Journal of Research and Academic Writing
Vol. 1 No. 2 (2024): ISSN (Online): 3007-5343
DOI: https://doi.org/10.58721/jraw.v1i2.785
Security Evaluation Framework for Virtualised Environments

Security Evaluation Framework for Virtualised Environments

Martha Were, Ruppra Satwinder Singh & Jairus Odawa
Masinde Muliro University of Science and Technology, Kenya

Article History
Received: 2024.07.24
Revised: 2024.10.02
Accepted: 2024.10.11
Published: 2024.10.13

Keywords
Attacks
Hypervisor
Resource-Exhaustion
Security
Virtualisation

How to cite:
Were, M., Singh, R. S. & Odawa, J. (2024). Security Evaluation Framework for Virtualised Environments. *Journal of Research and Academic Writing, 1*(2), 24-34.

Copyright © 2024

Abstract
With the expansion of cloud computing, virtual environments remain susceptible to sophisticated security threats, such as hypervisor vulnerabilities, VM escapes, inter-VM attacks, DoS attacks, and malware injections. Hence, ensuring that virtualised environments are secure, has become increasingly crucial. These threats are particularly affecting as many enterprises which have shifted to online services and remote work. This paper examines the existing frameworks which have been designed to address the existing challenges, their gaps and strengths; and proposes an enhanced security framework that can help to mitigate these threats. The framework was developed following an iterative process encompassing several stages. It has the hypervisor layer, virtual machine layer, network layer, management layer, and monitoring and response layer components. The framework aims to enhance detection capabilities, reduce response times, minimize system performance impact, and lower false positive rates while optimising resource utilisation by providing a practical and effective approach to securing virtualised infrastructures, thereby ensuring the resilience and reliability of cloud-based services.

Introduction

Virtualisation utilises software to create digital replicas of servers, applications, data centres, and other hardware components that operate just like their physical counterparts(European Union Agency for Network and Information Security, 2017). Virtualisation is a solution to shrinking IT budgets in today's economy. Organisations worldwide spend billions of dollars yearly on their information technology (IT) infrastructure (hardware and software) and related security. Today's businesses face mounting pressure to lower operational costs while enhancing flexibility, service delivery, and efficiency. Organisations are spending significant time, effort, and resources to accomplish this (STAMFORD, 2021).

In recent years, network virtualisation has grown in popularity. It promotes the instantiation of advantageous settings for developing and assessing new architectures and protocols; it enables the building of network infrastructures specifically customised to the requirements of various network applications. Network virtualisation has many applications; however, sharing communication channels and routing devices raises several security-related issues. Virtual network infrastructures must be protected to be used in actual, large-scale environments (Bays et al., 2015).

Kedia et al. (2013) noted that malicious code injection, side-channel attacks, rootkit attacks, VM sprawl, and insecure VM migration, among others, are some of the security issues that should be addressed when considering virtualisation. For cloud platforms, isolation becomes critical, as customers may share one physical host. In other words, the confidentiality of guest virtual machine (VM) data must be protected from attacks initiated by another guest on the same physical machine.

Similarly, a denial of service (DoS) attack initiated by a VM against a physical host can affect all VMs on the server and should be appropriately mitigated.

Most virtualisation solutions have at least one critical software component, the virtual machine monitor, which can be subject to software bugs that lead to security vulnerabilities. A new class of malware has emerged that targets virtualisation and runs at a privilege level higher than the operating system. It is suppressed by classical techniques such as antivirus software. Some classical security strategies for standalone systems have been weakened or rendered useless by the advent of virtualisation. For virtualised systems, classical security techniques could operate under presumptions that aren't always accurate (Sierra-Arriaga et al., 2020). A good security program must collaborate with a virtualisation administration framework that can supply that data, or it should offer an up-to-date inventory of virtual servers (Sierra-Arriaga et al., 2020).

Related Studies and Research Gaps

Despite advancements, existing security frameworks still have notable gaps and limitations. One major limitation is the lack of real-time threat intelligence sharing, which can delay the detection and mitigation of emerging threats. Studies by Jones and Smith (2023) highlight the need for more collaborative and real-time security solutions that can adapt to evolving threats in virtualised environments. Additionally, research by Williams et al. (2022) indicates that many organisations struggle with the cost and expertise required to deploy and maintain comprehensive security solutions, leading to gaps in their defence mechanisms. Table 1 summarises related literature, detailing the levels of analysis, limitations, technology used, and existing gaps.

Table 1: Related literature review

Research author	**Level of analysis**	**Limitation**	**Technology used for security**	**Existing Gap for Future Research**
(Pearce et al., 2013	hypervisor vulnerabilities and security for Xen and KVM hypervisors.	Does not consider emerging threats	Secure VM configuration, hypervisor hardening, VM monitoring	Integration of advanced threat detection mechanisms
(Li et al.,2021)	vulnerabilities in hypervisors	Limited focus on real-time data processing	Encryption, data masking, secure storage solutions	Real-time security measures for big data in cloud environments
(Xiao et al.,2022)	empirical analysis of VM escape incidents	insufficient isolation mechanisms and outdated software versions	Access control, regular audits, secure backup	Cost-effective security measures for cloud environments
(Tumpe & Jagdev, 2014)	security issues in cloud computing	Does not consider emerging threats Focuses on theoretical aspects without practical examples	Encryption, secure interfaces, continuous monitoring	Practical application of security solutions
(Tank et al., 2022)	internal and external VM vulnerabilities	Lack of focus on emerging technologies	Strong encryption, access control, compliance frameworks	Security measures for IoT and AI in cloud environments
(Zhang et al., 2011)	rootkit detection technology based on the KVM hypervisor	Does not consider evolving threats	CloudSkulk	Addressing evolving and advanced persistent threats

(Chen and Wang, 2023)	hypervisor security framework	Lack of practical implementation details	anomaly detection algorithms to identify and mitigate potential threats in real-time	Implementation challenges and solutions in real-world scenarios
(Liu and Zhang, 2023)	enhanced VM isolation protocol that uses hardware-based isolation in conjunction with software-level checks	Tailored security solutions for specific security threat	multi-layered isolation strategies	Practical application and performance analysis
(European Union Agency for Network and Information Security, 2017)	virtualisation vulnerabilities	Addresses general security issues, not specific No real time threat detection Does not address resource utilization Limited focus on evolving threats Limited to European context	Encryption, access control, regular security assessments	Global applicability and emerging threats
(Rupra & Omamo, 2020)	A Cloud Computing Security Assessment Framework for Small and Medium Enterprises.	-developed for small and medium enterprises -lack of real-time threat intelligence sharing	Backups, encryption, 2 factor authentication and transport later security (TLS)	Cost-effective and efficient security solutions
(Gupta and Singh, 2023)	a secure inter-VM communication framework	25% reduction in data breaches compared to existing solutions	uses encryption and continuous monitoring to detect and prevent unauthorized data transfers	Real-time detection and mitigation techniques
(Zhao et al., 2023)	AI-driven security framework	Not clear when it comes to system performance	Machine learning algorithms	Addressing evolving and advanced persistent threats

Methodology

Design Science Research (DSR) is a methodology to create and evaluate artifacts designed to solve identified problems. It focuses on the iterative development and refinement of artifacts through rigorous testing and evaluation. The core principles of DSR involve problem identification, artifact design, evaluation, and refinement, ensuring that the developed framework is both practical and theoretically sound (Hevner et al., 2004). The study adopted a design science research framework, integrating qualitative and quantitative methods. This encompassed a narrative literature review for secondary research to identify existing challenges, while primary data was collected through survey and virtualisation simulation. For simulation, the study used VMware to manage virtual environments, User Mode Linux to develop and test kernels, and Wireshark to monitor the network. Google Forms were used to create survey questionnaires that targeted IT security professionals. A

sample size of 462 participants was determined using (Cochran, 1977) the formula from a global population 10,000. This was achieved through stratified random sampling. Qualitative interviews involved 30 security experts, achieved through video conferencing. They were ensuring a comprehensive approach to both understanding and addressing security issues. Data was systematically gathered, providing reliability (pilot tests, structured interviews) and validity (triangulation, realistic attack scenarios in simulations): the research combined theory and practical tools to generate robust, actionable solutions. Due to time and resource constraints, only a few participants were selected for interviews and surveys. The study also relied on a few databases for narrative literature review, meaning that other resources could uncover more mitigation measures for security challenges in virtualised environments.

Results

Review of existing frameworks and protocols

SELinux (Security-Enhanced Linux) is a security module for Linux that provides a mechanism for supporting access control security policies, including mandatory access controls (MAC). It is integrated into many Linux distributions and offers a robust framework for restricting users and processes to the minimum permissions required. SELinux is highly effective in enforcing strict security policies and preventing unauthorised access. Studies show it significantly reduces the attack surface by controlling process interactions (Karajagi & Garg, 2015). The main limitation of SELinux is its complexity. Administrators often find it challenging to configure and manage, leading to potential misconfigurations (Bai & Zhai, 2012).

AppArmor is another Linux security module that provides MAC by binding access control attributes to programs rather than users. It offers an easier-to-use alternative to SELinux. AppArmor effectively confines programs to a limited set of resources, thereby reducing the potential damage from exploits. It is considered user-friendly and more accessible to deploy than SELinux (Bäckman & Hagfjäll, 2017). AppArmor's main limitation is that it is not as flexible or comprehensive as SELinux regarding policy enforcement (Delbugio & Vijay K. Madisetti, 2024).

Hypervisor-Specific Security is security mechanisms specific to hypervisors (e.g., Xen, VMware), including built-in security modules, introspection tools, and regular patching processes. These mechanisms are effective in isolating VMs and preventing inter-VM attacks. Hypervisor introspection tools, for example, provide deep visibility into VM activities (Bhongade & Karande, 2015). The effectiveness of hypervisor security heavily depends on timely updates and patches. Delays in patching can leave systems vulnerable (Urias et al., 2017).

Network Segmentation and Micro-Segmentation involve dividing a network into smaller segments to improve security and performance. Micro-segmentation takes this further by applying fine-grained policies to individual workloads. These strategies significantly enhance security by limiting the spread of malware and controlling east-west traffic within the data centre (Al-Ofeishat & Rafat, 2024). Implementation complexity and the need for robust management tools are significant challenges (Klein, 2019).

Encryption Protocols employ protocols like TLS (Transport Layer Security) and IPSec (Internet Protocol Security) to encrypt data in transit and at rest, ensuring data confidentiality and integrity. Encryption protocols are highly effective in preventing data breaches and providing secure communications. Studies highlight their role in protecting sensitive information (Huang, 2024). Performance overhead and fundamental management complexities are notable drawbacks (Barker et al., 2020).

The narrative literature review highlights that frameworks like SELinux and AppArmor provide robust security mechanisms for Linux environments, though they vary in complexity and comprehensiveness. Hypervisor-specific security tools offer effective isolation but are heavily reliant on timely updates. Network segmentation strategies, including micro-segmentation, significantly enhance security but require sophisticated management tools. Encryption protocols are crucial for data protection despite their performance impacts. A common theme across these frameworks is the balance between security effectiveness and complexity. SELinux, while comprehensive, is often underutilised due to its complexity. AppArmor, though more accessible to use, does not offer the same level of policy enforcement. Hypervisor security's dependence on timely patches presents a risk if not managed effectively. Network segmentation's complexity necessitates advanced tools and expertise. Encryption protocols, while essential, bring performance and management challenges.

Survey Data Analysis

As organisations increasingly rely on virtualisation technologies, this section explores the effectiveness of current security frameworks. The analysis focuses on the adoption rates, challenges, and perceived effectiveness of mitigation strategies. Metrics such as response rates and statistical assessments reveal trends crucial for enhancing security practices in virtualised environments. Using stratified sampling, 462 Google forms were distributed, yielding a 76% response rate (350 responses). Respondents rated mitigation strategies from 1 (ineffective) to 5 (very effective). High ratings were noted for Access Controls and Authentication (4.6), Regular Updates and Patch Management (4.5), and Encryption (4.4), all considered essential for securing virtualised environments. These strategies also had high adoption rates: Access Controls and Authentication (91.4%), Encryption (88.6%), and Regular Updates (85.7%). Other strategies like Network Segmentation (4.2), Intrusion Detection (4.3), and Virtual Machine Isolation (4.0), though slightly less popular, were still effective. Regarding challenges, Network Segmentation (3.2) and Virtual Machine Isolation (3.3) were rated more challenging than others. Regular updates, patch management, access controls, and authentication faced lower challenges despite being highly effective.

Challenges in Implementing Security Measures

The survey revealed significant barriers to implementing effective cybersecurity in virtualised environments. Lack of skilled personnel (75%) was the most cited issue, followed by continuous updating (65%), high implementation cost (60%), and the complexity of security tools (55%). Integration issues (50%) further complicated security efforts, indicating a need for enhanced training, more straightforward tools, and better interoperability among systems.

Effectiveness of Mitigation Strategies

Respondents rated strategies like Hypervisor Security, VM Isolation, and Network Segmentation based on their effectiveness. While 20% found hypervisor security very effective, the majority rated it as effective or moderately effective. Similarly, 45% of respondents found VM isolation effective or very effective, though 20% still had concerns about its efficacy. Overall, Intrusion Detection Systems (IDS) were perceived as the most effective, with 60% of respondents rating them as very effective or effective.

Interview Data Analysis

Interview Design and Participant Selection

The interview process was designed to gather qualitative insights from IT security professionals, focusing on current mitigation strategies and developing a security-based framework for virtualised environments. Participants were selected based on professional roles, experience (minimum of five years in IT security), industry (finance, healthcare, technology, and government), and geographical diversity. The 30 participants were interviewed using video conferencing tools (Zoom and Microsoft

Teams), each lasting 45 to 60 minutes. The interviews were recorded, transcribed, and analysed using thematic analysis to identify common themes.

The participants represented various cybersecurity professionals across different industries and regions. They were mainly mid-career and senior professionals with 6-25 years of experience. Industry representation was equally distributed, ensuring that findings were applicable across multiple sectors, and a range of roles (e.g., Senior Security Analyst, Chief Information Security Officer, Penetration Tester) enriched the study.

Thematic Analysis of Interviews
The thematic analysis revealed six critical themes regarding security in virtualised environments: hypervisor vulnerabilities, VM escape risks, Inter-VM risks, Inter-VM attacks, the effectiveness of current mitigation strategies, challenges in implementing security measures and recommendations for improving security frameworks.

The interviews provided valuable insights into the complexities and challenges of securing virtualised environments. Key takeaways included prioritising hypervisor security, strengthening isolation mechanisms, adopting advanced automation tools, and addressing the skills gap through training. These themes align with recommendations for a more adaptive and holistic security framework in virtualised infrastructures.

Recommendations for Improving Existing Security Frameworks:

1. *Reduce attack surface:* Implement micro-hypervisors to minimize complexity.
2. *Strengthen isolation:* Enhance VM isolation to prevent escape and inter-VM attacks.
3. *Advanced network segmentation:* Apply more sophisticated segmentation strategies.
4. *Integrate AI:* Use AI for real-time threat detection and response.
5. *Invest in training:* Provide continuous education for IT security professionals.
6. *Zero-trust approach:* Verify every access request, regardless of its origin.
7. *Vendor collaboration:* Encourage collaboration for holistic security solutions.

These recommendations aim to address existing gaps in security frameworks, improving resilience in virtualised environments. Besides, they made the basis of the framework development.

Proposed Framework Development

Design Science Research Approach
The development of the security framework followed an iterative process encompassing several stages:

1. *Problem Identification and Objectives Definition:* The first step involved identifying the security issues in virtualised environments through a comprehensive literature review, surveys, and interviews with IT security professionals. Objectives were defined to address these security issues, including improving hypervisor security, enhancing VM isolation, and preventing inter-VM attacks.
2. *Artefact Design:* Based on the identified problems and objectives, an initial version of the security framework was designed. The framework incorporated multiple layers of security measures, including micro-hypervisors, advanced isolation techniques, and AI-driven threat detection systems. The design also included protocols for continuous monitoring and updating, ensuring the framework remains robust against evolving threats.

3. *Development and Implementation:* The initial design was developed into a functional prototype using VMware, Virtual Box, and Wireshark tools. Coding for the security measures and protocols was done using development environments primarily in C++ and visualised using Python.
4. *Testing:* The prototype was tested in a controlled simulation environment using a virtual UML monitor. Various attack scenarios, such as hypervisor breaches, VM escapes, and inter-VM attacks, were simulated to evaluate the framework's effectiveness. Performance metrics such as system response time, resource usage, and detection rates were recorded.
5. *Evaluation and Refinement:* The testing phase provided valuable data on the framework's strengths and weaknesses. Based on the review, the framework was refined to address any identified shortcomings. This included optimising the code for better performance, enhancing isolation techniques, and improving the AI algorithms for more accurate threat detection. The iterative process of testing and refinement was repeated multiple times, each cycle leading to improvements in the framework's robustness and effectiveness.
6. *Finalisation and Documentation:* A final version of the security framework was developed after several iterations. Comprehensive documentation detailing the framework's architecture, implementation procedures, and usage guidelines was created. The final framework was ready for deployment in real-world virtualised environments, providing enhanced security against various threats.

Components of the Security Framework

The proposed security framework for virtualised environments addresses prevalent security threats such as hypervisor vulnerabilities, VM escape, and inter-VM attacks. It consists of several key components, each contributing to a multi-layered security architecture.

i. *Micro-Hypervisor Layer*

It is a minimalistic hypervisor designed to reduce the attack surface. Unlike traditional hypervisors, a micro-hypervisor has a smaller codebase, making it less vulnerable. Manages the essential functions of virtual machines (VMs) while delegating complex tasks to higher-level components. The reduced complexity and smaller codebase of a micro-hypervisor significantly decrease the attack surface compared to traditional hypervisors (Vasudevan, 2019). This selection enhances the overall security posture by minimising potential vulnerabilities.

ii. *VM Isolation Mechanism*

Advanced isolation techniques that ensure each VM operates in a completely separate environment prevent VM escape attacks by ensuring that actions within one VM do not affect others. Isolation is fundamental to the security of virtualised environments. Advanced isolation techniques, such as hardware-assisted virtualisation (Intel VT-x, AMD-V), ensure robust separation of VMs, preventing unauthorised access and VM escape attacks. (Di Pietro & Lombardi, 2018)

iii. *AI-Driven Threat Detection System*

An artificial intelligence system continuously monitors the virtualised environment for unusual patterns indicative of security threats, enhances real-time detection of potential attacks, and automates the response mechanisms. AI systems can analyse large volumes of data and identify patterns that might indicate security threats. Machine learning algorithms are particularly effective in detecting anomalies and evolving threats that traditional signature-based systems might miss (Sommer & Paxson, 2010).

iv. *Inter-VM Communication Security*

Secure communication protocols that manage data exchanges between VMs ensure that inter-VM communications are encrypted and authenticated, preventing eavesdropping and tampering. Ensuring secure communication between VMs is critical to avoid data breaches. Encryption and authentication protocols like TLS (Transport Layer Security) ensure that data exchanged between VMs remains confidential and untampered (Dierks & Rescorla, 2008).

v. *Continuous Monitoring and Auditing Tools*

Tools that provide continuous monitoring and periodic audits of the virtual environment detect and log suspicious activities, ensuring compliance with security policies. Constant monitoring allows for the timely detection of suspicious activities, while regular audits help maintain compliance and identify security gaps. Tools like Wireshark for network monitoring and Nagios for system monitoring provide comprehensive visibility into the virtual environment (Jani et al., 2018; Soepeno, 2023).

vi. *Patch Management System*

An automated system for deploying security patches and updates to VMs and the hypervisor ensures that all virtual environment components are up to date with the latest security patches, reducing the risk of known vulnerabilities. Keeping all software components up to date is crucial for security. Automated patch management systems ensure that all VMs and hypervisors receive the latest security updates promptly, mitigating the risk of exploits based on known vulnerabilities (Yong-Xiang, 2018).

The selection of specific technologies and protocols is based on their proven effectiveness and relevance to the identified security challenges, ensuring the framework is practical and theoretically sound.

Architecture of the Security Framework

The first layer of the architecture is the Hypervisor Layer, the foundation of the virtualised environment, which is responsible for managing multiple virtual machines (VMs) and ensuring resource allocation. It has tools and protocols to monitor the integrity of the hypervisor, ensuring it has not been compromised, and it provides strict access control policies to manage who can interact with the hypervisor and perform administrative functions.

The second layer of the architecture is the Virtual Machine (VM) Layer, which consists of multiple isolated VMs running on top of the hypervisor. It ensures that VMs are isolated from each other to prevent VM escape attacks and monitors VMs for signs of intrusion or malicious activity. It has security patching that performs regular updates and patches to the operating systems and applications running within the VMs.

The third layer of the architecture is the Network Layer, which provides networking components that connect VMs and the external network. It has configurable firewalls that control traffic between VMs and external networks. It divides the network into segments to limit the spread of attacks and provide secure communication between VMs and between the VMs and the external network using encryption protocols like SSL/TLS.

The fourth layer of the architecture is the Management Layer, which provides interfaces and tools for managing the virtualised environment. This has management access control that ensures that only authorised users can access management interfaces. Comprehensive logging of all management activities for auditing and forensic analysis and a Multi-Factor Authentication (MFA) that enhances security for accessing management interfaces.

The last layer of the architecture is the Monitoring and Response Layer, which provides continuous monitoring of the virtualised environment to detect and respond to security incidents. The layer has security features, including real-time tracking that has tools like Wireshark and Nagios for real-time

monitoring of network traffic and system performance, incident response automation, which are automated tools to respond to detected security incidents, such as isolating compromised VMs and threat intelligence integration, which incorporates threat intelligence feeds to stay updated on the latest threats and vulnerabilities. Combined with the critical construct, this was summarised and diagrammatic visualised as the framework architecture in Figure 4.3.

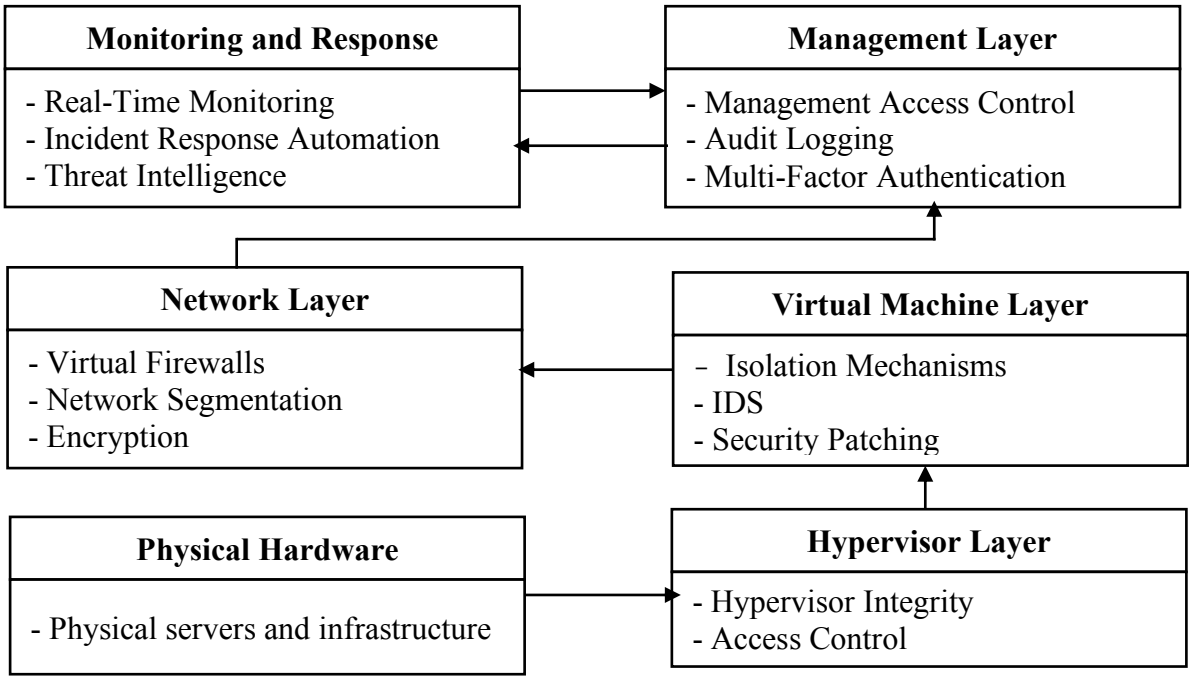

Figure 4.3: SBFVE Framework Architecture (Author (2024)

This framework ensures a comprehensive approach to securing virtualised environments by integrating multiple security measures and control layers. Physical Hardware represents the physical servers and infrastructure that provide the computational resources.

Discussion of the Findings

This section integrates the findings from the literature review, surveys, and interviews on security threats and mitigation strategies in virtualised environments.

Comparison and Contrast of Different Data Sources

Across all data sources—literature, surveys, and interviews—critical threats such as hypervisor vulnerabilities, VM escape, and inter-VM attacks were consistently identified. While the literature highlighted theoretical threats and mitigation strategies like micro-hypervisors and zero-trust models, surveys showed practical challenges, such as the complexity and cost of implementing these measures. Interviews provided real-world examples, emphasising practical difficulties, the need for continuous updates, and skilled personnel to maintain security.

The literature emphasised hypervisor vulnerabilities, and survey data confirmed that hypervisor security remains an organisation's top concern. Both interviews and surveys pointed out that current isolation mechanisms are insufficient to prevent VM escape and inter-VM attacks entirely. Network segmentation was frequently suggested in interviews as a viable mitigation strategy for inter-VM attacks, complementing the literature's recommendations on isolation techniques.

Implications for Security in Virtualised Environments

The integrated findings underscore the need for improved security in virtualised environments. Practitioners must prioritise hypervisor security, enhance isolation techniques, and address skills gaps through training. Additionally, AI-driven threat detection and automation offer promising solutions for improving security efficiency.

Policymakers need to establish and enforce standards that promote best practices, continuous training, and vendor collaboration to develop more effective and integrated security frameworks.

Conclusion

The study concludes that virtualised environments are susceptible to unique security threats that require specialised frameworks. The proposed security framework effectively addresses these challenges by enhancing detection, response, and resource optimisation. The framework's integration of advanced monitoring tools and automated response mechanisms significantly improves security posture in virtualised environments.

References

Al-Ofeishat, H. A., & Rafat, A. (2024). Build a secure network using segmentation and micro-segmentation techniques. *International Journal of Computing and Digital Systems*, *16*(1), 1499–1508. https://doi.org/10.12785/ijcds/1601111

Bäckman, M., & Hagfjäll, F. (2017). *Application security for embedded systems*.

Bai, J., & Zhai, G. (2012). Study on analysis for SELinux security policy. *2012 International Conference on Systems and Informatics, ICSAI 2012*, *Icsai*, 1231–1235. https://doi.org/10.1109/ICSAI.2012.6223257

Barker, E., Dang, Q., Sheila, F., Scarfone, K., & Wouters, P. (2020). Guide to IPsec VPNs. *Special Publication (Nist SP) - 800-77r1*, 166. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf%0Ahttp://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P., & Mauro Madeira, E. R. (2015). Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications*, *6*(1), 1–19. https://doi.org/10.1186/s13174-014-0015-z

Bhongade, P., & Karande, P. S. C. (2015). Securing virtual machine via virtual machine introspection. *International Journal of Innovative Science, Engineering & Technology*. 2(12), 968–971.

Cochran, W. G. (1977). *Sampling techniques* (3rd edition). John Wiley & Sons.

Delbugio, J. M., & Vijay K. Madisetti. (2024). Enhanced memory-safe linux security modules (eLSMs) for improving security of docker containers for data centers. *Journal of Software Engineering and Applications*, *17*(5).

Di Pietro, R., & Lombardi, F. (2018). Virtualisation technologies and cloud security: Advantages, issues, and perspectives. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11170 LNCS*, 166–185. https://doi.org/10.1007/978-3-030-04834-1_9

Dierks, T., & Rescorla, E. (2008). The transport layer security protocol. *Association for Computing Machinery*. https://doi.org/https://doi.org/10.17487/RFC5246

European Union Agency for Network and Information Security. (2017). Security aspects of virtualisation. In *ENISA Website* (Issue February). https://doi.org/10.2824/955316

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Huang, H. (2024). Research on the application of data encryption technology in computer network communication security. *Applied Science and Innovative Research*, *8*(2), pg80.

https://doi.org/10.22158/asir.v8n2p80

Jani, B., Jain, K., & Vishwakarma, N. (2018). Network monitoring tools and technologies. *Ijcrt*, *6*(2), 2320–2882. www.ijcrt.org

Karajagi, V., & Garg, M. (2015). *SELinux Integration into Linux Kernel* . *6*(4), 3388–3391.

Kedia, P., Nagpal, R., & Pal Singh, T. (2013). A survey on virtualisation service providers, security issues, tools and future trends. *International Journal of Computer Applications*, *69*(24), 36–42. https://doi.org/10.5120/12123-8491

Klein, D. (2019). Micro-segmentation: securing complex cloud environments. *Network Security*, *3*, 6–10. https://doi.org/10.1016/S1353-4858(19)30034-0

Rupra, S. S., & Omamo, A. (2020). A cloud computing security assessment framework for small and medium enterprises. *Journal of Information Security*, *11*(04), 201–224. https://doi.org/10.4236/jis.2020.114014

Sierra-Arriaga, F., Branco, R., & Lee, B. (2020). Security issues and challenges for virtualisation technologies. *ACM Computing Surveys*, *53*(2). https://doi.org/10.1145/3382190

Soepeno, R. (2023). Wireshark: An effective tool for network analysis. *CYBV - Introductory Methods of Network Analysis*, *October*, 1–15. https://doi.org/10.13140/RG.2.2.34444.69769

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *Proceedings - IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

STAMFORD, C. (2021). *Gartner Forecasts Worldwide IT Spending to Grow 6.2% in 2021*. Gartener. https://www.gartner.com/en/newsroom/press-releases/2020-01-25-gartner-forecasts-worldwide-it-spending-to-grow-6-point-2-percent-in-2021

Tank, D., Aggarwal, A., & Chaubey, N. (2022). Virtualisation vulnerabilities, security issues, and solutions: a critical study and comparison. *International Journal of Information Technology (Singapore)*, *14*(2), 847–862. https://doi.org/10.1007/s41870-019-00294-x

Tumpe, M., & Jagdev, B. (2014). Investigating security issues in cloud computing. *Investigating Security Issues in Cloud Computing*. doi:10.1109/CISIS.2014.21

Urias, V. E., Stout, W. M. S., Loverro, C., & Young, J. W. (2017). Hypervisor assisted forensics and incident response in the cloud. *Proceedings - 2016 16th IEEE International Conference on Computer and Information Technology, CIT 2016, 2016 6th International Symposium on Cloud and Service Computing, IEEE SC2 2016 and 2016 International Symposium on Security and Privacy in Social Netwo*, 768–775. https://doi.org/10.1109/CIT.2016.104

Vasudevan, A. (2019). Micro-Hypervisors: What? Why?. In *Practical Security Properties on Commodity Computing Platforms* (p. pp 1-10). Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-030-25049-2_1

Yong-Xiang, H. (2018). A study on the security of patch management in a cloud computing environment. *Proceedings - 2018 4th Annual International Conference on Network and Information Systems for Computers, ICNISC 2018*, 278–282. https://doi.org/10.1109/ICNISC.2018.00063

Zhang, Y., Juels, A., Oprea, A., & Reiter, M. K. (2011). HomeAlone: Co-residency detection in the cloud via side-channel analysis. *Proceedings - IEEE Symposium on Security and Privacy*, 313–328. https://doi.org/10.1109/SP.2011.31