Vol. 3 No. 1 July 2015 ISSN: 2321 – 788X

VIRTUALIZATION SECURITY IN CLOUD COMPUTING

S.Srividhya
Madurai Kamaraj University (University with Potential for Excellence), Madurai-625021

Dr. R.Rathinasabapathy
Madurai Kamaraj University (University with Potential for Excellence), Madurai-625021

Abstract

Cloud computing is a computing model which does computing using infrastructure and resources available in the interconnected machines. It provides services to its users on demand over the internet. The cloud stores the data and disseminated resources in the open environment through virtualization, security has become the main obstacle which is hampering and the error free deployment of Cloud environments. Even though the Cloud Computing is promising and efficient, there are many challenges for data security as there is no security of the data for the Cloud user. The data is vulnerable to several attacks; side channel attack is one of the challenging tasks in cloud. A method is proposed using a blend of virtual firewall apparatus and a modified cryptography algorithm to secure against side channel attack. The major features are creating different mystery keys and ciphering the client's secret data in a greatly secured methodology, it scale back time and no mounted key size.

Keywords*: Virtual machine, Side Channel Attack, Virtual Firewall, Algorithm, Chaos.*

Introduction

Cloud computing is an expression that is conveying facilitated administration over the web. Distributed computing is the utilization of processing asset (equipment and programming) that are provided as an administration over a web system.

There are two different classes of clouds: based on the deployment model and those based on the service model.

- Deployment Model
- Service Model

Cloud Computing Service Models:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

Infrastructure as a Service (IaaS): Its layer offers storage and infrastructure resources that are needed to deliver the Cloud services. It only comprises of the infrastructure or physical resource.

Platform as a Service (PaaS): It provides the combination of both, infrastructure and application. Hence, organisations using PaaS don't have to worry for infrastructure nor for services.

Software as a Service (SaaS): In this layer, the Cloud service provider hosts the software upon their servers. It can be defined as a model in which applications and softwares are hosted upon the server and made available to customers over a network.

Cloud Computing Deployment Models:

1. Private Cloud
2. Public Cloud
3. Hybrid Cloud
4. Community Cloud

Private Cloud : The cloud infrastructure is operated solely for an organization. It may be managed by the Cloud Computing provider or any other third party.

Public Cloud : The cloud infrastructure is made available to the general public or a large industry group and is owned by the Cloud providers.

Hybrid Cloud : It's a combination of two or more clouds (private, community or public).

Community Cloud : Its cloud infrastructure is shared by several organizations.

Cloud computing is a structural planning as shown in figure.1 that is partitioned into two sections: Frontend and Backend [5]. They associate with one another through computing system, generally web. The frontend is PC client or customer and backendis cloud supplier. The frontend incorporates the customer's PC and the application needed to get to the distributed computing framework. On the back end of the framework are the different PCs, virtual machines (VMs), servers and information stockpiling framework that make the flow of presuming organization. The data is being stored and processed in many common nodes which are also used by many other cloud users there by providing a platform for possible security attacks.

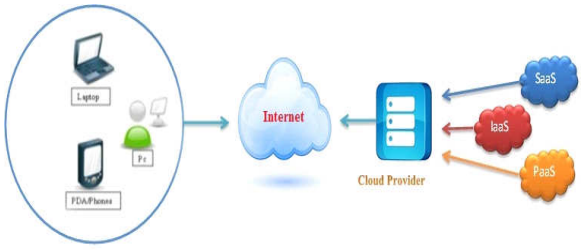


Figure 1: Cloud Computing Architecture

Hence data security is going to have an expanded significance; [1] security has been provided through several common algorithms. Chaos functions [1]have been basically used to create scientific models of nonlinear frameworks. They have pulled in the consideration of numerous mathematicians owing to their enormous complex nature. Since chaotic

functions are sensitive to initial conditions [16],any slight difference in the initial value used will radically diverse. This implies that the system will be strong against side channel attacks [16].

Preliminary:

Cryptography:

Cryptography is the practice and study of providing secured data transmission through cryptographic algorithms. It is achieving security by encoding messages to make them non-readable [15]. There are number of cryptographic algorithms which still exist to secure data. Basically Data is secured in two basic types of cryptography they are: symmetric Algorithm cryptography and Asymmetric Algorithm cryptography. In symmetric algorithm, it has only one key which is used to encrypt and decrypt the data.

In asymmetric algorithm it has one public key and one private key. Some of the existing algorithms are:

- RSA
- Diffe-Hellman
- Digital signature
- Elgamal
- Elliptic curve
- ECDSA

Side Channel Attack:

The first side-channel attack was introduced by Kocher [11]. Brute force, DDOS, are using the theoretical weakness of the algorithm [2], instead side channel attack is based on information gained from the physical implementation of a cryptosystem. The term has been extended to apply to any computing system now. A portion of the normal side channel attacks can be classified into the following:

- Timing Attack
- Power Consumption Attack
- Electromagnetic Attack
- Acoustic Cryptanalysis
- Differential Fault Analysis

These types of side channel attacks are found to attack our cloud data base through virtual machine. These attacks are implemented in the Amazon EC2 and analyzed how data is leaked through this attack [3].

Timing Attack:

Timing attacks exploit the distinction between execution times of methodologies with different inputs. Mostly timing attacks are occurred in asymmetric cryptography [12].

The running time of a cryptographic device can constitute an information channel, providing the attacker with invaluable information on the secret parameters involved. In timing attack, the information at the disposal of the attacker is a set of messages that have been processed by the cryptographic device and, for each of them; the corresponding running time is analyzed [1]. The goal is to recover the secret parameters for example timing attack watches data movement into and out of the memory, on the hardware running the cryptosystem or algorithm. Simply by observing variations in how long it takes to perform cryptographic operations, it might be possible to determine the entire secret key. Such attacks involve statistical analysis of timing measurements, and have been demonstrated across networks [14].

Chaos based cryptographic

Recently the chaos based cryptographic algorithms has been developed promptly. Chaos owns certain critical properties such as sensitive dependence on initial condition, random-like behavior, and continuous broadband power spectrum, which match the confusion, diffusion, and key sensitivity requirements for cryptography [1]. Chaos based cryptographic offer sundry features over the traditional encryption algorithms such as high security, speed, and sensible computational overheads and force [4].

Some Existing method

Side channel attack is an access-driven attack it is more vulnerable to attacks on Virtual machine. At first, One case study explore how such placement can then be used to mount cross-Virtual Machine side-channel attacks to extract information from a target Virtual Machine on the same machine [3]. One incident of side channel attacks is the timing side channel attack [6] which is based on measuring how much time different reckonings take to perform. Successful modulation of this measured time may lead to leakage of sensitive information about the owner of the computation or even the cloud provider. Timing based side channel attacks are especially hard to control and pervasive on clouds due to massive parallelism. Moreover, it is also hard to detect since they do not leave trails or raise any alerts. Cloud customers may not have the authorization to check these kinds of possible side channel attacks from other cloud mates obviously due to privacy concerns. On the other hand, cloud providers can thoroughly check and detect timing attack incidents but may not be willing to report such breaches due to many considerations such as protecting company reputation. These attacks are implemented in some cryptography algorithms [8]. Home Alone is introduced to detect side channel attack [7]. Through this attack most of the data were leaked to disposethat some models and techniques are developed to reduce data leakage [9] [10].

Proposed Method

The main aim of this proposed work is to secure the data from Time side channel attack. It is an asymmetric key cryptography that uses logistic map and nonlinear equation. First logistic map is used as a key generator for private key, the nonlinear equation for encryption.

Private Key generation part is described using the logistic map:

$$X = R * S (1-S) \quad (1)$$

Key Generation

Alice generates the public/private key pair.

1. Generate large integer value 'S' randomly and also generate large random value R.
2. Generate Public key using Logistic Map [X=R * S (1-S)] and Compute P=X * S.
3. Alice Public key is (P, X); Alice Private Key is S.

Using this map, multiple key can generate. And then another computation process is done in the form Compute P = X * S. The output of computed P is used as a shared key for encryption using nonlinear equation.

Nonlinear equation description:

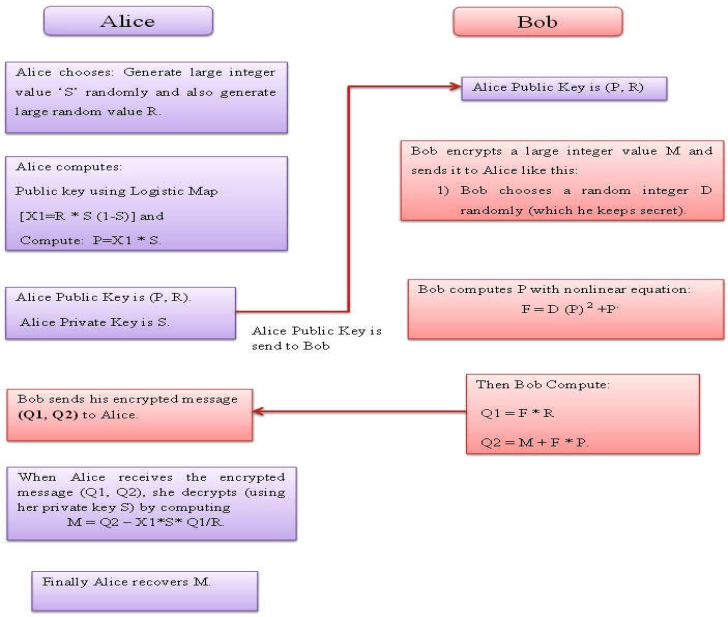
Data is encrypted using the descripted equation

$F = D (P)^2 + P \cdot$ -- (2)

Encryption Procedure:

Bob encrypts a message M to Alice

- Obtain Alice authentic public key (P, X).
- Represent the message as large integer value M.
- Select a large integer D randomly.
- Compute P with nonlinear equation $F = D (P)^2 + P \cdot$
- Compute Q1 = F * X and Q2 = M + F * P.
- Send cipher text Q1, Q2 to Alice.



Decryption process:

Alice receives encrypted message M from Bob

- Use private key S to compute M = Q2 – S* Q1.

Note: M = [M + F * P] – [S* F * X)].

= [M + F * X * S] – [S* F * X]

Cancelling Out [F * X * S].

- Recover M by computing.

Algorithm Flow Diagram:

In this proposed algorithm this system has following features:

- The proposed algorithm allows encryption of large length message.
- No relation between key size and plain size.
- Fast.
- No fixed key size.

Analysis with RSA and AES Algorithm:

The proposed method performance is analyzed with RSA and AES Algorithms. In the below figure.2 the text is encrypted and decrypted using the existing method and the execution time is measured.

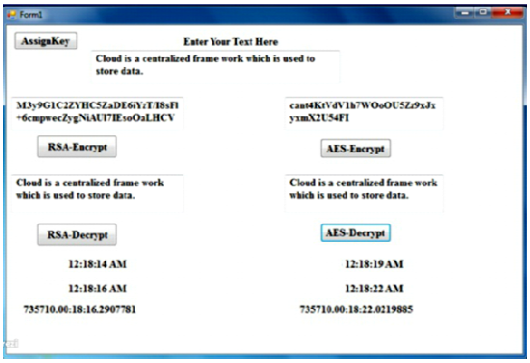


Figure 2: RSA and AES Performance Analysis

In this analysis the below figure.3 is the proposed method of key generation without key limitation key is generated.

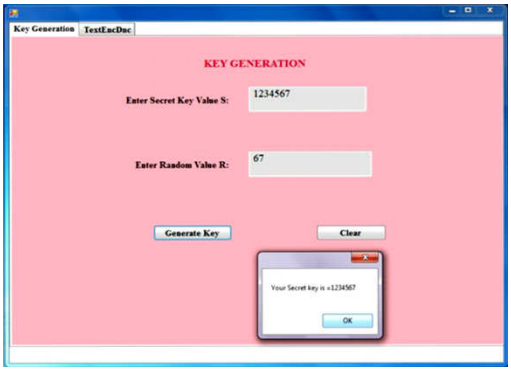


Figure 3: Key Generation

To analysis the performance of the proposed method, in the below figure.4 the text is encrypted and decrypted which is used in RSA and AES algorithm. The encryption and decryption is done by using the secret key which is faster and secure than the existing one.

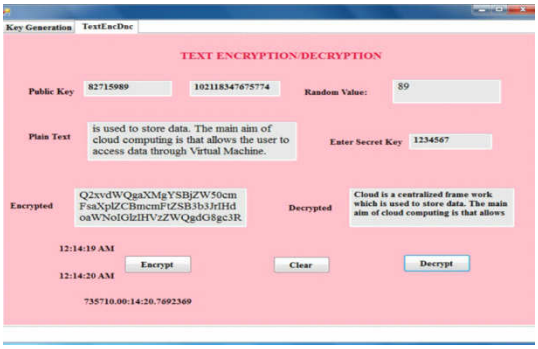
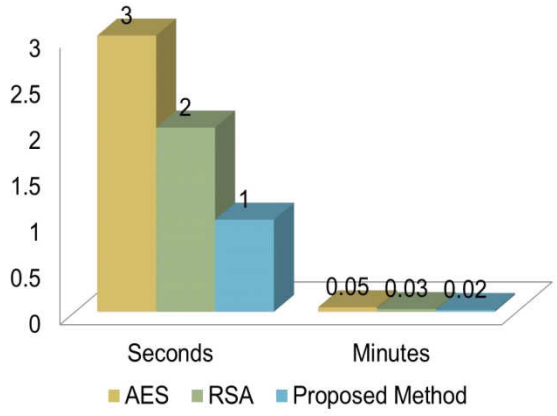


Figure 4: Encryption and Decryption

Here the performance is analyzed in the form of chart and the differences are shown in the figure.5.



Conclusion

In this paper new technique is followed in cryptography to secure data form critical attacks like side channel, Brute force, DDOS, etc., Through this problems are analyzed and overcome the problem using Cryptography Algorithm utilizing Logistic Map and nonlinear comparison for kind of attack and make the data secure in cloud computing. In future this new method can implement in Digital Image Processing. This technique performances are shows this proposed method is more flexible and secure one than the existing algorithms.

References

1. Bhavana Agrawal, Himani Agrawal, Monisha Mishra(2013),"Implementation of Various Cryptosystem Using Chaos"IOSR Journal of Computer Engineering (International Organization of Scientific Research)
2. http://en.wikipedia.org/.
3. Thomas Ristenpart, EranTromer, HovavShacham, Stefan (2009) " Hey,You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds" . Savage Attack on Amazon EC2 web services. Dept. of Computer Science and Engineering University of California, San Diego, USA.
4. Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien (2013)," Survey Report on Chaos Based Public-key Cryptosystem". International Journal of Emerging Technology and Advanced Engineering.
5. BhruguSevak (2012),"Security against Side Channel Attack in Cloud Computing". International Journal of Engineering and Advanced Technology (IJEAT).
6. Aviram, A.; Hu, S.; Ford, B.; Gummadi, R. "Determinating timing channels in compute clouds". In Proceedings of the 2010 ACM Workshop on Cloud Computing Security

Workshop (CCSW '10); ACM: New York, NY, USA, 2010; pp. 103–108.
7. Yinqian Zhang, Ari Juels, Alina Oprea, Michael K. Reiter. "HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis". In Proceedings of IEEE Computer Society: 2011 IEEE Symposium on Security and Privacy, DOI 10.1109/SP.2011.31.
8. P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems", in the Proceedings of Crypto 1996, LNCS, vol 1109, pp 104–113, Santa Barbara, CA, USA, August 1996.
9. Mr. Amol O. Gharpande, Prof. Ms. V. M. Deshmukh." DATA LEAKAGE DETECTION".International Journal Of Computer Science And Applications Vol. 6, No.2, Apr 2013 ISSN: 0974-1011.
10. Ms. N. Bangar Anjali1, Ms. P. RokadeGeetanjali, Ms. PatilShivlila, Ms. R. Shetkar Swati, Prof. N B Kadu." DATA LEAKAGE DETECTION".IJCSMC, Vol. 2, Issue. 5, May 2013, pg.283 – 288.
11. Kocher, P.C."Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems". In: Proceedings of CRYPTO'96, LNCS, vol. 1109. Springer, Berlin, pp. 104–113 (1996).
12. Jean-Luc Danger, Sylvain Guilley, PhilippeHoogvorst, CédricMurdica, David Naccache." A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards". Springer-Verlag Berlin Heidelberg 2013. Published on: 23 October 2013.
13. Prof. Jean-Jacques Quisquater, Math Rizk, "Side Channel Attack - State of the art", October 2002.
14. http://en.wikipedia.org/wiki/Side_channel_attack.
15. Ayushi, "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Application-2010.
16. Bhavana Agrawal, Himani Agrawal, "Implementation of AES and RSA using Chaos System".International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.