A Review of Malware Detection Techniques in Virtualization Environment

RITESHKUMAR H. PRAJAPATI
Research Scholar
Gujarat Technological University, Gujarat, India

DR.DARSHAN M. TANK
Government Polytechnic Rajkot
Gujarat Technological University, Gujarat, India

DR.SUNNY H. BHADLAWALA
Research Supervisor
Gujarat Technological University, Gujarat, India

Concept of virtualization is being used more these days due to the benefit of reducing cost and improved efficiency and scalability. Almost 90% of firms use server virtualization. But this increased use of virtualization has also increased risks of security in virtualization. Virtual Machines are susceptible to viruses, malware and ransomware attacks. Infected VMs are the source of these attacks. Once a VM gets infected, it infects the entire virtual infrastructure if there is no proper isolation and security controls. This review paper reviews the different malware detection techniques in virtualization environment. Although there are many other techniques available but this review paper focuses on two of the most used memory analysis and use of machine learning for malware detection. It also proposes how these techniques can be combined to detect zero day malwares i.e. unknown malware for whom signatures are not yet developed.

Keywords Virtualization, virtual machines, zero day malwares, malware analysis, memory forensics, machine learning

---

1. INTRODUCTION

Virtualization is the technology used to create virtual versions of servers, storage, networks and other physical machines. Virtualization is a key foundational technology for empowering cloud computing. In virtualization, multiple Virtual Machines (VMs) are created and run on a single physical machine using a Virtual Machine Monitor (VMM). The virtual software imitates the capabilities of physical hardware and enables the running of multiple virtual machines on a single physical machine. OS virtualization is a software that allows a piece of hardware to have multiple operating system images run on it concurrently.

2. VIRTUAL MACHINES AND HYPERVISOR

VMs are isolated computing environments or software that allows any user to run applications on an operating system through a physical machine. Every application

consists of separate libraries and a Guest OS. As shown in figure1, the hypervisor comes beneath the VM. VMs allow sharing, scale, and isolation. They are widely used in most of the computing such as testing environments, cloud computing, and security analysis.

A hypervisor, also known as virtual machine monitor (VMM), is the software layer which enables virtualization. It acts as a bridge between the physical hardware and the virtualized environments. There are two types of hypervisor:

* Type 1 hypervisor which is directly installed on the computer's hardware instead of the OS, examples: HyperKit on MacOS, HyperV on Windows, KVM on Linux.

* Type 2 hypervisor runs on a host operating system which provides hardware abstraction examples: VMware Workstations, Oracle VirtualBox.

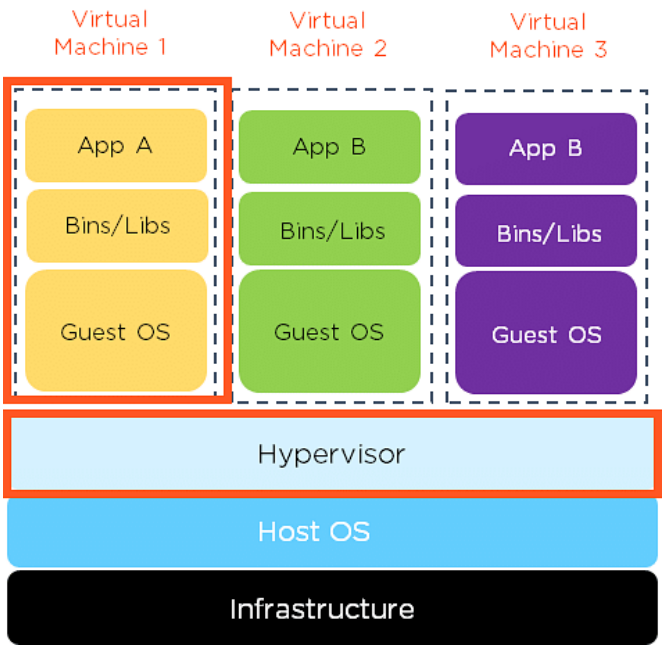

Fig. 1 Hypervisor and Virtual machines [17]

3. MALWARES

Malware is any malicious software with the intent to bring harm or to infect the machine. Malware is one of the biggest threats in terms of launching a cyber-attack in the information security realm. Unfortunately, the problem of uncontrolled growth of malicious code is likely to continue in the future, because writing malware is quickly turning into a profitable business.

Different types of malware can be seen in Table I.

TABLE I: TYPES OF MALWARE AND PRIMARY CHARACTERISTICS

Malware Types	Main Characteristics
Virus	Common and well-recognized malware
Worm	Spreads by using networks Allows unauthorized access to CPS systems
Trojan Horse	Appears to be a normal software Sends secret information to other parties
Backdoor	Bypasses security systems Opens systems to remote access
Rootkits	Provide privileged access Hide their suspicious codes from the host system
Ransomware	Encrypts the data on infected system
Obfuscated malware	Uses concealing techniques to hide itself in the systems

Fig 2: Types of malware [2]

4. MALWARE DETECTION

Malware detection is the process of identifying and responding to malicious software (malware) on systems or networks. The goal is to protect devices, data, and users from harm caused by malicious activities such as theft, corruption, or unauthorized access. Malware detection plays a critical role in cybersecurity, enabling proactive defenses and rapid response to potential threats. Malware analysis is a vital component of cybersecurity, enabling organizations to understand, detect, and mitigate threats effectively. By dissecting malware, security professionals can stay ahead of attackers, protect critical systems, and minimize the damage caused by cyber incidents.

The different types of malware detection are as follows:

A. Signature-Based Detection

Signature-based detection is a method used for the identification of malware. It works by comparing the characteristics of a threat/malware to a database of known malware signatures. Each signature serves as a distinctive marker for a specific category of threat/malware, which may present in various forms, like dimensions, hash values, strings, or other distinguishing features. The antivirus softwares implement signature-based detection to conduct scans for malware residing on the user's computer or within the network infrastructure.

B. Behavior-Based Detection

Behavior-based detection is a method for identifying malware by observing and analyzing the actions or behaviors of programs, processes, and systems in real-time. Instead of relying on static signatures (specific patterns or code), this approach monitors dynamic activities to detect potentially harmful behavior that indicates malicious intent.

C. Machine Learning-Based Detection

Machine Learning-Based Anomaly Detection is a technique utilizing machine learning algorithms to analyze VM behavior and detect anomalies. Machine learning models are trained on large datasets to recognize patterns associated with malware. These patterns can include file characteristics, behavior, or network activity. ML-based detection can adapt and identify new, previously unknown malware by recognizing features or behaviors not explicitly defined by signatures.

D. Memory Analysis technique

Memory analysis is a method used to examine the memory of active virtual machines (VMs) in order to detect indications of malicious software or behavior. This process involves scrutinizing the memory of a specific VM to observe its internal operations from an external perspective, utilizing the Virtual Machine Monitor layer. The activities under review pertain to memory usage, disk operations, CPU registers, network connections, and accessible kernel symbols of the VM. Through memory analysis, it is possible to identify malware that remains resident in memory, rootkits, and various sophisticated threats that conceal themselves within the operating system's memory environment.

5. SURVEY OF EXISTING WORK

We have reviewed the notable work done for malware detection using Machine learning methods and using Memory analysis methods and is summarized as below.

Title of Paper	**Published**	**Summary**
Detecting Zero Day Malware[1]	JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 08, Issue 05 (May 2019),DOI: 10.17577/IJERTV8IS050368	This paper gives an overview of the different malware analysis techniques namely static, dynamic and hybrid malware analysis techniques. This paper gives a Survey on the different existing malware detection systems and proposes a Zero-Day malware detection model based on static analysis and dynamic sandbox analysis and used Weka classification algorithms.
A review of Cloud-Based Malware Detection System: Opportunities, Advances and challenges[2]	Aslan, O., Ozkan-Okay, M., & Gupta, D. (2021). European Journal of Engineering and Technology Research, 6(3), 1–8. https://doi.org/10.24018/ejers.2021.6.3.2372	The paper presents the cloud-based malware detection approach and gives the vision to the reader to understand the benefit of the cloud protection from cyber-attack. This paper also presents the cloud-based malware detection framework, which uses hybrid approach for malware detection.

A Dynamic Malware Detection in Cloud Platform[3]	Fui, N. L. Y., Asmawi, A., & Hussin, M. (2020). International Journal of Difference Equations, 15(2), 243–258. https://doi.org/10.37622/ijde/15.2.2020.243-258	This paper shows examples of different types of malware attacks happened recently, types of malwares and its detection techniques, and uses Machine Learning Classification models for malware detection. There are three classifiers chosen in this work, which are Random Forest, J-48, and Naive Bayes and Datasets used is from Kaggle database.
Analyzing machine learning approaches for online malware detection in cloud[4]	Kimmell, J. C., Abdelsalam, M., & Gupta, M. (2021). arXiv (Cornell University). https://doi.org/10.48550/arxiv.2105.09268	This paper presents online malware detection based on process level performance metrics, and studied the performance of different ml models like Support Vector Classifier (SVC), Random Forest (RF), K- Nearest Neighbor (KNN), Gradient Boosted Classifier (GBC), Gaussian Naive Bayes (GNB) and Convolutional Neural Networks (CNN). And finds that CNN model has the best overall performance.
A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing [5]	Rabbani, M., Wang, Y. L., Khoshkangini, R., Jelodar, H., Zhao, R., & Hu, P. (2020). Journal of Network and Computer Applications, 151, 102507. https://doi.org/10.1016/j.jnca.2019.102507	This paper proposes a malicious behaviour detection and that includes two main modules- 1.Data Preprocessing and 2.Recognition. 1. Data preparation to extract informative features for learning and 2. Training and Prediction. They used a new optimized probabilistic neural network algorithm and evaluated on the UNSW-NB15 dataset.
Cloud Based Malware Detection System Using Support Vector Machine[6]	Das, Y. (2023, May 31). International Journal for Research in Applied Science and Engineering Technology, 11(5), 7416–7419. https://doi.org/10.22214/ijraset.2023.53253	This paper discusses how utilizing cloud environments for malware detection could be an effective approach, especially considering the rapid increase in malware and the lack of a reliable detection method. It proposes a framework that leverages machine learning techniques, specifically the Support Vector Algorithm, to identify the most relevant features from our provided dataset and produce accuracy assessments.
Malware Detection in Cloud Infrastructures Using Convolutional Neural Networks[7].	Abdelsalam, M., Krishnan, R., Huang, Y., & Sandhu, R. (2018, July) IEEE 11th International Conference on Cloud Computing (CLOUD). https://doi.org/10.1109/cloud.2018.00028	This paper presents a robust method for malware detection within cloud infrastructure utilizing Convolutional Neural Networks (CNN). Initially, a conventional 2D CNN is employed, trained on the metadata associated with each process in a virtual machine (VM). Subsequently, a novel 3D CNN is introduced, where the input consists of a series of samples collected over a specific time frame. This approach significantly minimizes the occurrence of mislabeled samples during both data collection and training phases.

Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment[8].	Aslan, O., Ozkan-Okay, M., & Gupta, D. (2021). IEEE Access, 9, 83252–83271. https://doi.org/10.1109/access.2021.3087316	This study introduces an advanced detection system that utilizes intelligent behavior-based methods within a cloud environment. Initially, the system generates a malware dataset across various virtual machines, effectively identifying unique characteristics. Subsequently, these selected features are provided to both learning-based and rule-based detection agents to differentiate between malware and benign samples.
A Method for Malware Analysis by Virtual Machine Introspection Technique[9].	Almaraz García, L. E. H., & Acosta Bermejo, R. (2018, December 31). Research in Computing Science, 147(12), 11–20. https://doi.org/10.13053/rcs-147-12-1	This paper presents a method utilizing Virtual Machine Introspection to capture the memory image of a Virtual Machine from an external perspective. It also facilitates the analysis of internal elements, including active processes, threads, network connections, and open files, through the Volatility Framework. By applying this technique to a VM, one can monitor process activities and, based on their behavior, detect potential malware.
API Call-Based Malware Classification Using Recurrent Neural Networks[10]	Li, C., & Zheng, J. (2021, May 27).Journal of Cyber Security and Mobility. https://doi.org/10.13052/jcsm2245-1439.1036	Malware execution is primarily influenced by the API calls made to the operating system to perform harmful activities. This study leverages the ability of Recurrent Neural Networks (RNNs) to identify long-term patterns in time-series and sequential data, aiming to evaluate the potential and efficiency of RNNs in detecting and analyzing both malware and benign software based on their behavioral characteristics.
KVMInspector: KVM Based introspection approach to detect malware in cloud environment[11].	Mishra, P., Verma, I., & Gupta, S. (2020, April). Journal of Information Security and Applications, 51, 102460. https://doi.org/10.1016/j.jisa.2020.102460	This study introduces a dynamic analysis-based introspection method known as KVMInspector, designed to identify malware within KVM-based cloud environments. KVMInspector operates both internally and externally to the virtual machine. It utilizes the LibVMI and Nitro libraries to gather low-level information from a running virtual machine by examining its memory, intercepting hardware events, and accessing the vCPU registers through KVM.
Designing in-VM-assisted light weight agent-based malware detection framework for securing virtual machines in cloud computing [12].	Patil, R., Dudeja, H., & Modi, C. (2019, June 26). International Journal of Information Security, 19(2), 147–162. https://doi.org/10.1007/s10207-019-00447-w	This paper introduces a framework for agent-based malware detection (AMD) that utilizes in-VM assistance. The framework consists of two key components: an agent operating within the virtual machine (VM) and an anomaly detection system at the hypervisor level. The agent is responsible for continuously monitoring the VM for any new executable deployments and employs signature-based detection methods to identify known malware.

TKRD: Trusted kernel rootkit detection for cybersecurity of VMs based on machine learning and memory forensic analysis[13].	Wang, X., Zhang, J., Zhang, A., & Ren, J. (2019). Mathematical Biosciences and Engineering, 16(4), 2650–2667. https://doi.org/10.3934/mbe.2019132	This study introduces a TKRD approach aimed at the automatic detection of kernel rootkits within virtual machines in a private cloud environment. This method integrates VM memory forensic analysis with machine learning techniques. Malicious characteristics are identified from the VM's memory dumps using memory forensic analysis. Utilizing these characteristics, several machine learning classifiers are trained, including Decision Trees, Rule-Based Classifiers, Bayesian classifiers, and Support Vector Machines (SVM). The findings indicate that the Random Forest classifier demonstrates the highest level of performance.
PlausMal-GAN Plausible Malware Training Based on Generative Adversarial Networks for Analogous Zero-Day Malware Detection[18]	Won, D. O., Jang, Y. N., & Lee, S. W. (2023). IEEE Transactions on Emerging Topics in Computing, 11(1), 82–94. https://doi.org/10.1109/TETC.2022.3170544	Enhances zero-day malware detection using generative adversarial networks for training Develop a malware training framework for generating analogous zero-day malware data. Proposed framework showed higher, stable performance for zero-day malware detection.
Classification and online clustering of zero-day malware[19]	Jurečková, O., Jureček, M., Stamp, M., di Troia, F., & Lórencz, R. (2024). Journal of Computer Virology and Hacking Techniques. https://doi.org/10.1007/s11416-024-00513-5	Focus: Classifying and clustering zero-day malware into families for cybersecurity. Classify and cluster zero-day malware into families for researchers' study. Done using Static analysis of portable executable files for Windows OS.
Malware Analysis and Detection Using Machine Learning Algorithms[20]	Akhtar, M. S., & Feng, T. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. Symmetry, 14(11). https://doi.org/10.3390/sym14112304	Malware Analysis and detection using ML algorithms like DecisionTree, CNN, and SVM. Detection accuracy of DecisionTree , CNN, and SVM algorithms compared. and DecisionTree method showed the highest accuracy of 99% for malware detection.
Can Machine Deep Learning Classifiers Detect Zero-Day Malware with High Accuracy[21]	F. Abri, S. Siami-Namini, M. A. Khanghah, F. M. Soltani and A. S. Namin, 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 3252-3259, doi: 10.1109/BigData47090.2019.9006514.	Investigates training algorithms for zero-day malware detection with machine learning. Explores feature selection, clustering, and classification techniques for malware detection. Random forest classifier showed the best accuracy among 34 classifiers. Used Kaggle dataset

Catch them alive A malware detection approach through memory forensics, manifold learning and computer vision[22]	Bozkir, A. S., Tahillioglu, E., Aydos, M., & Kara, I. (2021). Catch them alive:. Computers and Security, 103. https://doi.org/10.1016/j.cose.2020.102166	Recognize malware through memory dump images using computer vision techniques. Improve unknown malware detection through manifold learning and machine learning algorithms. Utilized machine learning algorithms: J48, RBF, Random Forest, XGBoost, SVM.
ZeVigilante: Detecting Zero-Day Malware Using Machine Learning and Sandboxing Analysis Techniques. [23]	Alhaidari, F., Shaib, N. A., Alsafi, M., Alharbi, H., Alawami, M., Aljindan, R., Rahman, A. U., & Zagrouba, R. (2022). Computational Intelligence and Neuroscience, 2022. https://doi.org/10.1155/2022/1615528	ZeVigilante detects Zero-Day malware using ML and sandboxing techniques. Extract API call sequences and PE imports using ML algorithms. Achieve high accuracy in malware detection with various ML classifiers. Utilize RF, NN, DT, kNN, NB, SVM classifiers for detection
When machine learning meets hardware cybersecurity: Delving into accurate zero-day malware detection.[24]	He, Z., Miari, T., Makrani, H. M., (2021). Proceedings - International Symposium on Quality Electronic Design, ISQED, 2021-April, 85–90. https://doi.org/10.1109/ISQED51717.2021.9424330	Focus: Hardware-Supported Malware Detection using Machine Learning for zero-day malware. Approach: Ensemble learning-based technique for enhanced malware detection performance. Present methodology for run-time zero-day HMD using limited HPC features.
Detecting Zero Day Malware[25]	Kumar R, A. H., ka, D. S., Priyanka, G. A., Bindinganavalle Manjunath, N. G., & Professor, A. (n.d.). (IJERT) Volume 08, Issue 05 (May 2019), DOI: 10.17577/IJERTV8IS050368	This paper explains about the different malware analysis techniques namely static, dynamic and hybrid malware analysis techniques. It also presents a Survey on the various existing malware detection systems and proposes a Zero-Day malware detection model based on static analysis and dynamic sandbox analysis and used Weka classification algorithms.
Malware-SMELL A zero shot learning strategy for detecting zero day vulnerabilities.[27]	Barros, P. H., Chagas, E. T. C., Oliveira, L. B., Queiroz, F., & Ramos, H. S. (2022). Computers and Security, 120. https://doi.org/10.1016/j.cose.2022.102785	Develop Malware-SMELL for zero-shot learning malware classification. Enhance class separability in malware detection using visual representation. Addressing the challenge of identifying unknown malware efficiently.

A survey of zero-day malware attacks and its detection methodology.[28]	K. Radhakrishnan, R. R. Menon and H. V. Nath, TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 533-539, doi: 10.1109/TENCON.2019.8929620.	Existing security solutions are inadequate against zero-day malware attacks. Detection methods for malware attacks are summarized in the paper. Zero-day vulnerabilities are exploited through various methods like malicious emails.
Leveraging malicious behavior traces from volatile memory using machine learning methods for trusted unknown malware detection in Linux cloud environments.[29]	Panker, T., & Nissim, N. (2021). International Journal of Knowledge-Based Systems, 226. https://doi.org/10.1016/j.knosys.2021.107095	Trusted framework detects unknown malware in Linux VM cloud-environments accurately. Uses machine learning to leverage informative features from volatile memory dumps. Detects new unknown malware categories and fileless malware effectively. Machine learning algorithms leverage informative features from Linux volatile dumps. Comprehensive set of 171 features extracted from trusted volatile memory dumps. Framework categorizes malware by attack type and works on unknown servers.
A Malware Detection Approach Using Autoencoder in Deep Learning[30]	Xing, X., Jin, X., Elahi, H., Jiang, H., & Wang, G. (2022. IEEE Access, 10, 25696–25706. https://doi.org/10.1109/ACCESS.2022.3155695	Proposed malware detection method using grey-scale images and autoencoder network. which Combines grey-scale malware image representation with autoencoder network for classification. Used Autoencoder network for feature extraction and classification of malware

6. PROPOSED SYSTEM

In this section we propose a system for detection of ZERO DAY Malwares in Virtualized environment using Hybrid approach by combining Memory Forensic Analysis and Machine learning algorithms.

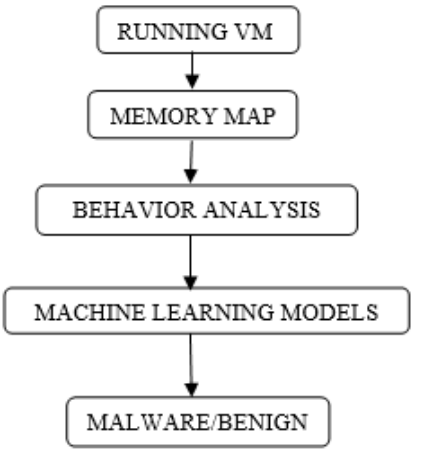

Fig. 3 Proposed system

A zero-day malware, also referred to as next-generation malware, is a type of malicious software that is not yet recognized by security systems due to the absence of specific signatures. A zero-day vulnerability, or 0-day, represents a flaw in a computer system that remains unknown to its developers or those who could potentially address it. Until such vulnerabilities are resolved, they remain open to exploitation by threat actors. An attack that leverages a zero-day vulnerability is termed a zero-day attack. A notable recent instance involved a series of vulnerabilities in Microsoft Exchange, which were addressed by the company in March 2021. Among these was a remote code execution (RCE) vulnerability, leading to the emergence of various zero-day malware variants that took advantage of these weaknesses. One such malware, known as Hafnium, was identified as an information-stealing tool that exploited the Microsoft Exchange vulnerabilities to infiltrate susceptible Exchange servers, resulting in the theft of emails and user credentials.

7. EXPECTED RESULTS

The result of the system would be the detection of zero day malwares in virtualization environment. The metrics can be calculated using number of true positive, false negative, true negative and false negative of the sample. The system will be tested for the existing systems and also to prove that zero day malwares are not detected in existing systems.

8. CONCLUSION

Advanced malware is a serious threat for the internet and user’s computer. The recent wide adoption of Virtualization has also increased the virtualization security concerns.

This review paper gives an overview of the different types of Malware and malware detection techniques, it also provides information on malware detection techniques using memory analysis and machine learning algorithms. Finally, an approach using a combination of both these techniques to detect zero day malwares (unknown malwares) has been proposed. This proposed approach can be very much useful to detect such malwares before they do any harm.

REFERENCES

[1] G A Priyanka , Ashwin Kumar H R , Deepika S , Neha Bindinganavalle, Manjunath G S, 2019, Detecting Zero Day Malware, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 08, Issue 05 (May 2019),

[2] Aslan, O., Ozkan-Okay, M., & Gupta, D. (2021). A review of Cloud-Based Malware Detection System: Opportunities, Advances and challenges. European Journal of Engineering and Technology Research, 6(3), 1–8. https://doi.org/10.24018/ejers.2021.6.3.2372

[3] Fui, N. L. Y., Asmawi, A., & Hussin, M. (2020). A dynamic malware detection in cloud platform. International Journal of Difference Equations, 15(2), 243–258. https://doi.org/10.37622/ijde/15.2.2020.243-258

[4] Kimmell, J. C., Abdelsalam, M., & Gupta, M. (2021). Analyzing machine learning approaches for online malware detection in cloud. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2105.09268

[5] Rabbani, M., Wang, Y. L., Khoshkangini, R., Jelodar, H., Zhao, R., & Hu, P. (2020). A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. Journal of Network and Computer Applications, 151, 102507. https://doi.org/10.1016/j.jnca.2019.102507

[6] Das, Y. (2023, May 31). Cloud Based Malware Detection System Using Support Vector Machine. International Journal for Research in Applied Science and Engineering Technology, 11(5), 7416–7419. https://doi.org/10.22214/ijraset.2023.53253

[7] Abdelsalam, M., Krishnan, R., Huang, Y., & Sandhu, R. (2018, July). Malware Detection in Cloud Infrastructures Using Convolutional Neural Networks. 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). https://doi.org/10.1109/cloud.2018.00028

[8] Aslan, O., Ozkan-Okay, M., & Gupta, D. (2021). Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment. IEEE Access, 9, 83252–83271. https://doi.org/10.1109/access.2021.3087316

[9] Almaraz García, L. E. H., & Acosta Bermejo, R. (2018, December 31). A Method for Malware Analysis by Virtual Machine Introspection Technique. Research in Computing Science, 147(12), 11–20. https://doi.org/10.13053/rcs-147-12-1

[10] Li, C., & Zheng, J. (2021, May 27). API Call-Based Malware Classification Using Recurrent Neural Networks. Journal of Cyber Security and Mobility. https://doi.org/10.13052/jcsm2245-1439.1036

[11] Mishra, P., Verma, I., & Gupta, S. (2020, April). KVMInspector: KVM Based introspection approach to detect malware in cloud environment. Journal of Information Security and Applications, 51, 102460. https://doi.org/10.1016/j.jisa.2020.102460

[12] Patil, R., Dudeja, H., & Modi, C. (2019, June 26). Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. International Journal of Information Security, 19(2), 147–162. https://doi.org/10.1007/s10207-019-00447-w

[13] Wang, X., Zhang, J., Zhang, A., & Ren, J. (2019). TKRD: Trusted kernel rootkit detection for cybersecurity of VMs based on machine learning and memory forensic analysis. Mathematical Biosciences and Engineering, 16(4), 2650–2667. https://doi.org/10.3934/mbe.2019132

[14] https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-zero-day-attack/what-is-zero-day-malware/#ZeroDayVulnerabilities

[15] https://www.getastra.com/blog/security-audit/biggest-ransomware-attacks/

[16] https://www.av-test.org/en/statistics/malware/

[17] https://www.ibm.com/blog/5-benefits-of-virtualization/

[18] Won, D. O., Jang, Y. N., & Lee, S. W. (2023). PlausMal-GAN: Plausible Malware Training Based on Generative Adversarial Networks for Analogous Zero-Day Malware Detection. *IEEE Transactions on Emerging Topics in Computing*, *11*(1), 82–94. https://doi.org/10.1109/TETC.2022.3170544

[19] Jurečková, O., Jureček, M., Stamp, M., di Troia, F., & Lórencz, R. (2024). Classification and online clustering of zero-day malware. *Journal of Computer Virology and Hacking Techniques*. https://doi.org/10.1007/s11416-024-00513-5

[20] Akhtar MS, Feng T. Malware Analysis and Detection Using Machine Learning Algorithms. Symmetry. 2022; 14(11):2304. https://doi.org/10.3390/sym14112304

[21] F. Abri, S. Siami-Namini, M. A. Khanghah, F. M. Soltani and A. S. Namin, "Can Machine/Deep Learning Classifiers Detect Zero-Day Malware with High Accuracy?," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 3252-3259, doi: 10.1109/BigData47090.2019.9006514.

[22] Bozkir, A. S., Tahillioglu, E., Aydos, M., & Kara, I. (2021). Catch them alive: A malware detection approach through memory forensics, manifold learning and computer vision. *Computers and Security*, *103*. https://doi.org/10.1016/j.cose.2020.102166

[23] Alhaidari, F., Shaib, N. A., Alsafi, M., Alharbi, H., Alawami, M., Aljindan, R., Rahman, A. U., & Zagrouba, R. (2022). ZeVigilante: Detecting Zero-Day Malware Using Machine Learning and Sandboxing Analysis Techniques. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/1615528

[24] He, Z., Miari, T., Makrani, H. M., Aliasgari, M., Homayoun, H., & Sayadi, H. (2021). When machine learning meets hardware cybersecurity: Delving into accurate zero-day malware detection. Proceedings - International Symposium on Quality Electronic Design, ISQED, 2021-April, 85–90. https://doi.org/10.1109/ISQED51717.2021.9424330

[25] Kumar R, A. H., ka, D. S., Priyanka, G. A., Bindinganavalle Manjunath, N. G., & Professor, A. (n.d.). Detecting Zero Day Malware. JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 08, Issue 05 (May 2019),DOI: 10.17577/IJERTV8IS050368

[26] Gibert, D., Mateu, C., & Planes, J. (2020). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. In Journal of Network and Computer Applications (Vol. 153). Academic Press. https://doi.org/10.1016/j.jnca.2019.102526

[27] Barros, P. H., Chagas, E. T. C., Oliveira, L. B., Queiroz, F., & Ramos, H. S. (2022). Malware-SMELL: A zero-shot learning strategy for detecting zero-day vulnerabilities. Computers and Security, 120. https://doi.org/10.1016/j.cose.2022.102785

[28] K. Radhakrishnan, R. R. Menon and H. V. Nath, "A survey of zero-day malware attacks and its detection methodology," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 533-539, doi: 10.1109/TENCON.2019.8929620.

[29] Panker, T., & Nissim, N. (2021). Leveraging malicious behavior traces from volatile memory using machine learning methods for trusted unknown malware detection in Linux cloud environments. Knowledge-Based Systems, 226. https://doi.org/10.1016/j.knosys.2021.107095

[30] Xing, X., Jin, X., Elahi, H., Jiang, H., & Wang, G. (2022). A Malware Detection Approach Using Autoencoder in Deep Learning. IEEE Access, 10, 25696–25706. https://doi.org/10.1109/ACCESS.2022.3155695