International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6187
***Article Received**: 10 December 2022 **Revised**: 19 January 2023 **Accepted**: 01 February 2023*

Critical Analysis on Detection and Mitigation of Security Vulnerabilities in Virtualization Data Centers

[1]J. Manikandan, [2] Dr. Sri Lakshmi Uppalapati
[1]Research Scholar,
Vignan's Foundation for Science, Technology & Research.
Vadlamudi, Guntur, Andhra Pradesh, India.
Email: jmanikandanme@gmail.com
[2]Associate Professor,
Vignan's Foundation for Science, Technology & Research.
Vadlamudi, Guntur, Andhra Pradesh, India.
Email: druppalapati2019@gmail.com

Abstract—There is an increasing demand for IT resources in growing business enterprises. Data center virtualization helps to meet this increasing demand by driving higher server utilization and utilizing un-used CPU cycles without causes much increase in new servers. Reduction in infrastructure complexities, Optimization of cost of IT system management, power and cooling are some of the additional benefits of virtualization. Virtualization also brings various security vulnerabilities. Theyare prone to attacks like hyperjacking, intrusion,data thefts, denial of service attacks on virtualized servers and web facing applications etc. This works identifies the security challenges in virtualization. A critical analysis on existing state of art works on detection and mitigation of various vulnerabilities ispresented. The aim is to identify the open issues andpropose prospective solutions in brief for these open issues.

Keywords: Virtualization, security challenges, VM vulnerabilities, Intrusion detection systems.

I. Introduction

There is an increasing adoption of virtualization in many enterprises over last few years. Virtualization is a computing environment which allows multiple virtual servers to run on this computing environment. Virtualization makes efficient use of available resources by making use of un-used CPU cycles, so that overall the need for additional servers and rack spaces are avoided. This brings considerable saving to enterprises in terms of energy for cooling, administration cost,maintenance expenses etc. With these advantages, virtualization also brings additional management complexities, performance and security complications. Among the various factors hindering the faster adoption of virtualization, security is an important factor. Thus it is important to study the security issues and their existing countermeasure.

Virtual data center is an infrastructure allowing sharing physical resources of multiple physical servers across an enterprise. This sharing is enabledusing a suite of virtualization software which is installed on physical resources in the data center. The most common elements in a typical virtual datacenter is given below.

The most common elements in a virtual data center are virtual machine (VM), hypervisors, network resources, and datastores like Network Attached Storage (NAS), Storage Attached Network (SAN) and IP Storage Attached Network (IP SAN). All the resources of data center like servers, routers, switches and links are virtualized. Hypervisor is the virtualization software which create virtual machine of different capabilities. A Virtual Network (VN) is a set of virtual networking resources: virtual nodes (end-hosts, switches, routers) and virtual links and it is a part of virtualized data center.

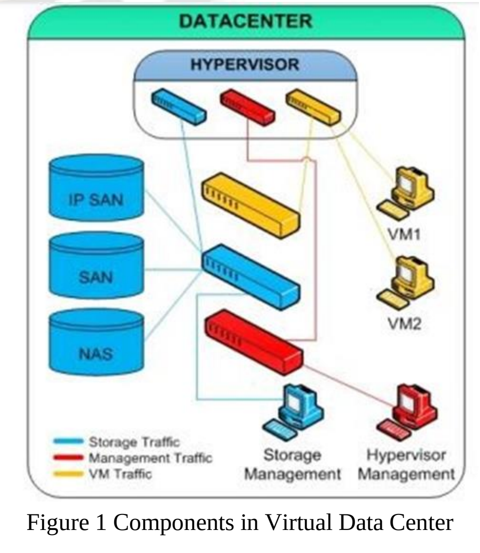

Figure 1 Components in Virtual Data Center

Like in all network infrastructures, security is an issue in virtual data center and it is even more severe due to complex interactions between tenants and infrastructure providers. Some of the security challenges in virtual data center is given below

Table 1 Attacks in Virtual Data Center

Traditional attacks	Flooding,DDoS,EDoS User to Root,Port Scanning and Backdoor channel
Virtualization specific attacks – Insider	Communication between VMs, VM monitoring from host, VM to VM Side channel and VMEscape etc
Virtualization specific attacks – External	Attack on hypervisor or VMs, Externalmodification of VM, External modification of hypervisor, Footprinting, Virtualized botnets, Virtual code injection, Breakout and Virtualization memory

Though there are many surveys on countermeasures for traditional attacks, a comprehensive survey on countermeasures for virtualization specific attacks both internal and external is not available. This work fills this gap and does a critical analysis on existing solutions for virtualization specific attacks in area of detection and mitigation.

II. Related Work

Klymash et al (2019) proposed a improved authentication process to ensure security in datacenters. Whenever hypervisor is accessing the users file, it is authenticated by a key, which is hidden in the encrypted file. By this way, modification of files by any attacker is prevented. The files are encrypted with 128-bit SSL encryption. To avoid the key management complexity, hypervisor belonging to same group of users are grouped into trusted virtual domain and keys are defined for each domain instead for each hypervisor. Authentication process proposed in this method is not secure against message capture attacks. Hu et al (2017) proposed an anomaly detection system which implements security in all layers of virtual data center. The data collected at interface points of each layer is manually labeled for anomalous behavior. A decision tree is then constructed to classify the anomalous behavior. But the anomaly detection model is only for traditional attacks and does not consider various insider and outsider attacks on virtualization layer. Palmieri et al (2015) detailed a subtle and a stealthy attack energy based DOS on virtualized data center. Attack is launched with intention to increase the energy consumption of datacenter thereby causing loss of revenue, penalty for green house emissions etc. As on today, there are no solutions to detect and mitigate the effect of these attacks in virtualized data center. Jia et al (2019) proposed a secure and effective allocation strategy to solve the security issues associated with VM co-residence.VM are placed in such way across physical hosts so that it becomes difficult to compromise on other VM's data by using the shared resources. Though this mechanism is able to secure against co-residence issues, it reduces the data center utilization. Qiu et al (2017) proposed a secure allocation strategy to prevent from co-residence security problems. Two novel metrics were proposed to evaluate the deployment in terms of co-residency probability. The work also defined four thresholds to arrive at a balance between security and load balancing. But any deployment strategy based solution to co- residency security issues reduces the data center utilization and increases the cost for data center owner. Jin et al (2015) proposed a secure resource accounting technique for virtualized data center. The secure accounting is realized using hardware.

Table 2 Survey summary

Solution	Technique used	Pros	Gap
Klymash et al (2019)	Files are encryptedwith 128 bit SSL encryption and	Key managementcomplexity is by grouping users to	The method is notrobust against message capture
	hypervisor access tofile is authenticated	virtual domain andkey management done at level of virtual domain	attacks
Hu et al (2017)	Decision tree based classification of malicious behaviour in the virtualizationlayer	Work well for traditional attackslike DoS, guess attacks etc	Method is insecureagainst insider attacks in the virtualization layer
Palmieri et al (2015)	Detect energy dos attack on data centerby matching access against threshold	Reduced the energy expense at datacenter	Filter even valid patterns during peak traffic. Thresholdingis not efficient in handling this problem
Jia et al (2019)	Allocation strategy toprevent VM co-residence attack by thresholding	Allocation is donebalancing security and load balancing	Could not reduce VMcoresidence attack as it did not consider thedynamic behaviour of each applications in it
Jin et al (2015)	Hardware assisted resource accounting	Able to detectresource overutilization attacks	Not scalable due tocost of hardware
Singh et al (2021)	Malicious threads areidentified using HPCcounter statistics	Protection against micro architectural attacks	Statistics based filtering is not effective against intelligent attacks. Machine learning must be used to learn more intricate attackpatterns
Li et al (2019)	New hypervisor design called HypSecto improve the confidentiality and integrity of virtual machine	Trusted core is isolated and protected using hardware support. Itexecutes at highest privilege level and can protect VM datain the CPU and memory	The security is provided at the costof increased performance overhead
Wu et al (2018)	data confidentiality in guest VM againstuntrusted hypervisor using memory encryption hardware	Revokes the permissions of accessing specific resources from theun-trusted hypervisor.	The approach could not solve the problem of data leakage through network
Inokuchi et al (2020)	bonding technique toprotect from VM redirection attack.	Users are strongly bound their VM andthey are prevented from redirection to other VM	Can result is resourceunderutilization
Zhu et al (2017)	light weight hardware assistedVM isolation approach	run time protection ofguest VM even with compromised hypervisor	performance overhead for applications with least or without any security requirements
Tadokoro et al (2012)	VMCrypt to secure the data in VM's memory using trustedvirtual machine monitor. Dual memory view is provided in this work.	Protection of VM data from others VMco-residing in same host	Performance overhead is very highdue to dual view
Li et al (2012)	secure execution environment on virtualized computing infrastructure underassumption of un- trusted management OS	Security is providedat a minimal performance overhead	There is no adaptability based onthe security needs of the application
Kourai et al (2015)	preventing information leakage in out of band remotemanagement using virtual serial console	Only a trusted virtualmachine monitor cansecurely decrypt the console inputs encrypted in an SSH client	The solution cannotprevent any malicious commanddetect through console
Miyama et al (2017)	Nested virtualizationbased Intrusion Detection System	It can obtain the target state of VMand use it for detecting any	The solution is not secure against rulesand decision logic corruption in the

		intrusions.	memory of IDS
Li et al (2021)	micro-verification framework to prove the security properties ofhypervisor	The entire hypervisorsecurity properties are verified by reducing to verifyingthe core alone.	The approach doesnot monitor hypervisor in run time environment
Kolesnikova et al (2016)	A new methodologyfor hypervisor stability evaluation.	A formal model forinsider attacks on hypervisor is developed	The stability was measured in terms ofits compromise in privileges without consideration for leakage and risk to data stored in VM
Tu et al (2021)	solution addressing the problem of vulnerability windowof critical flaws called as hypervisor transplant	Two approaches of n-place server micro- reboot based hypervisor transplant (noted InPlaceTP) and live VM migration-based hypervisor transplant	management of VMbecomes difficult even for a medium size data center
Wu et al (2017)	An access control model based on BLP(Bell-La Padula) model is proposed	Provided solution forVM escape attack	Enforcing access control on each APIincurs performance overhead
Nathiya et al (2019)	intrusion detectionsystem to monitor security in virtual network layer	Attacks are detectedusing signature and anomaly techniques	There is no prevention mechanisms proposed in this workagainst malicious modifications of IDS rules
Pan et al (2012)	An novel hypervisordesign is done splitting the hypervisor functionality into small enough components in the TCB	prevented hypervisor compromise based ontrusted computing base	The attack of hypervisor on VM data is not consideredin this work
Dildar et al (2017)	Virtual Machines andHypervisor Intrusion Detection System to detect and prevent hypervisor attacks	An extensibleframework isproposed	The work did not address any specific internal and externalattacks

assisted system management mode and virtualization. Even when a hypervisor is compromised, the proposed technique can provide an accurate accounting. Hardware assisted management mode is costly, instead prediction based approaches can be applied to realize secure accounting. Singh et al (2021) proposed a security mechanism for micro architectural attacks due to virtualization. The malicious behaving threads are denied CPU slots; thereby they don’t have time and resources to carry out attack. Malicious threads are identified in this work based on HPC counter statistics and it does not consider parameters specific to virtualization inside and outside attacks. Li et al (2019) proposed a new hypervisor design called HypSec to improve the confidentiality and integrity of virtual machine. Hypervisor is partitioned into two portions of un-trusted host performing complex hypervisor functionality without access to virtual machine data and trusted core performing CPU and memory virtualization and providing access control to the virtual machine data. Trusted core is isolated and protected using hardware support. It executes at highest privilege level and can protect VM data in the CPU and memory. The security is provided at the cost of increased performance overhead. Wu et al (2018) proposed a solution for data confidentiality in guest VM against untrusted hypervisor using memory encryption hardware SME and SVE.A software based extension to SVE is provided to address the security issues without any performance overhead. This extension separates the management of critical resources from service provisioning and revokes the permissions of accessing specific resources from the un-trusted hypervisor. Though protection for data in memory is provided, the approach could not solve the problem of data leakage through network. Inokuchi et al (2020) proposed a bonding technique to protect from VM redirection attack. This bonding technique called UVbond boots user’s VM by decrypting its encrypted disk inside the trusted hypervisor. VM is given a descriptor to securely identify the VM. Users are strongly bound their VM and they are prevented from redirection to other VM via management console and API’s. Certain genuine need for inter VM communication is also protected in this approach. Zhu et al (2017) proposed a light weight hardware assisted VM isolation approach. The approach is able to provide run time protection of guest VM even with compromised hypervisor. The approach decouples the functions of memory isolation among VMs from the hypervisor into the security monitor. As a result, the hypervisor can only update the Stage-2 page tables of VMs via the security monitor, which inspects and approves each new mapping. By this way VM are protected from any attacks launched through hypervisor. But this introduces performance overhead for applications without any security requirements. Tadokoro et al (2012) proposed VMCrypt to secure the data in VM's memory using trusted virtual machine monitor. Dual memory view is provided in this work. Normal memory view and encrypted memory view. The portions for normal and encrypted memory view are identified in supervised manner in the life cycle of VM. It becomes tedious to identify the portions for normal and encrypted view for all different VM in supervised manger and this necessitates machine learning. Li et al (2012) provided a secure execution environment on virtualized computing infrastructure under assumption of un-trusted management OS. Secure virtualization architecture is provided to secure run time environment, network interface and secondary storage. Security is provided at a minimal performance overhead and there is no adaptability based on the security needs of the application. Kourai et al (2015) proposed a solution for preventing information leakage in out of band remote management. Encrypted virtual serial consoles are provided in the management VM. Only a trusted virtual machine monitor can securely decrypt the console inputs encrypted in an SSH client. During reconnection, key is automatically changes and re-encryption of serial console is done. The solution cannot prevent any maliciouscommand detect through console and it can only prevent information leakage. Miyama et al (2017) proposed a nested virtualization based Intrusion Detection Systems (IDS). IDS can obtain the target state of VM and use it for detecting any intrusions. IDS are also prevented from any compromises. But the solution is not secure against rules and decision logic corruption in the memory of IDS. Li et al (2021) proposed micro-verification framework to prove the security properties of hypervisor. The hypervisor is decomposed into single core and multiple un-trusted services. The entire hypervisor security properties are verified by reducing to verifying the core alone. Hypervisor is checked if it can provide confidentially and integrity of VM data. The approach does not monitor hypervisor in run time environment and does security proof only in test run. Kolesnikova et al (2016) proposed a new methodology for hypervisor stability evaluation. A formal model for insider attacks on hypervisor is developed. The formal model did not consider any specific events. The stability was measured in terms of its compromise in privileges withoutconsideration for leakage and risk to data stored in VM. Also the work was not specific to any insider attack. Tu et al (2021) proposed a solution addressing the problem of vulnerability window of critical flaws called as hypervisor transplant. Two approaches of n-place server micro-reboot basedhypervisor transplant (noted InPlaceTP) and live VM migration-based hypervisor transplant (noted MigrationTP) are combined to address the vulnerabil ity window till a patch for the hypervisor is made. But management of VM becomes difficult with multiple approaches. Wu et al (2017) proposed a solution for VM escape attack. An access control model based on BLP (Bell-La Padula) model is proposed to prevent virtual machine escape. Enforcing access control on each API incurs performance overhead. Nathiya et al (2019) proposed a intrusion detection system to monitor security in virtual network layer. Attacks are detected using signature and anomaly techniques. Correlation module is used to detect distributionattacks. Dempster-Shafer theory is applied in the decision making process. But the IDS behavior can be affected by malicious modification of its decision. There is no prevention mechanisms proposed in this work against these malicious modifications. Pan et al (2012) proposed a mechanism to prevent hypervisor compromise based on trusted computing base. An novel hypervisor design is done splitting the hypervisor functionality into small enough components in the TCB. By this way TCB size is reduced. The attack of hypervisor on VM data is not considered in this work. Saeed et al (2018) introduced a new attack by malicious VM using TAP impersonation and mirroring to redirect and monitor network traffic of other VM. These attacks are very difficult to monitor as the malicious VM is not violating any resource capacity. There are no methods currently to detect this kind of attacks. Dildar et al (2017) proposed Virtual Machines and Hypervisor Intrusion Detection System to detect and prevent hypervisor attacks. The work only proposed a framework without addressing any specific internal and external attacks. Also the mechanism to detect the IDS before malicious decision modification is also not considered in this work. The summary of survey is presented in Table 1.

III. Open Issues

From the survey following open issues are identified in handling of security vulnerabilities in virtualized data center.

Issue 1: Co-residence of VM creates many security vulnerabilities in terms of overriding logical isolation of resources. The current mechanisms for solving these problems are based on allocation strategy which reduces the data center utilization. Thus it is necessary to solve the Co-residence problem, by observing the behavior dynamically and selective de-allocation of VM's. By this way, the reduction in data center utilization can be avoided.

Issue 2: Most intrusion detection systems are designed only for traditional attacks. These systems capture packets and analyses it based on signature or anomaly techniques to detect traditional attacks. But there are no systems which can analyze at semantic level, the interaction between hypervisor and VM and between VM to detect attacks.

Issue 3: Intrusion detection systems themselves canbe attacked in virtualized environment by comprising on the decision logic in memory of VM.Current IDS systems designed for virtualized environment are not secure against these attacks.

Issue 4: The current mechanisms for attack mitigation are not adaptive and they apply the same treatment for all VM without consideration for the nature of the applications on VM. Due to this, there is a increase in performance overhead. This can be avoided by fine tuning the protection mechanism depending on the securing requirement in the VM and its current security vulnerability in terms of co-residence etc.

Issue 5: Currently there are no models which can access the vulnerability of the virtualized data center components in terms of various internal and external attacks. These models are important to assess the vulnerability and design an adaptive mitigation strategy.

IV. Addressing the Open Issues

To address the open issues, this work suggests a framework as shown in Figure 2.

The VM's and the hypervisor components in virtualization environment must be probed for any incoming and outgoing events. The events can be at network level, memory level, API calls, disk level etc. From these events, essential features must be extracted. The features must be at semantic level compared to packet level in traditional intrusion detection systems. The events must be classified into various types like data sensitivity, interface sensitivity, service denial, session hijacking etc.

The mitigation strategy for these attacks must be adaptively fine tuned based on the application characteristics on VM, vulnerability assessment etc. The decision must be learnt automatically using Q- Learning based reinforcement.

Issue 1 can be solved by observation of events fromVM and decision to de-allocate VM to separate physical resource can be made.

Issue 2 can be solved by mapping packets to semantic events in the virtualization network andreasoning based on semantic events.

Issue 3 can be solved by isolation of VM to separate physical machine but still allowing to access other network interfaces using mirroring in virtual data center.

Issue 4 can be solved by adaptive enforcement ofmitigation schemes based on application characteristics, security assessments etc.

The facilitator to address all these issues is to virtualization vulnerability assessment model considering both inside and external attack. Using the model, the mitigation strategy can be adaptivelyfine tuned.

***Article Received**: 10 December 2022 **Revised**: 19 January 2023 **Accepted**: 01 February 2023*

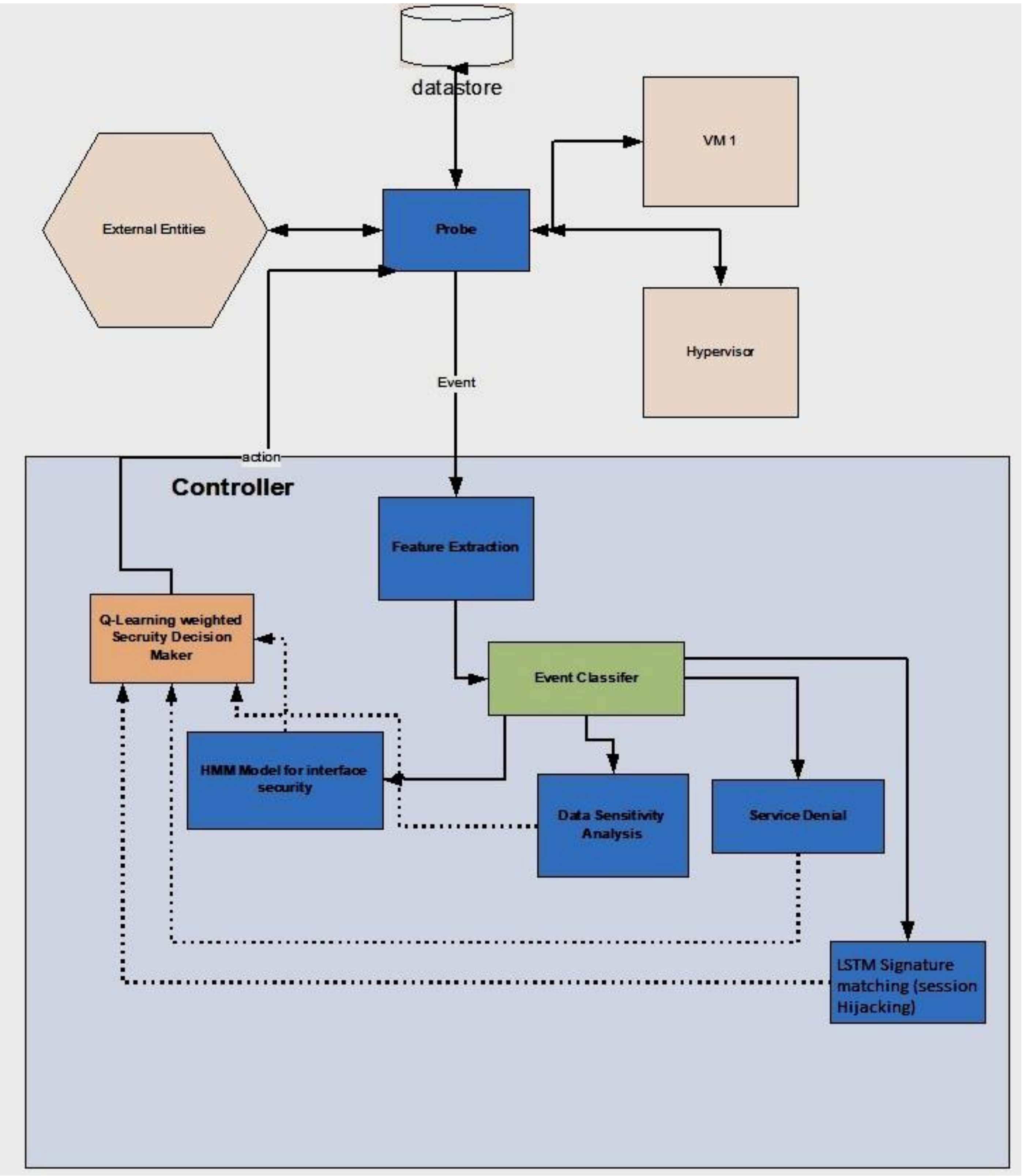
datastore
VM 1
External Entities
Probe
Hypervisor
Event
action
Controller
Feature Extraction
Q-Learning weighted Secruity Decision Maker
Event Classifer
HMM Model for interface security
Data Sensitivity Analysis
Service Denial
LSTM Signature matching (session Hijacking)

Figure 2 Security framework for Virtualization

V. Conclusion

A survey on various attacks and mitigation schemesin virtualized data center is presented in this work. Differing from earlier survey on traditional attack, this work focused more on virtualization specific attack both inside and external. The survey identified the open issues and provided

***Article Received**: 10 December 2022 **Revised**: 19 January 2023 **Accepted**: 01 February 2023*

directions for further research. Virtualization is being rapidly adopted and it is very important to identify the various insider and external attacks and mitigate those issues. Towards this end, this survey work is significant as it identified important issues in way of handling insider and external attacks on virtualization.

References

[1] M. Klymash, O. Shpur, O. Lavriv and N. Peleh, "Information Security in Virtualized Data Center Network," *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 419-422.

[2] Z. Hu, S. Gnatyuk, V. Gnatyuk and S. Bondarovets, "Anomaly Detection System in Secure Cloud Computing Environment", *International Journal of Computer Network and Information Security*, pp. 10-21, 2017.

[3] F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco and A. Castiglione, "Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures", *Journalof Supercomputing*, pp. 1620-1641, 2015.

[4] Jia, Hefei & Liu, Xu & Di, Xiaoqiang & Qi, Hui & Ligang, Cong & Li, Jinqing & Yang, Huamin. (2019). Security Strategy for Virtual Machine Allocation in Cloud Computing. Procedia Computer Science. 147. 140-144. 10.1016/j.procs.2019.01.204.

[5] Y. Qiu, Q. Shen, Y. Luo, C. Li, and Z. Wu. (2017) "A secure virtual machine deployment strategy to reduce co-residency in Cloud." IEEE Trustcom\BigDataSE\ICESS : 347–354.

[6] S. Jin, J. Seol, J. Huh, and S. Maeng, "Hardware-assisted secure resource accounting under a vulnerable hypervisor," ACM SIGPLAN Notices, vol. 50, no. 7, pp. 201–213, 2015

[7] Nikhilesh Singh and Chester Rebeiro,"LEASH: Enhancing Micro-architectural Attack Detection with a Reactive Process Scheduler",arXiv,2021

[8] Shih-Wei Li, John S. Koh, and Jason Nieh. 2019. Protecting cloud virtual machines from commodity hypervisor and host operating system exploits. In Proceedings of the 28th USENIX Conference on Security Symposium (SEC'19). USENIX Association, USA, 1357–1374.

[9] Y. Wu, Y. Liu, R. Liu, H. Chen, B. Zang, and H. Guan. Comprehensive VM Protection Against Untrusted Hypervisor Through Retrofitted AMD Memory Encryption. In 2018 IEEE International Symposium on High Performance Computer Architecture (HPCA 2018), pages 441-453, Vienna, Austria, Feb. 2018

[10] Inokuchi, K., Kourai, K. Secure VM management with strong user binding in semi-trusted clouds. J Cloud Comp 9, 3 (2020)

[11] Zhu M, Tu B, Wei W, Meng D (2017) HA-VMSI: A Lightweight Virtual Machine Isolation Approach with Commodity Hardware for ARM In: Proceedings of the 13th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, 242–256.

[12] Tadokoro H, Kourai K, Chiba S (2012) Preventing Information Leakage from Virtual Machines' Memory in IaaS Clouds. IPSJ Online Trans 5:156–166

[13] Li C, Raghunathan A, Jha NK (2012) A Trusted Virtual Machine in an Untrusted Management Environment. IEEE Trans Serv Comput 5(4):472–483

[14] Kourai K, Kajiwara T (2015) Secure Out-of-bandRemote Management Using Encrypted Virtual Serial Consoles in IaaS Clouds In: Proceedings of International Conference on Trust, Security and Privacy in Computing and Communications, 443–450

[15] Miyama S, Kourai K (2017) Secure IDS Offloading with Nested Virtualization and Deep VM Introspection In: Proceedings of European Symposium on Research in Computer Security, 305–323

[16] Li, Shih-Wei & Li, Xupeng & Gu, Ronghui & Nieh, Jason & Hui, John. (2021). A Secure and Formally Verified Linux KVM Hypervisor. 10.1109/SP40001.2021.00049.

[17] Kolesnikova, Svetlana. (2016). Evaluation of Hypervisor Stability towards Insider Attacks. JOURNAL OF ELECTRONIC SCIENCE AND TECHNOLOGY. 14. 10.11989/JEST.1674-862X.510022.

[18] Dinh Ngoc Tu, Boris Teabe Djomgwe, Alain Tchana, Gilles Muller, Daniel Hagimont. Mitigating vulnerability windows with hypervisor transplant. EuroSys 2021 - European Conference on Computer Systems, Apr 2021, Edinburgh / Virtual, United Kingdom. pp.1-14

[19] Wu, Jiang & Lei, Zhou & Chen, Shengbo & Shen, Wenfeng. (2017). An Access Control Model for Preventing Virtual Machine Escape Attack. Future Internet. 9. 20. 10.3390/fi9020020.

[20] Nathiya, T.; Suseendran, G. An Effective Hybrid Intrusion Detection System for Use in Security Monitoring in the Virtual Network Layer of Cloud Computing Technology. In Data Management, Analytics and Innovation. Advances in Intelligent Systems and Computing; Balas, V., Sharma, N., Chakrabarti, A., Eds.; Springer: Singapore, 2019; Volume 839.

[21] Pan, W.; Zhang, Y.; Yu, M.; Jing, J. Improving virtualization security by splitting hypervisor into smaller components. In IFIP Annual Conference on Data and Applications Security and Privacy, Paris, France, 11–13 July 2012. Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer Nature: Basel,Switzerland, 2012; Volume 7371, pp. 298–313.

[22] A. Saeed, P. Garraghan, B. Craggs, D. v. d. Linden, A. Rashid and S. A. Hussain, "A Cross-Virtual Machine Network Channel Attack via Mirroring and TAP Impersonation," *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 606-613

[23] M. S. Dildar, N. Khan, J. B. Abdullah and A. S. Khan, "Effective way to defend the hypervisor attacks in cloud

computing," *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, 2017, pp. 154-159