Journal of Applied Data Sciences
Vol. 4, No. 2, May 2023, pp. 76-83

Research on New Virtualization Security Protection Management System Based on Cloud Platform

Zhihong Li [1,*], Guangxu Liu [2], Yijie Dang [3], Zhijie Shang [4], Nan Lin [5]

[1,2,3,4,5] State Grid Information & Telecommunication Branch, Beijing, China, 100761
Lizhihong@sgit.sgcc.com *
* corresponding author

(Received January 15, 2023 Revised February 17, 2023 Accepted February 22, 2023, Available online March 1, 2023)

Abstract

As an emerging product under the condition of informatization, the utilization of cloud platforms in many industries has brought fundamental changes to the production and business model in related fields. The cloud platform provides rich and diverse utilization services to terminals through multi-dimensional integration of different IT resources. With the in-depth utilization of cloud platforms, the security problems it faces are becoming more and more prominent. The traditional network security protection means have been difficult to effectively adapt to and deal with the security threats under the new situation of cloud platform utilization. As a prominent part of building cloud platforms, the construction level of virtualization security protection system will have an intuitive impact on the security of cloud platforms. At present, the virtualization security protection management system under cloud platform is facing direct threats from virtual machine deployment, virtual machine communication and virtual machine migration. Based on this, this paper studies the virtualization security protection management system of cloud platform from the perspective of virtualization security tech, so as to ameliorate the stability, reliability and security of cloud platform

Keywords: Virtualization Security Protection, Cloud Platform, Informatization

1. Introduction

The in-depth utilization of cloud computing platform in various fields has changed the operation mode of relevant industries to a great extent. The cloud platform organically integrates information resources represented by networks, servers and software, so as to provide information services to customers in the form of overall packaging [1-3]. The service resources provided by the cloud platform can be easily accessed and used by users, so it can bring higher utilization value to users. The utilization of cloud platform virtualization tech not only brings the innovation of enterprise and industry information business architecture, but also introduces new information security risks and challenges [4]. This requires cloud computing related service providers to formulate targeted virtualization security protection schemes and management systems based on the typical characteristics and practical needs of virtualization information security protection, so as to provide more effective support for more extensive and in-depth utilization protection of cloud platform.

With the increasingly severe threat of network security, cloud platform operators are not only improving resource utilization, but also actively improving the security of cloud platform [5-7]. In the process of providing information services, the security threats faced by the cloud platform are mainly manifested in unauthorized malicious access, modification and damage to the cloud platform. Secondly, the cloud platform is also facing internal and external security threats, mainly in malware attacks. The clustering and layering characteristics of cloud platform make the traditional security protection measures unable to effectively deal with the security attacks and threats against cloud platform. Therefore, according to the virtualization characteristics of cloud platform, focus on improving the security and stability of cloud platform, so as to strengthen the stability and robustness of cloud platform.

In addition, as an prominent system providing systematic services, cloud platform plays an prominent role in its security, information integrity and availability. The cloud computing platform fully integrates several aspects of virtualization tech, as shown in Figure 1 below, and realizes the prominent transformation of cloud platform in the

safe operation of virtualization. On the one hand, the new virtualization security protection management architecture based on cloud platform supports the practical requirements for data collection, storage and forwarding; On the other hand, it supports structured and unstructured multi-level security situational awareness.

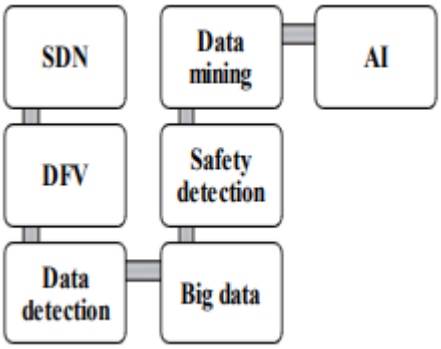

Figure. 1. Integration elements of cloud computing platform virtualization tech

In short, with the deepening utilization of cloud platform, in order to effectively deal with the severe security situation faced by cloud platform, targeted countermeasures need to be established according to the virtualization characteristics of cloud platform and new attack methods. Build a new virtualization security protection management system based on cloud platform [8]. While improving the virtualization security service capability carried on the cloud platform, it supports multidimensional security mode and realizes the customization and self-service of cloud platform security policy. Therefore, the research on the new virtualization security protection management system based on cloud platform has prominent practical value.

2. Virtualization characteristics of cloud platform and its security threats

2.1. Typical characteristics of cloud computing platform

The typical characteristics of cloud computing platform include virtualization of computing and services and parallel processing of large-scale data [4,9,10]. Each physical environment of the traditional security protection model is relatively independent, including security products to protect servers and utilizations. After the virtualization of cloud platform, all virtual machines share resources. The virtualization of cloud platform computing and services makes virtual machines and utilizations likely to move or change at any time. Traditional security software causes resource conflict, reduces the density of virtual machines, and protects the system security through regular scanning, virus database updating and resident in memory. The virtual machine of the cloud platform needs to have a fully configured client and the latest virus library.

Cloud computing is a technology that allows users to access computing resources over the internet. A cloud computing platform provides users with access to a pool of computing resources, such as servers, storage, and networking, that can be used to build and deploy applications [11]. The following are some of the typical characteristics of a cloud computing platform. On-demand self-service: A cloud computing platform allows users to provision computing resources on demand, without the need for human intervention. Users can quickly provision and deprovision computing resources, such as servers, storage, and networking, as needed [12,13]. Broad network access: A cloud computing platform provides access to computing resources over the internet from any device, including desktops, laptops, tablets, and smartphones. Users can access the cloud computing platform from anywhere in the world, as long as they have an internet connection. Resource pooling: A cloud computing platform allows multiple users to share computing resources, such as servers, storage, and networking. The resources are dynamically allocated to users based on their needs. This allows for efficient use of computing resources and reduces costs. Rapid elasticity: A cloud computing platform can quickly scale up or down the amount of computing resources allocated to a user, based on their demand. This allows users to quickly respond to changes in demand for their applications, without having to invest in additional infrastructure. Measured service: A cloud computing platform provides users

with metrics to measure their usage of computing resources, such as CPU usage, storage usage, and network bandwidth. This allows users to monitor their resource usage and optimize their usage for cost and performance.

In conclusion, cloud computing platforms have several typical characteristics, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. These characteristics allow users to efficiently provision and deprovision computing resources, access computing resources from anywhere, share computing resources with others, quickly scale up or down computing resources, and monitor their resource usage for cost and performance optimization. These characteristics have made cloud computing platforms a popular choice for building and deploying applications in various fields, including business, education, healthcare, and government.

2.2. Security challenges faced by cloud computing platform

The unique characteristics of cloud computing platform, such as data and service outsourcing, virtualization, multi-tenant and cross domain sharing, have brought new challenges to the security of the whole platform. The security and privacy problems faced by cloud platform have become an prominent obstacle to its further utilization. The computing environment faced by the cloud platform makes it more dependent on the network and servers, resulting in greater security and privacy problems and security and confidentiality risks [5,14-17]. Firstly, the characteristics of data and service outsourcing of cloud platform make it at risk of privacy disclosure and information theft. Secondly, the characteristics of multi-tenant and cross domain sharing of cloud platform make the establishment, management and maintenance of trust relationship more difficult, and service authorization and access control become more complex. In addition, the virtualization characteristics of cloud platform make a large number of virtual services rented by users more vulnerable to covert collaborative attacks [6,18]. Resource virtualization supports the deployment of virtual resources of different tenants on the same physical resources, which facilitates malicious users to implement side channel attacks with the help of shared resources.

While cloud computing offers many benefits, it also poses significant security challenges. The following are some of the security challenges faced by cloud computing platforms. Data breaches: Data breaches are a major security challenge for cloud computing platforms [19]. Cloud providers store sensitive data for many users, and a single data breach can expose data for all of them. Cloud providers need to implement strict security measures to prevent data breaches, such as encryption, access control, and intrusion detection. Insider threats: Insider threats are a significant security challenge for cloud computing platforms [20]. Cloud providers employ many employees who have access to sensitive data. Malicious insiders can steal data, modify data, or cause other security incidents. Cloud providers need to implement strict access controls and monitor employee activity to prevent insider threats. Compliance: Compliance is a significant security challenge for cloud computing platforms. Cloud providers need to comply with various regulations, such as HIPAA, GDPR, and PCI-DSS. Failure to comply with these regulations can result in legal and financial penalties. Malware: Malware is a significant security challenge for cloud computing platforms. Malware can infect virtual machines, compromise data, and cause service disruptions. Cloud providers need to implement strict malware protection measures, such as antivirus software and intrusion detection. Denial of service attacks: Denial of service attacks are a significant security challenge for cloud computing platforms. Denial of service attacks can overload cloud servers, causing service disruptions. Cloud providers need to implement strict measures to prevent denial of service attacks, such as network segmentation and intrusion prevention.

In conclusion, cloud computing platforms face significant security challenges, such as data breaches, insider threats, compliance, malware, and denial of service attacks. Cloud providers need to implement strict security measures to prevent these security incidents, such as encryption, access control, intrusion detection, malware protection, and network segmentation. Cloud users also need to be aware of these security challenges and take appropriate measures to protect their data, such as strong passwords, two-factor authentication, and encryption. Overall, cloud computing platforms can be secure if proper security measures are implemented and monitored.

2.3. Challenges of cloud platform virtualization security management protection

The security challenges and threats faced by the cloud platform under the new situation make the traditional and single means of security management and protection unable to effectively meet and adapt to the security protection

requirements under the new system [21]. Safety control needs to be carried out in multiple dimensions and levels such as policy, tech and supervision [22]. Secondly, the traditional security management system, such as encryption mechanism, security authentication and access control, cannot effectively meet the security protection needs of cloud platform [7]. In addition, the establishment of multi-dimensional and multi-level privacy security system, fully homomorphic encryption algorithm, dynamic service authorization protocol and virtual machine isolation strategy has become an prominent measure to carry out cloud platform security protection.

Cloud platform virtualization enables the use of virtual machines (VMs) that run on a shared physical server, allowing multiple users to share computing resources. While virtualization provides many benefits, it also poses significant security challenges [23]. The following are some of the challenges of cloud platform virtualization security management and protection. VM isolation: VM isolation is a significant security challenge for cloud platform virtualization. VMs are isolated from each other to prevent data breaches and other security incidents. However, VM isolation is not foolproof, and VMs can be vulnerable to attacks, such as VM escape attacks, that compromise VM isolation. Hypervisor security: Hypervisor security is a significant security challenge for cloud platform virtualization. The hypervisor is a critical component of virtualization that controls access to computing resources. If the hypervisor is compromised, all VMs on the physical server can be compromised.

Cloud providers need to implement strict hypervisor security measures, such as access control, intrusion detection, and encryption [24,25]. Resource sharing: Resource sharing is a significant security challenge for cloud platform virtualization. Cloud providers need to ensure that users are allocated the appropriate computing resources and that resources are not over-provisioned or under-provisioned. Over-provisioning can result in performance degradation, while under-provisioning can result in denial of service attacks. Data protection: Data protection is a significant security challenge for cloud platform virtualization. Cloud providers need to ensure that data is protected from unauthorized access, modification, and deletion. Data protection measures, such as encryption and access control, need to be implemented at both the VM and host levels. Compliance: Compliance is a significant security challenge for cloud platform virtualization. Cloud providers need to comply with various regulations, such as HIPAA, GDPR, and PCI-DSS. Failure to comply with these regulations can result in legal and financial penalties.

In conclusion, cloud platform virtualization poses significant security challenges, such as VM isolation, hypervisor security, resource sharing, data protection, and compliance. Cloud providers need to implement strict security measures to protect VMs and computing resources, such as access control, intrusion detection, encryption, and compliance. Cloud users also need to be aware of these security challenges and take appropriate measures to protect their data, such as strong passwords, two-factor authentication, and encryption. Overall, cloud platform virtualization can be secure if proper security measures are implemented and monitored.

3. Construction of cloud platform virtualization security protection management system

3.1. Security protection scheme for cloud platform virtualization environment

The architecture of the virtual environment solution is shown in Figure 2 below. Firstly, the cloud platform virtualization environment is facing the problem of resource contention. In order to build agent-free security, have the ability to perceive the virtual environment, and establish the security tasks distributed based on the overall resources of the virtual machine, it can effectively avoid resource contention. Cloud platform virtualization has become an essential technology in the field of cloud computing. However, virtualization also brings security challenges, such as VM isolation, hypervisor security, resource sharing, data protection, and compliance. The following are some security protection schemes for the cloud platform virtualization environment.

VM isolation: VM isolation is a significant security challenge for cloud platform virtualization. To protect VMs from each other, cloud providers need to implement strict VM isolation measures, such as network segmentation, firewall, and access control. Virtual machines should be separated by different virtual networks, and only authorized users should be able to access the virtual network.

Hypervisor security: Hypervisor security is a significant security challenge for cloud platform virtualization. Cloud providers need to implement strict hypervisor security measures, such as access control, intrusion detection, and encryption. Hypervisors should be updated regularly, and unauthorized access should be prevented by strong authentication mechanisms.

Resource sharing: Resource sharing is a significant security challenge for cloud platform virtualization. Cloud providers need to ensure that resources are allocated based on users' needs and that resources are not over-provisioned or under-provisioned. Over-provisioning can result in performance degradation, while under-provisioning can result in denial of service attacks. Data protection: Data protection is a significant security challenge for cloud platform virtualization. Cloud providers need to ensure that data is protected from unauthorized access, modification, and deletion. Data protection measures, such as encryption and access control, need to be implemented at both the VM and host levels. Compliance: Compliance is a significant security challenge for cloud platform virtualization. Cloud providers need to comply with various regulations, such as HIPAA, GDPR, and PCI-DSS. Compliance requirements should be integrated into the security protection scheme to ensure that security measures meet regulatory standards.

In conclusion, cloud platform virtualization poses significant security challenges, and cloud providers need to implement strict security protection schemes to protect VMs and computing resources. VM isolation, hypervisor security, resource sharing, data protection, and compliance are critical components of the security protection scheme for the cloud platform virtualization environment. Cloud users also need to be aware of these security challenges and take appropriate measures to protect their data, such as strong passwords, two-factor authentication, and encryption. Overall, cloud platform virtualization can be secure if proper security protection schemes are implemented and monitored.

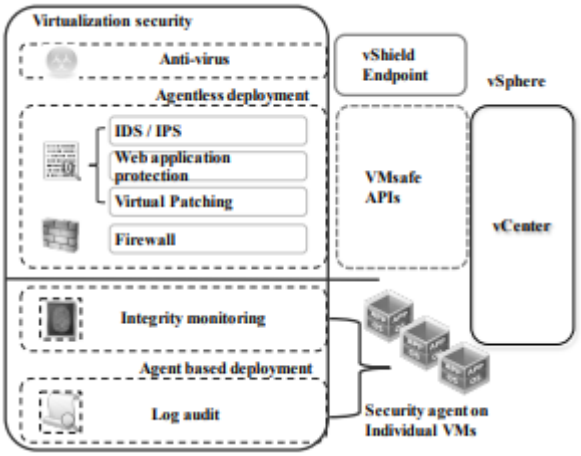

Figure. 2. Architecture of solutions for virtual environments

Secondly, aiming at the problem of protection gap during the real-time startup of cloud platform, it is necessary to establish a security virtual machine deployed based on the virtual machine and use the latest threat feature library in real time, so as to identify security threats in real time and offline. In addition, aiming at the protection blind spots between cloud platform virtual machines, a virtual environment aware security solution integrated with virtualization platform is established to effectively eliminate the protection blind spots [8]. To solve the problem that individual virtual machines on the cloud platform are difficult to manage effectively, it is necessary to integrate with the virtual environment management platform VMware vCenter, so as to effectively detect virtual machines with insufficient security level.

3.2. Cloud platform desktop virtualization security protection scheme

The architecture of cloud platform desktop virtualization security protection is shown in Figure 3 below. With the help of IDS/IPS, known zero-day attacks launched through security vulnerabilities are detected and prevented. Secondly, use web utilizations to protect web utilization security vulnerabilities. Use virtual patches to provide patch free protection measures when patch updates cannot be provided in time in the user environment [9]. In addition, the firewall is used to reduce the attack level, prevent DoS attacks and defects, and realize monitoring scanning. Using virus killing software to detect and intercept malware. Detect malicious and unauthorized changes in prominent system directories, files and registry entries through integrity monitoring. Log audit is used to optimize and identify prominent security events from massive data.

Cloud platform desktop virtualization (CPDV) enables users to access virtual desktops that run on a shared physical server. CPDV provides many benefits, such as increased mobility, flexibility, and cost savings. However, CPDV also poses significant security challenges, such as data breaches, malware infections, and unauthorized access. The following are some security protection schemes for the CPDV environment.

1. Access control: Access control is a critical component of the security protection scheme for the CPDV environment. Cloud providers need to implement strict access control measures, such as strong authentication mechanisms, role-based access control, and virtual private networks (VPNs). Only authorized users should be able to access the virtual desktop, and access should be restricted to specific devices and locations.
2. Encryption: Encryption is a critical component of the security protection scheme for the CPDV environment. All data transmitted between the virtual desktop and the user's device should be encrypted to protect against eavesdropping and data theft. Encryption should be implemented at both the network and data levels, using strong encryption algorithms and key management techniques.
3. Malware protection: Malware protection is a critical component of the security protection scheme for the CPDV environment. Cloud providers need to implement strict malware protection measures, such as antivirus software, intrusion detection, and application whitelisting. All virtual desktops should be scanned regularly for malware infections, and infected desktops should be isolated and cleaned.
4. Data protection: Data protection is a critical component of the security protection scheme for the CPDV environment. Cloud providers need to ensure that data is protected from unauthorized access, modification, and deletion. Data protection measures, such as encryption and access control, need to be implemented at both the virtual desktop and host levels.
5. Compliance: Compliance is a critical component of the security protection scheme for the CPDV environment. Cloud providers need to comply with various regulations, such as HIPAA, GDPR, and PCI-DSS. Compliance requirements should be integrated into the security protection scheme to ensure that security measures meet regulatory standards.

In conclusion, CPDV poses significant security challenges, and cloud providers need to implement strict security protection schemes to protect virtual desktops and user data. Access control, encryption, malware protection, data protection, and compliance are critical components of the security protection scheme for the CPDV environment. Cloud users also need to be aware of these security challenges and take appropriate measures to protect their data, such as strong passwords, two-factor authentication, and encryption. Overall, CPDV can be secure if proper security protection schemes are implemented and monitored.

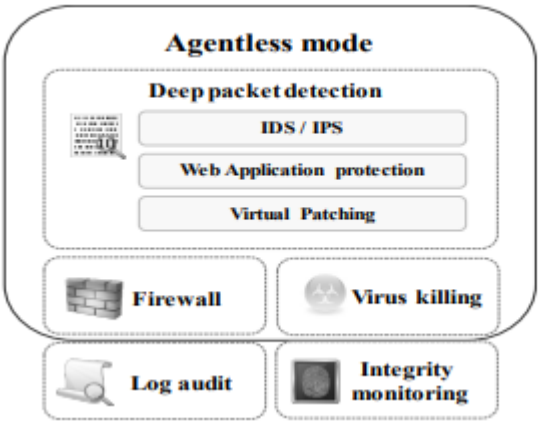

Figure. 3. Architecture of solutions for virtual environments

4. Results and Discussion

4.1. Functions of virtualization security protection management system of cloud platform

The design of the virtualization security protection management system of the cloud platform needs to be carried out from the dimensions of access security, design security, host security, multi-tenant resource isolation and data storage security. The virtualization security protection system of cloud platform needs to establish DDoS attack defense, intrusion defense, and vulnerability analysis and situation awareness [10]. The implementation formula of container virtualization tech is shown in formula 1-2 below. In addition, the virtualization security protection management system of the cloud platform can provide traffic traction and services, realize centralized platform management, provide permission management and development interfaces, and provide cloud security function services. In which, L is the container engine and D is the container, so as to ensure the consistency between the execution environment of the hosted utilization and the previous definition.

$$L = C_{goup} + N + CH_{root} + V \quad (1)$$

$$D = L + AUFX + L = C_{goup} + N + T \quad (2)$$

4.2. Utilization of virtualization security protection management system of cloud platform

The cloud platform introduces network traffic into the virtual service chain or virtual machine according to the user service chain and virtual machine configuration, and processes the returned traffic and sends it to the user. Secondly, provide differentiated security protection services according to the personalized strategy of the cloud platform. In addition, the access point equipment realizes user differentiation, drainage and diversion, and ensures the availability of the network. The virtualization security protection management system of the cloud platform provides traffic traction and services, centralized management of the platform and cloud security function services

5. Conclusion

In recent years, cloud platforms have become an essential part of many businesses, providing users with the ability to access virtualized resources and services from anywhere in the world. However, cloud platforms are not immune to security threats, and it is crucial to implement a robust security protection management system to protect the virtualized environment. This paper proposes a new virtualization security protection management system based on the cloud platform, aimed at improving the virtualization security service capability carried on the cloud platform while supporting a multidimensional security mode. The proposed system also enables the customization and self-service of cloud platform security policy to enhance the security protection of virtualized resources and services.

The paper first analyzes the virtualization characteristics of cloud platforms and the security threats they face. It then studies the trend and challenges of cloud platform virtualization security management and protection. This research provides a comprehensive understanding of the security challenges of cloud platforms and the need for a security protection management system. The paper then analyzes the security protection scheme of cloud platform virtualization environments, emphasizing access control, encryption, malware protection, data protection, and compliance. These measures are critical to protecting virtualized resources and services and ensuring the confidentiality, integrity, and availability of data.

Finally, the paper proposes a construction scheme and utilization function of security protection for the cloud platform virtualization environment. This proposed system aims to provide robust security protection, with the customization and self-service of security policies to suit the needs of different businesses. In conclusion, this paper proposes a new virtualization security protection management system based on cloud platforms. The proposed system provides a comprehensive solution to the security challenges faced by virtualized resources and services. By implementing the proposed security protection measures, cloud platforms can ensure the confidentiality, integrity, and availability of data and improve the security service capabilities of the platform.

References

[1] S. Vinoth, H. L. Vemula, B. Haralayya, P. Mamgain, M. F. Hasan, and M. Naved, "Application of cloud computing in banking and e-commerce and related security threats," *Mater. Today Proc.*, vol. 51, pp. 2172–2175, 2022.
[2] S. Liu, L. Guo, H. Webb, X. Ya, and X. Chang, "Internet of Things monitoring system of modern eco-agriculture based on cloud computing," *IEEE Access*, vol. 7, pp. 37050–37058, 2019.
[3] O. Demigha and R. Larguet, "Hardware-based solutions for trusted cloud computing," *Comput. Secur.*, vol. 103, p. 102117, 2021.
[4] D. Cotroneo, L. De Simone, P. Liguori, R. Natella, and N. Bidokhti, "How bad can a bug get? an empirical analysis of software failures in the openstack cloud computing platform," in *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 2019, pp. 200–211.
[5] H. Ben Hassen, N. Ayari, and B. Hamdi, "A home hospitalization system based on the Internet of things, Fog computing and cloud computing," *Informatics Med. Unlocked*, vol. 20, p. 100368, 2020.
[6] J. Shen, X. Deng, and Z. Xu, "Multi-security-level cloud storage system based on improved proxy re-encryption," *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, pp. 1–12, 2019.
[7] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, 2020.
[8] M. Compastié, R. Badonnel, O. Festor, and R. He, "From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models," *Comput. Secur.*, vol. 97, p. 101905, 2020.
[9] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application," *IEEE Access*, vol. 8, pp. 101079–101092, 2020.
[10] Y. Allahvirdizadeh, M. P. Moghaddam, and H. Shayanfar, "A survey on cloud computing in energy management of the smart grids," *Int. Trans. Electr. Energy Syst.*, vol. 29, no. 10, p. e12094, 2019.
[11] L. Ding, Z. Wang, X. Wang, and D. Wu, "Security information transmission algorithms for IoT based on cloud computing," *Comput. Commun.*, vol. 155, pp. 32–39, 2020.
[12] N. Mansouri, R. Ghafari, and B. M. H. Zade, "Cloud computing simulators: A comprehensive review," *Simul. Model. Pract. Theory*, vol. 104, p. 102144, 2020.
[13] A. Bhardwaj and C. R. Krishna, "Virtualization in cloud computing: Moving from hypervisor to containerization—a survey," *Arab. J. Sci. Eng.*, vol. 46, no. 9, pp. 8585–8601, 2021.
[14] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions," *J. Cloud Comput.*, vol. 10, no. 1, pp. 1–34, 2021.
[15] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in iot-based cloud computing: A comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, 2022.
[16] F. K. Parast, C. Sindhav, S. Nikam, H. I. Yekta, K. B. Kent, and S. Hakak, "Cloud computing security: A survey of service-based models," *Comput. Secur.*, vol. 114, p. 102580, 2022.
[17] F. K. Parast, C. Sindhav, S. Nikam, H. I. Yekta, K. B. Kent, and S. Hakak, "Cloud computing security: A survey of service-based models," *Comput. Secur.*, vol. 114, p. 102580, 2022.
[18] P. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," *J. Netw. Comput. Appl.*, vol. 160, p. 102642, 2020.

[19] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 4, p. 1550147719844159, 2019.
[20] S. Al-Mashhadi, M. Anbar, R. A. Jalal, and A. Al-Ani, "Design of cloud computing load balance system based on SDN technology," in *Computational Science and Technology: 6th ICCST 2019, Kota Kinabalu, Malaysia, 29-30 August 2019*, 2020, pp. 123–133.
[21] Q. Qi and F. Tao, "A smart manufacturing service system based on edge computing, fog computing, and cloud computing," *IEEE access*, vol. 7, pp. 86769–86777, 2019.
[22] J. Koo, Y.-G. Kim, and S.-H. Lee, "Security requirements for cloud-based C4I security architecture," in *2019 International Conference on Platform Technology and Service (PlatCon)*, 2019, pp. 1–4.
[23] A. Alam, "Cloud-Based E-learning: Scaffolding the Environment for Adaptive E-learning Ecosystem Based on Cloud Computing Infrastructure," in *Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2*, Springer, 2022, pp. 1–9.
[24] P. Y. Abdullah, S. R. Zeebaree, K. Jacksi, and R. R. Zeabri, "An hrm system for small and medium enterprises (sme) s based on cloud computing technology," *Int. J. Res.*, vol. 8, no. 8, pp. 56–64, 2020.
[25] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," *J. Reliab. Intell. Environ.*, vol. 7, pp. 69–84, 2021.