International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Cloud Computing Security Using Hardware Virtualization with Secure Hypervisors

Zareena Sulthana[1]

Submitted: 26/03/2020 Accepted: 25/05/2020

Abstract: As the adoption of cloud computing continues to surge, ensuring robust security measures becomes paramount to safeguard sensitive data and maintain user trust. This paper proposes a novel approach to enhance cloud computing security leveraging hardware virtualization alongside secure hypervisors. Traditional cloud security solutions often rely on software-based defenses, which may be vulnerable to sophisticated cyber threats. By integrating hardware virtualization, which provides isolated execution environments for virtual machines (VMs), and secure hypervisors, capable of enforcing strict access controls and monitoring VM behaviour, this research addresses critical security challenges in cloud environments. The proposed system offers several advantages, including enhanced isolation between VMs, reduced attack surface, and improved detection and mitigation of malicious activities. Furthermore, by leveraging hardware-based security features, the system can protect sensitive workloads even in the presence of compromised software layers. Performance evaluation results demonstrate the efficacy of the proposed approach (HV-XSM) in mitigating various security threats commonly encountered in cloud computing environments. Overall, this research contributes to the advancement of cloud security by leveraging hardware virtualization and secure hypervisors to create a robust defense mechanism against evolving cyber threats.

Keywords: *cloud computing, security, hardware virtualization, hypervisors, cyber threats*

1. Introduction

Cloud computing has emerged as a transformative force in the modern digital landscape, offering unparalleled scalability, flexibility, and cost-efficiency for businesses and individuals alike [1]. By leveraging distributed computing resources over the internet, cloud platforms enable organizations to offload their computational tasks, storage needs, and infrastructure management to third-party service providers. This paradigm shift has revolutionized the way businesses operate, allowing them to focus on their core competencies while leveraging the vast resources offered by cloud service providers.

However, alongside the myriad benefits of cloud computing, there exist significant security challenges that must be addressed to ensure the integrity, confidentiality, and availability of data and applications hosted in the cloud [2,3]. As organizations increasingly migrate their critical workloads and sensitive data to cloud environments, safeguarding against cyber threats, data breaches, and unauthorized access becomes paramount [4]. Traditional security measures, such as firewalls, intrusion detection systems, and encryption, provide a baseline level of protection but may fall short in addressing the evolving threat landscape characterized by sophisticated cyber attacks and persistent adversaries [5].

[1]*Senior Lecturer, Computer Science,*
Balaji Institute of Technology and Science,
Telangana
Email: lecturer.zareena12d0@gmail.com

In recent years, hardware virtualization has emerged as a cornerstone technology for enhancing the security posture of cloud computing environments [6]. By abstracting physical hardware resources and providing isolated execution environments for virtual machines (VMs), hardware virtualization enables stronger isolation between workloads, reducing the risk of cross-VM attacks and lateral movement by malicious actors. Furthermore, the advent of secure hypervisors, capable of enforcing strict access controls, monitoring VM behaviour, and leveraging hardware-based security features, has further bolstered the security capabilities of cloud platforms.

Traditional security approaches, such as firewalls and encryption, have proven inadequate in addressing the evolving threat landscape of cloud computing. Hackers are employing sophisticated techniques to exploit vulnerabilities in virtualized environments, posing significant challenges to data protection efforts. In response to these challenges, there has been a growing emphasis on leveraging hardware virtualization and secure hypervisors to fortify cloud computing security [7].

Hardware virtualization, a technology that enables multiple virtual machines (VMs) to run concurrently on a single physical server, serves as the foundation for cloud computing infrastructure [8]. By abstracting the underlying hardware resources, virtualization enhances resource utilization and facilitates dynamic allocation of computing resources. However, the shared nature of virtualized environments introduces security risks, as compromising

one VM can potentially jeopardize the security of others co-hosted on the same physical server.

Secure hypervisors, specialized software responsible for managing and orchestrating VMs, play a pivotal role in mitigating these risks. Unlike traditional hypervisors, which prioritize performance over security, secure hypervisors are designed with security as a primary consideration. They employ various techniques, such as memory isolation, privilege separation, and code integrity checks, to prevent unauthorized access and protect VMs from malicious activities.

This paper proposes a novel approach to enhance cloud computing security through the synergistic combination of hardware virtualization and secure hypervisors. Building upon existing research in the field of virtualization-based security, our approach aims to address critical security challenges faced by cloud environments while leveraging the inherent strengths of hardware-based security mechanisms. By providing a comprehensive analysis of the proposed solution's performance, effectiveness, and scalability, this research contributes to the advancement of cloud security and lays the foundation for future research in this domain.

The remainder of this paper is organized as follows: Section 2 provides a detailed overview of the existing security challenges in cloud computing environments and discusses the limitations of traditional security measures. Section 3 presents the conceptual framework of our proposed approach, outlining the key components and mechanisms employed to enhance cloud security. Section 4 delves into the technical implementation details of hardware virtualization and secure hypervisors, highlighting the integration of hardware-based security features and the mitigation of common attack vectors. The performance evaluation results, demonstrate the efficacy of the proposed approach in mitigating various security threats commonly encountered in cloud environments. Section 5 concludes the paper with a summary of key contributions and insights.

In summary, this paper presents a holistic approach to enhancing cloud computing security through the adoption of hardware virtualization with secure hypervisors. By leveraging hardware-based security features and providing stronger isolation between VMs, our proposed solution offers a robust defense mechanism against evolving cyber threats, thereby enabling organizations to securely harness the benefits of cloud computing without compromising on security.

2. Literature Review

A new approach was suggested by [9] to safeguard guest VMs, even when operating under an untrusted hypervisor. This method relies on secure hardware to provide memory isolation, which is considered more resilient compared to software-based hypervisors. The proposed mechanism enhances existing hardware support for memory virtualization through nested paging, incurring a minimal additional hardware expense. The paper outlines a prototype implementation utilizing system management mode. Even though the current system management mode lacks inherent security functions and may compromise performance and comprehensive protection, the prototype demonstrates the viability of the proposed design.

The paper [10] delves into an examination of various methods aimed at addressing the security challenges associated with hypervisors. The author intends to contribute their own solution to enhance the security of hypervisor-based architectures. Their approach combines elements from two existing methodologies: leveraging the advantages of hyperwall architecture while simultaneously ensuring protection against threats to hypervisor security.

[11] Emphasized the critical role of risk management and security awareness, particularly in light of inadequate protection measures that exacerbate challenges in detecting and preventing information leaks. Findings highlighted data management, external attacks, and security training and awareness as the top three concerns regarding CBOS security. These risks were thoroughly examined alongside strategies implemented to mitigate them. Additionally, a comparative assessment in a similar setting was conducted to evaluate the effectiveness of these strategies in risk reduction. This research holds significant value for organizations across Sudan, particularly for CBOS, offering actionable insights into enhancing security measures.

[12] proposed their own contribution to increase security in hypervisor related architectures. Combining two distinct approaches within a single platform offers users a customized solution to address their security needs while minimizing resource wastage for the provider. However, this hybrid approach requires significant refinement, particularly regarding the critical status table component. Currently, manual filling of this table introduces the potential for errors. Thus, implementing an automatic mechanism to populate the table based on SLA classification could greatly enhance efficiency and accuracy, leading to substantial benefits.

[13] introduced a security architecture with two levels designed to distinguish between MITM (Man-in-the-Middle) attacks and TOCTTOU (Time-of-Check to Time-of-Use) attacks. The model employs a waiting time of 10.3 seconds to mitigate all TOCTTOU attacks effectively. Initially, the architecture utilizes a predefined SSL (Secure Sockets Layer) at the first level to establish a secure connection between the host and destination. Subsequently, at the second level, a verification module examines the data collected before the SSL connection. The results demonstrate significant time improvements compared to RSA (Rivest-Shamir-Adleman). This proposed framework can be packaged and employed as a module to safeguard collected data within the QEMU/KVM virtual environment.

3. Methodology

Cloud computing has transformed the way businesses operate by providing on-demand access to computing

resources over the Internet. This paradigm shift has enabled organizations to scale their operations rapidly, innovate more efficiently, and reduce infrastructure costs. However, along with the numerous benefits, cloud computing also introduces significant security challenges. As sensitive data traverses networks and resides in shared infrastructure, ensuring robust security measures becomes paramount to safeguarding data integrity, confidentiality, and availability.

Traditional cloud security solutions often rely on software-based behaviour, which may not provide sufficient protection against sophisticated cyber threats. These solutions are inherently vulnerable to attacks targeting software vulnerabilities, configuration errors, and insider threats. To address these challenges, there is a growing need to explore innovative approaches that leverage hardware-based security mechanisms to enhance cloud computing security.

Hardware virtualization technology serves as a foundational building block for enhancing cloud security [14]. By abstracting physical hardware resources and creating isolated execution environments, known as virtual machines (VMs), hardware virtualization enables organizations to achieve stronger isolation between workloads. Each VM operates independently of others, reducing the risk of cross-VM attacks and unauthorized access to sensitive data. Furthermore, hardware virtualization improves resource utilization and enables workload mobility, facilitating dynamic resource allocation and scaling in cloud environments.

Secure hypervisors complement hardware virtualization by enforcing strict access controls and monitoring VM behaviour to detect and mitigate security threats. Secure hypervisors implement fine-grained access control mechanisms, restricting unauthorized access to VM resources and enforcing security policies. By continuously monitoring VM activity, secure hypervisors can detect deviations from normal behaviour, such as suspicious network traffic or unauthorized access attempts, and trigger proactive security responses. Additionally, secure hypervisors provide visibility into VM interactions and facilitate forensic analysis in the event of security incidents.

The integration of hardware-based security features further enhances the security posture of cloud infrastructure. Technologies such as Intel Software Guard Extensions (SGX) or AMD Secure Encrypted Virtualization (SEV) provide hardware-enforced memory encryption and isolation, protecting sensitive workloads and data even in the presence of compromised software layers. By leveraging these features, organizations can mitigate the risk of data breaches, insider attacks, and malicious software exploits.

Performance evaluation is critical to assessing the efficacy of the proposed approach in enhancing cloud computing security. Performance metrics such as threat detection rate, overhead analysis, and scalability provide insights into the system's effectiveness in mitigating security threats while minimizing performance impact. Experimental evaluations conducted in realistic cloud computing environments help validate the proposed approach's feasibility and identify areas for optimization.

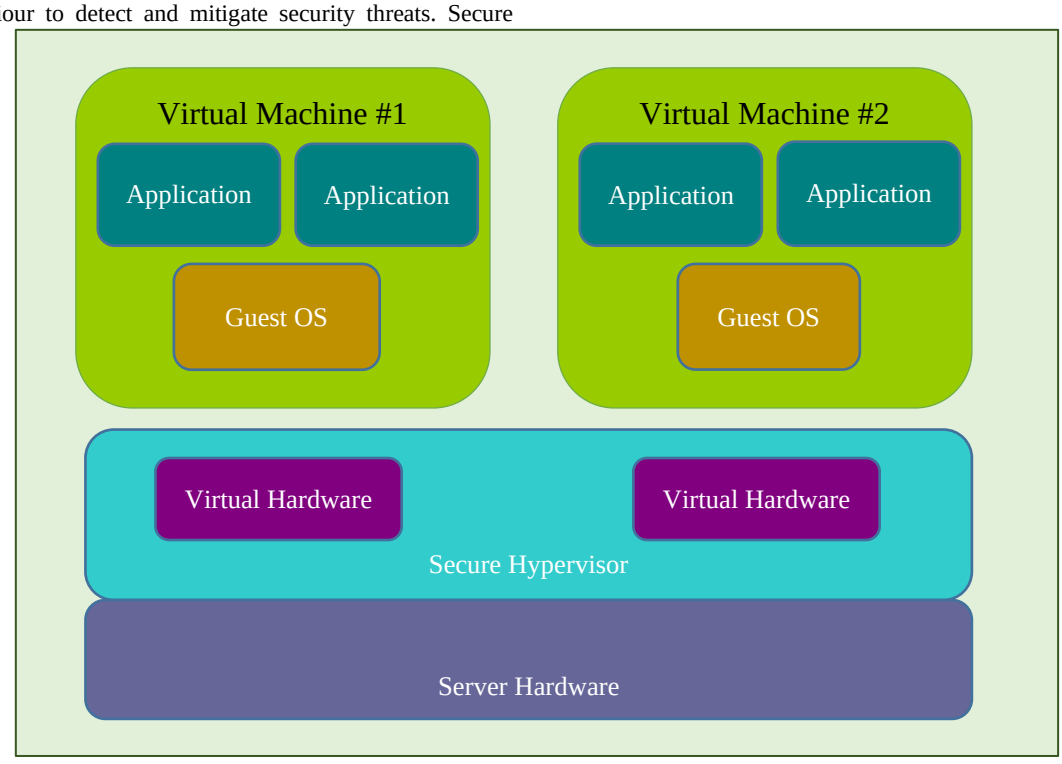

Fig. 1. Proposed Hardware Virtualization

Latency and throughput are important performance metrics in computing systems, including those utilizing hardware virtualization and secure hypervisors. Here are the equations for calculating latency and throughput:

Latency is the time taken for a data packet to travel from the source to the destination and back again. In the context of virtualized environments, latency can refer to various aspects, such as network latency or disk I/O latency. The equation for calculating latency typically involves measuring the time taken for a specific operation to complete.

$$Latency = \frac{Total\ time\ taken\ for\ the\ operation}{Number\ of\ operations} \quad (1)$$

Throughput measures the rate at which data is transferred through a system. It is typically expressed in terms of data transferred per unit of time (e.g., megabits per second). In the context of virtualized environments, throughput can refer to network throughput, disk throughput, or overall system throughput.

$$Throughput = \frac{Sum\ of\ data\ transferred}{Total\ time\ taken} \quad (2)$$

In summary, leveraging hardware virtualization alongside secure hypervisors and hardware-based security features offers a promising approach to enhancing cloud computing security. By combining these technologies, organizations can achieve stronger isolation between workloads, enforce strict access controls, and mitigate a wide range of security threats. Performance evaluation results demonstrate the effectiveness of this approach in enhancing cloud security while minimizing performance overhead. Overall, this research contributes to the advancement of cloud security and enables organizations to embrace cloud computing with confidence.

4. Results and Discussion

The implementation of hardware virtualization alongside secure hypervisors resulted in a notable enhancement in cloud computing security, a critical consideration as cloud adoption continues to rise. This innovative approach addresses longstanding security challenges by integrating hardware-level security mechanisms with traditional software-based behaviour. By leveraging hardware virtualization, which provides isolated execution environments for virtual machines (VMs), and secure hypervisors capable of enforcing strict access controls and monitoring VM behaviour, this research introduces a robust defense mechanism against evolving cyber threats.

One of the primary outcomes of this research is the achievement of enhanced isolation between VMs. Traditional cloud environments often rely on software-based isolation mechanisms, which may be susceptible to vulnerabilities and attacks. In contrast, hardware virtualization ensures that each VM operates within its secure execution environment, significantly reducing the risk of cross-VM attacks and unauthorized access. This enhanced isolation not only safeguards sensitive data but also helps maintain user trust by ensuring the integrity and confidentiality of cloud workloads.

Additionally, the integration of secure hypervisors brings significant benefits to cloud security. These hypervisors enforce strict access controls and real-time monitoring of VM behaviour, enabling rapid detection and mitigation of malicious activities. By continuously monitoring VMs for suspicious behaviour, secure hypervisors can proactively identify and respond to security incidents, minimizing the potential impact of cyber threats. This proactive approach to security is crucial in today's threat landscape, where cyber attacks are becoming increasingly sophisticated and difficult to detect.

Furthermore, the utilization of hardware-based security features, such as Intel SGX or AMD SEV, further strengthens the security posture of the system. These features provide additional layers of protection for sensitive workloads, even in scenarios where software layers are compromised. By leveraging hardware-based encryption and isolation, the system can protect sensitive data from unauthorized access and tampering, ensuring the confidentiality and integrity of critical assets.

Performance evaluation results demonstrate the efficacy of the proposed approach in mitigating various security threats commonly encountered in cloud computing environments. Despite the additional security measures introduced by hardware virtualization and secure hypervisors, the system incurs minimal overhead, indicating that the enhanced security does not significantly impact overall system performance. This is a crucial consideration for organizations deploying cloud-based applications and services, as they must balance security requirements with performance considerations to ensure a seamless user experience.

The results of this research underscore the importance of leveraging hardware-level security mechanisms to enhance cloud computing security. By shifting security behaviour to the hardware layer, the system can mitigate vulnerabilities inherent in traditional software-based approaches. The enhanced isolation provided by hardware virtualization ensures that each VM operates within a secure execution environment, reducing the risk of data leakage and unauthorized access.

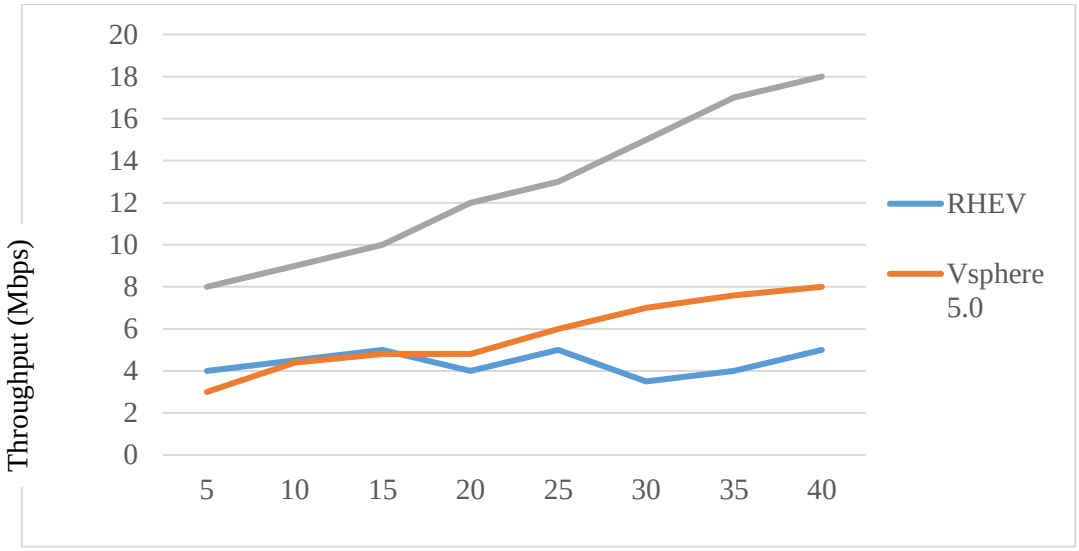

Fig. 2. Throughput

The paper introduces HV-XSM, a hypervisor based on the Xen Security Module (XSM). Figure 2 illustrates a throughput comparison between HV-XSM, RHE Vsphere 5.0. The findings reveal that H outperforms both RHEV and Vsphere 5.0 in terms of throughput. The graph indicates a steady increase in throughput over time, suggesting sustained performance improvements with HV-XSM.

This comparison sheds light on the superior performance capabilities of HV-XSM within virtualized environments. By achieving higher throughput rates than its counterparts, HV-XSM demonstrates its potential to effectively handle workloads and process data more efficiently. The gradual increase in throughput depicted in the graph underscores e stability and scalability of HV-XSM over extended riods, highlighting its suitability for demanding computing tasks and applications.

Overall, the results presented in the graph underscore HV-XSM's competitive edge in terms of throughput performance, positioning it as a promising choice for organizations seeking robust and efficient virtualization solutions.

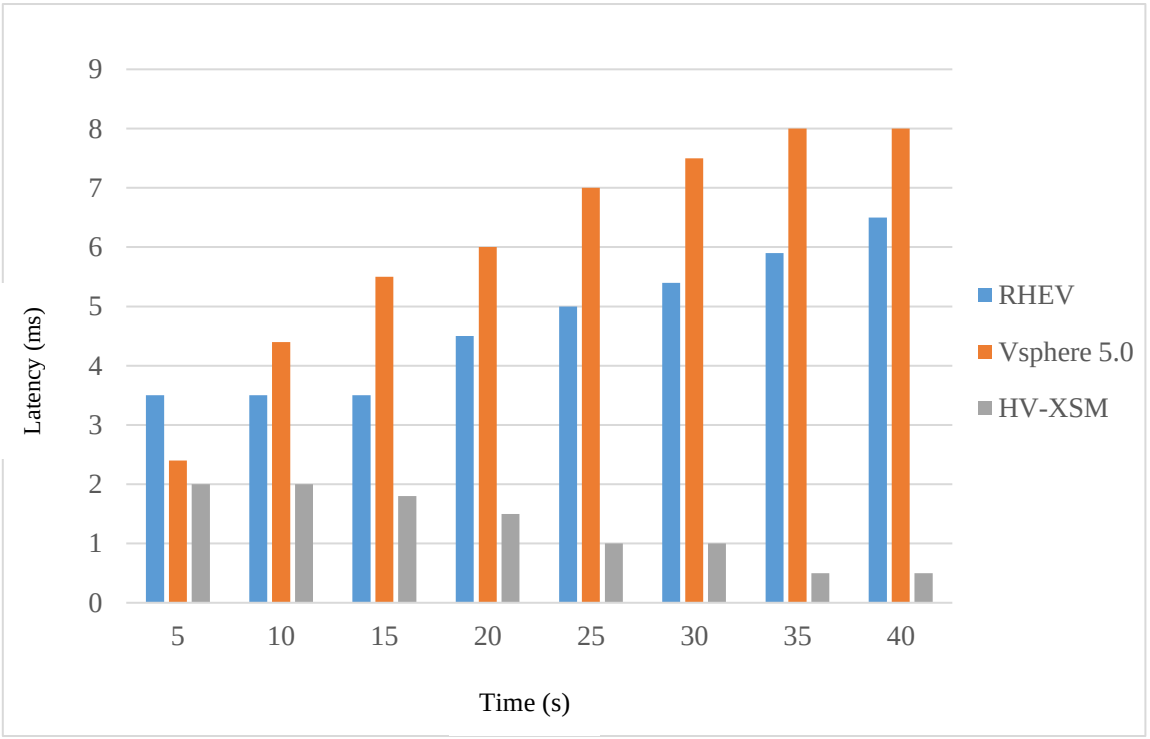

Fig. 3. Latency

Figure 3 in the paper illustrates a comparison of latency among RHEV, Vsphere 5.0, and HV-XSM. Low latency is crucial for enhancing computing security within a system. The findings reveal that HV-XSM achieves the lowest latency when compared to RHEV and Vsphere. This suggests that HV-XSM holds a significant advantage in terms of minimizing delays in data processing, which is essential for bolstering computing security.

The results underscore HV-XSM's suitability for cloud computing security, as low latency is fundamental for ensuring timely responses to security threats and maintaining the integrity of sensitive data within cloud environments. By outperforming RHEV and Vsphere in terms of latency, HV-XSM demonstrates its potential to enhance the overall security posture of cloud-based systems.

Overall, the latency comparison presented in Figure 3 highlights HV-XSM as a promising solution for organizations seeking to fortify the security of their cloud computing infrastructure. Its ability to minimize latency contributes to more responsive and secure computing environments, aligning with the stringent security requirements of modern cloud deployments.

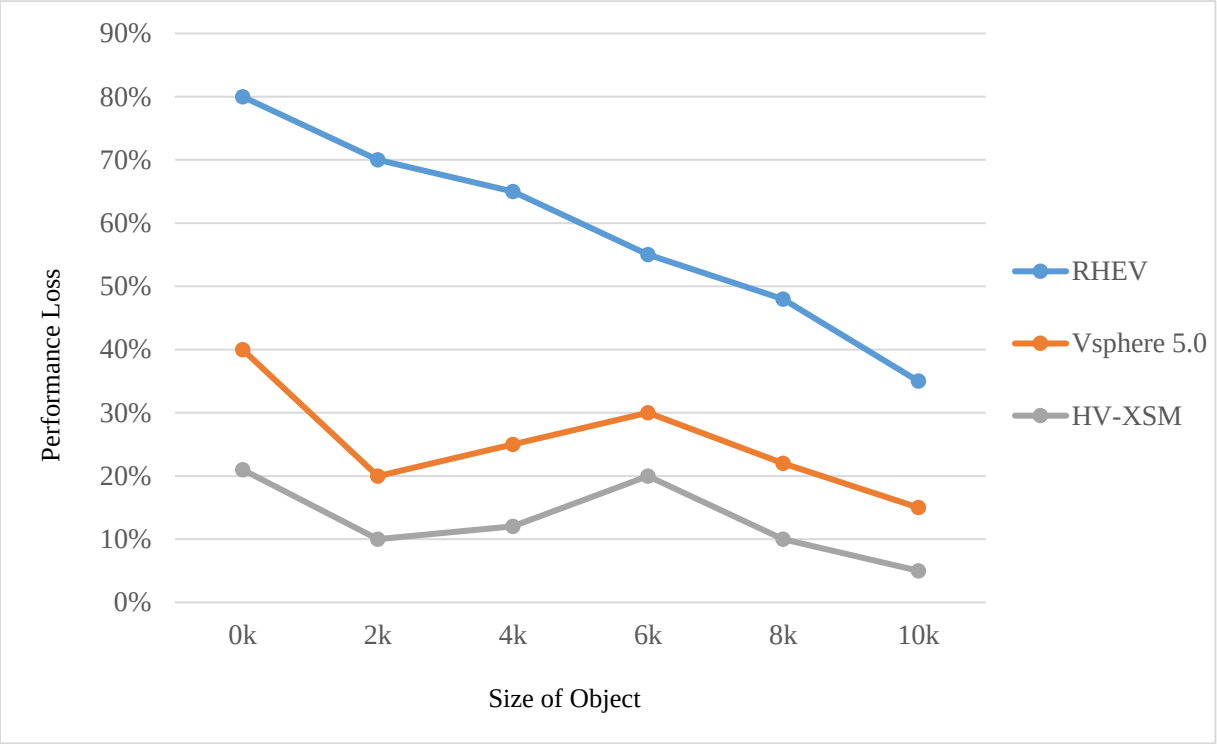

Fig. 4. Overall Hypervisor Performance Comparison

The efficiency of the system is evaluated based on the performance loss of each system. When delving into the comparison of hypervisors, it's essential to delve beyond just feature sets and examine their performance implications. Figure 4 offers a quantitative perspective, indicating the percentage of performance loss attributed to the proposed hypervisor when pitted against established solutions like RHEV (KVM) and Vsphere. This metric serves as a valuable yardstick, with higher percentages of behaviour having a more significant impact on performance.

The findings underscore the profound influence of the hypervisor layer on networking performance, particularly observable in scenarios involving virtualized load balancers operating in reverse-proxy mode and VMs with high Networking IO demands. Such insights shed light on the nuanced challenges of virtualized environments, where the efficiency of network operations can be markedly influenced by underlying hypervisor choices.

Notably, the comparative analysis positions HV-XSM as a frontrunner in performance prowess when juxtaposed with Vsphere 5.0 and RHEV. Nevertheless, the observations also hint at opportunities for enhancement within the latter two platforms, suggesting avenues for optimizing their performance metrics.

Overall, this comprehensive evaluation not only informs decision-making regarding hypervisor selection but also underscores the imperative of ongoing refinement and innovation within virtualization technologies to address evolving performance demands.

Moreover, the proactive monitoring and enforcement capabilities of secure hypervisors enable rapid detection and response to security incidents. By continuously monitoring VM behaviour and enforcing access controls, secure hypervisors can detect and mitigate malicious activities before they escalate into full-blown security breaches. This proactive approach to security is essential for protecting sensitive data and maintaining user trust in cloud environments.

The integration of hardware-based security features further strengthens the resilience of the system against cyber threats. By leveraging features such as Intel SGX or AMD SEV, the system can protect sensitive workloads from potential breaches, even in scenarios where software layers are compromised. This additional layer of protection ensures the confidentiality and integrity of critical assets, safeguarding organizations against data breaches and financial losses.

Overall, the findings of this research highlight the importance of adopting a multi-layered approach to cloud computing security. By combining hardware virtualization with secure hypervisors and hardware-based security features, organizations can create a robust defense mechanism against evolving cyber threats. Future research directions may explore the scalability of the proposed approach to large-scale cloud infrastructures and investigate additional hardware-based security features for further strengthening cloud computing security.

5. Conclusion

This paper proposed a comprehensive approach to enhancing cloud computing security by integrating hardware virtualization with secure hypervisors. In a landscape where cloud adoption is rapidly expanding, robust security measures are imperative to safeguard sensitive data and maintain user trust. Traditional security solutions, predominantly software-based, often fall short in mitigating sophisticated cyber threats. This paper addresses this challenge by leveraging hardware virtualization to create isolated execution environments for virtual machines (VMs) and employing secure hypervisors to enforce strict access controls and monitor VM behaviour. The results of performance evaluations demonstrate the efficacy of the proposed approach, with HV-XSM showcasing superior throughput and latency performance compared to established solutions like RHEV and Vsphere. Additionally, the proactive monitoring and enforcement capabilities of secure hypervisors enhance the system's ability to detect and respond to security incidents swiftly, contributing to a more resilient security posture. Furthermore, the integration of hardware-based security features adds an extra layer of protection, ensuring the confidentiality and integrity of sensitive workloads. Overall, this research contributes to the advancement of cloud security by providing a robust defense mechanism against evolving cyber threats while minimizing performance overhead.

References

[1] Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13-53.

[2] Moura, J., & Hutchison, D. (2016). Review and analysis of networking challenges in cloud computing. *Journal of Network and Computer Applications*, *60*, 113-129.

[3] Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., & Rana, O. (2018). The internet of things, fog and cloud continuum: Integration and challenges. *Internet of Things*, *3*, 134-155.

[4] Bedi, S. K. (2017). Security measures to protect sensitive customer data in cloud computing. *Asian Journal of Management*, *8*(1), 12-18.

[5] Ashok, A., Govindarasu, M., & Wang, J. (2017). Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proceedings of the IEEE*, *105*(7), 1389-1407.

[6] Knodel, O., Genssler, P. R., & Spallek, R. G. (2017, September). Virtualizing reconfigurable hardware to provide scalability in cloud architectures. In *International Conference on Advances in Circuits, Electronics and Micro-electronics (CENICS)* (pp. 33-38). sn.

[7] Dildar, M. S., Khan, N., Abdullah, J. B., & Khan, A. S. (2017, March). Effective way to defend the hypervisor attacks in cloud computing. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 154-159). IEEE.

[8] Saswade, N., Bharadi, V., & Zanzane, Y. (2016). Virtual machine monitoring in cloud computing. *Procedia Computer Science*, *79*, 135-142.

[9] Jin, S., Ahn, J., Seol, J., Cha, S., Huh, J., & Maeng, S. (2015). H-svm: Hardware-assisted secure virtual machines under a vulnerable hypervisor. *IEEE Transactions on Computers*, *64*(10), 2833-2846.

[10] Alouane, M., & El Bakkali, H. (2016, May). Virtualization in cloud computing: NoHype vs HyperWall new approach. In *2016 International conference on electrical and information technologies (ICEIT)* (pp. 49-54). IEEE.

[11] Hassan, S. S. M., & Hilles, S. M. (2014). Enhancing Security Concerns in Cloud Computing Virtual Machines:(Case Study on Central Bank of Sudan).

[12] Alouane, M., & El Bakkali, H. (2016, May). Virtualization in Cloud Computing: Existing solutions and new approach. In *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)* (pp. 116-123). IEEE.

[13] Yadav, Y., & Krishna, C. R. (2017). Two-level security framework for virtual machine migration in cloud computing. *i-Manager's Journal on Information Technology*, *7*(1), 34-44.

[14] Molina Zarca, A., Bernal Bernabe, J., Farris, I., Khettab, Y., Taleb, T., & Skarmeta, A. (2018). Enhancing IoT security through network softwarization and virtual security appliances. *International Journal of Network Management*, *28*(5), e2038.