Global Journals Inc.

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 14 Issue 4 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# Security of Side Channel Power Analysis Attack in Cloud Computing

By Sajjad Waheed, Nazrul Islam, Barnaly Paul Chaity
& Saddam Hossain Bhuiyan

*Mawlana Bhashani Science and Technology University, Bangladesh*

*Abstract-* Future world is moving towards cloud computing. In a word cloud computing can be defined as remote access computing resources through the Internet. It provides a lot of services at a very low cost. It can improve an organization's performance by minimizing its cost. It also helps to maximize their revenue with fewer resources. It is becoming popular among organizations and people. They can store their data in cloud at low cost. Attackers aim to attack cloud environment for getting valuable information from cloud users. They attack on it by taking different approaches. They try to access confidential information of different organizations from the cloud. Among different attacks side channel power analysis attack is a newer type of attack. In this paper, we proposed a way to mitigate these types of attacks through a Police Virtual Machine (Police VM). The Police VM provides false power consumption information to attackers and they cannot get real power consumption information from user VM.

*Keywords:* *cloud computing, side channel attack, power analysis attack, cloud security.*

*GJCST-B Classification :* *C.2.4 D.4.7 B.4.2*

SECURITYOFSIDECHANNELPOWERANALYSISATTACKINCLOUDCOMPUTING

*Strictly as per the compliance and regulations of:*

Open Association of Research Society, USA
Research | Diversity | Ethics

© 2014. Sajjad Waheed, Nazrul Islam, Barnaly Paul Chaity & Saddam Hossain Bhuiyan. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

# Security of Side Channel Power Analysis Attack in Cloud Computing

Sajjad Waheed [α], Nazrul Islam [σ], Barnaly Paul Chaity [ρ] & Saddam Hossain Bhuiyan [Ѡ]

*Abstract-* Future world is moving towards cloud computing. In a word cloud computing can be defined as remote access computing resources through the Internet. It provides a lot of services at a very low cost. It can improve an organization's performance by minimizing its cost. It also helps to maximize their revenue with fewer resources. It is becoming popular among organizations and people. They can store their data in cloud at low cost. Attackers aim to attack cloud environment for getting valuable information from cloud users. They attack on it by taking different approaches. They try to access confidential information of different organizations from the cloud. Among different attacks side channel power analysis attack is a newer type of attack. In this paper, we proposed a way to mitigate these types of attacks through a Police Virtual Machine (Police VM). The Police VM provides false power consumption information to attackers and they cannot get real power consumption information from user VM.

*Keywords: cloud computing, side channel attack, power analysis attack, cloud security.*

## I. Introduction

Cloud computing is a type of Internet based computing. It provides different services through the Internet – such as servers, storage and applications. It is beneficial for enterprises because of its reliability, security and performance.

Here the computing resources are easy to obtain and access, cheap, simpler to use. It also provides self-service, on-demand-service and pay-as-use consumption [1] and [2]. The virtual data centers where some virtual machines (VMs) are hosted on servers are becoming more popular due to cloud computing [3]. The main purpose of cloud computing is to provide the users instant access to the resources they need [4].

Clouds are said as the next-generation data centers [5]. But there are some specific types of attacks that take place in cloud by attackers. According to [6] and [8] some common attacks are Denial of Service Attack (DoS), Side Channel Attacks, Man in the Middle Attack, Cloud Malware – Inject Attack, Authentication Attack.

According to [7], author addresses to three types of Side Channel Attacks. These are called Timing Power Consumption Attacks and Differential Fault Analysis (DFA) Attacks. Among these attacks the Attacks, analysis of power traces is an effective way to obtain the encryption key from secure processors [11]. Attackers are often very successful in the power analysis attacks [13].

According to [7] and [10], attackers take approach of Simple Power Analysis (SPA), Differential Power Analysis (DPA) and High-Order Differential Power Analysis (HO-DPA) after getting power information from the cloud. Attackers directly observe a system's power consumption in SPA attacks. According to the microprocessor instruction performed, the amount of power consumes varies. The leakage of power consumption is the source of side channel information. The side channel is characterized on the leakage of power [12].

Such as, at the time of performing Advanced Encryption Standard (AES), Data Encryption Standard (DES) rounds or RSA (RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman) operations by the microprocessor, can be identified during different parts of the operations. For example, RSA can be broken by revealing differences between multiplication and squaring operations as well as DES has differences within permutations and shifts. SPA can break these operations [10].

Side channel power analysis is a newer type of attack, based on the side channel power consumption information. According to [7], author discussed some solutions of power analysis attacks by adopting approaches of shielding, reduction of signal size, addition of noise, power consumption balancing, and modification of algorithm design. There are also some other approaches discussed in [8] and [9] by using a virtual firewall appliance and randomly encryption decryption.

Leakage of power and side channel information is the main causes of power analysis attacks. These approaches discussed by the authors are used to prevent leakage of power or providing wrong information. But all these techniques are designed and proposed for user machines. Cloud providers have to prepare all user machines according to these designs for protecting them. It might be better not to make any

*Author α σ ρ Ѡ : Associate Professor Department of Information and communication Technology. Mawlana Bhashani Science and Technology University, Tangail-1902, Bangladesh.*
*e-mails: sajad302@yahoo.com, nazrul.islam@mbstu.ac.bd, chaity_paul_s@yahoo.com, thesamrat383562@gmail.com*

change in the user machines and to think of a different way. It might be better if cloud providers use a virtual machine (VM) in physical machines to guard user's data, stored in other VMs. The guard virtual machine could be said as Police VM. It can change the real power information and provide false information.

A Police VM can hide the power consumption information by providing false information. For example, at the time of performing AES rounds in user VM, a Police VM starts a different operation, such as DES operation. At that time, attackers get the power consumption information from the Police VM instead of the real information. Side channel power consumption attack can mitigate using a Police VM.

The remainder of this paper is structured as follows. Section II provides details about the research methodology. Section III presents the design and implementation of this work. Section IV shows results and discussion from the study. Finally, Section V contains the summary of our study and concludes with future work.

## II. Research Methodology

Cloud computing is becoming popular day by day because of its less cost and more profit. Because of its popularity, hackers target clouds to get valuable information. After studies, we came to know about different types of attacks take place in a cloud environment. Among them side channel attack is newer. We also came to know about power analysis attack which is one type of side channel attack.

After studying about side channel power analysis attack, we prepared a block diagram. The block diagram represents how these attacks take places. In cloud environment a physical machine consists of some virtual machines (VMs). Users use these virtual machines in different purposes. Attackers place his VM beside the target user VM and get power consumption information. Using this information, they try to find out the secret key of the user VM.

We are proposing to use a Police VM beside the user VM on the purpose of preventing this attack. It is same as the normal VM, but it stands for protecting other VMs from getting power consumption information. It consists of some anti-attack units. Here is another block diagram based on how a police VM should be installed and how it could be used.

We prepared a flow chart that represents the process how a user VM may work at the time of performing any encryption operation and attackers get the power consumption information during this period. Furthermore, here is a flow chart to represent the work of a Police VM. A Police VM works when a user VM starts to perform any encryption operation; such as DES or RSA operations. During this period Police VM provides false information through doing a different encryption operation from the user VM; such as AES operation. By doing this it generates false information and provides this in the cloud environment. Attackers get the false information from the police VM rather than from any user VMs and attackers cannot generate the secret key that is used in the user VM and it becomes hard for them to access the user VM through side channel attack. We made a pseudo code based on our theory and implemented this by making a program on it. Furthermore, we discuss about the results we get from our work and analyze it.

## III. Design and Implementation

Cloud provides different types of services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). In IaaS model cloud provides infrastructure. This is like a collection of multiple computers, VMs and also other resources where users can store their applications [9].

A physical machine mainly has more than one VM. That means more than one client share the same physical host. The VMs are could be in co-residence in a physical host. But side channel attacks mostly occurred because of sharing resources. The co-residence of VMs is a part of cloud computing and this cannot go away and this can be concerned as a drawback, but the cloud has to go with this as well. Allowing this co-residence cloud can take an approach to handle the attackers.

### *a) Power Analysis Attack Approach*

When a regular VM converts a plaintext to a cipher text by using a particular operation such as AES operation, then the power consumption information can be got by the attacking VM. The attacking VM analyses the power consumption information by SPA, DPA or HO-DPA techniques and can recognize the operation that is used to make the cipher text. Then the attacker can generate the private key and can attack the target VM. Power analysis attacking approach is shown in Fig.1.

© 2014 Global Journals Inc. (US)

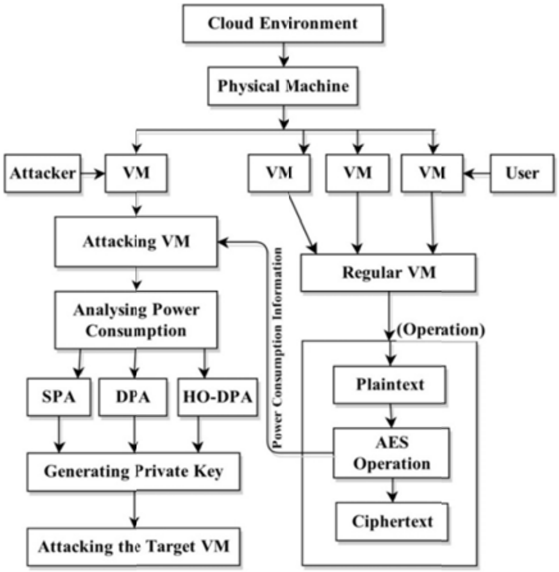

*Figure 1 :* Side Channel Power Analysis Attack

These attacks are based on analyzing the power consumption of the unit at the time of the encryption operation. By some simple differential power analysis attackers can gain information. Using this, he can get the secret key.

*b) A Police VM*

A police VM is similar like a regular virtual machine that is launched by a physical host, but the difference of this from a regular VM is that, a police VM is created to prevent and handle side channel attacks [14]. A police VM consists of some units inside it which are called as anti-attack units. There could be none or more than one unit inside a VM. This is a software component which is made for preventing and handling side channel attacks. A Police VM containing some anti-attack units inside it are shown in Fig. 2.

These are installed inside the VM according to the attack and the situation. Different units can work in different situations and they can work for the different user VMs at a time. The structure has some advantages like scalability and varied execution timing. Scalability means that the units can be installed when they are necessary [14].

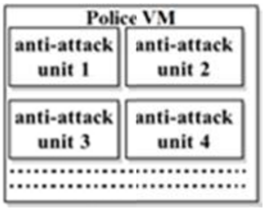

*Figure 2 :* A Police VM containing Anti-Attack Units

When there is a new attack, then new types of units can be developed and installed. Varied execution timing means a police VM could be used in timing need. The operation of a Police VM is shown in Fig.3.

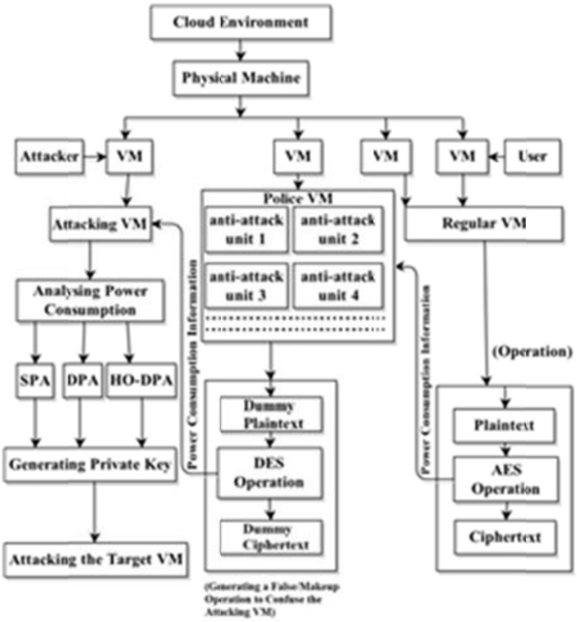

*Figure 3 :* The Solution of Power Analysis Attack Using Police VM

*c) Flowchart*

In cloud, attackers get power consumption information when a user is doing any operation. By analyzing them, they try to find out the operation. A flow chart is given in Fig. 4 which shows how an operation is performed in a user VM.

A user VM gets the message and key from the user and check for their validity. After getting them it starts for encrypting the message. At the time of doing any encrypting operation the power consumption information was released from the user VM. In such a way side channel information is leaked from any user VM.

© 2014 Global Journals Inc. (US)

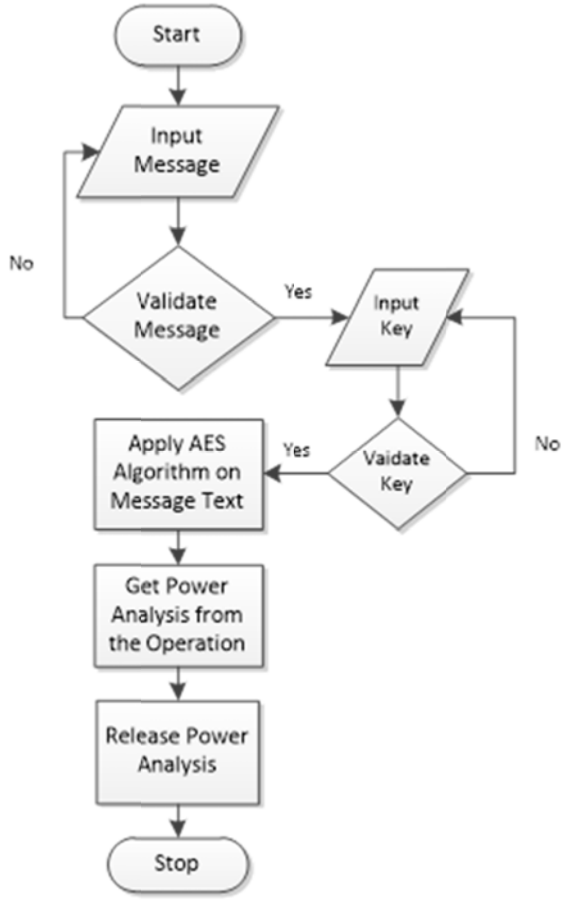

*Figure 4 :* The Operation of a User VM

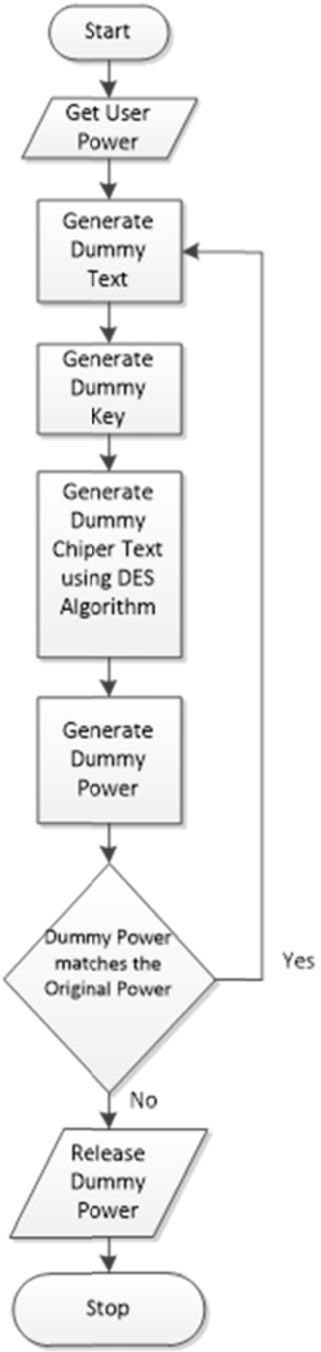

*Figure 5 :* The Operation of a Police VM

At the time of doing any encryption operation inside the user VM the Police VM got power from the user and starts working. A dummy message and a dummy key are generated inside it. It starts to do another encryption operation. In this way it creates false power information which can confuse attackers. Police VM can also compare the real and false information after that it releases it. A flow chart is given in Fig. 5 to show how an operation is performed in a Police VM.

### *d) Pseudo Code*

User VM:

*Step 1:* Input Message Text

© 2014 Global Journals Inc. (US)

```
Step 2: Input Key Text
Step 3: Check the Key Validity
Step 4: Check the Message Validity
Step 5: Encrypt the message using AES   Algorithm
Step 6: Find the Power from user VM during AES operation
Police VM:
Step 1: Capture the power of user VM
Step 2: Create Dummy Text
Step 3: Create Dummy Key
Step 4: Encrypt the Dummy text using DES Algorithm
Step 5: Find the False Power from the Police VM during DES operation
Step 6: Compare False power and Captured Power
If              false power == captured power
Then,    go to Step 1.
Else,    transmit false power.
```

## IV. Results and Discussion

RSA In cloud environment the power which is consumed by a regular machine can easily be traceable. DES rounds and RSA operations can be identified. SPA monitoring can find out the permutation and shifting, which is performed in every round in a DES operation. Fig. 5 represents the power traces of DPA operation. Here the DPA values are measured in watts.

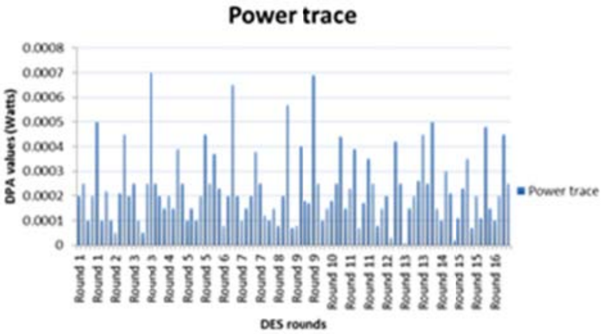

*Figure 6 :* DPA power traces of DES rounds

RSA operation can also be traced by SPA analysis. The square and multiply sequences can easily be identified. Fig. 6 shows the power traces of RSA exponential operation, which is vulnerable to SPA analysis. The square and multiply are shown figure. The power trace of square is shown by blue color and the power trace of multiply is shown by orange color.

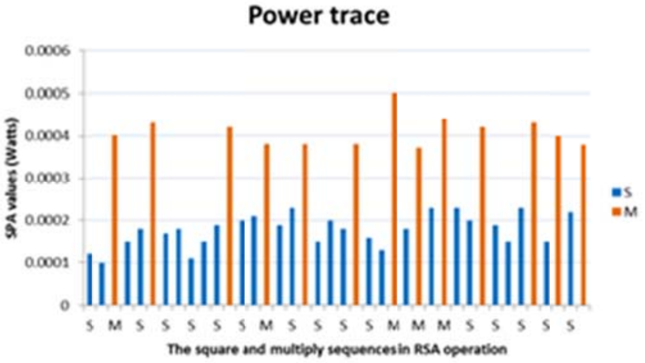

*Figure 7 :* SPA power traces of RSA operation

The Police VM can be made in such a way so that the power consumption information of any user VM could be kept hidden and it releases false power. It generates false power consumption information to protect the real power consumption information. When a regular VM converts a plaintext to a cipher text by using a particular operation such as AES operation, then the Police VM starts to convert a dummy plaintext to a dummy cipher text by using a different type of operation; such as DES operation.

Police VM generates different power consumption information. As a result, attackers get false information from the Police VM. They analyse the information by using SPA, DPA or HO-DPA operations and think that the user is doing a DES operation rather than AES. Attackers cannot break the real key that is generated by the real user rather than they make the dummy key that is used in the Police VM. In such a way a Police VM can change the real power consumption information which is generated by the user and provides false power consumption information generated by it.

Besides power analysis information a Police VM can also be used to prevent other types of side channel attacks. Any side channel information that can be leaked from a user VM can easily be changed by it. It can also be programmed not only for generating false information but also comparing the false and the real power. After comparing the false and real power it tries to find out whether they are same or not. If these are same, it runs the operation again with a different encryption system and then compare again. If the both power information are not same, then the Police VM provides the made up power that is generated by it.

If a Police VM is used in a cloud environment, there is no need to make any change in every VM for protection. A single police VM can work for different user VMs for different purposes. It's easy to install and also programmable. In this way a Police VM can handle or mitigate any types of side channel attacks including the power analysis attack.

Based on this research, we made a program that shows how a user VM works at the time of doing any encryption operation. We have used AES operation

© 2014 Global Journals Inc. (US)

in the user VM. We also show the power consumption information at the time of the AES operation in the user VM. We also made a Police VM beside. We have used DES operation for it. When the user VM starts its operation, the Police VM starts its work and makes false information. If attackers try to get power consumption information, they get this from the Police VM not from the user VM.

## V. Conclusion

Cloud computing brings many benefits, but it also causes several security issues. One of these issues are the side channel attacks. These attacks are based on information gained from the physical implementation of a machine. Attackers can easily gain secret information from a device by using side channel attack. It is a good idea to provide security against this attack by using different approaches. Here, we aim at providing a platform to prevent side channel power analysis attacks using a newer approach named as "Police VM". It can provide false power information to attackers. They become unable to find out the secret key which is used in the user VM. The main purpose of this work is to make the cloud more secure by hiding the real power information of users. The program is developed for desktop based cloud computing. The future work can be addressed for mobile based cloud computing that will also provide less time complexity and to find out an easier solution to prevent side channel power analysis attack which will be more effective.

## References Références Referencias

1. Rajan, A. P., & Shanmugapriyaa. (2013). Evolution of Cloud Storage as Cloud Computing Infrastructure Service. *arXiv:1308.1303 [cs].* Retrieved from http://arxiv.org/abs/1308.1303
2. Buyya, R., Yeo, C. S., & Venugopal, S. (2008). Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. In *10th IEEE International Conference on High Performance Computing and Communications, 2008. HPCC '08* (pp. 5–13). doi:10.1109/HPCC.2008.172
3. Hlavacs, H., Treutner, T., Gelas, J.-P., Lefevre, L., & Orgerie, A.-C. (2011). Energy Consumption Side-Channel Attack at Virtual Machines in a Cloud. In *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC)* (pp. 605–612). doi:10.1109/DASC.2011.110
4. U. Goyal, G. Bhatti, and S. Mehmi, "A dual mechanism for defeating ddos attacks in cloud computing model," *International Journal of Application or Innovation in Engineering and Management,* vol. 3, no. 3, 2013.
5. K. Lee, "Security threats in cloud computing environments," *International Journal of Security and Its Applications,* vol. 6, no. 4, pp. 25–32, 2012.
6. Ajey Singh, Dr. Maneesh Shrivastava. "Overview of Attacks on Cloud Computing." *International Journal of Engineering and Innovative Technology (IJEIT).* Volume 1, Issue 4, April 2012. pp.-321-323.
7. Standaert, F.-X. (2010). Introduction to Side-Channel Attacks. In I. M. R. Verbauwhede (Ed.), *Secure Integrated Circuits and Systems* (pp. 27–42). Springer US. Retrieved from http://link.springer.com/chapter/10.1007/978-0-387-71829-3_2
8. Data Security Issues in Cloud Computing," www.scipublish.com/journals/MCCC/papers/download/3302-207.pdf, [Online; Accessed: 26-March-2014].
9. B. Sevak, "Security against side channel attack in cloud comput-ing," *International Journal of Engineering and Advanced Technology (IJEAT),* ISSN: 2249 8958, vol. 2, no. 4, pp. 184–186, 2012.
10. Kocher, P., Jaffe, J., & Jun, B. (1999). Differential Power Analysis. In M. Wiener (Ed.), Advances in Cryptology — CRYPTO' 99 (pp. 388–397). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/3-540-48405-1_25
11. Ambrose, J. A., Parameswaran, S., & Ignjatovic, A. (2008). MUTE-AES: A Multiprocessor Architecture to Prevent Power Analysis Based Side Channel Attack of the AES Algorithm. In *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design* (pp. 678–684). Piscataway, NJ, USA: IEEE Press. Retrieved from http://dl.acm.org/citation.cfm?id=1509456.1509605
12. Zadeh, A. K., & Gebotys, C. (2009). Leakage Power and Side Channel Security of Nanoscale Cryptosystem-on-Chip (CoC). In *IEEE Computer Society Annual Symposium on VLSI, 2009. ISVLSI '09* (pp. 31–36). doi:10.1109/ISVLSI.2009.46
13. Ambrose, J. A., Ragel, R. G., & Parameswaran, S. (2007). A smart random code injection to mask power analysis based side channel attacks. In *2007 5th IEEE/ACM/IFIP International Conference on Hardware/Software Code sign and System Synthesis (CODES+ISSS)* (pp. 51–56).
14. "A Mechanism to Prevent Side Channel Attacks in Cloud Computing Environments," http://worldcomp-proceedings.com/proc/p2013/ICM4282.pdf, [Online; Accessed: 16-Jun-2014].

© 2014 Global Journals Inc. (US)

Global Journals Inc. (US) Guidelines Handbook 2014

www.GlobalJournals.org