World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:18, No:8, 2024

Cloud Monitoring and Performance Optimization Ensuring High Availability and Security

Inayat Ur Rehman, Georgia Sakellari

Open Science Index, Computer and Systems Engineering Vol:18, No:8, 2024 publications.waset.org/10013788.pdf

Abstract**—**Cloud computing has evolved into a vital technology for businesses, offering scalability, flexibility, and cost-effectiveness. However, maintaining high availability and optimal performance in the cloud is crucial for reliable services. This paper explores the significance of cloud monitoring and performance optimization in sustaining the high availability of cloud-based systems. It discusses diverse monitoring tools, techniques, and best practices for continually assessing the health and performance of cloud resources. The paper also delves into performance optimization strategies, including resource allocation, load balancing, and auto-scaling, to ensure efficient resource utilization and responsiveness. Addressing potential challenges in cloud monitoring and optimization, the paper offers insights into data security and privacy considerations. Through this thorough analysis, the paper aims to underscore the importance of cloud monitoring and performance optimization for ensuring a seamless and highly available cloud computing environment.

Keywords**—**Cloud computing, cloud monitoring, performance optimization, high availability.

I. Introdu.ction

THE introduction of this paper emphasizes the significance of cloud monitoring and performance optimization in ensuring the high availability of cloud-based systems. Cloud monitoring involves the continuous assessment of the health, performance, and availability of cloud resources, while performance optimization strategies aim to maximize resource efficiency and responsiveness. In recent years, significant advancements in cloud monitoring tools and techniques have provided real-time insights into the performance of cloud infrastructures, applications, and services. This proactive monitoring approach enables early detection of potential issues, allowing timely corrective actions to be taken before impacting the user experience [1].

Performance optimization in the cloud encompasses various strategies, including efficient resource allocation, load balancing, and auto-scaling. These techniques ensure optimal resource utilization, preventing bottlenecks and maintaining consistent performance under varying workloads [2].

The objective of this paper is to explore different aspects of cloud monitoring and performance optimization and their critical role in ensuring high availability. It discusses best practices for implementing a robust cloud monitoring strategy and provides insights into effective performance optimization techniques. Additionally, the paper addresses potential challenges in cloud monitoring and optimization, such as handling large-scale data and addressing data security and privacy concerns.

As the adoption of cloud computing continues to grow, organizations must prioritize high availability and performance optimization to meet user expectations, uphold service level agreements, and safeguard their reputation. Through a comprehensive understanding of cloud monitoring and performance optimization, businesses can create a seamless and highly available cloud computing environment, enabling them to leverage the full potential of cloud technology to drive innovation and business growth.

II. Literature Review

The existing body of literature on cloud monitoring and performance optimization underscores the importance of these practices in guaranteeing the high availability and optimal performance of cloud-based systems. Researchers and practitioners have thoroughly investigated different facets of cloud monitoring and optimization, encompassing the utilization of monitoring tools, strategies for enhancing performance, and their influence on overall cloud performance [3]. This literature review amalgamates key findings and trends from pertinent studies to offer a comprehensive understanding of the role played by cloud monitoring and performance optimization in sustaining a seamless and highly available cloud computing environment [4].

A. Significance of Cloud Monitoring

Multiple studies accentuate the pivotal role of cloud monitoring in ensuring high availability and facilitating proactive issue resolution. Real-time insights from cloud monitoring tools and techniques enable organizations to promptly detect and address performance bottlenecks and potential issues [5]. Effective monitoring practices empower businesses to meet service level agreements (SLAs) and ensure consistent user experiences, thereby enhancing customer satisfaction and loyalty [6].

B. Performance Optimization Strategies

The literature extensively deliberates on various performance optimization strategies in the cloud. Key techniques highlighted include efficient resource allocation, load balancing, and auto-scaling, all of which aim to maximize resource utilization and maintain responsiveness under varying workloads [7]. Crucial resource allocation algorithms and load balancing mechanisms play a vital role in evenly distributing workloads across cloud resources, preventing resource contention, and ensuring

Inayat Ur Rehman is with University of Greenwich, UK (e-mail: inayat.akram921@gmail.com).

Open Science Index, Computer and Systems Engineering Vol:18, No:8, 2024 publications.waset.org/10013788.pdf

optimal performance [8].

C. Impact of Performance Optimization on Cloud Services

Researchers delve into the impact of performance optimization on cloud services and applications. Techniques such as auto-scaling dynamically adjust resource allocation based on workload demands, allowing applications to scale up or down as needed, resulting in cost savings and enhanced performance [9]. Additionally, load balancing mechanisms optimize resource utilization, preventing overloading of specific resources and improving overall system efficiency [10].

D. Challenges in Cloud Monitoring and Performance Optimization

The literature also sheds light on challenges associated with cloud monitoring and optimization. Handling large-scale data generated by monitoring tools can be resource-intensive and necessitate efficient data storage and processing mechanisms [11]. Moreover, ensuring data security and privacy is crucial, given that monitoring data may contain sensitive information. Addressing these challenges requires careful consideration and adherence to data protection regulations.

E. Real-world Applications and Case Studies

Researchers explore various real-world applications of cloud monitoring and performance optimization. Case studies showcase successful implementations of monitoring tools and optimization strategies, illustrating their transformative impact on maintaining high availability and enhancing cloud performance [12]. These studies serve as examples of best practices and provide insights into effective cloud monitoring and optimization.

In conclusion, the literature on cloud monitoring and performance optimization emphasizes their crucial role in guaranteeing the high availability and optimal performance of cloud-based systems. Cloud monitoring tools and techniques offer real-time insights into the performance of cloud resources, facilitating proactive issue resolution and ensuring consistent user experiences. Performance optimization strategies, including resource allocation, load balancing, and auto-scaling, contribute to maximizing resource utilization and responsiveness, leading to cost savings and enhanced cloud performance [13].

Addressing challenges in cloud monitoring and optimization, such as managing large-scale data and ensuring data security, is imperative for constructing a robust and reliable cloud computing environment. Through the implementation of effective cloud monitoring practices and optimization strategies, organizations can uphold high availability, meet service level agreements (SLAs), and deliver seamless cloud services to users [14].

As the adoption of cloud computing continues to expand, the roles of cloud monitoring and performance optimization will become increasingly vital in shaping the success of businesses and organizations. Proactive monitoring and efficient optimization empower enterprises to unlock the full potential of cloud technology, fostering innovation, and providing exceptional user experiences in the digital age.

A. Challenges in Cloud Security

Cloud systems operate on the internet, inheriting security challenges present in the online environment. Similar to traditional PC systems, cloud computing is susceptible to both familiar and unique security issues. The primary apprehensions associated with cloud computing revolve around security and privacy.

Cloud systems, like traditional systems, face security threats such as vulnerabilities, viruses, and hacking attacks. However, these threats can have more severe consequences in the realm of cloud computing due to its inherent characteristics. Malicious actors may exploit vulnerabilities to hack into cloud accounts, compromising sensitive data stored within cloud systems. With data and business applications centralized in cloud centres, robust protection measures are essential.

Cloud computing, characterized by virtualization, service-oriented architecture, and utility computing over the Internet, encompasses applications, platforms, and services. Fast recovery from system failures poses a challenge. The complexity of cloud systems hides the intricacies of service implementation technology and management from users. Consequently, users lack control over data processing details and must trust the cloud provider to ensure data security.

Critical data resources and private information demand stringent protection. Cloud systems should offer user-controlled data management systems, including data security audits. Ensuring data availability, integrity, and confidentiality requires robust user access control mechanisms that encompass licensing, certification, and quarantine protocols.

In the dynamic landscape of cloud computing, providers cater to numerous users with varying service needs. Users are unaware of the data's physical location, processing servers, or the network transmitting the data due to the flexibility and scalability of cloud systems. This lack of transparency raises concerns about data privacy and confidentiality. Additionally, deploying cloud centres in different regions introduces legal complexities, as each area may have distinct laws governing security management. Hence, legal protection measures must be enhanced in cloud computing services.

III. Discussion

The conversation on cloud monitoring and performance optimization revolves around how they significantly transform cloud computing, the advantages of proactive monitoring, the efficacy of optimization strategies, and the difficulties associated with managing monitoring data and ensuring data security.

A. Transformative Impact on Cloud Computing

The realm of cloud monitoring and performance optimization has brought about a transformative change in how organizations oversee and provide cloud services [15]. The incorporation of real-time monitoring tools allows organizations to acquire valuable insights into the well-being and performance of cloud resources, empowering them to proactively address issues and uphold high availability. The smooth integration of optimization strategies guarantees the efficient utilization of cloud resources, promoting cost-effectiveness and enhancing overall system efficiency [16].

B. Benefits of Proactive Monitoring

The literature underscores the significance of proactive monitoring within cloud environments. Detecting performance issues early on enables organizations to promptly tackle them, thereby reducing the risk of service disruptions and dissatisfaction among users. Proactive monitoring also empowers organizations to fulfil SLAs, ensuring the delivery of consistent and reliable cloud services, ultimately enhancing customer satisfaction and fostering loyalty.

C. Effectiveness of Optimization Strategies

Strategies for optimizing performance, such as resource allocation, load balancing, and auto-scaling, have demonstrated their effectiveness in maximizing the utilization of cloud resources. Well-designed resource allocation algorithms and load balancing mechanisms evenly distribute workloads, mitigating resource contention and enhancing overall cloud performance. Auto-scaling dynamically adjusts resource allocation in response to workload demands, ensuring that applications can scale up or down as necessary. This dynamic approach optimizes cost-effectiveness and responsiveness.

D. Challenges of Handling Monitoring Data and Data Security

Deploying cloud monitoring generates extensive data that necessitates streamlined storage and processing mechanisms. Organizations need to confront these challenges to guarantee the effective management of monitoring data without compromising system performance. Moreover, prioritizing data security and privacy in monitoring processes is essential, given that monitoring data may include sensitive information. Strict compliance with data protection regulations and the implementation of robust security measures are crucial for safeguarding monitoring data and upholding data integrity [17].

The integration of cloud monitoring and performance optimization has demonstrated its transformative impact on cloud computing, ensuring the high availability and optimal performance of cloud-based systems. Proactive monitoring practices empower organizations to promptly identify and address performance issues, preventing potential service disruptions and maintaining consistent user experiences. Optimization strategies, such as resource allocation, load balancing, and auto-scaling, enhance resource utilization and responsiveness, fostering cost-effectiveness and system efficiency [18].

Despite challenges related to handling monitoring data and ensuring data security, organizations can overcome them through effective data management strategies and robust security measures. By embracing cloud monitoring and performance optimization, businesses can fully unlock the potential of cloud technology, driving innovation and delivering seamless, reliable cloud services to users.

As the adoption of cloud computing continues to expand, the importance of cloud monitoring and performance optimization will only grow. Organizations prioritizing proactive monitoring and optimization strategies will be better prepared to meet user expectations, uphold high availability, and leverage the benefits of cloud computing in the digital era. Through continuous monitoring and optimization, businesses can remain at the forefront of cloud technology, propelling growth and success in an increasingly data-driven and interconnected world [19].

Data stored in cloud systems face the risk of unauthorized theft and modification. While encryption can enhance security, the process becomes more time-consuming and resource-intensive with larger data sizes. Confidential data, when accessible by external entities, pose a significant concern. Traditional techniques, including encryption, security authentication, and access control policies, offer some level of data privacy and security in cloud environments [20].

Encryption methods, such as symmetric and asymmetric key systems, provide varying levels of security. While asymmetric key encryption offers high security, it comes with slower encryption and decryption processes. Security authentication relies on widely accepted technologies like PKI, X.509 certificates, and X.500 standards [21].

Access control policies, crucial for preventing illegal use of network resources, encompass network access control and directory-level security control. Users with access to the cloud system include the cloud provider, operations and maintenance personnel, and customer users. Ensuring that customer data remain secure and are not unlawfully utilized by other cloud providers is a significant challenge.

Operation and maintenance personnel are tasked with data storage, backup, and data classification management based on security levels. Cloud computing storage security involves aspects like data storage isolation, storage location, data recovery, and long-term survivability. Once data is in the cloud, control shifts to the cloud computing provider, raising concerns about privacy breaches [22].

Monitoring and auditing become critical issues for cloud providers, as achieving full transparency in cloud computing services is challenging for customers. Customers lack insight into internal processes, data storage locations, and the potential impact of accidents. Granting customers the right to supervise and audit cloud computing services is crucial for ensuring the security of their data.

Control measures for communication of worms, viruses, and Trojans within the cloud computing platform are vital. Timely isolation of malicious programs, immediate system repairs following damage, and real-time monitoring of data traffic and system status are essential. Deploying network attack detection and defence systems is necessary to prevent service interruptions and system failures caused by hackers.

Implementing disaster recovery mechanisms, including system backups and data recovery, is crucial for addressing emergency situations. Establishing and improving emergency response mechanisms and capabilities further safeguards user information availability, privacy, and integrity. Security isolation and protection for user systems and data, along with network data transmission security through encryption and

VPN technology, contribute to a comprehensive security framework.

Considering the cloud system as a service-oriented architecture (SOA) hides underlying details and provides transparent services to customers. Treating cloud services as web services allows for reference to security mechanisms in SOA, including WS-Security, WS-Reliability, WS-Trust, WS-Authorization, and WS-Secure Conversation. SOA facilitates interoperability between different systems and programming languages, forming the basis for integration between applications on various platforms through communication protocols.

IV. Cloud Computing Service Delivery Models and Security Implications

We outline the primary security concerns and vulnerabilities associated with each service delivery model. Some of these issues fall under the jurisdiction of cloud providers, while others are the responsibility of cloud consumers.

A. IaaS Security Issues

Securing virtual machines (VMs) involves protecting the operating systems and workloads from common security threats, such as malware and viruses, akin to safeguarding traditional physical servers. Cloud consumers bear the responsibility for VM security, employing their own security controls based on specific needs, anticipated risk levels, and internal security management processes.

The security of the VM images repository is crucial, as VMs remain vulnerable even when offline. Potential risks include compromise through the injection of malicious code into VM files or the theft of VM files. Cloud providers are accountable for ensuring a secure VM images repository. Additionally, concerns may arise with VM templates retaining original owner information, potentially impacting new consumers.

Virtual network security becomes paramount when sharing network infrastructure among different tenants within the same server or physical networks. This sharing increases the likelihood of exploiting vulnerabilities in DNS servers, DHCP, IP protocols, or vSwitch software, leading to network-based VM attacks [23].

VM boundaries, distinct from physical server boundaries, require attention as VMs sharing the same physical server lack physical isolation among resources like CPU, Memory, I/O, and NIC. Securing VM boundaries falls under the responsibility of the cloud provider [24].

The hypervisor, acting as the virtualizer mapping between physical and virtualized resources, plays a critical role in controlling access to physical server resources by VMs. Compromising the hypervisor jeopardizes VM security, as all VM operations become traceable in an unencrypted manner. Hypervisor security is a joint responsibility of cloud providers and service providers. The service provider, in this context, refers to the company delivering the hypervisor software, such as VMware or Xen.

B. PaaS Security Issues

Security concerns related to SOA are inherent in the Platform as a Service (PaaS) model, which is built upon the SOA framework. These concerns encompass various issues from the SOA domain, including Denial of Service (DOS) attacks, Man-in-the-Middle attacks, XML-related vulnerabilities, Replay attacks, Dictionary attacks, Injection attacks, and input validation-related threats [9], [16]. To secure cloud-provided services in the PaaS model, it is crucial to implement mutual authentication, authorization, and adhere to WS-Security standards. The responsibility for addressing these security issues is shared among cloud providers, service providers, and consumers.

API Security is a focal point within PaaS, as it often involves APIs delivering essential functions such as business operations, security functions, and application management. These APIs must incorporate robust security controls and standards, such as OAuth to ensure consistent authentication and authorization for API calls. Additionally, the isolation of APIs in memory is essential. The responsibility for addressing this security concern lies with the cloud service provider [25].

C. SaaS Security Issues

Within the Software as a Service (SaaS) model, the responsibility for enforcing and maintaining security is a collaborative effort between cloud providers and service providers, which include software vendors. Inheriting security concerns from the underlying Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) models, SaaS encompasses data security management addressing aspects such as data locality, integrity, segregation, access, confidentiality, and backup and network security.

To ensure the security of web applications hosted on cloud infrastructure, it is imperative to conduct thorough validation and scanning for vulnerabilities using up-to-date web application scanners [26]. These scanners should stay current with recently discovered vulnerabilities and attack paths documented in the National Vulnerability Database (NVD) and the Common Weaknesses Enumeration (CWE) implementing web application firewalls is essential for mitigating existing or discovered vulnerabilities by scrutinizing HTTP requests and responses for application-specific weaknesses. OWASP's list of the ten most critical web application vulnerabilities in 2010, including injection and cross-site scripting (input validation) weaknesses, serves as a reference.

Addressing web application security misconfigurations and vulnerabilities in application-specific security controls is a significant concern in SaaS. Security misconfigurations become particularly critical in multi-tenancy scenarios, where each tenant may have unique security configurations that could conflict, potentially leading to security vulnerabilities. While it is generally recommended to rely on the security controls provided by the cloud provider for consistent, dynamic, and robust security enforcement and management, ensuring proper configurations at the application level remains crucial.

V. CONCLUSION

Ensuring the continuous availability and optimal functioning of cloud-based systems requires the essential practices of cloud monitoring and performance optimization. Employing real-time monitoring tools and proactive strategies provides organizations with valuable insights into the health and performance of their cloud resources. This capability enables timely detection and resolution of performance issues, minimizing potential service disruptions and ensuring a consistent user experience.

Critical to maximizing the utilization and responsiveness of cloud resources are performance optimization strategies, including efficient resource allocation, load balancing, and auto-scaling. These strategies play a vital role in enhancing cost-effectiveness, preventing resource contention, and improving overall system efficiency, even when faced with varying workloads.

The transformative impact of cloud monitoring and performance optimization is evident in their ability to drive innovation and deliver reliable cloud services. Proactive monitoring practices enable organizations to meet service level agreements (SLAs) and ensure customer satisfaction, thereby fostering loyalty and trust. Optimization strategies not only enhance system efficiency but also result in cost savings, rendering cloud services more economically viable.

Despite these benefits, challenges exist in managing large-scale monitoring data and ensuring data security and privacy. Efficient data management strategies and robust security measures are necessary for addressing these challenges and safeguarding sensitive information to maintain data integrity.

In conclusion, cloud monitoring and performance optimization are indispensable for organizations aiming to unleash the full potential of cloud computing. Prioritizing proactive monitoring and optimization strategies allows businesses to sustain high availability, meet user expectations, and deliver seamless and reliable cloud services. As cloud technology evolves, these practices will remain integral components of cloud-based systems, empowering organizations to stay at the forefront of innovation and thrive in the dynamic and competitive digital landscape.

The issue of data privacy has become increasingly significant in comparison to traditional networks, given the substantial reliance of data in the cloud computing environment on networks and servers. Numerous customers harbour scepticism regarding the security and privacy of cloud computing, leading to hesitancy in transferring data from company or private systems to cloud platforms. These concerns pose obstacles to the advancement of cloud computing, with security emerging as the central challenge. To address these issues effectively, cloud computing providers must implement a range of measures to enhance security.

REFERENCES

[1] Syed, H.J., Gani, A., Ahmad, R.W., Khan, M.K. and Ahmed, A.I.A, "Cloud monitoring: A review, taxonomy, and open research issues," Journal of Network and Computer Applications, pp. 11-26, 2017.

[2] Simic, V., Stojanovic, B. and Ivanovic, M.,, "Optimizing the performance of optimization in the cloud environment–An intelligent auto-scaling approach," Future Generation Computer Systems, vol. 1, no. 101, pp. 909-920, 2019.

[3] Moses, J., Iyer, R., Illikkal, R., Srinivasan, S. and Aisopos, K., "Shared resource monitoring and throughput optimization in cloud-computing datacenters," in IEEE International Parallel & Distributed Processing Symposium, Alaska USA, 2011.

[4] Zeb, S., Mahmood, A., Hassan, S.A., Piran, M.J., Gidlund, M. and Guizani, M, "Industrial digital twins at the nexus of nextG wireless networks and computational intelligence: A survey," ournal of Network and Computer Applications, vol. 1, no. 200, p. 103309, 2022.

[5] S. Pargaonkar, "A Comprehensive Review of Performance Testing Methodologies and Best Practices," Software Quality Engineering. International Journal of Science and Research (IJSR), vol. 12, no. 8, pp. 2008-2014, 2023.

[6] Prasad, V.K., Dansana, D., Bhavsar, M.D., Acharya, B., Gerogiannis, V.C. and Kanavos, A, "Efficient Resource Utilization in IoT and Cloud Computing," Information, vol. 14, no. 11, p. 619, 2023.

[7] Alipour, H., Liu, Y. and Hamou-Lhadj, A, "Analyzing auto-scaling issues in cloud environments," CASCON, vol. 14, pp. 75-89, 2014.

[8] Hussain, H., Malik, S.U.R., Hameed, A., Khan, S.U., Bickler, G., Min-Allah, N., Qureshi, M.B., Zhang, L., Yongji, W., Ghani, N. and Kolodziej, J, "A survey on resource allocation in high performance distributed computing systems," Parallel Computing, vol. 39, no. 11, pp. 709-736, 2013.

[9] Lorido-Botran, T., Miguel-Alonso, J. and Lozano, J.A., 2014., "A review of auto-scaling techniques for elastic applications in cloud environments," Journal of grid computing, vol. 12, pp. 559-592, 2014.

[10] Milani, A.S. and Navimipour, N.J., 2016, "Load balancing mechanisms and techniques in the cloud environments: Systematic literature review and future trends," Journal of Network and Computer Applications, no. 71, pp. 86-98, 2016.

[11] Rodríguez-Mazahua, L., Rodríguez-Enríquez, C.A., Sánchez-Cervantes, J.L., Cervantes, J., García-Alcaraz, J.L. and Alor-Hernández, G., "A general perspective of Big Data: applications, tools, challenges and trends," The Journal of Supercomputing, no. 72, pp. 3073-3113, 2016.

[12] T. Muhammad, " A Comprehensive Study on Software-Defined Load Balancers: Architectural Flexibility & Application Service Delivery in On-Premises Ecosystems," International Journal of Computer Science and Technology, vol. 6, no. 1, pp. 1-24, 2022.

[13] Raj, P., Raman, A., Raj, P. and Raman, A., "Multi-cloud management: Technologies, tools, and techniques. Software-Defined Cloud Centers," Operational and Management Technologies and Tools, pp. 219-240, 2018.

[14] Odun-Ayo, I., Udemezue, B. and Kilanko, "Cloud service level agreements and resource management," Adv. Sci. Technol. Eng. Syst, vol. 4, no. 2, pp. 228-236, 2019.

[15] Hugos, M.H. and Hulitzky, D, "Business in the cloud: what every business needs to know about cloud computing," John Wiley & Sons, 2010.

[16] A. J. A. P. P. C. H. a. G. L. Sangaiah, "Cost-effective resources for computing approximation queries in mobile cloud computing infrastructure," Sensors, vol. 23, no. 17, p. 7416, 2023.

[17] R. Dittakavi, "Evaluating the Efficiency and Limitations of Configuration Strategies in Hybrid Cloud Environments," International Journal of Intelligent Automation and Computing, vol. 5, no. 2, pp. 29-45, 2022.

[18] A. Kunduru, "Artificial intelligence usage in cloud application performance improvement," Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 8, pp. 42-47, 2023.

[19] Hassan, A. and Mhmood, A.H, "Optimizing Network Performance, Automation, and Intelligent Decision-Making through Real-Time Big Data Analytics," International Journal of Responsible Artificial Intelligence, vol. 11, no. 8, pp. 12-22, 2021.

[20] Kaaniche, N. and Laurent, M., 2017, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," Computer Communications, no. 111, pp. 120-141, 2017.

[21] Alenezi, M.N., Alabdulrazzaq, H. and Mohammad, N.Q, "Symmetric encryption algorithms: Review and evaluation study," International Journal of Communication Networks and Information Security, vol. 12, no. 2, pp. 256-272, 2020.

[22] Wang, L., Ranjan, R., Chen, J. and Benatallah, B. eds, Cloud computing: methodology, systems, and applications. CRC press., 2017.

[23] S. Faizan, "SDN based security using cognitive algorithm against DDOS," 2018.

[24] Xu, F., Liu, F., Jin, H. and Vasilakos, A.V., 2013, "Managing performance overhead of virtual machines in cloud computing: A survey, state of the art, and future directions," Proceedings of the IEEE, vol. 102, no. 1, pp. 11-31, 2013.

[25] Devi, T. and Ganesan, R., 2015, "Platform-as-a-Service (PaaS): model and security issues," TELKOMNIKA Indonesian Journal of Electrical Engineering, vol. 15, no. 1, pp. 151-161, 2015.

[26] M. 2. Wilgus, "Best Practices When Implementing Web Application Scanning into an SDLC," ISSA Journal, vol. 15, no. 5, 2017.