic encryption techniques can perform more than one operation but can only support limited number of addition and multiplication operations. A Homomorphic Cryptosystem which is capable of both addition and multiplication, and can compute any function is known as a Fully Homomorphic Encryption system. These programs never decrypt their inputs, thus they can be run by un-trusted individuals without the risk of leaking the privacy. Among these methods PHE and SWHE methods have one advantage over FHE techniques; they have been found to be more efficient in their processes.

IV. PARTIAL HOMOMORPHIC ENCRYPTION SCHEMES

Both the RSA and ElGamal encryption schemes were earlier seen to follow homomorphic properties, but only with respect to one operation. But at that time researchers could not understand the importance of this aspect, but now the community has grown to trust the security of these schemes and, recently, the work of Gentry and others demonstrate that, when carefully employed, such homomorphic properties can be quite valuable[24,25].

Earliest discovery in this category was the Goldwasser-Micali cryptosystem whose security is based on the quadratic residuosity problem and which allows homomorphic evaluation of a bitwise exclusive-or. This scheme has already been applied to the problem of securing biometric information. Other additive homomorphic encryption schemes that provide semantic security are Benaloh, Naccache-Stern, Paillier, Damgard-Jurik, Okamoto-Uchiyama and Boneh-Goh-Nissim. Paillier's scheme is the most efficient among currently known additively homomorphic schemes [25].Our current research work is about analyzing the Benaloh & Paillier Partial Homomorphic Systems in terms of Total Execution Time and Speed-Up Ratio for cloud network. As partial homomorphic algorithms are less time consuming than of Fully Homomorphic Algorithms and have shown some positive results, our research analyzed both the algorithms to find out the performance of these algorithms for the cloud environment.

The Benaloh Homomorphic Cryptosystem is an extended version of the Goldwasser-Micali cryptosystem developed in 1994 by Josh Benaloh. The chief advantage of the Benaloh Cryptosystem over GM is that now, longer message blocks can be encrypted at in one go, while in GM each message bit is encrypted on bit by bit basis; moreover, the encryption cost is not too high.

The Paillier scheme was first published by Pascal Paillier in 1999. This probabilistic scheme has proved to be very interesting due to the homomorphic property, which allows this scheme to do normal additions on encrypted values and achieving the encrypted sum. Later, this encrypted sum can be decrypted without even knowing the actual values that constitutes the sum. Because of this useful characteristic this scheme is suggested for use in voting protocols, watermarking, secret sharing schemes and in private information retrieval etc.

V. PARAMETERS USED FOR PROBLEM ANALYSIS

A. Total Execution Time:

Total Execution time is the sum of the total time taken during the homomorphic operation including the key generation time, encryption time and decryption time. It will be evaluated both on local system and on cloud network.

B. Speed-Up Ratio:

Speed-Up Ratio is defined as the ratio of Total Execution Time on a local processor to the Total Execution Time on the cloud network.

VI. PROPOSED METHODOLOGY & EXECUTION ENVIRONMENT

In the proposed methodology, performance analysis of the given algorithms on the basis of the parameters- Total Execution Time and Speed-Up Ratio and is done on local system as well as on the cloud network.JavaSE-1.7 on Eclipse SDK 4.3.0 release is used for the development of both the algorithms.

Cloud software environment provider supplies the developers with programming-level-environment with well defined set of API's. Cloud-enabled applications on Spoon allow software developers to make available their existing desktop applications in the cloud, without any installations. Spoon offers many software through their SAAS offerings; we used Eclipse 4.3.0, as cloud SAAS for executing my java algorithms in cloud environment so that performance comparison can be made on the basis of aforesaid parameters.

Both algorithms are tested on Intel core i5 third generation processor with MS Windows 7 Home Premium 64 bit SP-1.Processor speed is 2.50 GHz and with 2 GB RAM.

VII. RESULTS & DISCUSSIONS

VIII.

a. Paillier is considerably faster than Benaloh on local system and on cloud network as well.

b. Both algorithms are found very slow on cloud network as compared to local system.

c. Both algorithms achieved almost equal speed –Up Ratio, less than one, almost half, which indicates their slow processing over cloud network.

d. Slow execution on cloud network suggests that both algorithm needs an extra processing power for its fast operation from cloud network, it needs better configuration machines (more number of processors, fast processors, more RAM and cache memory) to operate efficiently from cloud network.

e. As we know that fully homomorphic encryption process is not efficient to apply on cloud network in its present form, due to its extremely time consuming process, in such situation, partial homomorphic algorithms may do well on cloud comparatively, as time taken by these algorithms is very less than Fully homomorphic encryption process.

All the results are obtained with due care for achieving higher accuracy five samples of Total Execution Time were taken then an average of five samples were taken for the measurement and comparative analysis among algorithms

and for the graph plotting as well. All the respective observation readings and graph are shown for both of the analyzed algorithms.

IX. OBSERVATION RESULTS & GRAPHS OF DIFFERENT ALGORITHMS

Table: 1. Total Execution Time for Paillier Cryptosystem on Local System

Table: 2. Total Execution Time for Paillier Cryptosystem on Cloud Network

ALGO	SAMPLE-1	SAMPLE-2	SAMPLE-3	SAMPLE-4	SAMPLE-5	AVERAGE
PAILLIER	708	668	925	718	681	**740**

Speed-Up Ratio = Total Execution Time on local system / Total Execution Time on cloud network

=>345/740

=>0.466

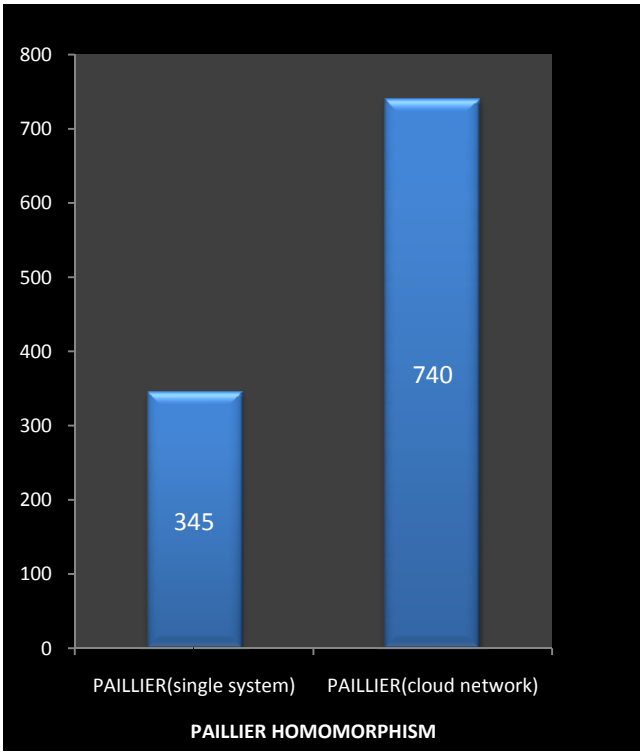

Figure 1: PAILLIER: Single System vs. Cloud Network

\

Fig 1 illustrates the Total Execution Time for Paillier Cryptosystem on single system as well as on cloud network. Graph clearly indicates that Paillier homomorphic operation on single system is significantly fast from cloud network.

Table: 3. Total Execution Time for Benaloh Cryptosystem on Local System

ALGO	SAMPLE-1	SAMPLE-2	SAMPLE-3	SAMPLE-4	SAMPLE-5	AVERAGE
BENALOH	667	556	600	625	583	**606**

ALGO	SAMPLE-1	SAMPLE-2	SAMPLE-3	SAMPLE-4	SAMPLE-5	AVERAGE
PAILLIER	344	330	360	356	337	**345**

Table: 4. Total Execution Time for Benaloh Cryptosystem on Cloud Network

ALGO	SAMPLE-1	SAMPLE-2	SAMPLE-3	SAMPLE-4	SAMPLE-5	AVERAGE
BENALOH	1145	1253	1137	1461	1225	**1244**

Speed-Up Ratio = Total Execution Time on local system / Total Execution Time on cloud network.

=>606/1244

=>0.487

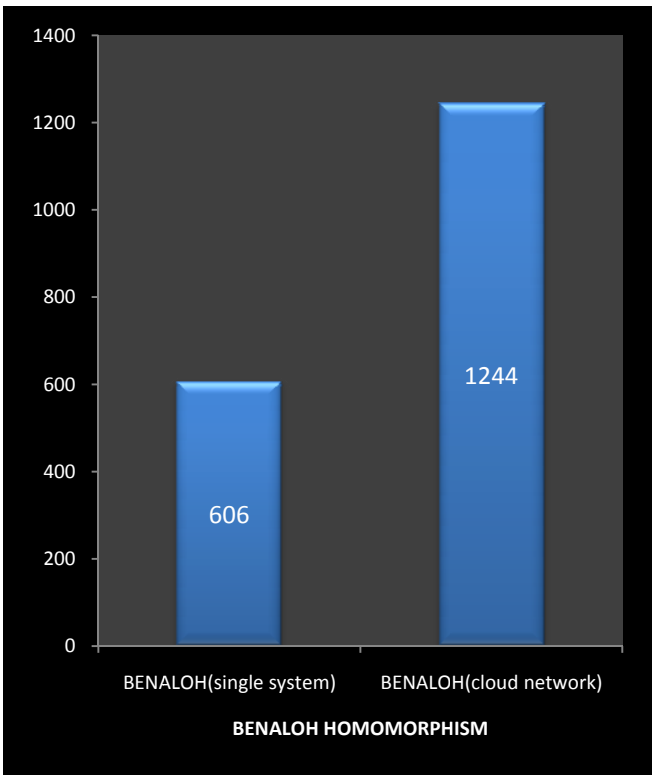

Figure 2: BENALOH: Single System vs. Cloud Network

Fig 2 illustrates the Total Execution Time for Benaloh Cryptosystem on single system as well as on cloud network. Graph clearly indicates that Benaloh homomorphic operation on single system is significantly fast from cloud network.

X. CONCLUSION

Cloud computing is a big technological opportunity for the IT world, there is no doubt about it. Pay-as-per usage model of cloud computing has created great opportunities, that were at some time even beyond the limit, without paying much more money for the same usage. We strictly feel that there is an instant need to make cloud services more reliable and safe to use, so that more and more clients can adopt this technology. Our paper is an attempt to make cloud more safe and reliable by means of very secure Homomorphic Cryptosystem, so we analyzed the Partial Homomorphic Cryptosystem, which are relatively efficient than other homomorphic cryptosystems, for the cloud usage. Our research work results that Paillier is considerably faster than Benaloh on local system and on cloud network as well. Both algorithms need an extra processing power for its fast operation from cloud network, need better configuration machines (more number of processors, fast processors, more RAM, more cache memory) to operate on cloud network. Our current research work is an attempt to analyze the performance of Partial Homomorphic Algorithms so that its use in the cloud computations can make it more secure to use & organizations may come forward to adopt cloud computing.

XI. REFERENCES

[1]. National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.

[2]. Rohit Bhaduria, Sugata Sanyal, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques”, International Journal of computer applications, Vol: 47, No: 18, June 2012, pp. 47-66.

[3]. Armbrust, M. et. al., (2009), “Above the clouds: A Berkeley view of Cloud Computing”, UC Berkeley EECS, Feb 2010.

[4]. R. Maggiani, Communication Consultant, Solari Communication, “Cloud computing is changing How we Communicate”, IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.

[5]. Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, “Automated Control in Cloud Computing: Opportunities and Challenges”, Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.

[6]. Murat Kantarcioglu, Alain Bensoussan and SingRu, “Impact of Security Risks on Cloud Computing Adoption”, IEEE, 2011, pp. 670-674.

[7]. Manabu Hirano, Takahiro Shinagawa, Hideki Eiraku, Shoichi Hasegawa, Kazumasa Omote, Takeshi Okuda, Eiji Kawai, and Suguru Yamaguchi, “A Two-step Execution Mechanism for Thin Secure Hypervisors”, Third International Conference on Emerging Security Information, Systems and Technologies, IEEE, 2009, pp. 129-134

[8]. Udaya Tupakula and Vijay Varadharajan, “TVDSEC: Trusted Virtual Domain Security”, IEEE, 2011, pp. 57-63.

[9]. Amarnath jasti, “Security in Multi-tenancy Cloud”, IEEE, 2010.

[10]. Jen-Sheng Wang, Che-Hung Liu and Grace TR Lin, “How to Manage Information Security in Cloud Computing”, IEEE, 2011, pp. 1405-1410

[11]. Ramgovind, S.; Eloff, M.M.; Smith, E., "The management of security in Cloud computing," Information Security for South Africa, 2010 , vol., no., pp.1-7, 2-4 Aug. 2010.

[12]. https://cloudsecurityalliance.org/research/top-threats/

[13]. Dimitrios Zissis and Dimitrios Lekkas “Addressing cloud computing security issues”, Future Generation Computer System, Elsevier 2010, pp. 583–592.

[14]. D. Polemi, Trusted third party services for health care in Europe, Future Generation Computer Systems 14 (1998), pp. 51–59.

[15]. Bernard Golden. Defining private clouds, 2009/http://www.cio.com/article/492695/Defining_Private_Clouds_Part_One.

[16]. Cavoukian A. Information and Privacy Commissioner, Ontario, Canada. 2009. Nov, [2011-07-13]. website A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight http://www.ipc.on.ca/images/Resources/privacy_externalities.pdf.

[17]. Javelin Strategy & Research. 2011. [2011-07-23]. website Data Breach Notifications: Victims Face Four Times Higher Risk of Fraud. https://www.javelinstrategy.com/brochure-158.

[18]. Daniel J. Abadi, “Data Management in the Cloud: Limitations and Opportunities”, Bulletin of the IEEE Computer Society Technical Committee on Data Engineering/http://sites.computer.org/debull/A09mar/abadi.pdf.

[19]. Cloud Computing: Benefits, Risks and Recommendations for Information Security, European Network and Information Security Agency, ENISA, 2009.

[20]. https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766.

[21]. Park, Daejun, Jeehoon Kang, Kihong Heo, Sungkeun Cho, Yongho Yoon, and Kwangkeun Yi. "Encrypted Execution."

[22]. Naehrig, Michael, Kristin Lauter, and Vinod Vaikuntanathan. "Can homomorphic encryption be

practical?" Proceedings of the 3rd ACM workshop on Cloud computing security workshop, ACM, 2011.

[23]. Ogburn, Monique, Claude Turner, and Pushkar Dahal. "Homomorphic Encryption" Procedia Computer Science 20 (2013), pp. 502-509.

[24]. C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.

[25]. Hu, Yin. Improving the Efficiency of Homomorphic Encryption Schemes, Diss. Virginia Tech, 2013.