Securing Virtual Machines using Cloning in Cloud Services

Naveen Kumar Adalagere Nemirajaiah
Department of Computer Science & Engineering, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
naveenkumaran@ssit.edu.in (corresponding author)

Channa Krishna Raju
Department of Artificial Intelligence & Machine Learning, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
rajuck@ssit.edu.in

Received: 23 October 2024 | Revised: 26 November 2024, 19 December 2024, and 26 December 2024 | Accepted: 29 December 2024

 DOI: https://doi.org/10.48084/etasr.9391

ABSTRACT

Cloud Computing (CC) is now a service available to everyone, where all computing resources are made available as a service over the internet, based on the user's needs. Virtualization is a critical component of cloud services that significantly reduces costs and improves resource utilization by creating Virtual Machines (VMs), which are essentially virtual resources that can serve multiple users simultaneously. VMs are subject to security threats and attacks such as malware, and it is very important to create a secure environment for VMs to run seamlessly. In this novel strategy, we create cloned instances for the VMs so that instead of using the VMs directly to run the application, we allow one of the cloned VMs to run it. If something happens to that cloned VM instance, another cloned VM takes over without interrupting the VM's functionality. This provides security for the VM in the cloud environment.

Keywords-cloud services; Virtual Machine (VM); security; instance

I. INTRODUCTION

Cloud Computing (CC) provides IT resources such as computing power, server capacity, applications, and software to users over the internet on an as-needed basis [1-3]. Virtualization transforms physical computing resources into virtual resources, enabling more efficient use of IT resources by serving multiple users simultaneously. This dramatically reduces the cost of physical resources, allowing cloud service providers to deliver services to many customers with low infrastructure costs. A critical component of cloud services is the Virtual Machine Manager (VMM) or hypervisor, a software package that enables the creation and management of Virtual Machines (VMs). The hypervisor plays a critical role in virtualization by partitioning the physical resources of a server to create multiple virtual instances. The VMM enables resource provisioning based on customer demand and facilitates resource sharing among multiple customers, a feature known as multi-tenancy, which helps to reduce costs. There are two main types of hypervisors:

- Type 1 hypervisors, also known as bare-metal hypervisors, run directly on the physical hardware, allowing for improved performance and efficiency. Examples include Microsoft Hyper-V, Xen, and VMware ESXi.
- Type 2 hypervisors which run on top of an existing host Operating System (OS) that serves as the host that communicates with the hardware, and have slightly lower performance than Type 1 hypervisors because they are driven by the host OS. Examples include Oracle VM VirtualBox and VMware Workstation. In this case, the guest VMs are the virtual instances created by the hypervisor that can run their own OS, called the guest OS. The host machines are the physical servers running the host OS.

While there are many benefits to virtualization, data security remains the most important challenge, requiring appropriate security measures to protect the information at both the logical and physical levels [4-15]. Authors in [16] proposed CloudSafe, a novel security assessment and management system that provides automated security assessment and enforcement of security controls. To demonstrate its applicability, CloudSafe was implemented in Amazon AWS. The system automatically selects countermeasures such as patching, network hardening, and moving target defense, and uses graphical security models to assess the security of the cloud. Cloud Access Security Brokers (CASB) provide a layer of protection, acting as intermediaries between applications and users to extend the enterprise shield to third parties. Authors in [17] explore customer experiences with CASBs and evaluate

the goals, impacts, architectures, and planning through the published research. In [18], the main focus is on the Intrusion Detection System (IDS) and the Intrusion Prevention System (IPS), collectively referred to as IDPS. The main objective of IDS is to detect the unauthorized access and malicious activities on the cloud data, which is done by analyzing the huge amount of network traffic data and user activities inside or outside the cloud infrastructure. If any abnormal patterns are observed during data analysis, which may lead to data compromise, the IDS automatically detects the attempt and immediately notifies the cloud administrator. IPS is a solution that is designed to block any potential threat to a cloud system, and when it detects such activity, it immediately takes action to prevent or mitigate such potential attacks. It can prevent access to the cloud server or cloud network by using a traffic monitoring system and blocking the request to the server or dropping malicious packets. It also maintains logs of any attacks it detects for future prevention. Authors in [19] introduce the concept of information security in smart grids and the main strategies for cloud security construction in electric power companies. Authors in [20] propose a hybrid cloud-based distributed model to enhance data storage and security in e-commerce applications. The applications are deployed on multi-tier distributed cloud systems where all servers are virtualized and load balanced. This approach provides better storage performance, data handling capabilities and security.

The present paper examines the challenges and vulnerabilities associated with virtualization security and proposes a method to overcome these issues.

A. Cloud Virtualization Implementation Issues

The hosting VMM serves as the central control point for allocating resources to virtual instances and releasing them when processing is complete. Because of its central role in creating, managing, and releasing resources, this control point is vulnerable to malware attacks, security vulnerabilities, data leakage, isolation failures, and Denial-of-Service (DoS) attacks. Addressing these challenges requires robust security measures, continuous monitoring, and efficient resource management to ensure the secure and effective operation of cloud services [21]. The key challenges in implementing cloud virtualization are:

- Reduced performance: A significant issue with virtualization is that as the number of virtual resources derived from a single physical resource increase, the performance of these VMs tends to degrade, resulting in increased latency. This performance degradation can be noticeable to users.
- Authorized users and access: The risk of attacks and unauthorized access to resources is often higher for authorized users because basic security measures typically prevent regular users from causing significant damage in the early stages. Since authorized users can easily exploit the virtual environment and have legitimate access to resources, identifying them when they are engaged in harmful activities is the biggest challenge. This insider threat is a major concern.
- Resource availability: Achieving consistently high levels of resource availability typically requires cloud providers to make significant investments in infrastructure and virtualization frameworks to ensure that logical resources are equipped with robust security measures to protect physical and virtual assets.
- Service privacy: When customers request cloud resources, they interact directly with the cloud services. During these interactions, data and confidential information related to the cloud services are exchanged over network transactions. Unauthorized users may attempt to hack into customers' confidential data, posing serious risks.
- Migration of instances: Typically, instances or VMs built from physical machines exist as files that can be moved between physical machines. However, while they are moving, they are open to attack and potential problems. Malware or viruses can infect these instances and cause disruptions such as changing the settings and configurations of other virtual instances, corrupting files and folders, and even corrupting the underlying physical machines. This can result in data leakage, abnormal behavior of virtual instances, and occasionally impact the host OS. A corrupted OS on physical machines might fail to allocate necessary resources to virtual instances or release resources prematurely.
- Service Level Agreement (SLA): A cloud service provider and its users have a critical contract known as an SLA, that defines+ the terms and conditions before resources are provisioned. It plays a key role in setting expectations for service availability, response times, and resource reliability, while delineating the responsibilities of both parties. This agreement specifies how users may use allocated resources without violating the terms and conditions, and provides guidelines for the provider on issues such as provisioning resources, maintaining quality standards, performing backups, isolating malicious activity, and continuously improving service delivery.

II. PROPOSED APPROACH

In the present study we propose a novel approach to mitigate the persistent threat of malware and other security risks that often disrupt the normal operation of VMs. When the VMs encounter situations where they are rendered ineffective due to threats, the application workflow is disrupted. To avoid such problems, it is essential to create an environment where each VM can operate seamlessly with the necessary resources provisioned by the VMM. A promising solution is to take advantage of the cloning feature available in Java programming and the Security Supervisors (SSs). Cloning is a way to create an exact replica of an object. A SS should include various security measures such as methods for identifying and resolving problems, preventing unauthorized access, techniques for obfuscating data origins, and strategies for detecting and thwarting intruders, attackers, malware, and viruses. It should also incorporate updates and patches necessary for the VMs and the application and be adaptable to incorporate the latest techniques and emerging solutions. Regular redesign and periodic updates are essential to ensure that the SS is always

employing the most current, sufficient, and effective security measures and enables the integration of specific security solutions directly into the VMs. However, implementing such security solutions within the SS can result in performance issues. The algorithm below outlines the overall execution flow of the proposed system:

```
Step 1: Set up a cloud environment with
adequate physical computing resources.
Step 2: Create 1 to N VMs as per
requirements.
Step 3: Install a SS for each VM.
Step 4: Apply variable size inputs and
analyze the overall response time of each
VM.
Step 5: Create clone instances 2 and 3 for
each VM by allocating the required
resources.
Step 6: Allocate the workload to the clone
instances instead of the actual VMs by
selecting 2 or 3 clone instances.
Step 7: If any running instance is
affected by threats, then stop that
instance and migrate its work to any of
the new instances and continue the process
without interruption.
Step 8: Install SS for each instance as a
second layer of protection layer for the
cloud environment.
Step 9: Repeat step 6 and then step 7
until the work is completed.
```

Figure 1 depicts the initial installation of SSs for each VM and figure 2 shows the creation of 2 additional clone instances for each VM. Having multiple clones of the same VM ensures business continuity even if one instance is compromised and the users can seamlessly switch to one of the remaining instances to continue running applications without interruption. It should be noted that deploying multiple clones requires sufficient storage and compute resources to effectively support each instance. This approach is an important step in protecting VM environments in CC from security vulnerabilities. As shown in Figure 3, in addition to using the cloning feature, we enhance VM security by deploying SS in both the VMs and the cloned instances. This two-layered protection strategy fortifies VMs against potential threats and significantly increases their availability even during disruptions caused by external factors.

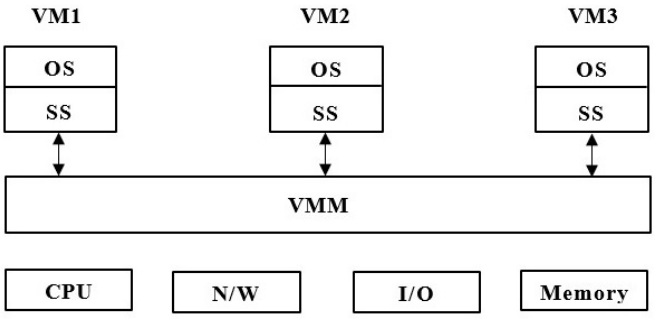

Fig. 1. SS creation for each VMs.

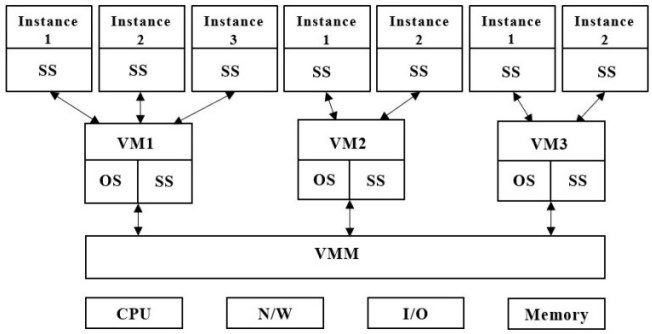

Fig. 2. Creation of instances for each VM.

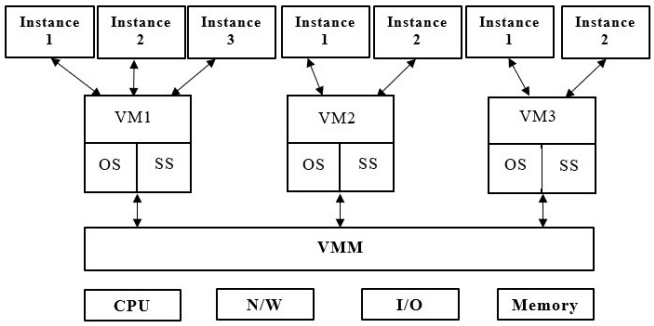

Fig. 3. SS creation for each instance.

III. EXPERIMENTAL RESULTS

Figure 4 illustrates the standard status where all VMs are functioning normally without the inclusion of the SS or the cloning mechanism. In this scenario, the VM response times, VMM response time, and memory usage per VM are within normal limits.

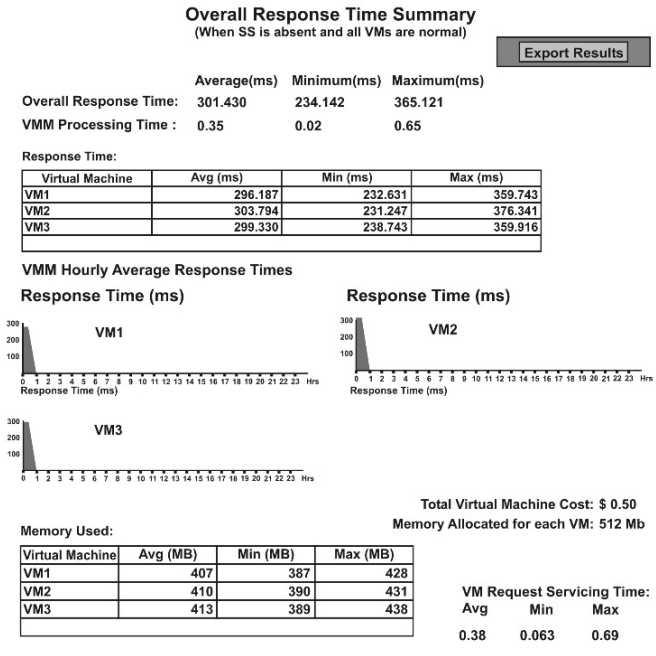

Fig. 4. VM response times without SS or cloning.

In Figure 5, the SS is integrated without the cloning mechanism. In this scenario, if VM1 becomes infected for any reason, it is evident that the response time and memory consumption of VM1 increases. In addition, the overall response time of the VMM is increased compared to the normal values observed in the previous case.

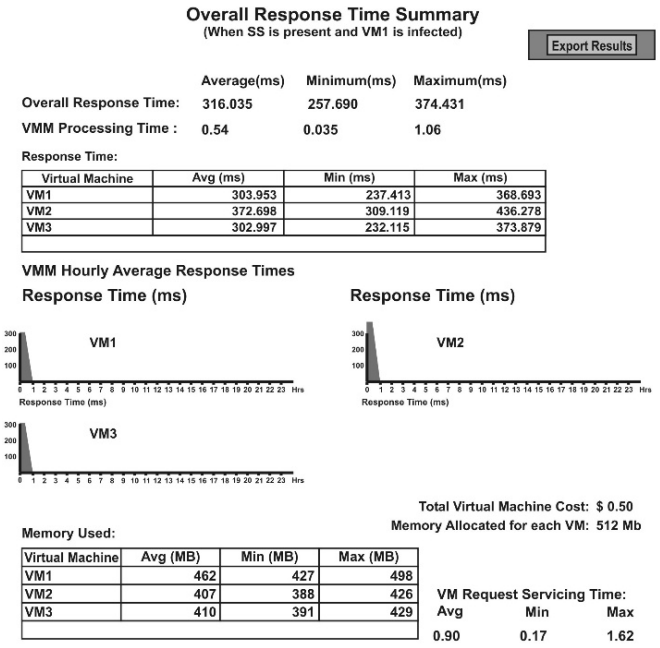

Fig. 5. VM response times with SS but without cloning.

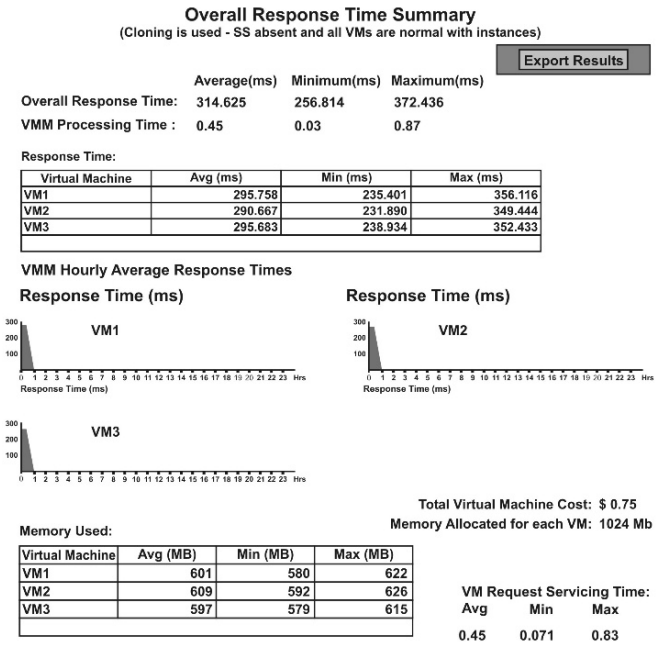

Fig. 6. VM response times with cloning but without SS.

In Figure 6, the cloning mechanism is used without the SS. All VMs operate normally without any infections and show standard resource consumption values for both the VMs and the VMM. However, the overall response time of the VMM increases as a result of creating instances using the cloning mechanism, which also results in higher memory consumption by the VMs.

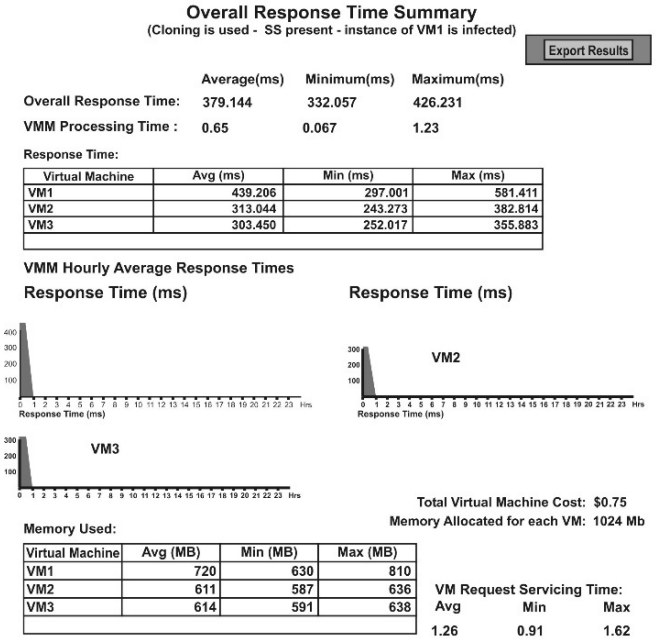

Fig. 7. VM response times with cloning and SS.

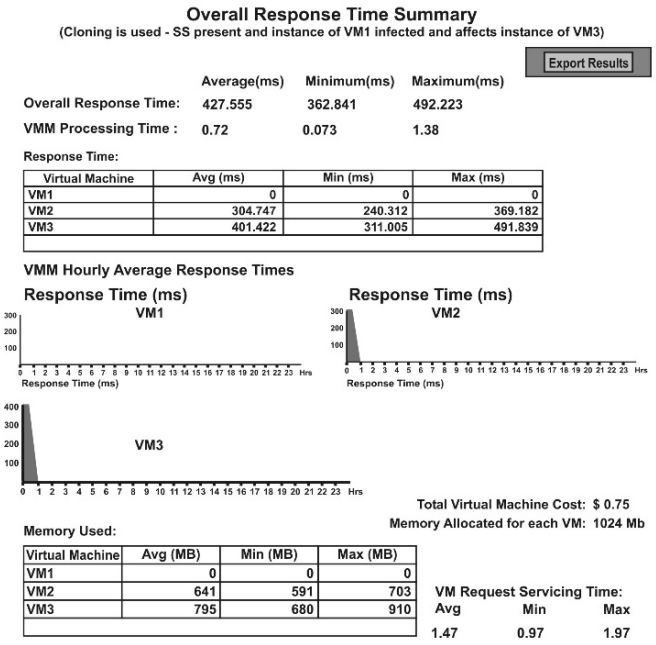

Fig. 8. VM response times with cloning, SS and infection spreading to another VM.

Figure 7 illustrates the scenario where the cloning mechanism is present along with the SS. In this scenario, an infected instance of VM1 experiences increased response time

and memory consumption. The overall response time of the VMM is also increased, along with increased service time for VM requests.

In Figure 8, the infected instance of VM1 spreads the infection to the instance of VM3. Despite this, the SS successfully deallocates resources from the infected instance of VM1, making its values zero in the results. However, the memory consumption and response time of VM3 increases due to its infection.

IV. CONCLUSION AND FUTURE SCOPE

In this study, we explored the security challenges associated with cloud virtualization and proposed an innovative approach to mitigate Virtual Machine (VM) vulnerabilities. Our approach improves VM management by deploying multiple instances of the same VM, ensuring resilience against VM corruption caused by external threats. If one instance of a VM becomes infected or fails, the remaining instances seamlessly continue to operate without interruption, maintaining service continuity. This capability enables users to meet their operational needs even in the event of VM failures due to external attacks. We recommend that IT infrastructures should consider using the cloning feature to implement multiple instances of the same VM to increase resilience against external threats. Implementing this approach by providing dual Security Supervisors (SSs) in the VM as well as cloned VMs can significantly strengthen VM security, as depicted in Figure 2 of our study. However, it's important to note that this approach requires additional memory space to accommodate multiple VM instances, as well as high computing power to support applications with enhanced security features. These considerations are essential for effectively implementing and maintaining resilient VM environments in cloud computing.

The following is the future scope of VM cloning:

- Use of Intrusion Detection Systems (IDSs) to improve the efficiency of the devops workflow.
- In the era of devops, especially containerization, VM cloning can support the easy integration of containerized applications and balance the workload of kubernetes clusters.
- Integrating VM cloning with automation can further improve security. For example, when VM cloning is performed using AI automation with Deep Learning (DL), the DL algorithms can automatically verify security compliance standards for encryption, authentication, authorization and auditing.

REFERENCES

[1] T. Velte, A. Velte, and R. C. Elsenpeter, *Cloud Computing, A Practical Approach*. New York, NY, USA: McGraw Hill Professional, 2009.

[2] B. Sosinsky, *Cloud Computing Bible*, 1st ed. Hoboken, NJ, USA: Wiley Publishing, Inc., 2011.

[3] D. S. Linthicum, *Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide*, 1st ed. Boston, MA, USA: Addison-Wesley Professional, 2009.

[4] S. Gadde, G. S. Rao, V. S. Veesam, M. Yarlagadda, and R. S. M. L. Patibandla, "Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions," *Ingénierie des Systèmes d'Information*, vol. 28, no. 6, pp. 1467–1477, Dec. 2023, https://doi.org/10.18280/isi.280604.

[5] A. N. N. Kumar, M. Mallegowda, A. V. K. Mohan, K. N. Shreenath, and C. K. Raju, "Movement Mode Harmony Search Based Multi-objective Firefly Algorithm Feature Selection for Detecting the Security Threats in Virtual Machine," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 1, pp. 159–168, Feb. 2024, https://doi.org/10.22266/ijies2024.0229.16.

[6] A. N. N. Kumar and N. L. Udayakumar, "Novel approach for Securing Virtual Machines in Cloud Environment," *SSAHE Journal of Interdisciplinary Research*, vol. 1, no. 1, pp. 60–66, 2020.

[7] N. L. U. Kumar, S. S. R, and M. Siddappa, "Security Issues and Solutions for Virtualization in Cloud Computing Service," *International Journal of Engineering Research & Technology*, vol. 3, no. 14, Apr. 2018, https://doi.org/10.17577/IJERTCONV3IS14006.

[8] G. Peterson, "Don't Trust. And Verify: A Security Architecture Stack for the Cloud," *IEEE Security & Privacy*, vol. 8, no. 5, pp. 83–86, Sep. 2010, https://doi.org/10.1109/MSP.2010.149.

[9] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, Nov. 2010, https://doi.org/10.1109/MSP.2010.186.

[10] N. L. U. Kumar and M. Siddappa, "Ensuring security for virtualization in cloud services," in *2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques*, Mysuru, India, 2016, pp. 248–251, https://doi.org/10.1109/ICEECCOT.2016.7955224.

[11] J. Szefer, E. Keller, R. B. Lee, and J. Rexford, "Eliminating the hypervisor attack surface for a more secure cloud," in *Proceedings of the 18th ACM conference on Computer and communications security*, Chicago, IL, USA, 2011, pp. 401–412, https://doi.org/10.1145/2046707.2046754.

[12] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," in *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, San Jose, CA, USA, 2010, pp. 35–41, https://doi.org/10.1109/CCST.2010.5678682.

[13] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, Chicago, IL, USA, 2009, pp. 199–212, https://doi.org/10.1145/1653662.1653687.

[14] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, Indianapolis, IN, USA, 2010, pp. 693–702, https://doi.org/10.1109/CloudCom.2010.66.

[15] P. Saripalli and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security," in *2010 IEEE 3rd International Conference on Cloud Computing*, Miami, FL, USA, Jul. 2010, pp. 280–288, https://doi.org/10.1109/CLOUD.2010.22.

[16] S. An, A. Leung, J. B. Hong, T. Eom, and J. S. Park, "Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security," *IEEE Access*, vol. 10, pp. 75117–75134, 2022, https://doi.org/10.1109/ACCESS.2022.3190545.

[17] S. Ahmad, S. Mehfuz, F. Mebarek-Oudina, and J. Beg, "RSM analysis based cloud access security broker: a systematic literature review," *Cluster Computing*, vol. 25, no. 5, pp. 3733–3763, Oct. 2022, https://doi.org/10.1007/s10586-022-03598-z.

[18] K. Shanthi and R. Maruthi, "A Comparative Study of Intrusion Detection and Prevention Systems for Cloud Environment," in *2023 4th International Conference on Electronics and Sustainable Communication Systems*, Coimbatore, India, 2023, pp. 493–496, https://doi.org/10.1109/ICESC57686.2023.10193694.

[19] G. Feng, Q. Huang, Z. Deng, H. Zou, and J. Zhang, "Research on cloud security construction of power grid in smart era," in *2022 IEEE 2nd International Conference on Data Science and Computer Application*, Dalian, China, 2022, pp. 976–980, https://doi.org/10.1109/ICDSCA56264.2022.9987863.

[20] V. A. K. Gorantla, V. Gude, S. K. Sriramulugari, N. Yuvaraj, and P. Yadav, "Utilizing Hybrid Cloud Strategies to Enhance Data Storage and Security in E-Commerce Applications," in *2024 2nd International Conference on Disruptive Technologies*, Greater Noida, India, 2024, pp. 494–499, https://doi.org/10.1109/ICDT61202.2024.10489749.

[21] N. L. U. Kumar and M. Siddappa, "Meeting the challenge of Virtualization impact on Cloud services," *International Journal of Computer Science and Information Technologies*, vol. 7, no. 1, pp. 457–461, 2016.