IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Review of Existing Encryptions Techniques used to Prevent Side Channel Attacks in Cloud Computing

Toa Bi Irie Guy-Cedric[1], Suchithra. R.[2]

[1] Research scholar, Jain University, Bangalore-560043, India
[2]Head of Department of MSc IT, Jain University, Bangalore-560043, India

Available online at: www.ijcseonline.org

Accepted: 25/Jul/2018, Published: 31/Jul/2018

***Abstract*—** Cloud computing is a popular paradigm in today's world that exposes it to various threats and attacks. Security is one of the major challenges as basic administrations are regularly outsourced to the cloud vendors. The major concern in cloud environment is how to make the environment safe and secured. This paper investigates some of the security attacks and the existing solutions for cloud security threat.

***Keywords*—**Security, cloud computing, side channel attacks

I. INTRODUCTION

Security is a primary concern in computing and considerable research exertion has been committed to for it. Applying a cryptographic technique for approved client is the most mainstream existing answer for settling security issues and expanding the dependability of cloud situations. However, building and implementing a good policy against threat in cloud computing is not easy and depends on what types of threats like data breach, data leak, ddos, malicious insider and so on. Therefore, data breach is one of the important threats and one of the well-known attacks is called side channel attack.

Side channel attack can be defined as a process to gain access of data stored on cryptographic system and takes the sources in cloud by using the weakness between multi-tenants on the same virtual machine. Side channel attack is simple to implement and can be called as a most successful attack in data breaches because it takes advantage by targeting the weakness of cryptosystems and also avoiding to leave a fingerprint of the attack perform. One of the techniques used to prevent side channel attack and data breach is by using cryptography and also depends on the architecture of the algorithm used.

Cryptography is a technique which is intended to convert data and can be used to provide various security related concepts such as confidentiality, data integrity, au-thentication, authorization and non-repudiation [1]. Nowadays many cryptographic algorithms are used like AES, DES, and RSA and they are divided between two types' symmetric and asymmetric techniques. This paper presents a comparative algorithms and techniques used to prevent side channel attack. The rest of the paper is organized as follows. In Section II, we briefly describes side channel attacks. In Section III, contain the survey of side channel attack focus on some attack. Comparisons and analysis are shown in Section IV and finally, we conclude this paper in Section V.

II. BACKGROUND

Side-channel attack is a technique bypassing a virtual machine by observing and monitoring all the hardware system during the execution task to retrieve secret data stored in cryptosystem. Security of a cryptosystem is based on the architecture of the algorithm used. Figure 1, describe the process of side channel attack on how they break algorithm of cryptosystem, using message authentication, signature scheme, and even cryptographic protocols. They are many attacks technics they can be utilized by the attacker like timing attack, power analysis attack, electromagnetic attack, acoustic attacks and so on.

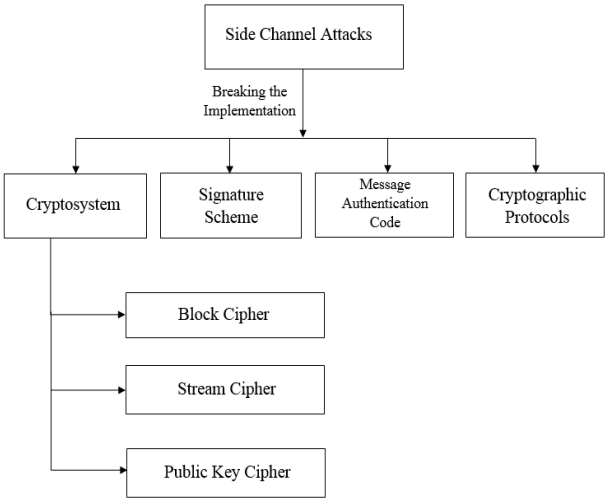

Figure 1. Process of side channel attack

- Timing Attack

Timing attack is a technique in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute the cryptographic algorithms and uses statistical analysis to find the right decryption key and gain access. For example, Paul Kocher designed a timing attack to expose secret keys used for RSA decryption. However, timing side-channel attack works remotely unlike other attack [3].

- Power Attack

Power attack is based on power analysis when attacker collect and analyze power consumption of a cryptographic hardware system. That attack is divided in two types:

- Simple power analysis

Simple Power Analysis (SPA) is an exploit using the variation between power consumption during an operation executed by the processor with the goal to discover secret key. These attacks are achieved by monitoring some operations of power consumption. This is achieved by mapping certain operation types to consumption patterns.

- Differential power analysis

Differential power analysis (DPA) attack is a technique based on statistical analysis and use a method called the correlation to derive the encryption key of cryptosystem. These attacks takes advantages of the noise and power used by computer when they are computing (running). DPA as a similarity of simple power analysis but are more efficient to crack secret key of smart card, processor even with RSA, AES running without leaving a trace.

III. SURVEY OF SIDE CHANNEL ATTACK

Security is a primary concern in computing and considerable research exertion has been committed for it. We briefly describe some survey cover side channel attack.

Carlos Morino et al. proposed a new exponentiation algorithm based on idea of buffering the operations to mitigate power attack using randomization compute. The goal of this method is to achieve better computational performance and reduce the cost of additional storage to encrypt and decrypt key avoiding too long time require by attacker to use power attack to decrypt secret key from RSA and exponentiation algorithm [2].

Kopf and Durmuth proposed the novel counter measure for timing attack. The amount of information about the key by an unknown message using which the attacker can extract from the deterministic side channel is bounded from above as in (1). This method leads to implementation with minor performance overhead and formal security guarantees [3].

$$(O)\ (\log2\ (N+1)\ \text{bits} \quad (1)$$

With O set of possible observation, N is the number of side channel measurement.

Chen et al. proposed an improving method for mitigating timing attack on RSA-CRT via error detection and correction strategy and this technique consists of implementing and mixing different algorithms used to secure RSA for example algorithm, CRT algorithm, Montgomery reduction and uses statistical method to determine how timing attack can rebuilt the entire secret key RSA [4].

Giraud. C proposed a new technique to countermeasure fault attack and simple power analysis based on a new technique of implementation of exponentiation algorithms. This method is simple to implement and resistant against the Straightforward Method and Chinese Remainder Theorem modes to recovery RSA signature generations [5].

Gulmezoglu *et al.* have investigated the efficacy of cache attacks in various categories. Two different methods like Flush +Reload and Prime +Probe are used to mount the cache side-channel attacks on a popular OpenSSL implementation of AES. It works across various cross-VM setting and fulfill the recovery of full encryption keys in a short period. The results intimated that the information leakage and implementation of software should be approached with attention. They proved the efficacy of this attacks on the Amazon cloud, but also argued for the usage of AES, are more efficient for good security [6].

Zhang *et al.* [7] have designed a Cloud Radar which is a real time detection system to detect the cache based side channel attacks in cloud. It leverages the previous performance counter of the hardware and monitors both operation of cryptographic VM and abnormal behavior of VM. The Cloud Radar was designed in a light weight to the system and there was no need of new hardware, hypervisor/OS or application modifications. The result shows that the Cloud Radar can detect high constancy of cache based side-channel attacks while introducing little overhead to the cloud applications.

IV. DISCUSSION

In this section we briefly explain some advantage and limitations of existing techniques used to mitigate side channel attack, as shown on table 1.

Solution	Advantage	limitation
Exponentiation algorithm based on idea buffering against timing attack	The goal of this method to is reduce decryption time to be independent of size of data and reduce the cost of additional storage to encrypt and decrypt key avoiding too long time require by attacker.	Efficient only on embedded system and on RSA algorithm.
RSA and CRT algorithm via Error Detection and Correction	The aim of that technique is efficient on timing attack and provide an equal time	Only uses statistical analysis to design a

Strategy	between the running time of the private key and the compute time. Simple to implement in real life.	pattern to prevent side channel attack, and efficient on RSA algorithm.
OpenSSL + AES algorithm	Detect Flush +Reload and Prime +Probe method when used to launch side channel attack and proved the good security key by using AES 128bits.	Need third parties (cloud provider) to support that and apply another security on their side.
Dual-spacer dual-rail delay-insensitive Logic + AES	Security is applied on device circuit by mixing new dual-spacer dual-rail delay with 3 AES couches and synchronous logic, making it much more difficult for an attacker to correlate data with power consumption and timing analysis.	Apply at the level of circuit system which will be more costly to design and implement.
Randomness Algorithm and Optical Asymmetric Encryption Padding (OAEP)	Improve security key of RSA by using random techniques during decryption process with the purpose the provide fault positive time to induce the attacker in error.	Double verification needs to be applied to avoid detection error during encryption and decryption process.

Table 1. Resume of existing techniques.

IV. CONCLUSION

Cryptographic algorithms are always implemented in software or hardware by which interactions is influenced their environments that can be used by attackers to retrieve information. Encryption calculations take an important place in information security in cloud computing and by examination of various parameters utilized as a part of calculations. Indeed, encryption is mostly used as a countermeasure.

We presented some existent countermeasures to mitigate and prevent side channel attack.

REFERENCES

[1] William, S "Cryptography and network security: principles and practice", pp. 23-50, 1999 Prentice- Hall,

[2] Carlos Moreno, Anwar Hasan and Sebastian Fischmeister "A Family of Fast Exponentiation Algorithms Resistant to SPA, Fault, and Combined Attacks", pages 157- 166, 2015 IEEE

[3] Paul Kocher "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems. Advances in Cryptology", pages 104-113, 1996.

[4] Chen C., Wang T., and Tian J., "Improving Timing Attack on RSA-CRT via Error Detection and Correction Strategy," Information Sciences, vol.232, pp. 464-474, 2013 for paper

[5] Giraud C., "An RSA Implementation Resistant to Fault Attacks and to Simple Power Analysis", IEEE Transactions on Computers, vol.55, no. 9, pp. 1116-1120, 2006.

[6] Berk Gulmezoglu, Mehmet Sinan Inci, Gorka Irazoqui, Thomas Eisenbarth and Berk Sunar "Cross-VM cache attacks on AES "issue No.03- July-Sept (2016 vol.2), p 211-222.

[7] Y Zhang, A Juels, MK Reiter, T Ristenpart "Cross-VM side channels and their use to extract private keys" 2012 for paper

[8] Amuthan Arjunan, Praveena Narayanan, and Kaviarasan Ramu "Securing RSA Algorithm against Timing Attack" The International Arab Journal of Information Technology, Vol. 13, No. 4, July 2016 for journal

[9] Washington Cilio , Michael Linder a, Chris Porter , Jia Di , Dale R. Thompson , Scott C .Smith " Mitigating power- and timing-based side-channel attacks using dual-spacer dual-rail delay-insensitive asynchronous logic", 2012 Elsevier Ltd paper

[10] Amazon elastic compute cloud.

[11] O. Aciic¸mez, W. Schindler, and C¸. K. Koc¸. Cache based remote timing attack on the AES. In Topics in Cryptology— CT-RSA 2007, The Cryptographers' Track at the RSA Conference 2007, pages 271–286, February 2007.

Authors Profile

Mr. Toa Bi Irie Guy-Cedric pursed Bachelor of Science from Institut National Polytechnique Felix Houphouet-Boigny, of Cote d'Ivoire in 2011 and Master of Information Technology from Shridhar University, India in year 2013. He is currently pursuing Ph.D. in Computer Science from Jain University, India. He has published many research papers in reputed international journals and conferences. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy.

Dr. Suchithra R pursed Bachelor of Commerce, Master of Computer Application and Ph.D in Computer Science from Manonmaniam Sundaranar University , India in year 2009. She worked as Associate Professor and Head of MS (IT) Department in Jain university since 2010. She has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & other) and conferences and it's also available online. Her main research work focuses on Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Programming. She has 15 years of teaching experience and 6 years of Research Experience.

