ARTICLE

Cite This: J. of Busi. Intell. and Data Analy.2025, 2, 1-05

Sciforce

Journal of Business Intelligence and Data Analytics

Journal homepage: www.sciforce.org

Frameworks and Tools for Enhancing Cloud Network Security: A Review

Seetaram RayaRao*

VP, Senior Tech Lead, JP Morgan Chase, USA

ARTICLE INFO

Article history:
Received:20241228
Received in revised form: 20250106
Accepted: 20250106
Available online: 20250114

Keywords:
Security frameworks;
Cloud tools;
Network security and Enhancements.

ABSTRACT

Cloud Networking Security" isn't a specific entity or person but rather a concept that refers to the overarching principles and practices involved in securing cloud networking environments. It encompasses the strategies and tools used to protect cloud-based infrastructure, data, and applications from cyber threats. The advent of cloud computing has transformed industries by promoting rapid innovation, improving collaboration, and deploying complex applications. However, despite its many advantages, cloud computing presents challenges related to security, privacy and data sovereignty. Addressing these issues is critical to fully realizing the benefits of cloud technology.

*Corresponding author. Tel.: +1(302)-304-8402; e-mail: seetaram.r@gmail.com

Introduction:

The cloud works like a plug-and-play ERP system. Network virtualization is important in the development of cloud computing, enabling multiple independent virtual networks to operate on a shared infrastructure. However, setting up a cloud computing environment can be quite complex. Both businesses and government organizations are increasingly adopting cloud-based systems to improve business processes and operational efficiency. Various enterprise services and applications are constantly evolving, new solutions are emerging and outdated ones are being phased out. 75% of companies in North America and Europe outsource various aspects of their operations, meaning that critical business data is not only spread across different systems within a company, but also across different IT infrastructures. Technological advances such as more affordable processors, low-latency networks, and major improvements in virtualization have enabled this change.

As a result, computing tasks can now be moved from local IT systems to distributed cloud infrastructures. The cloud service delivery model enables users to lease and release computing resources through self-service interfaces and a flexible payment system. Key cloud features, including resource sharing, on-demand scaling, customizable self-service, application monitoring, and pervasive access, are fueling the expansion of cloud-based business applications and use cases. These enhancements greatly increase the performance and functionality of existing and new software.However, despite growing adoption and interest in cloud computing, existing concerns may slow its progress and hinder its potential to revolutionize IT procurement models.

When analyzing barriers to cloud computing adoption, various issues emerge from historical and contemporary contexts and may gain importance over time. Corporate partnerships and offshore outsourcing face similar challenges related to trust and regulatory compliance. Likewise, open source software allows IT departments to quickly develop and deploy applications, although this involves some trade-offs in terms of control and management.

Cloud Computing:

Cloud computing includes IT services such as infrastructure, platforms and applications available over the Internet. This model operates on a pay-as-you-go basis, where costs are based on actual resource usage It sounds like you're asking who or what "cloud framework" refers to, rather than a specific framework. In general, "cloud framework" is not a person, but rather a collection of various tools, platforms, or best practices used in cloud computing This adaptive approach is designed to manage the rapid growth of Internet-connected devices and handle large volumes of data. In addition, various IPTABLES configurations are used to regulate network traffic, where rules are applied via shell scripts.

Cloud providers use a multi-tenant model to pool computing resources, dynamically allocating them to different users as needed.This loop identifies all possible connection pairs between nodes in the cloud cluster by generating each possible pair wise permutation and determining the shortest path for each

pair. It explores all possible routes between a start node and an endpoint, allowing for multiple paths. Cloud infrastructure is used only by one organization It provides enhanced control over resources and security. In computing, the term "cloud" encompasses the hardware, software, networks, storage, services, and interfaces that together provide computing capabilities as a service.

Cloud computing enables users to access standardized IT resources on demand, allowing them to quickly deploy new applications, services or computing resources without having to replace their entire infrastructure, thereby increasing flexibility. The main idea of cloud computing is to reduce the processing load on users' devices by continuously improving cloud computing capabilities. Cloud security is a hotly debated issue among experts and researchers. Major international events focused on cloud security include the European Conference, the ACM Workshop on Cloud Computing Security, and the International Conference on Cloud Security Management.

In addition, you can find many research articles on related topics in journals focused on cloud security. Using cloud storage to handle and process large volumes of traffic data on a cloud computing platform is recommended to detect malicious attacks.Resources are controlled and managed by third-party cloud service providers spread across the Internet. Cloud computing offers many benefits, including reduced costs and capital expenditures, improved operational efficiency, and greater adaptability, flexibility, and scalability. Although these advantages are attractive to researchers and IT professionals, security concerns continue to be a major challenge. If these security issues are not effectively addressed, they will hinder the adoption and use of cloud computing in the future.

Cloud Framework:

This article explores security threats and vulnerabilities in cloud architecture. emphasizing the importance of organizational preparedness by informing organizations of the risks and necessary tools for effective cloud computing. This paper introduces a proposed cloud architecture designed to facilitate cloud adoption for small businesses and improve cloud security. These frameworks (such as the Microsoft Azure Cloud Adoption Framework) provide a set of tools, best practices, and documentation to help organizations plan and implement cloud adoption strategies.

These frameworks provide a structured approach to the adoption and implementation of cloud services, ensuring that best practices are followed in areas such as security, compliance, performance and cost management. A significant security challenge in software applications is the presence of millions of lines of code written by different programmers in different programming languages, each of which may have its own inherent vulnerabilities. This section reviews the security challenges faced in cloud computing applications. It is necessary to use various techniques and strategies to maintain robust and reliable services against threats like SQL injection, denial of service, viruses, trojans, anti-spoofing, port scanning, cross-site scripting, phishing etc. attacks.

Unauthorized access An effective approach includes a comprehensive and integrated framework that not only outlines security guidelines, training, and best practices, but also provides targeted solutions for each critical security aspect. For example, adopting a cloud computing architecture demonstrates a tailored approach by implementing specific security measures and solutions, thereby providing a multi-layered, adaptive security service. [45]

Network Security:

Monitor and control incoming and outgoing network traffic based on predefined security rules. Regardless of their location, data centers introduce security and privacy concerns that require thorough attention. This chapter explores basic cloud computing security concepts, including security services, policies, requirements, and testing methods. Privacy aims to protect users' identities, especially in situations involving threats to personal information such as vehicle user identities, geographic locations, and unauthorized disclosure of sensitive data.

Fault management addresses issues related to malfunctioning devices and their repair, configuration management includes setting up initial configurations for network components and infrastructure, and accounting management focuses on billing and payment for resource usage. Performance management is concerned with monitoring and improving the performance of network components, whereas security management focuses on strengthening network security and disseminating security-related information across the network. Regular updates to network policies are essential to improve security.

In addition, Cyber Guard a security tool designed for cloud computing is proposed to protect the network from potential attacks. It includes measures to maintain the integrity, confidentiality and availability of data transmitted and accessed across networks. It protects data from unauthorized access whether it is being transmitted or stored. Organizations depend on cloud computing to securely store important data in the cloud. Even with a firewall, it's important to properly manage and secure cloud computing environments. Ensuring robust security in the cloud is a significant challenge, as traditional security measures often fall short of providing comprehensive protection. The flexibility and mobility inherent in cloud computing brings additional security concerns such as protecting data, ensuring user privacy, maintaining platform stability, and managing the overall cloud environment.

Cloud Security:

The security paradigm has been a major topic of debate among experts and researchers. Leading international conferences such as the European Conference, the ACM Workshop on Cloud Computing Security, and the International Conference on Cloud Security Management are dedicated to cloud security. A number of international journals also publish in-depth research on the topic, exploring various dimensions of cloud security. Companies such as Amazon Web Services

(AWS), Microsoft Azure, Google Cloud Platform (GCP) and IBM Cloud offer a range of security tools and services to protect cloud infrastructure, applications and data.

. They provide basic cloud security services and follow a shared responsibility model to define security responsibilities between themselves and their customers. Security risks associated with software versions depend on consumer choices, and strategic dynamics between sellers and buyers may lead high-end consumers to choose products with lower intrinsic quality. Compared to on-premises definitions, software diversification generally results in lower average security losses for users, especially when patching costs are high. As software versions advance, so do security investments.

The Cloud Security Alliance offers a comprehensive best practices manual although such comprehensive guides are often overlooked. Conversely, concise, actionable lists are more readily accepted. Once IT professionals solve the most critical problems, they can focus on less critical or organization-specific problems. Successfully managing initial challenges builds confidence to tackle more complex security issues. Despite the increased demand for cloud security, the current level of security remains low. We expect improvements over time, with cloud services eventually offering stronger security guarantees. Individuals such as cloud security architects, engineers, analysts, and consultants work within organizations or as third-party experts to design, implement, and maintain security controls and policies in cloud environments.

They often hold certifications such as Certified Cloud Security Professional (CCSP) or AWS Certified Security - Specialty. First, these advanced services prioritize basic security features such as isolation, encryption for confidentiality, and authentication to ensure data integrity. Firewalls are important in this context as they act as a barrier between a private network and the outside internet, ensuring the safe handling of all data packets. However, since traditional firewalls are insufficient for comprehensive protection, integrating an intrusion detection system can provide additional protection. [15]

Software Defined Network:

Software-defined networking (SDN) involves a central software application called a controller that manages overall network behavior, while network devices mainly handle basic packet forwarding. In this model, the central controller manages the control logic (control plane), while the network devices focus on packet forwarding (data plane). A software defined network (SDN) is an approach to network management that enables more flexible and efficient network operation by decoupling the network control plane from the data plane.

Here's a breakdown of SDN Technologies such as Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) are poised to revolutionize the telecommunications industry to address the needs of next-generation networks as outlined by 3GPP. NFV and SDN offer key benefits, particularly through the automation of network management tasks, resulting in improved flexibility and agility in services. This automation simplifies network operations. Also, "cloud elasticity" enables networks to dynamically adapt to fluctuating traffic demands, and new methods have been developed to further increase network elasticity. In addition, a central controller or multiple controllers can manage the control plane, giving the upper application layer a complete overview of the SDN state.

This section examines the design and performance of controllers in software-defined networking (SDN). It provides a comparison between traditional networks and SDNs, evaluating network packets based on complexity, flexibility, capacity and overall capabilities. How SDN improves performance Network traffic is analyzed by using tools such as Imperf for performance evaluations and Wireshark to measure latency and TCP connections. Analysis of network monitoring data shows that an SDN architecture improves security, flexibility, capacity, and functionality while maintaining overall performance. Also, combining SDN with network functions virtualization (NFV) improves network capabilities by leveraging virtualized control logic.

Although software-defined networking is a relatively new area, it is evolving rapidly and offers considerable potential. It consists of a software application that manages the control plane of the network, making decisions about traffic handling and network behavior. It communicates with both the data plane devices and external applications Centralized network control that manages network policies and configurations. In SDN, this is handled by a software-based controller that communicates with network devices to control traffic flow.

Conclusion:

This paper provides an in-depth overview of cloud security strategies, tools, and countermeasures. It begins by highlighting the security challenges faced by both cloud users and providers and explores the various types of attacks that target cloud-based services. The article also discusses common countermeasures used to prevent these attacks. Phishing filtering processes were performed using cloud-based solutions, and the evaluation indicates that the proposed method will be useful and applicable for forensic analysis of other network attacks in the future. Cloud computing is, unsurprisingly, a focal point of significant attention in both academic research and industry As security professionals, we often observe bugs that echo back to the early days of the Internet.

These problems arise because of a greater emphasis on functionality and performance than on security. In fact, security should be integrated into both functionality and performance. Cloud computing offers benefits such as rapid deployment cost savings adequate storage, and convenient access from any location, which is driving its rapid global expansion. Despite its growing popularity, major security and privacy issues have slowed its wider adoption. Transferring detection capabilities to a network service offers many benefits, such as improved detection coverage, simplified mobile applications, and reduced resource usage.

References:

1. Maithili, K., V. Vinothkumar, and P. Latha. "Analyzing the security mechanisms to prevent unauthorized access in cloud and network security." Journal of Computational and Theoretical Nanoscience 15, no. 6-7 (2018): 2059-2063.
2. He, Xiangjian, Thawatchai Chomsiri, Priyadarsi Nanda, and Zhiyuan Tan. "Improving cloud network security using the Tree-Rule firewall." Future generation computer systems 30 (2014): 116-126.
3. Shin, Seungwon, and Guofei Gu. "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)." In 2012 20th IEEE international conference on network protocols (ICNP), pp. 1-6. IEEE, 2012.
4. Khan, Imran Ahmad, and Rosheen Qazi. "Data security in cloud computing using elliptic curve cryptography." International Journal of Computing and Communication Networks 1, no. 1 (2019): 46-52.
5. Singh, Ashish, and Kakali Chatterjee. "Cloud security issues and challenges: A survey." Journal of Network and Computer Applications 79 (2017): 88-115.
6. Chen, Zhen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen. "Cloud computing-based forensic analysis for collaborative network security management system." Tsinghua science and technology 18, no. 1 (2013): 40-50.
7. Sharma, Pradip Kumar, Saurabh Singh, and Jong Hyuk Park. "OpCloudSec: Open cloud software defined wireless network security for the Internet of Things." Computer Communications 122 (2018): 1-8.
8. Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption framework." Procedia Computer Science 94 (2016): 485-490.
9. Praveena, D., and P. Rangarajan. "A machine learning application for reducing the security risks in hybrid cloud networks." Multimedia Tools and Applications 79, no. 7 (2020): 5161-5173.
10. Singh, Saurabh, Young-Sik Jeong, and Jong Hyuk Park. "A survey on cloud computing security: Issues, threats, and solutions." Journal of Network and Computer Applications 75 (2016): 200-222.
11. Ramachandran, Muthu, and Victor Chang. "Towards performance evaluation of cloud service providers for cloud data security." International Journal of Information Management 36, no. 4 (2016): 618-625.
12. Ahmad, Farhan, Muhammad Kazim, Asma Adnane, and Abir Awad. "Vehicular cloud networks: Architecture, applications and security issues." In 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), pp. 571-576. IEEE, 2015.
13. Tripathi, Alok, and Abhinav Mishra. "Cloud computing security considerations." In 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), pp. 1-5. IEEE, 2011.
14. Panneerselvam, John, Lu Liu, Richard Hill, Yongzhao Zhan, and Weining Liu. "An investigation of the effect of cloud computing on network management." In 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems, pp. 1794-1799. IEEE, 2012.
15. Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." Information sciences 305 (2015): 357-383.
16. Liu,Wentao .Research on cloud computing security problem and strategy." In 2012 2nd international conference on consumer electronics, communications and networks (CECNet), pp. 1216-1219. IEEE, 2012.
17. Singh, Ashish, and Kakali Chatterjee. "Cloud security issues and challenges: A survey." Journal of Network and Computer Applications 79 (2017): 88-115.
18. August, Terrence, Marius Florin Niculescu, and Hyoduk Shin. "Cloud implications on software network structure and security risks." Information Systems Research 25, no. 3 (2014): 489-510.
19. Halton, Wolf Michael, and Syed Rahman. "The top ten cloud-security practices in next-generation networking." International Journal of Communication Networks and Distributed Systems 8, no. 1-2 (2012): 70-84.
20. Coppolino, Luigi, Salvatore D'Antonio, Giovanni Mazzeo, and Luigi Romano. "Cloud security: Emerging threats and current solutions." Computers & Electrical Engineering 59 (2017): 126-140.
21. Glott, Rüdiger, Elmar Husmann, Ahmad-Reza Sadeghi, and Matthias Schunter. Trustworthy clouds underpinning the future internet. Springer Berlin Heidelberg, 2011.
22. Ghosh, Partha, Abhay Kumar Mandal, and Rupesh Kumar. "An efficient cloud network intrusion detection system." In Information Systems Design and Intelligent Applications: Proceedings of Second International

Conference INDIA 2015, Volume 1, pp. 91-99. Springer India, 2015.

23. Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." IEEE Communications Magazine 51, no. 2 (2013): 114-119.
24. Battula, Laxmana Rao. "Network security function virtualization (nsfv) towards cloud computing with nfv over openflow infrastructure: Challenges and novel approaches." In 2014 international conference on advances in computing, communications and informatics (ICACCI), pp. 1622-1628. IEEE, 2014.
25. Hu, Fei, Qi Hao, and Ke Bao. "A survey on software-defined network and openflow: From concept to implementation." IEEE Communications Surveys & Tutorials 16, no. 4 (2014): 2181-2206.
26. Patel, Parthkumar, Vineeta Tiwari, and Manish Kumar Abhishek. "SDN and NFV integration in openstack cloud to improve network services and security." In 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp. 655-660. IEEE, 2016.
27. Nunes, Bruno Astuto A., Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti. "A survey of software-defined networking: Past, present, and future of programmable networks." IEEE Communications surveys & tutorials 16, no. 3 (2014): 1617-1634.