ISSN 2347 - 3983

Volume 8. No. 4, April 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter11842020.pdf

https://doi.org/10.30534/ijeter/2020/11842020

Survey on Cache-Based Side-Channel Attacks in Cloud Computing

Hesham Abusaimeh[1], Halah Atta[2], Hadeel Shihadeh[3]

[1] Associate Professor in Computer Science, Middle East University Amman, Jordan. habusaimeh@meu.edu.jo
[2] IT Developer, Ministry of Local Administration, Amman, Jordan. halah.fares@yahoo.com
[3] Instructor Alqadeseh college, Amman, Jordan. Hadool_ce_89@yahoo.com

ABSTRACT

Cache based side-channel attacks are powerful, agile and more suitable to be executed in a cloud environment rather than in traditional networks because of cloud computing architecture. The Cache based side-channel attacks in cloud computing happened when a single physical host in a cloud computing data center run programs of two different corporations each program runs in its Virtual Machine thru a hypervisor the logical separation between different VMs occur ensuring that a VM cannot access the allocated space of the main memory to a different VM. However, it is difficult to implement such separation in the cache memory. since the Last Level Cache (LLC) in the cache memory is shared amongst them all cores. The SCA attacks are five types the Timing attacks, Cache attacks, Power-monitoring, and Electromagnetic attacks. All types of side-channel attacks occurred when they take advantage of the changing in the processing performance through algorithm implementation. In cache based attack the VMs attacker is attentive to the method that the target uses cache memory when executed.

In this survey paper, we are employing the related work to analyze and determine the method to prohibit the Cache based side-channel attacks we present the finding of their work and possible countermeasures that can be implemented to reduce the Cache based side-channel attacks.

Key words :side channel attack ,cloud computing ,cache based side channel.

1. INTRODUCTION

The challenge coming from the rapid growth of linked devices made it very hard for most corporations to protect their devices and data from attacks. A although using cloud computing is useful and cost-effective still has to address some challenge [1].

On-demand access to a shared pool of computing, storage, and networking resources, are qualify of Cloud computing, yet virtualization is the key for sharing resources of a host amongst VMs through a hypervisor layer, virtualization enables software isolation between virtual machines by partitioning physical resources. However, resource sharing among different users is challenging [2].

Sharing resource among numerous entities has a huge influence on isolation in a cloud computing environment. Host in a cloud data center runs each program in its VMs and there is a hypervisor who is in charge to logically separated between different VMs but there is difficulty to apply separation in cache memory [3].

Side-Channel Attacks (SCA) a known threat to data security in a cloud computing environment that targeting greatly sensitive data and computations, Side-Channel Attacks use a concealed channel that leaks data so an process like AES encryption usually performance time or access to cache patterns. To launching an SCA an attacker could place a malicious virtual machine near to a target cloud server [4].

According to the users of the channel, there are five types of the side-channel attack which they are the Timing attacks, Cache attacks, Power-monitoring, and Electromagnetic attacks. All types of SCA occurred when they take advantage of the changing in the processing performance through algorithm implementation. The highest software attacks that arise in cloud computing are timing attacks and Cache-based [4].

The side-channel attack is an procedure that aims to extract data from the system's input and output. And from specifics of its execution. Therefore, in Cache attacks, the attacker is attentive in the method that the target uses cache memory [5].

All recent cloud providers use multi-core chip architectures that have two or three levels of cache. while the Last Level Cache (LLC) is shared among all cores the other Cache memory on all the levels is attached to a single core. With that the attacker can take advantage of the shared LLC then obtain some of the target’s most sensitive and secret data if the attacker's VM is co-located with a target VM [5].

2. METHODOLOGY

1- In this paper we identify those research question

A. Why the Cache based side-channel attacks happened in cloud computing

B. Is there possible countermeasures that can be implemented to reduce the Cache based side-channel attacks

2-We did this research to answer those question by employing the related work to analyze and determine the method to prevent the Cache based side-channel attacks

3- After gathering all information about the Cache based side-channel attacks, we present the finding of their work and methods

3. RELATED WORK

side-channel attacks are well-known attacks yet there is a shortage of countermeasures that we could use in cloud computing to prevent from occurring. while in cloud computing Multi-tenancy and co-residency gained the researcher's attention to study the impact and scale of damage can the SCA do in cloud computing still we are lacking[4].

So here will be focusing on some of the proposed approaches to address cache SCA in cloud computing

A software approach thru Zhou, Ziqiao 2016 [5] present to lessen access driven SCA which effect last-level caches shared among cores, called "CacheBar " and applied as a memory management subsystem in Linux kernel so it could affect on side channels across container limits, for implementing resident isolation in clouds they use the containers as a method, it just for defense against LLC-based SCA and they built it based on two principles.

The step to beating Flush- Reload attacks, they propose a copy on access technique which used to handle physical pages which are shared through reciprocally mistrusting security territories with outcomes that the page that been copied so that each territory has its copy, so like that the victim access to its copy will be unseen to an attacker Reload in a Flush Reload attack. And to overcome Prime Probe attacks they design a technics to handle the cache ability of memory pages so that to decrease the amount of lines each cache set which the assailant could Probe, after evaluation the result shows that Cache Bar accomplishes strong security with trivial overheads performance for Platform as a Service workloads

M Godfrey & M Zulkernine 2013 [6] they goal to deliver a protection against cache-based SCA without meddling with the Cloud model their approach to prevent the probing instance from sighted a manner in the cache hit data by control the PTP technique and use the "Prime" and "Trigger" steps to flushing the cache between them .They attempt to lessen the data loss due to repeated cache flushing , when the CPU switches domains then only flushing the cache, when suitable isolation in VMs is performed.

the only data that can stay useful after a context switch away from a territory it is the data that is untouched by the time the territory recover the use of the CPU, their solution prevents the PTP method, thereby forbidding the probing instance from sight a manner in the cache hit data, all that can be achieved without alterations client-side or their hardware, the result shows that the side channel could not effectively occur with their countermeasures, their hypervisors secure method can successfully stop cache-based SCA and their overhead less than 15%

Intelligent Detection algorithm proposed via R. Vanathi, SP. Chokkalingam 2018 [7] the Intelligent Detection algorithm used to detect the attack against the encryption algorithm and that happened by calculating the mean value of the Cache Miss Sequence of the various VM before the target could lose its data to the spy procedure, it could detect the attack by including the logic of signature-based detection to measure the cache miss time the timer is used, based on the two parameters, sampling and instrumentation the profiler is select, the sampling profiler would ask the JVM in each certain point of time about the present execution point of all active threads.

They use several parameters to find out the attack happened by the Flush+Reload attack, the profiler and timer is used to measure the CMT and the CMT are gathered together to form the CMS and the highest level cache (L3) is used as a medium by the spy process to detect whether the target access is done or not also the mean value is calculated for the CMS to find out the range at which the attack is supposed to happen and if they found that if the CMT value is nearing 340 then there is more chance of attack to happened, Therefore by using the concept of signature-based algorithm along with Intelligent Detection algorithm the attack against the cache can be found based on the data stored in the SB database and the attacker can be banned by stealing the data from the cache.

Liu, Fangfei, et al 2016 [8] also work on LLC side-channel attacks and they want to show that attacks like LLC SCA can be overcome using a performance optimization merit which is newly presented in ware processors. they used the Intel Cache Allocation Technology (CAT) to deliver a protection technics system-level to secure from SCA on the shared LLC, CATalyst which is a pseudo locking mechanism using the CAT Technology to split the LLC into a hardware-software hybrid -managed cache and by using Xen and Linux which running on a server with Intel processors they could apply a proof of concept system, they display the defeat LLC SCA.Also, the small CATalyst overhead performance used for security has trivial impact on applications legacy, CATalyst use secure pages which is cache pinned page frames, by utilizing the CAT on Intel processors they could defend the sensitive data against LLC based SCA.

So the CATalyst could be used for the cloud providers as well as the customers, this system offers the isolation of secure and insecure cache partitions, the result shows that CATalyst lessens the LLC based SCA with very small performance regression.

Si Yu, Xiaolin Gui 2013 [9] they deliver CSDA system which is two-stage detection method it contains guest detection and host detection they differentiate the attack VMs from the genuine VMs by using pattern recognition techniques, they use two testes the regularity shape tests and shape tests they use it to extract features of the attack from the sampled measurements, which they are the memory utilization and CPU utilization gathered from the guest and the cache miss times gathered from host, to define the detection result they use k Means clustering.

they used mean test to catch the suspicious attack sequence according to the cache miss in host detection, and to define the attack features of memory utilization and CPU utilization in the suspicious attack window in guest detection by using URI, and after they do a sequence of tests to validate their system so the result shows that their technique is efficient in detecting the cache-based SCA. In Godfrey, Zulkernine 2014 [10] they proposed a technique to respect the association between the Cloud provider with the user and stop cache-based SCA, it is defense of two server-side on a hypervisor of a Cloud system one is concentrate on parallel side channels and the other on sequential side channels.

By employed a cache coloring technique to avert their incidence and to improve cache effectiveness in specific situations, and that happened in the parallel side channels and on sequential side channels an algorithm planned to apply the technique, they applied the defenses above in an experimental Cloud environment and running them against the attacks to evaluated the technique, the result shows that the technique effectively avoid sequential cache-based SC with less than 15% overhead and it efficiency on a large L2 cache.

Chiappetta,Yilmaz 2016 [11] deliver three methods, they could be used together or used individually, one method is founded on correlation two from this approaches are built on machine learning mechanism and it uses the FLUSH+RELOAD technique, there is no need for any alteration to require in the operating system also work as user-level processes.

New tool is offered it is the "quickhpc" to achieve a counters higher temporal resolution for hardware performance than the existing tools, the two methods which use machine learning mechanism reach a minimum F-score of 0.93, they show how running their revelation system as a user-space process they could avoid and detect the attack and they did that without changing any of the components of the system without too much overhead also the system could be inserted in a virtual cloud environment or physical whichever as a plugin for the hypervisor or as a separate process.

Crane, Stephen, et al 2015 [12] by randomly control the flow of programs dynamically and methodically they study software variety as a protection against side-channel attacks, software variety techniques Currently convert each program trace identically but their variety grounded technique in state converts programs to make each trace unique for each program, and it could be protected versus both online and offline side-channel attacks, so they use the dynamic control flow variety to prevent cache-based SCA on cryptographic algorithms, which implements fine-grained program trace randomization they also applied a prototype diversifier atop LLVM.

By mechanically generating varied replicas for portions of an input program they generate a big number of unique program implementation paths, when it the runtime they then regularly and randomly switch between these replicas, then they evaluate their method against SCA, where an attacker aim to regain cryptographic keys by investigating side effects of program implementation, their result shows that the method lessens side channels cryptographic with high efficiency and reasonable overhead of 1.5–2x in practice.

B Gras, K Razavi, H Bos, C Giuffrida 2018 [13] they explain how as long as there is another shared hardware resource then the problem will become much deeper, they said that even when the CPU cache action is protected by state of the art cache SC defenses such (CAT and TSX) still there will be leak fine-grained data about a victim action when hardware translation lookaside buffers (TLBs) be a target, yet take advantage of the TLB channel is hard because of the unknown addressing functions inside the TLB and also the invader restricted control ability so they inverse engineer the unknown addressing function in latest Intel processors and innovate an approach that utilize high-resolution temporal features about a victim memory action which is it a supervised machine learning approach.

using their prototype implementation (TLBleed) which has strengthened against FLUSH+RELOAD attacks that happened in state of the art cache isolation, (TLBleed) rebuilds 92% of RSA keys from an execution , They show us that TLBleed is powerful and explains that the problem of microarchitectural side channels is much deeper than what we thought before, also they shown that TLB action monitoring as it t offers an applied new side-channel .

Also the process of the TLB is an essential hardware feature so we need new research to design flexible and effective technique that isolate TLB partitions based on the correspondent security domains, so it is important to overall side-channel protection which should wisely take into consideration all shared resources.

Sevak, Bhrugu (2013)[14]: expected to introduce how to prevent the side channel attacks in cloud computing regardless of its type or source. using of Virtual firewall appliance and randomly encryption decryption and provide RAS of client’s data or information

The "Side channel attack " takes two necessary steps: Placement and Extraction. Placement refers to the adversary that happen is in Cloud Computing 184 in order to place their mean VM attack on the original physical machine. As to Extraction it refers to After successfully placement of the malicious VM to the targeted VM so that the confidential data, and folder are extracted and taken on the targeted VM. To make it safe, focus or care must be taken with regard to the defense against the vulnerabilities that can be present in the these attack . This can be achieves through both the integration of firewall and the random encryption decryption (confusion and diffusion).

Firewall is a software that aims to protect the resources of the users from the hackers. Here when we speak about the cloud computing , rely on the virtual firewall in the cloud server back end of the cloud computing. B. while Randomly Encryption Decryptions the other For providing more security for prevent the second step of extraction of the side channel attack. So as to Confusion, it refers to making the link between the plaintext and the ciphertext as complex and related as possible

Bazm, Mohammad-Mahdi, et al. 2017[15]: they make a room for a overall survey of the side-channel attacks (SCA) and mitigation techniques that can be for virtualized environments, with our focus on (SCA). So they review the isolation challenges, attack classes and counter-measure;

from the hardware to the application level, besides the assessment of their effectiveness being done here.

the security challenges of virtualization:

First The Shared Cache for Processor and multi VMs

Second The overall caches:(L1,L2,LLC) Simultaneous multi-threading

Third Data Deduplication :the Merge of any redundant data in order to optimize memory potential..

Another challenge is The Preemptive Scheduling: Time scheduling algorithm in which the schedule program or technique split CPU's time to many slices And last one Non-Privileged access :here the process is related to Using hardware .

Bazm, Mohammad-Mahdi, et al. , 2018[16]: In this paper, they shed the lights on the approach used to find out cross-VM cache-based side channel vulnerable or breaches through the use of hardware information present in the Hardware Performance Counters (HPCs) and Intel Cache Monitoring Technology (CMT) following the method of Gaussian anomaly detection . This reflects a high level of detection rate with 2% performance overhead on the computing platform.

the two mainly hardware sources for providing cache-related information on the process of running VMs that may be used CMT method main objective here is to monitor the use of shared resources. New processors have quite a lot of cores allowing to run concurrently varied workloads on CPU cores then(HPCs): These are platform hardware registers that are used for statistics storing about several CPU events like clock cycles

Yu, Si, et al. (2013) [17]: here, investigate this type of security threat and VMs Co-residency Detection plan that can be exploited via the cache-based side channel attacks to determine the location of the any VM. By Using load pre-processor based on cubic spline interpolation, the VCDS takes the raw measurements that are more smooth and relevant at the same time . With the load predictor being based on the linear regression model, VCDS probes cache load any changes that are produced by the victim VM more accurately. But with regard to the normal cloud model,

VCDS made up modules which are raw measurement processing and distinguisher.3steps:Step 1. Load preprocessor. then. Load predictor

Liu, Fangfei, et al 2015.[18]: In this study, they focus on the execution of the PRIME+PROBE side-channel attack against the last level of cache., they demonstrate the cross-core and cross-VM attack on the different versions of GnuPG. Our technique , here , delivers a high attack resolution without weakening the OS or VMM.

In The A-Attack model, the objective information dripping that happens in the clouds. they assume that the attacker dominate a VM that is accompanying the victim VM on the same multi-core processor. The victim VM deals with the secret data such as: secret information keys. At this stage, the attacker is familiar with the crypto software . At the same time, neither take the possibility of any vulnerability in the VMM,

The PRIME+PROBE :common method used by the attacker to learn which cache set is accessed by the victim VM. The attacker, A, first, runs a spying process by which monitoring the cache usage of the victim, V, as follows: PRIME: A fills one or more cache sets with its own information . IDLE: A waits for a pre-defined time period while V executes and utilizes the cache. PROBE: A continues his implementation and measures the time to each set loading of his information.

Zhang, Yinqian, and Michael K. Reiter, 2013.[19]

This paper sheds the lights on both the design, implementation and evaluation of a new system called the "Duppel "which provides the tenant virtual machine the ability to defend itself against any cache-based side-channel attacks. The Duppel system containing pleading for time shared caches . Experiments made in the lab and on the public clouds reveal that the system effectively sends timing signals available to an attacker VM through these caches and provides a room for the modest performance alongside, Duppel does not requires any changing to hypervisors or from cloud operatives.

Depoix, Jonas, and Philipp Altmeyer. (2018): [20]

At this paper, the researchers provide us with a glimpse over a real-time detection system, that can uncover any Specter attacks by detecting cache side-channel attacks. Based, they realize that Hardware Performance Counters the attack to observe the CPUs cache activity and use of the neural network here in order to analyze the collected data. Since the cache side-channels, generally , cause or make a very distinct cache usage pattern, our neural network will be able to identify good any attack with an accuracy percentage that reaches over 99%, in our test.

Here, The role of so called " the Process Lifecycle Service" is to track any of the processes that are control by the operating system, to start monitoring these processes for any sly behavior. And This is usually done by using netlink. . The Process Life cycle Service starts by opening a socket to this interface ,in order to be informed when a process is launched . All of The PIDs of relevant processes regarding both the prevent system to start and stop watching them, and make all forwarded to other service through a pipe. The HPC Service takes care of the process by controlling the HPCs of the processes. This is done using a system called " PAPI", PAPI works by providing a specific structure of data for this thing , which can be reserved by the HPCService and attached to the HPCs of choice. It then goes by focusing in writing the current values of the attached HPCs into this data structure. All of The PIDs of the watched processes with its accompanying HPC values are then left to the next service.

4. SUMMARY

Table 1: List of approaches to prevent Cache Side Channel attack

Approach	Technique	Result
defense against LLC based side channel attacks its called "CacheBar " which implemented as a memory management subsystem within the Linux kernel to hinder on side channels across container boundaries	built on two values 1) Prevent "Flush-Reload" side channels thru LLCs by using dynamic managing physical memory pages shared between security domains to disable sharing of LLC lines (copy on access for physical pages shared among multiple security domains) 2) to obstruct the cross tenant "Prime-Probe" attacks in LLCs.(cache ability management for pages to limit the amount of cache lines each cache set that an opponent can occupy concurrently	shows that Cache Bar achieves strong security with trivial performance overheads for Platformas a Service workloads and that was via formal verification, principled analysis, and empirical evaluation.che Bar
a technique is a two server side defenses on hypervisor of a Cloud system one is concentrate on parallel side channels and the other on sequential side channels.	By employed a cache coloring technique to avert their incidence and to improve cache effectiveness in specific situations, and that happened in the parallel side channels and on sequential side channels an algorithm planned to applied the technique, they applied the defenses above in an experimental Cloud environment and running them against the attacks to evaluated	the result shows that the technique effectively avoid sequential cache based side channels with generating less than 15% overhead and it efficiency on a large L2 cache.
The Intelligent Detection algorithm proposed is used to detect the attack against the encryption algorithm by calculating the mean value of the Cache Miss Sequence of the various VM before the target could lose its data to the spy procedure	by including the logic of signature based detection to measure the cache miss time the timer is used based on the two parameters, sampling and instrumentation the profiler is select,the sampling profiler would ask the JVM in each certain point of time about the present execution point of all active threads.	using the concept of signature based algorithm along with Intelligent Detection algorithm the attack against the cache can be found based on the data stored in the SB database and the attacker can be banned by stealing the data from the cache
They want to shows that LLC SCA can be overcome using a performance optimization feature in processors	they present CATalyst which is a pseudo-locking tool uses CAT to divided the LLC into hardware software a hybrid managed cache., useing CAT as a cache partitioning mechanism and used to pins certain page frames in the LLC are called secure pages to store sensitive data	they display that LLC SCA could defeat Also CATalyst causes very small performance overhead and has trivial impact on legacy applications.
regardless of the side channel attacks type or source how to avoid it in cloud computing	by using mixture of Virtual firewall appliance and randomly encryption decryption (concept of confusion diffusion)	have many advantage like enhance the response time

to detect cross-VM cache-based SC vulnerable or breaches via the use of hardware	Use the two mainly hardware foundations for deliver high resolution cache-related data on the process of running VMs that Intel CMT and HPCs may be utilized for analysis:	they show very well they increased performance 2% when used 6 running VM so we can increase these value when increase number of VM
they deliver CSDA system which is two stage detection method it contain guest detection and host detection they differentiate the attack VMs from the genuine VMs by using pattern recognition techniques	they use two testes the regularity shape tests and shape tests they use it to extract the attack features from the sampled measurements ,which they are the memory utilization and CPU utilization gathered from the guest and the cache miss times gathered from host	after they do a series of experiments to validate there system so the result shows that their technique is efficient in detecting the cache based side channel attacks
by dynamically and methodically randomizing the control flow of programs they study software variety as a protection against side channel attacks	their variety grounded technique in state converts programs to make each program trace unique, and it could be protection against both online and off line side channel attacks, so they use the dynamic control flow variety to prevent cache based side channel attacks on cryptographic algorithms, which implements fine grained program trace randomization they also applied a prototype diversifier atop LLVM. By mechanically generating varied replicas for parts of an input program they generate a big number of unique program execution paths, when it the runtime they then regularly and randomly switch between these replicas,	they evaluate their method against cache-based side channel attacks,where an attacker aim to regain cryptographic keys by investigating side effects of program execution. their result shows that the method lessens cryptographic side channels with high efficiency and reasonable overhead of 1.5–2x in practice.
the design, implementation and evaluation of a new system called the "Duppel" {hardware and software}	The Duppel system containing defenses for time- ¨ shared caches such as per-core L1 and L2 cache , Duppel requires ¨ no changes to hypervisors or support from cloud operators.	effectively sends timing signals available to an attacker VM through these caches and provides a room for the modest performance alongside (at most 7% and usually much less)
the researchers provide us with a glimpse over a real-time detection system	the Process Lifecycle Service" is to track any of the processes that are happening and stopped by the OS, to start monitoring these processes for any hateful behavior	. The actual detection of potentially ongoing side-channel attacks is done by the SCA Detection Service. It uses the HPC data it receives from the HPC Service, to expect using NN(neural network

Server Side solution hinders the PTP technique by flushing the cache between the “Prime” and “Trigger” steps, thereby stopping the probing instance from ever seeing a pattern in the cache hit data.	they try to lessen the data loss due to frequent cache flushing they do it by only flushing the cache when the CPU switches domains, when suitable isolation between VMs is perform, one territory must not have any cache data in shared with another when they have no shared data then flushing the data from the prior territory will	This result shows that the side channel could not be effectively occur with the countermeasures in place, their secure hypervisors can successfully stop SCA and still create less than 15% overhead.

	not have any less cache hits .	
deliver three methods , one method is founded on correlation two from this methods are built on machine learning techniques and it use the FLUSH+RELOAD technique	New tool is offered it is the “quickhpc” to achieve an counters higher temporal resolution for hardware performance than the existing tools ,there is no need for any modification to require in the operating system also run as normal user level processes	they show how running there detection system as a user space process they could avoid and detect the attack and they did that without too much overhead also the system could be inserted in a virtual cloud environment or physical whichever as a plugin for the hypervisor or as a separate process
they said that even when the CPU cache action is protected by state of the art cache side channel defenses such (CAT and TSX) still their will be leak fine grained information about a victim activity when hardware translation look aside buffers (TLBs) be a target	they inverse engineer the unknown addressing function in latest Intel processors and innovate a approach that exploits high resolution temporal features about a victim memory action which is it a supervised machine learning approach. The leakage can be a 256-bit (EdDSA) secret key from a lone capture after 17 seconds of computation time with a 98% success rate by using their prototype implementation (TLBleed)	They show us that TLBleed is powerful and basically new side channel attack through the TLB and that explain to us that the problem of microarchitectural side channels is much deeper than what we thought before, also they shown that TLB action monitoring as it t offers a applied new side channel it also avoids all the state of the art cache side channel defenses.
security threat and propose the VMs Co-residency Detection	Using load pre-processor based on cubic spline interpolation, the	higher true deduction above 20% when used pre-processoe
	VCDS takes the raw measurements	
effective implementation of the PRIME+PROBE side-channel attack against the last level of cache	PRIME+PROBE Our LLC-based cross-core, cross-VM attack is based on The b-PRIME+PROBE :which is a general method used by the attacker to learn which cache set is accessed by the victim VM.	they make on line observation and offline observation on server and desktop and average cluster size in server 20.4 on desktop17.7

We recommend some considerations to improve the systems offered (in tables above) such as consider the level of overhead generated in their configuration and performance also consider their impact on legacy applications

the important to consider not to interfere with the Cloud model when performing the security systems offered to not made changes require to the client-side code and the underlying hardware they have and they may use some improvement of the virtual machine allocation policy.

5. CONCLUSION

Cloud computing succeeds in saving costs by sharing hardware resources amongst many customers, yet this sharing in resources creates variability.

In cloud environments, the Last Level Cache (LLC) is shared amongst all cores so it easy to the attacker VM which is co-located with the target VM to take advantage of the shared LLC and then to get some of the target sensitive and secret data.

To protect systems and devices from the Cache based side-channel attacks, we display a variety of countermeasures software based such as CacheBar system, CATalyst system, and TLBleed system or hardware based as a technique server-side defenses on hypervisor of a Cloud system, While each of the countermeasures has its strengths and weaknesses yet can be used to defeat or at least hold back the Cache based side-channel attacks

ACKNOWLEDGEMENT

The authors are grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

REFERENCES

[1] Peter Mell , Timothy Grance , ***The NIST Definition of Cloud Computin***g , Special Publication 800-145 NIST

[2] J. Sahoo, S. Mohapatra, and R. Lath, ***Virtualization: A survey on concepts, taxonomy and associated security issue***s, in Computer and Network Technology (ICCNT), 2010 Second International Conference on, pp. 222–226, IEEE, 2010.
https://doi.org/10.1109/ICCNT.2010.49

[3] G. Neiger, A. Santoni, F. Leung, D. Rodgers, and R. Uhlig, ***Intel virtualization technology: Hardware support for efficient processor virtualization,*** Intel Technology Journal, vol. 10, no. 3, 2006.
https://doi.org/10.1535/itj.1003.01

[4] Qiasi Luo1 and Yunsi Fei, ***Algorithmic Collision Analysis for Evaluating Cryptographic System and Side-Channel Attacks***, International Symposium on H/w-Oriented Security and Trust, 2011.
https://doi.org/10.1109/HST.2011.5955000

[5] Zhou, Ziqiao, Michael K. Reiter, and Yinqian Zhang. ***A software approach to defeating side channels in last-level caches,*** Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.

[6] Godfrey, Michael, and Mohammad Zulkernine. ***A server-side solution to cache-based side-channel attacks in the cloud***, 2013 IEEE Sixth International Conference on Cloud Computing. IEEE, 2013.
https://doi.org/10.1109/CLOUD.2013.21

[7] Vanathi, R., and S. P. Chokkalingam, ***Cache-Based Side Channel attack Discovery using Intelligent-Detection Algorithm for Securing the Cloud Computing Environment,*** International Journal of Pure and Applied Mathematics 119.17 (2018): 1929-1936.

[8] Liu, F., Ge, Q., Yarom, Y., Mckeen, F., Rozas, C., Heiser, G., & Lee, R. B. (2016, March***). Catalyst: Defeating last-level cache side channel attacks in cloud computing***. In *2016 IEEE international symposium on high performance computer architecture (HPCA)* (pp. 406-418). IEEE.

[9] Yu, Si, Xiaolin Gui, and Jiancai Lin, ***An approach with two-stage mode to detect cache-based side channel attacks,*** The International Conference on Information Networking 2013 (ICOIN). IEEE, 2013

[10] Godfrey, Michael Misiu, and Mohammad Zulkernine. ***Preventing cache-based side-channel attacks in a cloud environment,*** IEEE transactions on cloud computing 2.4 (2014): 395-408.
https://doi.org/10.1109/TCC.2014.2358236

[11] Chiappetta, Marco, Erkay Savas, and Cemal Yilmaz, ***Real time detection of cache-based side-channel attacks using hardware performance counters,*** Applied Soft Computing 49 (2016): 1162-1174

[12] Crane, S., Homescu, A., Brunthaler, S., Larsen, P., & Franz, M. (2015, February***). Thwarting Cache Side-Channel Attacks Through Dynamic Software Diversity***. In *NDSS* (pp. 8-11).
https://doi.org/10.14722/ndss.2015.23264

[13]. Gras, B., Razavi, K., Bos, H., & Giuffrida, C. (2018). ***Translation leak-aside buffer: Defeating cache side-channel protections with {TLB} attacks***. In *27th {USENIX} Security Symposium ({USENIX} Security 18)* (pp. 955-972).

[14] Sevak, Bhrugu , ***Security against side channel attack in cloud computing***, International journal of engineering and advanced technology (IJEAT) 2.2 (2013): 183

[15] Bazm, M. M., Lacoste, M., Südholt, M., & Menaud, J. M. (2017***). Side Channels in the Cloud: Isolation Challenges, Attacks, and Countermeasures***.

[16] Bazm, M. M., Sautereau, T., Lacoste, M., Sudholt, M., & Menaud, J. M. (2018, April***). Cache-based side-channel attacks detection through intel cache monitoring technology and hardware performance counters***. In *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 7-12). IEEE.

[17] Yu, S., Xiaolin, G., Jiancai, L., Xuejun, Z., & Junfei, W. (2013). ***Detecting vms co-residency in cloud: Using cache-based side channel attacks***. *Elektronika ir Elektrotechnika*, *19*(5), 73-78.
https://doi.org/10.5755/j01.eee.19.5.2422

[18] Liu, F., Yarom, Y., Ge, Q., Heiser, G., & Lee, R. B. (2015, May). ***Last-level cache side-channel attacks are practical***. In *2015 IEEE symposium on security and privacy* (pp. 605-622). IEEE.

[19] Zhang, Y., & Reiter, M. K. (2013, November). **Düppel: retrofitting commodity operating systems to mitigate cache side channels in the cloud**. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 827-838).

[20] Depoix, J., & Altmeyer, P. (2018). ***Detecting Spectre Attacks by identifying Cache Side-Channel Attacks using Machine Learning***. *Advanced Microkernel Operating Systems*, *75*.

[21] Lyu, Y., & Mishra, P. (2018***). A survey of side-channel attacks on caches and countermeasures***. *Journal of Hardware and Systems Security*, *2*(1), 33-50.
https://doi.org/10.1007/s41635-017-0025-y