DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.013 ***Int. J. Exp. Res. Rev.*, Special Vol. 31: 131-140 (2023)**

Original Article | *Peer Reviewed* | *Open Access*

International Journal of Experimental Research and Review (IJERR)

ISSN: 2455-4855 (Online)
www.iaph.in

ISSN 2455-4855

Prevention of VM Timing side-channel attack in a cloud environment using randomized timing approach in AES – 128

Animesh Kumar, Sandip Dutta and Prashant Pranav*

Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi, Jharkhand, India

E-mail/Orcid Id:

AK, nimeshkumarcse@gmail.com, https://orcid.org/0009-0007-3679-8025;
SD, sandipdutta@bitmesra.ac.in, https://orcid.org/0000-0002-3932-3048; *PP,* prashantpranav19@gmail.com, https://orcid.org/0000-0002-3932-3048

Article History:
Received: 22nd Mar., 2023
Accepted: 27th Jun., 2023
Published: 30thJul., 2023

Keywords:
Cloud computing, Security, Cryptography, VM side-channel attack, Side channel attack, Virtual Machine (VM)

Abstract: The term "cloud computing" refers to the delivery of various computer services to users via the Internet. These services include servers, storage, databases, networking, software, and analytics. The ability for businesses to swiftly and easily access computing resources as needed is one of the primary benefits of cloud computing, along with scalability, flexibility, and cost savings. To protect themselves from data breaches, distributed denial of service attacks, and insider threats, cloud providers and consumers alike need to deploy adequate security measures. Shared resources and timing inconsistencies within the hypervisor can make it possible for attackers to deduce sensitive information from other Virtual Machines (VMs). In this research, a software-based solution to the problem of VM timing side-channel assaults (SCAs) in CC (Cloud Computing) is proposed. Following an analysis of the process's empirical complexity, the solution uses a randomized timing method, which is compatible with all of the AES–128 sub-steps.

Introduction

Cloud computing has changed how organizations and individuals' access, store, and manage data and applications (Agapito and Cannataro, 2023). It entails the provision of computing resources, such as storage, processing power, and applications, via the Internet, as opposed to relying on local servers or personal devices. The most significant advantage is that it eliminates the need for large upfront investments in hardware, software, and IT infrastructure. Instead, users can access cloud-based services on a pay-per-use basis, which reduces costs and increases flexibility (Al-Jumaili et al., 2023). Additionally, users can scale their usage of cloud services up or down as their needs change, which makes it easier to respond to fluctuations in demand. It enables users to access their data and applications anywhere, anytime, and from any device (Jain and Rajak, 2023). It offers several benefits to organizations and individuals, including reduced costs, increased flexibility, and enhanced security (Rajak et al., 2023). Figure 1 shows the cloud network consisting of two different Local Area Networks (LANS), each connected to four sub-networks comprised of various networking devices like routers (Zou et al., 2023) and switches (Ueno et al., 2023).

Some of the Cloud Attacks are as follows

Denial-of-service (DoS) occurs when an attacker overloads a cloud service with requests, causing it to become unavailable to legitimate users (Tian and Nogales, 2023). To mitigate this risk, organizations should implement robust network security measures and have contingency plans to address DoS attacks. Insider threat occurs when an employee, contractor, or other insider with access to sensitive information in the cloud deliberately misuses that information (Asha et al., 2023). Organizations should implement strict policies and procedures for access to sensitive information to mitigate this risk. Account hijacking occurs when an unauthorized individual gains access to a user's cloud account by exploiting vulnerabilities in the authentication process or by successfully guessing their password (Devi et al., 2023).

To mitigate this risk, organizations should implement multi-factor authentication and encourage employees to

***Corresponding Author:** prashantpranav19@gmail.com

use strong passwords and update them regularly. Cloud misconfiguration attack occurs when organizations or individuals configure their cloud systems and data in an insecure manner, exposing them to potential attacks (Haimed et al., 2023). Side-channel attacks utilize information obtained from the system's behaviour, such as timing or resource usage, rather than directly targeting cryptographic algorithms or implementation flaws (Picek et al., 2023). Virtual machine side-channel attacks are a class of security vulnerabilities that exploit information leakage in virtualized environments (Dhinakar et al., 2023). These attacks take advantage of the shared hardware resources and the lack of complete isolation between virtual machines (Balai et al., 2023) running on the same physical host. To mitigate this risk, organizations should implement best practices for cloud security. Figure 2 below shows different types of CC attacks like VM SCAs, DDoS, Insecure API, and Insider Threats. VMSCAs are divided into Timing, Power Analysis, Electromagnetic, and Fault Analysis attacks.

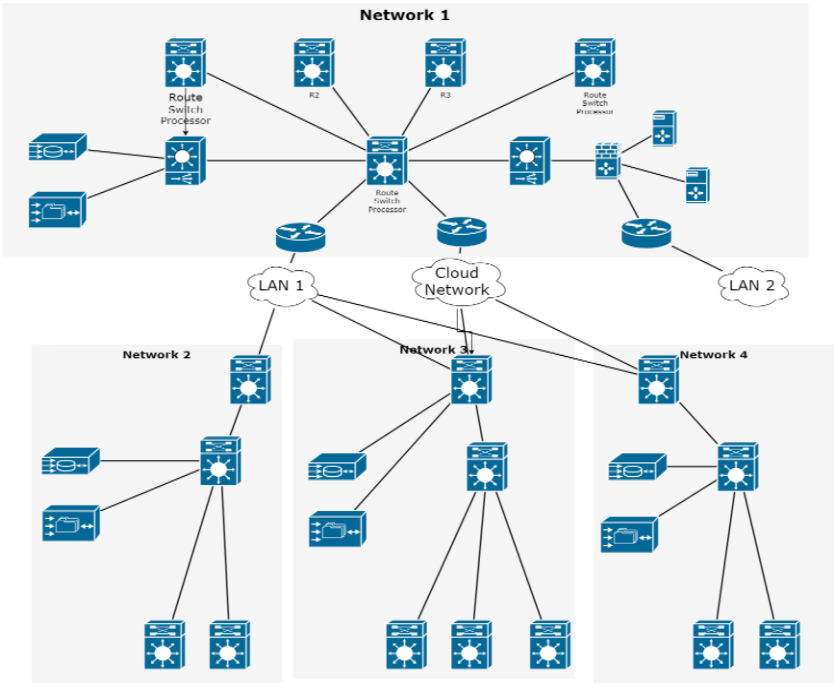

Figure 1. Cloud Network

Figure 3 Shows different types of VM SCAs consisting of Timing, cache-based, covert channel, and Page Table attacks. Cache-based VM SCAs attacks, where an attacker uses cache timing information to infer which memory locations have been accessed by a victim VM (Gonzalez et al., 2023). It is divided into Prime+Probe (Chakraborty et al., 2023) and Flush+Reload (Qie et al., 2023). In Prime+Probe attacks, the attacker primes the cache with their data and waits for the victim VM to access the exact memory location, causing a cache miss. The attacker then probes the cache to determine if the victim VM has accessed the memory location. In Flush+Reload attacks, the attacker flushes a memory location from the cache, waits for the victim VM to access the exact location, causing a cache miss, and reloads the data from memory. Memory-based VM SCAs attack, where an attacker uses memory access patterns to infer sensitive information. It is further divided into Row hammer (Mutlu et al., 2023) and Page Fault Attacks (Qin et al., 2023). In Row hammer attacks, the attacker repeatedly accesses adjacent memory rows to cause bit flips in neighboring rows. By observing the timing of page faults, the attacker can determine which rows have been flipped and infer sensitive information. In Page Fault Attacks, the attacker triggers page faults by accessing memory pages not currently used by the victim VM. By observing the timing of page faults, the attacker can infer which pages have been accessed by the victim VM.

Protecting VM SCAs is challenging due to the shared nature of resources in the cloud. However, several mitigation techniques can be employed. Continuously monitor and analyze the behavior of VMs for potential side-channel attacks. Employ countermeasures such as noise injection, access pattern randomization, or resource scheduling techniques to mitigate the impact of side-channel vulnerabilities. One approach is to use hardware-based isolation mechanisms, such as Intel SGX or AMD SEV, to protect sensitive data from accessing other VMs on the same physical host.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.013

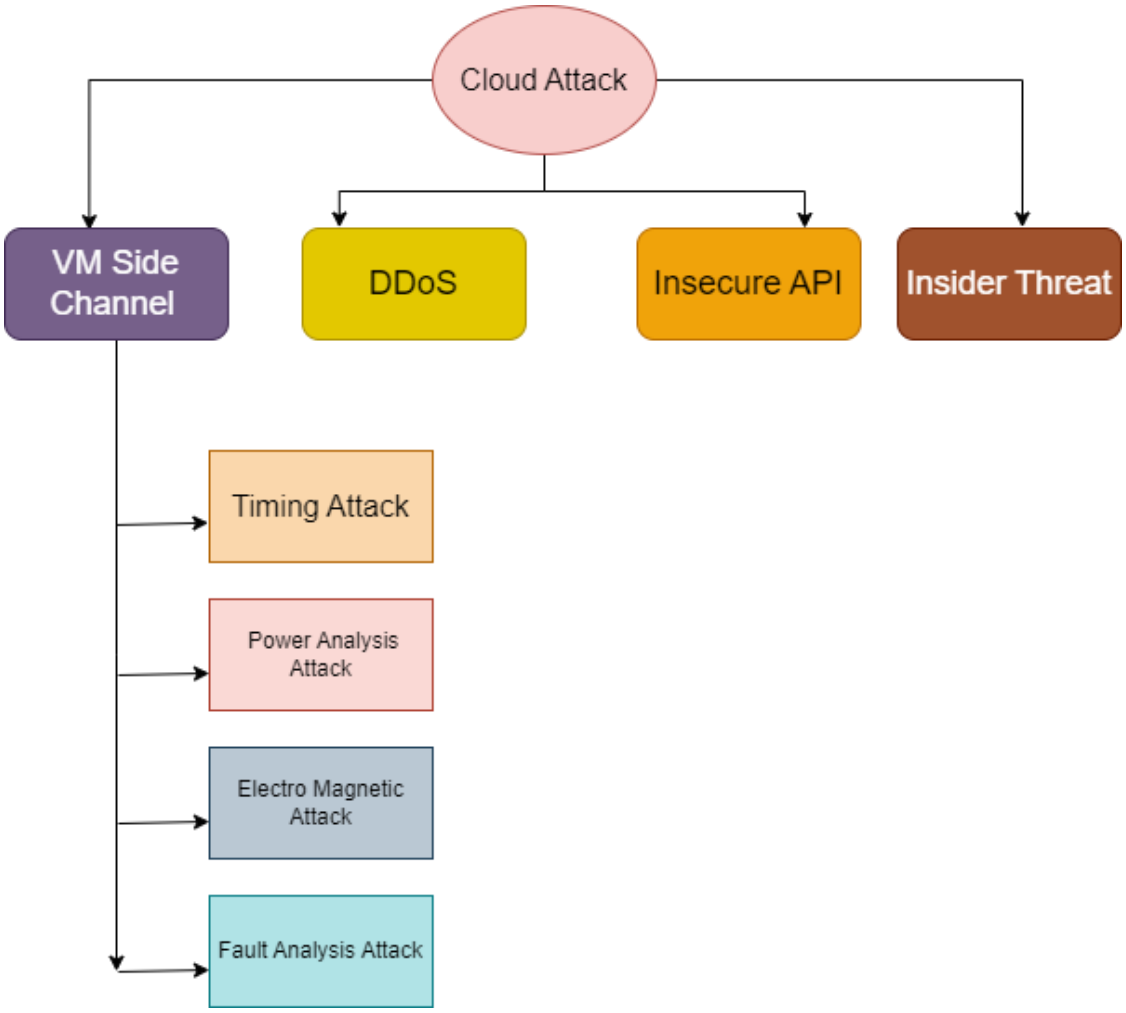

Figure 2. Different types of Cloud Attacks

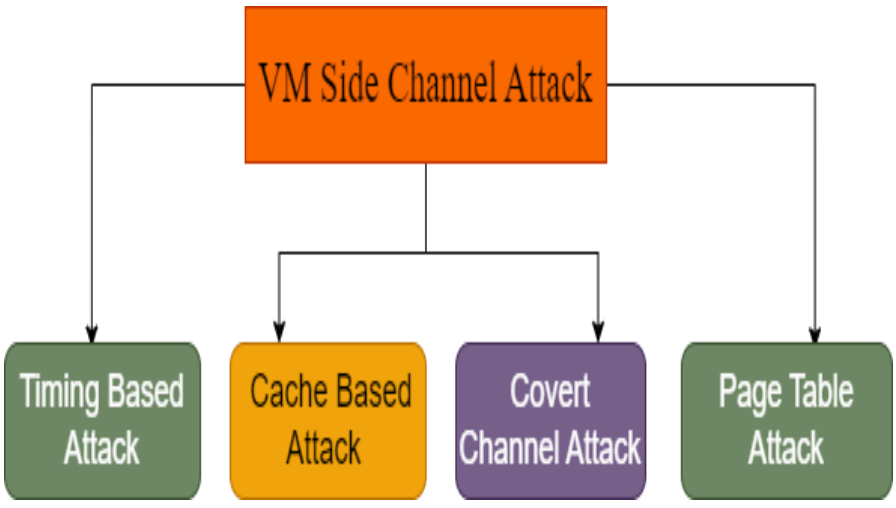

Figure 3. Different Types of Virtual Machine Side Channel Attacks (VM SCAs)

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.013

It is essential for cloud providers and users to be aware of these risks and to implement appropriate mitigation techniques to protect against them. This includes hardware-based isolation mechanisms and regular vulnerability assessments to identify and address potential security threats. In this paper, we approach AES Encryption Technique to counter VM SCAs attacks. Advanced Encryption Standard (AES) (Hasija et al., 2023) is a widely used symmetric encryption algorithm that provides high security for protecting sensitive data. The algorithm uses a fixed block size of 128 bits and a variable key size of 128, 192, or 256 bits. The key size determines the level of security the algorithm provides, with 256-bit keys offering the highest level of protection. AES works by breaking the input data into blocks of 128 bits and then applying a series of mathematical operations to each block. The algorithm uses a round-based approach, each consisting of four primary operations: Sub Bytes, Shift Rows, Mix Columns, and Add Round Key (Mohanmmad et al., 2023). Anwar et al. (2017) discussed all the hardware and software-based techniques to counter VM SCAs. Hypervisor-based solutions can be implemented in the future. Using RSA Technique, Dhinakar et al. (2023) defended the cache-based SCAs in CC. Gonzalez et al. (2023) proposed a task migration method to mitigate cache-based SCAs. Rout et al. (2022) proposed VM allocation policy based on PSSF with improved security and low energy consumption. Xu et al. (2020) focused on the performance of the different CC environments. It provides significant performance benefits, including increased scalability and improved resource utilization. However, they also found that cloud environments can be susceptible to performance degradation due to network congestion and resource contention. Liu et al. (2020) investigated the cost of CC and the impact of different deployment models on cost. The cost of CC varies greatly depending on the deployment model, with public clouds typically being the most cost-effective, followed by hybrid clouds, and then private clouds. They also found that organizations can reduce the cost of the cloud by optimizing resource utilization and choosing cost-effective deployment models. Kim et al. (2021) examined the security of CC environments. They proposed a framework for enhancing cloud security, including encryption, multi-factor authentication, and access control. Machine learning (ML) algorithms can be used to dynamically allocate resources in the cloud, improving performance and reducing the risk of resource contention. ML algorithms can be used to optimize resource utilization and reduce costs.CC also presents various challenges, including security risks, performance degradation, and cost optimization. To address these challenges, organizations must carefully consider their deployment models, implement adequate security measures, and explore new technologies such as machine learning to improve performance and cost optimization. Liu et al. (2018) explored the utilization of encryption to safeguard data within the cloud. They determined that encryption is an effective measure to protect data in the cloud; however, they also highlighted the inherent challenges associated with its implementation. They proposed a framework for encryption in the cloud that includes key management, data partitioning, and data access control. Xu et al. (2019) focused on the security risks associated with cloud computing and proposed a risk assessment framework to help organizations mitigate those risks. The proposed framework includes risk assessment, security controls, monitoring, and evaluation. Wang et al. (2020) examined the role of cloud service providers (CSPs) in securing the cloud. CSPs play a critical role in securing cloud environments, but organizations must also take responsibility for securing their systems and data. They proposed a framework for cloud security that includes security policies, architecture, and monitoring and evaluation. Kim et al. (2021) investigated the use of multi-factor authentication (MFA) to enhance security in the cloud. MFA can effectively reduce the risk of unauthorized access. They proposed a framework for MFA that includes user, device, and network authentication. Cloud storage services are vulnerable to various security risks, including data breaches and unauthorized access. They proposed a framework for securing cloud storage services, including data encryption, access control, and security monitoring and evaluation. Some of the other relevant papers are (Sarkar et al., 2019; Paramanik et al., 2022; Sarkar et al., 2020; Pramanik et al., 2021; Sarkar et al., 2021; Dey et al., 2023; Das and Sarkar, 2022).

VM SCAs Timing attack is one of the most hidden attacks in the CC Domain. Most mitigation techniques are hardware-based approaches that increase the cost and overhead expenses. This paper uses software-based mechanisms to counter VM SCAs with the AES-128 Technique.

Materials and Methods

Table 1 explains all the working sub-steps of AES-128. This work involves five steps: Step 1, Calculation of Execution time. Step 2 consists of determining the execution time of sub-steps of AES. Step 3 consists of statistical modelling. Step 4 is about estimating empirical

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.013

Table 1. Proposed Methodology

Input: Plain text messages in bits or bytes can be encrypted using the Advanced Encryption Standard (AES) with a 128-bit key.
Output: Cipher Text
Step 1: Calculate the execution time for three separate trials of Plain Text with changing and increasing sizes for the following sub-steps:
Step 1.1: Shift Row
Step 1.2: Substitute Bytes
Step 1.3: Mix Column
Step 1.4: Add Round Key
Step 2: To determine the total execution time for the sub-steps above for various inputs, take the mean of the three attempts.
Step 3: Fit a statistical model considering input size and mean execution time.
Step 4: Estimate the empirical complexity of the following sub–steps.
Step 4.1: Shift Row
Step 4.2: Substitute Bytes
Step 4.3: Mix Column
Step 4.4: Add Round Key
Step 5: Randomly choose any of the below sub-step by selecting a number at random between [1 to 3]
Step 5.1: Shift Row
Step 5.2: Substitute Bytes
Step 5.3: Add Round Key
Step 6: "By creating a random variable between the "least execution time" and "mean execution time" for the above sub-steps in Step 5, add a random amount of time for a certain input size from Step 2 in any of the above three sub-steps".

complexity, and step 5 is the random timing approach in sub-steps of AES. In this paper, we derive the theoretical and Empirical Complexity of AES-128 bit. The theoretical complexity of AES-128 means that it would take an attacker 2^128 operations to crack the encryption, which is considered to be computationally infeasible. The most time-consuming part of the AES-128 algorithm is the encryption or decryption process, which involves a series of mathematical operations, including substitution,

permutation, and matrix multiplication. These operations are performed on blocks of data, typically 128 bits in length, which means that the computational complexity of AES-128 is proportional to the size of the data being encrypted or decrypted. Empirical Complexity of AES-128 measuring the actual time and resources required to execute the algorithm on a particular set of inputs, we can obtain a practical measure of the algorithm's complexity that may differ from its theoretical complexity. We empirically determined the complexity of each sub-step by conducting three distinct trials with different input sizes. We have developed the following algorithm to make it impossible for outsiders to guess how long the AES-128 encryption and decryption operations take.

Figure 4 explains that the AES consists of four parts. Sub Byte, Shift Rows, Mix Column, and Add Round Key are sub-parts. In this paper, we add a random timing approach in the Mix column step to get the modified timing in AES. This addition of timing in the Mix column distracts the attacker so they cannot guess the original timing from the network traffic from the cloud server end. Our proposed model is deployed on the cloud server end for better results.

Result and Discussion

The execution times for the three trials for different input sizes with the replacement of the mix-column sub–step of AES–128 are shown in Table 2. For the execution time for other sub-steps, interested readers are advised to see (Pranav et al., 2021). We plotted the fitted line plot for the mix column sub-step, as shown in Figure 5 below. The mix column sub-step holds significant importance within AES-128, as depicted in Figure 2, making it the most prevalent sub-step. Consequently, its influence on the overall time complexity of AES-128 cannot be overlooked. A fitted line plot analysis shows that the mix column sub-step exhibits an empirical complexity of O(n), aligning with the theoretical time complexity of AES-128, which is also O(n), where n represents the number of inputs.

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.013

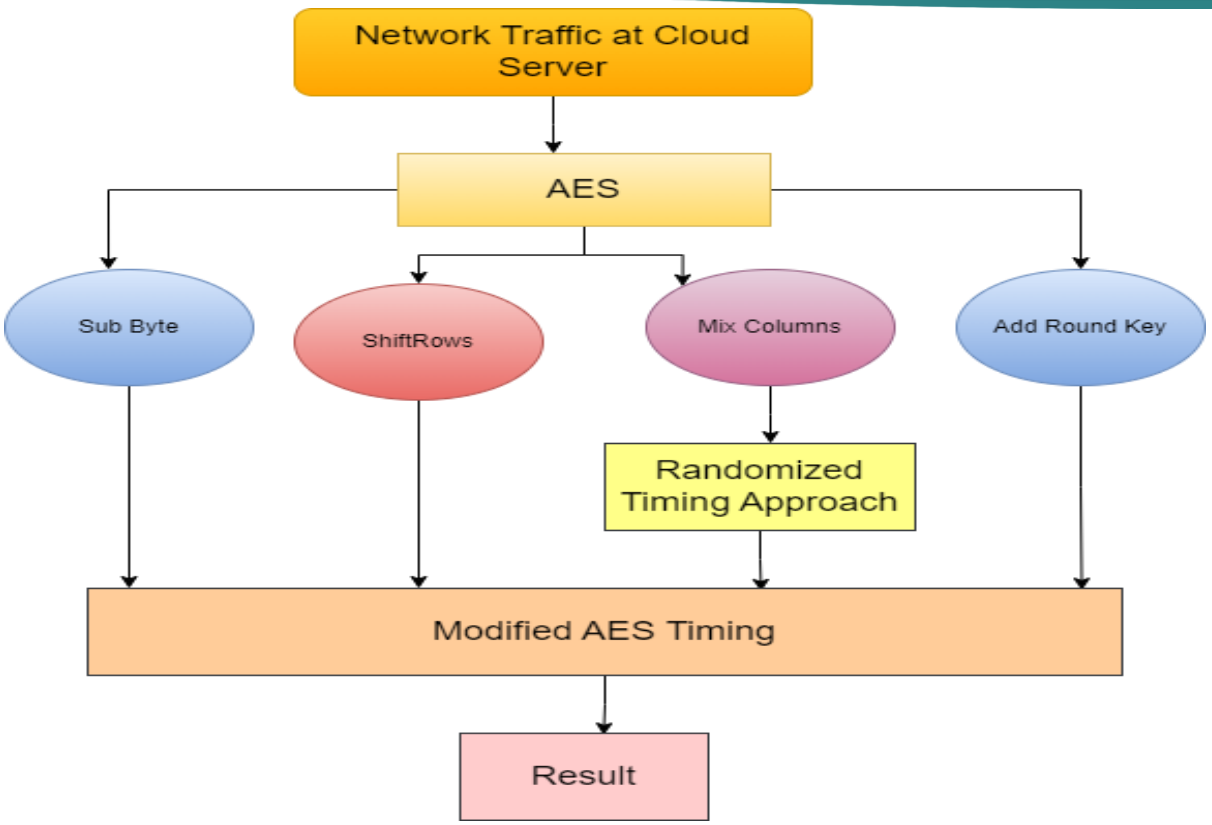

Figure 5. Flow Diagram

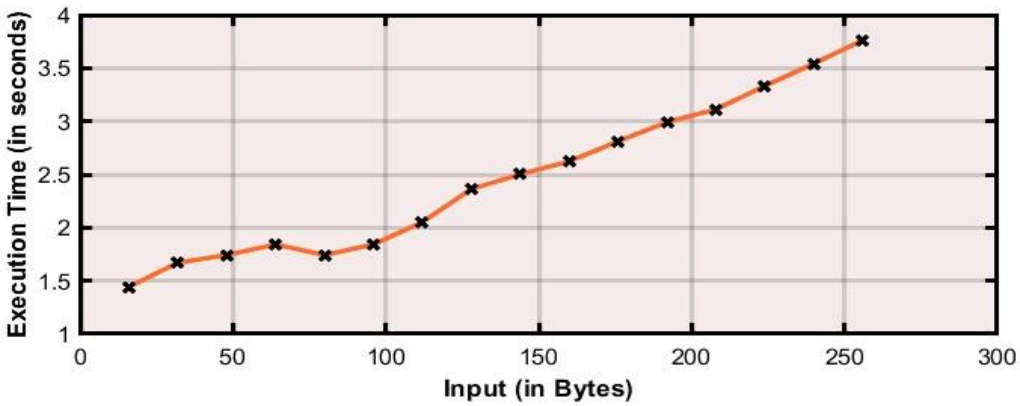

Figure 4. Fitted Line Plot of Mix Column Sub – Step

Hence, we can assert that the empirical complexity of the process primarily relies on the mix column sub-step. In contrast, the remaining three sub-steps are executed expeditiously. The time complexity of AES-128 can be described by the notation O(n), where 'n' denotes the number of inputs. Therefore, the process's empirical complexity solely depends on the mix column sub-step. The other three sub-steps are executed swiftly, leading us to suggest the introduction of a random time increment to one of them in our study. By incorporating various and progressively larger input sizes, the execution times of these sub-steps will correspond to the randomly assigned time added to either the shift-row, sub-byte, or add-round vital steps.

Figure 5 depicts the fitted line plot for the mix column sub-step. The fitted line plot shows that the time complexity of the mix column sub–step of AES – 128 is O (n), as the line is almost linear.

Comparison

The method we proposed in this paper is a software-based approach to defy VM timing side-channel attacks in CC. Most prevailing solutions to counter the attack (Liu et al., 2016; Younis et al., 2015) rely on modification in the underlying hardware implementation of AES -128. Although these approaches provide an acceptable degree of security, they suffer from the following flaws: The specific hardware implementation of AES–128 in a cloud environment requires a trained professional, whose number is minimal. The cost incurred in changing the overall hardware implementation of AES–128 increases significantly. Our solution, a

DOI: https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.013

randomized timing approach, requires inserting a random amount of time into any of the three discussed sub-steps of AES-128. The cost incurred is significantly less and, to be precise has no change in the overall cost. Further, changing the underlying hardware implementation of the whole CC environment is not required. Table 3 shows the comparative analysis of our work with other existing methods (Rout et al., 2022; Gomez et al., 2023; Dhinakar et al., 2023).

Table 2. Mean Execution Time for Mix Column

Input (In Bytes)	Test 1	Test 2	Test 3	Mean Execution Time (In Sec)
16	0.688680743	0.578348831	0.176224641	1.443254215
32	0.589542473	0.886876387	0.193393725	1.669812585
48	0.723980043	0.020057249	0.998181643	1.742218935
64	0.254100177	0.768838386	0.248942889	1.271881452
80	0.271963131	0.066367488	0.783238912	1.12156953
96	0.061218353	0.443645498	0.493465374	0.998329225
112	0.475011146	0.384272758	0.563830342	1.423114247
128	0.880798247	0.205194246	0.993010614	2.079003108
144	0.21142611	0.841146755	0.108745962	1.161318826
160	0.927462842	0.550249233	0.299240763	1.776952837
176	0.072170256	0.954781244	0.877552339	1.904503839
192	0.373167798	0.176454407	0.795209633	1.344831838
208	0.198414263	0.230365267	0.128994506	0.557774036
224	0.173548679	0.491291424	0.423123318	1.087963420
240	0.332677927	0.655218163	0.307606652	1.295502742
256	0.669659282	0.80518191	0.84689625	2.321737441

Conclusion

This paper presented a novel AES-based approach to guard against VM side-channel attacks. The results are encouraging and can be taught to be a potential solution to VM SCAs. We have illustrated a VM side-channel timing attack prevention by adding random timing to the already-existing AES 128 sub-steps. This provides a simple yet powerful solution to prevent the cloud infrastructure from the VM timing SCAs. Although secure, this work can have these potential limitations, which can be considered in the future. The algorithm may repeatedly choose the same step to insert the randomized timing, which may again reflect the intruder about the underlying implementation procedure. In the future, the algorithm can be tested using different cloud datasets, and such deployment can be done for other encryption mechanisms such as RSA and Blowfish.

Acknowledgment

The laboratory facilities and support for this study were provided by the Birla Institute of Technology, Mesra, Jharkhand, India, which the authors gratefully acknowledge.

Conflict of Interest

The authors declare no conflict of interest.

Table 3. Comparison Table

Methods	Implementation	Cost	Overhead
Proposed Method	Software Based	No effect on the overall cost	No extra overhead as the method does not require skilled human resources for the installation or migration of VMs.
Rout et al., 2022	Hardware Based	Overall cost increases because of VM mitigation	Extra overhead is incurred as the method requires a skilled workforce for VM mitigation.
Gomez et al., 2023	Hardware Based	Overall cost increases because of VM migration	Extra overhead is incurred as the method requires a skilled workforce for the VM migration.
Dhinakar et al., 2023	Hardware Based	Overall cost increases because of VM migration	Extra overhead is incurred as the method requires skilled human resources for the VM migration.

References

Agapito, G., & Cannataro, M. (2023). An Overview of the Challenges and Limitations Using Cloud Computing in Healthcare Corporations. *Big Data and Cognitive Computing*, *7*(2), 68. https://doi.org/10.3390/bdcc7020068

Al-Jumaili, A. H. A., Muniyandi, R. C., Hasan, M. K., Paw, J. K. S., & Singh, M. J. (2023). Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems: Status, Constraints, and Future Recommendations. *Sensors*, *23*(6), 2952. https://doi.org/10.3390/s23062952

Anwar, S., Inayat, Z., Zolkipli, M. F., Zain, J. M., Gani, A., Anuar, N. B., Khan, M.K., & Chang, V. (2017). Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey. *Journal of Network and Computer Applications*, *93*, 259-279. https://doi.org/10.1016/j.jnca.2017.06.001

Asha, S., Shanmugapriya, D., & Padmavathi, G. (2023). Malicious insider threat detection using a variation of sampling methods for anomaly detection in cloud environment. *Computers and Electrical Engineering*, *105*, 108519. https://doi.org/10.1016/j.compeleceng.2022.108519

Balaji, K., Sai Kiran, P., & Sunil Kumar, M. (2023). Power aware virtual machine placement in IaaS cloud using discrete firefly algorithm. *Applied Nanoscience*, *13*(3), 2003-2011. https://doi.org/10.1007/s13204-021-02337-x

Chakraborty, A., Bhattacharya, S., Saha, S., & Mukhopadhyay, D. (2023). Are Randomized Caches Truly Random? Formal Analysis of Randomized-Partitioned Caches. In *2023 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*. pp. 233-246. https://doi.org/10.1109/HPCA56546.2023.10071041.

Das, S., & Sarkar, S. (2022). News media mining to explore speed-crash-traffic association during COVID-19. *Transportation Research Record*, 03611981221121261. https://doi.org/10.1177/03611981221121261

Devi, R., Gill, S., & Narwal, E. (2023). Securing Account Hijacking Security Threats in Cloud Environment Using Artificial Neural Networks. Singapore: Springer Nature Singapore. In *International Conference On Emerging Trends In Expert Applications & Security*, pp. 119-127.

Dey, P. K., Chowdhury, S., Abadie, A., Vann Yaroson, E., & Sarkar, S. (2023). Artificial intelligence-driven supply chain resilience in Vietnamese manufacturing small-and medium-sized enterprises. *International Journal of Production Research*, 1-40. https://doi.org/10.1080/00207543.2023.2179859

Dhinakar, N.M., Rao, K.K., Jayanath, N., Prasad, R.D.V., Jadala, V.C., & Chintala, R.R. (2023). Defending

against Cache-based Side-Channel Attack using Virtual Machine Migration in Cloud. In *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, pp. 239-242. https://doi.org/10.1109/ICSCDS56580.2023.10104625.

Gonzalez-Gomez, J., Bauer, L., & Henkel, J. (2023). Cache-based Side-Channel Attack Mitigation for Many-core Distributed Systems via Dynamic Task Migration. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/TIFS.2023.3266630.

Haimed, I.B., Albahar, M., & Alzubaidi, A. (2023). Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks. *Future Internet*, *15*(7), 226. https://doi.org/10.3390/fi15070226

Hasija, T., Kaur, A., Ramkumar, K. R., Sharma, S., Mittal, S., & Singh, B. (2023). A Survey on Performance Analysis of Different Architectures of AES Algorithm on FPGA. *Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021*, pp. 39-54. https://doi.org/10.1007/978-981-19-6383-4_4

Jain, A., & Rajak, R. (2023). A systematic review of workflow scheduling techniques in a fog environment. *International Journal of Experimental Research and Review*, *30*, 100-108. https://doi.org/10.52756/ijerr.2023.v30.011

Jain, R., Jain, A., & Singh, R. (2019). Deployment models of cloud computing: A review. *Journal of Cloud Computing*, *8*(1), 10. https://doi.org/10.1186/s13677-018-0104-x

Kim, J., Lee, J., & Kim, D. (2021). Multi-factor authentication for cloud computing security. *Journal of Computer Science*, *17*(1), 1-8. https://doi.org/10.11648/j.cs.20210101.11

Liu, Q., Li, Q., & Li, J. (2018). Secure data storage in cloud computing: A framework based on encryption. *Journal of Cloud Computing*, *7*(1), 8. https://doi.org/10.1186/s13677-017-0067-x

Liu, F., Ge, Q., Yarom, Y., Mckeen, F., Rozas, C., Heiser, G., Lee, R.B. (2016). CATalyst: Defeating last-level cache side channel attacks in cloud computing. *IEEE International Symposium on High Performance Computer Architecture* (HPCA), pp. 406-416. https://doi.org/10.1109/HPCA.2016.7446082

Liu, Q., Li, Q., & Li, J. (2020). The cost of cloud computing: A review. *International Journal of Information Management*, *47*, 102-112.

Mohammed, N.Q., Amir, A., Ahmad, B., Salih, M.H., Arrfou, H., Thalji, N., Matem, R., Abbas, J.K.K., Hussien, Q.M., & Abdulhassan, M. M. (2023, April). A Review on Implementation of AES Algorithm Using Parallelized Architecture on FPGA Platform. In *2023 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET)*, pp. 1-6. https://doi.org/10.1109/IC_ASET58101.2023.10150938.

Mutlu, O., Olgun, A., & Yağlıkcı, A.G. (2023, January). Fundamentally understanding and solving rowhammer. In *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, pp. 461-468. https://doi.org/10.1145/3566097.3568350

Paramanik, A. R., Sarkar, S., & Sarkar, B. (2022). OSWMI: An objective-subjective weighted method for minimizing inconsistency in multi-criteria decision making. *Computers & Industrial Engineering*, *169*, 108138. https://doi.org/10.1016/j.cie.2022.108138

Picek, S., Perin, G., Mariot, L., Wu, L., & Batina, L. (2023). Sok: Deep learning-based physical side-channel analysis. *ACM Computing Surveys*, *55*(11), 1-35. https://doi.org/10.1145/3569577

Pramanik, A., Sarkar, S., & Maiti, J. (2021). A real-time video surveillance system for traffic pre-events detection. *Accident Analysis & Prevention*, *154*, 106019. https://doi.org/10.1016/j.aap.2021.106019

Pranav, P., Dutta, S. & Chakraborty, S. (2021). Empirical and statistical comparison of intermediate steps of AES-128 and RSA in terms of time consumption. *Soft Comput*., *25*, 13127–13145. https://doi.org/10.1007/s00500-021-06085-6

Qin, H., Song, Z., Zhang, W., Huang, S., Yao, W., Liu, G., Jia, X., & Du, H. (2023, April). Protecting Encrypted Virtual Machines from Nested Page Fault Controlled Channel. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, pp. 165-175. https://doi.org/10.1145/3577923.3583659

Qiu, P., Gao, Q., Wang, D., Lyu, Y., Wang, C., Liu, C., Sun, L.R., & Qu, G. (2023). PMU-Leaker: Performance Monitor Unit-based Realization of Cache Side-Channel Attacks. In *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, pp. 664-669 https://doi.org/10.1145/3566097.3567917

Rajak, R., Choudhary, A., & Sajid, M. (2023). Load balancing techniques in cloud platform: A systematic study. *International Journal of*

Experimental Research and Review, *30*, 15-24. https://doi.org/10.52756/ijerr.2023.v30.002

Rout, C., Sethi, S., Badajena, J. C., & Sahoo, R. K. (2022). Secure virtual machine allocation for prevention of side channel attacks in cloud computing. In *2022 International Conference on Intelligent Controller and Computing for Smart Power (ICICCSP)*, pp. 1-6. https://doi.org/10.1109/ICICCSP53532.2022.9862404.

Sarkar, S., Pramanik, A., Maiti, J., & Reniers, G. (2020). Predicting and analyzing injury severity: A machine learning-based approach using class-imbalanced proactive and reactive data. *Safety Science*, *125*, 104616. https://doi.org/10.1016/j.ssci.2020.104616

Sarkar, S., Vinay, S., Djeddi, C., & Maiti, J. (2021). Text mining-based association rule mining for incident analysis: a case study of a steel plant in India. Springer International Publishing. In *Pattern Recognition and Artificial Intelligence: 4th Mediterranean Conference, MedPRAI 2020, Hammamet, Tunisia, December 20–22, 2020, Proceedings 4*, pp. 257-273. https://doi.org/10.1007/978-3-030-71804-6_19

Sarkar, S., Vinay, S., Raj, R., Maiti, J., & Mitra, P. (2019). Application of optimized machine learning techniques for prediction of occupational accidents. *Computers & Operations Research*, *106*, 210-224. https://doi.org/10.1016/j.cor.2018.02.021

Tian, Y., & Nogales, A. F. R. (2023). A Survey on Data Integrity Attacks and DDoS Attacks in Cloud Computing. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0788-0794.

Ueno, Y., Tsukahara, A., & Miyaho, N. (2023, June). Next Generation Connectionless IP router architecture with Switching Delay for URLLC Services. In *2023 IEEE 24th International Conference on High-Performance Switching and Routing (HPSR)*, pp. 1-6. https://doi.org/10.1109/HPSR57248.2023.10147935

Wang, Y., Ma, Y., & Li, Y. (2020). The role of cloud service providers in securing cloud computing environments. *Journal of Network and Computer Applications*, *142*, 13-22. https://doi.org/10.1016/j.jnca.2019.10.005

Xu, X., Hu, J., & Zhang, Y. (2019). A risk assessment framework for cloud computing security. International Journal of Information.

Younis, Y. A., Kifayat, K., Shi, Q., & Askwith, B. (2015). A new prime and probe cache side-channel attack for cloud computing. *In 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 1718-1724. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.259.

Zou, X., Gong, G., Lin, Y., Fu, B., Wang, S., Zhu, S., & Wang, Z. (2023). Metasurface-based polarization color routers. *Optics and Lasers in Engineering*, *163*, 107472. https://doi.org/10.1016/j.optlaseng.2022.107472

How to cite this Article:

Animesh Kumar, Sandip Dutta and Prashant Pranav (2023). Prevention of VM Timing side-channel attack in a cloud environment using randomized timing approach in AES – 128. *International Journal of Experimental Research and Review*, *31*, 131-140.

DOI : https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.013