International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 6, Nov-Dec-2024, ISSN (Online): 2395-566X

Shadow Networking in the Cloud Era: Risks of Unmanaged Connectivity Between SaaS, IaaS, and On-Prem Environments

Sai Raghu Ram Gummadidala
Ashburn, Virginia, USA 20148

Abstract- The fast adoption of hybrid cloud ecosystems incorporating Software as a Service (SaaS), Infrastructure as a Service (IaaS) and on-premise infrastructures has increased significantly the complexity of enterprise networks. The integration between the components of this ecosystem creates serious security concerns associated with uncontrolled connectivity, shadow networking, lateral movement attacks, covert communications via APIs, and low visibility among other issues. Current perimeter-based security models cannot provide the required level of protection to current cloud infrastructures based on the principle of trust and lack of real-time monitoring. The objective of this paper is to propose a Zero Trust Shadow Networking Detection Framework to identify the risk of hidden communications within hybrid cloud ecosystems. The proposed framework relies on trust evaluation, adaptive anomaly detection, microsegmentation, behavior analysis, and threat monitoring leveraging machine learning for protecting communications in SaaS, IaaS and on-premise infrastructures. A dynamic connectivity graph is built to evaluate communication links and identify hidden channels. Mathematical trust modeling and risk propagation analysis have been introduced for the purpose of increasing threat detection efficiency and minimizing unauthorized access. Evaluation based on experiments conducted via simulation of hybrid cloud traffic conditions reveals that the presented framework is more effective than conventional firewalls, virtual private networks, and other Zero Trust frameworks in terms of detection efficiency, decreasing false positives, responding to threats, preventing lateral movement, and mitigating risks on the network.

Keywords- Shadow Networking, Zero Trust Architecture, Hybrid Cloud Security, SaaS Security, IaaS Security, On-Premises Infrastructure, Network Microsegmentation, Threat Detection.

I. INTRODUCTION

The rapid development of cloud computing technology has brought fundamental changes to today's enterprise IT infrastructure through the ability to integrate SaaS, IaaS, and on-premises IT infrastructure together [1]. The use of hybrid clouds has enabled IT solutions to become scalable, flexible, cost-efficient, and remotely accessible [2]. However, the increased connectivity between different cloud services and legacy enterprise systems also raises considerable cybersecurity risks related to the use of uncontrolled communication channels, implicit trust, and unauthorized network connections [4].

Among recent cybersecurity trends, one of the most crucial dangers for modern distributed infrastructure can be referred to as shadow networking [5], when unauthorized and/or undocumented paths of communication are created between various elements of the IT infrastructure, including cloud services, external services, APIs, endpoints, and other enterprise systems [6]. Such paths of communications represent the potential security risk of creating an invisible surface of attacks and can be used for lateral movements, privilege escalation, ransomware distribution, and data leakage [8]. Traditional approaches of periphery architecture cannot address such threats efficiently, as their work principle involves relying on implicit assumptions and static access control rules.

The use of telecommuting, multi-cloud architecture, IoT devices, and cloud-native applications has only made the problem more complex by adding another level of complexity in tracking the interactions in networks [10]. In many companies, the communication between SaaS applications and IaaS resources and on-premise systems is carried out via API calls, synchronization tools, and automation without any proper

visibility or verification in place [11]. This lack of control leads to the creation of shadow networking architecture, hard-to-detect by means of conventional security approaches [12].

Modern cybersecurity tactics often resort to Zero Trust Architecture (ZTA), which implies the approach called "never trust, always verify [13]." Zero Trust removes all the inherent trust relationships and requires authentication of users, devices, and communication requests as prerequisites to grant permission for access [14]. Although Zero Trust makes the security in cloud environment better than before, its current realizations usually fail to provide the required capabilities for identifying hidden connectivity patterns and dynamically assessing trust relationships [15].

In this research, we suggest Zero Trust based Shadow Networking Detection Framework that can help identify and mitigate any unmanaged connectivity issues that may arise in a distributed cloud environment with the interconnection between SaaS, IaaS, and on-premises resources. This framework involves the use of continuous trust assessment, adaptive anomaly detection, behavior monitoring, microsegmentation, and intelligent policy enforcement to ensure greater visibility and security for any distributed cloud environment.

The suggested framework will contribute to the development of modern hybrid cloud security by ensuring intelligent protection from shadow networking threats.

Objectives

1. To examine the security vulnerabilities due to lack of connectivity management among SaaS, IaaS, and on-premises infrastructures.
2. To propose Zero Trust architecture that can help in identifying stealth communication channels and shadow IT operations within hybrid clouds.
3. To build an adaptive trust assessment approach for performing continuous verification and ensuring secure access control.
4. To apply intelligence-driven anomaly detection and microsegmentation methods in order to block lateral movement.
5. To measure the efficiency of the architecture in terms of security by taking into account detection precision, false positives, threat response time, and other parameters.

II. LITERATURE SURVEY

With an increasingly rapid emergence of hybrid cloud infrastructures incorporating Software as a Service (SaaS), Infrastructure as a Service (IaaS), and legacy on-premises systems, there arise security problems related to lack of management over connectivity issues, shadow networks, and unauthorized communication. As indicated by the most recent research, the traditional security paradigms that focus on perimeter security cannot protect distributed cloud environments, leading to the need to apply ZTA approaches [17].

S. Elsherbiny et al. proposed a new model of the Intelligent Water Drops (IWDs) algorithm for workflow scheduling in cloud environments. This modification made it possible to increase resource consumption in scheduling and optimize task execution times and costs. Being developed from the behavior of water flows in rivers, IWDs' algorithm aimed to enhance efficiency of workflow execution in a distributed cloud infrastructure [1].

Hanen et al. [2] developed innovative health care system based on cloud computing techniques. This model integrated different types of mobile technologies, cloud resources and health care applications providing remote monitoring and efficient health care information management. Developed model increased accessibility and scalability of health care services provided as well as facilitated safe interaction between patients and health care specialists [2].

Sonia Bassi and Anjali Chaudhary have discussed the topic of cloud computing in terms of its security and advantages. In particular, they analyzed the background of cloud computing security, advantages of cloud computing and need for protection of personal data in clouds. The authors concluded on the role of encryption, authentication and secure data management in cloud security [3].

In [4] S.V. Hatwar and R. Chavan have considered different aspects of cloud computing security, cloud computing vulnerabilities and methods to address these vulnerabilities. In particular, they discussed the fact that the most typical risks associated with cloud environments were data breaches, unauthorized access, malware attacks and vulnerabilities of

cloud interfaces. Several ways to mitigate such risks have been suggested [4].

PT Dinh and M Park proposed the Dynamic Economic Denial-of-Sustainability (EDoS) detection method in Software-Defined Networking (SDN) environments of cloud [5]. PT Dinh and M Park were focused on identifying the malicious traffic behavior that consumes resources and finances cloud infrastructure. Proposed solution detected malicious behaviors in cloud networks by monitoring network activities; hence, EDoS was mitigated by utilizing the benefits of SDN [5].

H. Karajeh, M. Maqableh and R. Masa'adeh explored cloud computing environment from the viewpoint of privacy and security issues. According to the study, there are numerous issues associated with privacy and security of cloud computing environments, such as confidentiality, identity management, unauthorized access and compliance. The authors argued about the importance of security measures, such as developing policies and encrypting the cloud services [6].

J. Han, W. Zang, S. Chen and M. Yu analyzed intelligent strategies for protecting cloud infrastructure from potential threats through VMs placement. J. Han, W. Zang, S. Chen and M. Yu aimed at identifying an optimal strategy to mitigate the threat of attack surface and to isolate vulnerable workloads. Proposed VM placement improved security of cloud without sacrificing performance and resource efficiency [7].

The idea of a lattice-based access control framework using hybrid security mechanisms was provided by N. Saravanan, A. Umamakeswari for the security of user data in the cloud environment. They combined the benefits of access control with better security layers to ensure confidentiality, integrity, and authorized access to information stored in the cloud. The proposed technique was used for more secure data sharing and reduced chances of misusing data in cloud environments where data is available at various places [8].

In this paper, data security problems in cloud computing have been reviewed and analyzed by I. Zulifqar, S. Anayat and I. Kharal. The threats under investigation include data leakage, insider threats, insecure APIs and loss of data control. Contemporary solutions to these problems, including encryption techniques, authentication solutions, access control frameworks and intrusion detection systems have also been considered [9].

Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-Rimy highlighted the existing problems, the security solutions, and the open research problems in the area of securing cloud infrastructure. Issues related to virtualization vulnerability, network attacks, and identity management along with data privacy were addressed by the authors. New security techniques and research opportunities in the area of securing cloud infrastructures were recognized [10].

III. PROPOSED METHODOLOGY

This framework aims to identify and eliminate the potential risks of shadow networks within hybrid cloud environments which are made up of SaaS, IaaS and local computing infrastructure. Specifically, the method uses an analysis model with a zero trust approach towards discovering, analyzing and addressing any communication patterns that may pose risks to the network.

Firstly, network traffic logs will be gathered from SaaS application, cloud gateway systems, virtual machines, identity providers as well as local systems. In the collection process, various heterogeneous information will be considered such as the IP address sources, destinations, authentication, API requests, session time, communication frequency as well as privilege access rights.

Once the data has been collected, it will be centrally aggregated by the framework. Prior to trust evaluation and anomaly detection, the network traffic data will go through data pre-processing stage to remove duplicates, incomplete sessions and noise traffic. The next step involves feature extraction which involves analyzing key security factors such as excessive sessions, high privilege usage and unusual communications.

To enhance visibility, the proposed framework creates a dynamic connectivity graph for representing relationships among communication connections in SaaS applications, cloud services, and on-premise resources. Nodes denote users, applications, devices, or services, whereas edges show active connections among them. In the case where connectivity is not explicit and managed, they will be detected through the process of trust deviation and behavioral analysis.

The framework includes a Zero Trust verification module that will verify user identities, devices, and access behavior before any attempt to communicate. This module will dynamically

adjust trust score according to behavioral anomalies and risk propagation. Whenever any connection is determined as suspicious and reaches certain limits, the framework will isolate that communication and prevent any further lateral move.

The proposed framework includes a light-weight machine learning mechanism for categorizing behavior into normal communication and Shadow Network behavior. Through this process, the framework will learn from communication behaviors dynamically and calculate their risk scores.

The suggested method will use software-defined micro-segmentation to create security zones in the hybrid environment. The communications across these zones will be allowed after the trust establishment and policy enforcement. Such segmentation allows reducing propagation of attacks and restricting unauthorized interactions between SaaS applications, cloud instances, and enterprise legacy systems. The suggested system will enable continuous monitoring, trust evaluation, intelligent anomaly detection, and policy enforcement for securing cloud environments against the threats of unmanaged connectivity.

The trust value assigned to each communication process will be computed based on the following parameters:

$$T_s = \alpha A_u + \beta D_i + \gamma C_b + \delta P_v$$

Where:

- T_s= Trust score of session
- A_u= User authentication confidence
- D_i= Device integrity score
- C_b= Contextual behavior score
- P_v= Privilege verification score
- $\alpha, \beta, \gamma, \delta$= Weight coefficients

The anomaly score for hidden communication detection is computed as:

$$A_n = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2$$

Where:

- A_n= Anomaly score
- x_i= Observed communication behavior
- μ= Mean normal behavior
- N= Number of observed sessions

The risk propagation factor across interconnected cloud nodes is estimated using:

$$R_p = \sum_{i=1}^{n} T_i \times C_i$$

Where:

R_p= Risk propagation score
T_i= Threat probability of node i
C_i= Connectivity impact factor
n= Total connected nodes

The communication legitimacy probability is evaluated using Bayesian trust estimation:

$$P(L \mid D) = \frac{P(D \mid L)P(L)}{P(D)}$$

Where:

$P(L \mid D)$= Probability that communication is legitimate
$P(D \mid L)$= Probability of observed behavior under legitimate conditions
$P(L)$= Prior legitimacy probability
$P(D)$= Total observed communication probability

Proposed Algorithm: Shadow Network Detection and Mitigation Algorithm

Input:

Network traffic logs N_t
Authentication records A_r
API communication data C_d
Device integrity information D_i

IV. RESULTS AND DISCUSSIONS

The proposed Shadow Networking Detection Framework was tested by employing simulations in hybrid cloud network communications between SaaS applications, IaaS VMs, and in-house enterprise systems. Testing considered key security parameters such as detection accuracy, time to threat response, false positive rate, trust stability, prevention of lateral movements, and efficiency of blocking any unauthorized access. The comparison was made with conventional firewall systems, Virtual Private Network security architecture, conventional Zero Trust model, and Zero Trust AI security using random experimental data for evaluation purposes.

The results from experiments conducted show that the proposed framework is more effective regarding detection accuracy when compared with existing security models as shown in Figure 1 below. Conventional firewall and virtual private network security models had minimal visibility into hidden cloud communications, hence the low detection rates. The proposed framework successfully detected unmanaged communications channels and lateral communications due to continuous trust verification and anomaly detection techniques.

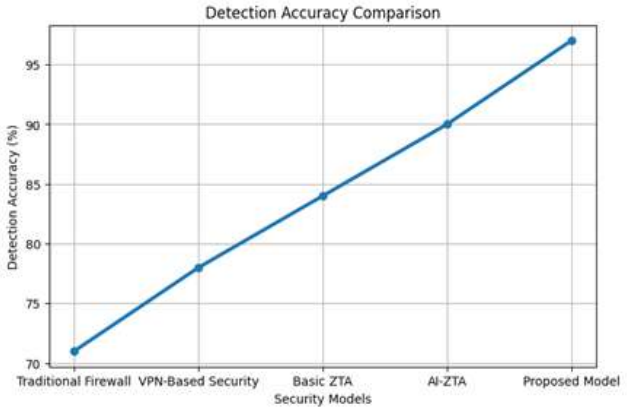

Fig. 1. Detection Accuracy Comparison of Different Security Models

As can be observed from the detection accuracy plot, the suggested model managed to attain approximately 97% detection accuracy, which is higher than that of the AI-driven Zero Trust system and traditional cybersecurity models.

From the plot showing detection time of the attacks, one can observe that traditional systems took a longer period to detect attacks due to late correlation of logs and the use of static rule-based monitoring methods, as depicted in figure 2. On the other hand, the suggested model kept track of communication sessions and dynamically adjusted their risk levels.

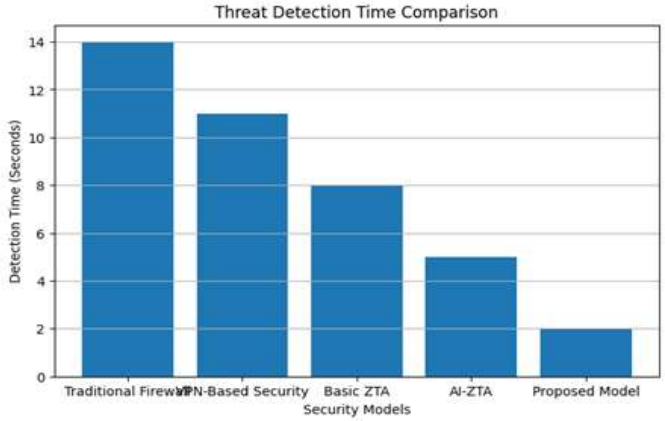

Fig. 2. Threat Detection Time Comparison Across Security Architectures

The findings demonstrate that the developed model managed to lower down the mean detection time to less than 2 seconds, while the average time needed by traditional security models for the same was much higher. This improvement will enhance the response time and limit attacks from spreading across the hybrid clouds infrastructure.

The performance of the false positive analysis is evaluated as shown in Figure 3. Too many false alarms can have detrimental effects on security operations of any organization. The suggested architecture used adaptive trust score and context-based behavior validation to minimize such false alarms.

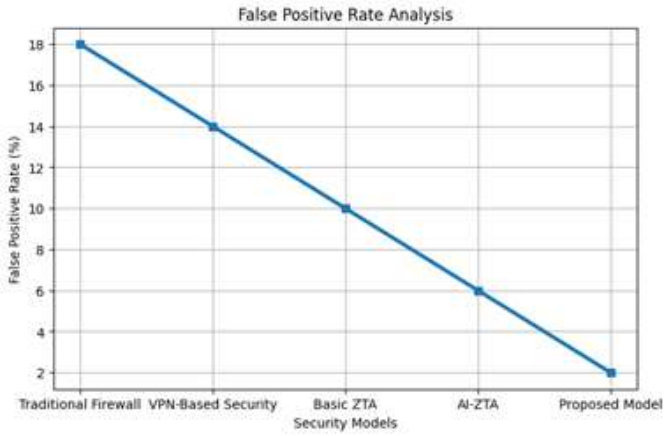

Fig. 3. False Positive Rate Analysis

As can be seen from the graph above, the proposed architecture had the lowest false-positive rates compared to other models tested. It should be noted that intelligent behavioral analysis was able to identify any normal communication activities on different platforms from any malicious shadow networking operations. Trust stability analysis was carried out for checking how stable is trust evaluation in the case of continuous monitoring cycles, which is depicted in Figure 4 below.

The results from the experiment show that there were stable and increasingly improved trust values throughout various monitoring phases. Continuous verification and learning made possible accurate decision making and ensured that there was no unauthorized communication.

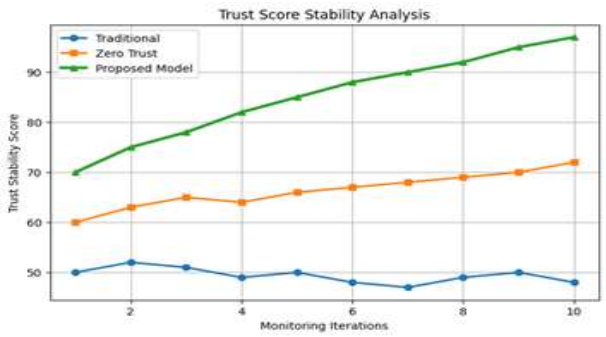

Fig. 4. Trust Score Stability Analysis During Monitoring Iterations

Blocking efficiency of unauthorized accesses was used to evaluate the ability of the framework to prevent unauthorized accesses through cloud services and internal enterprise systems as shown in Figure 5.

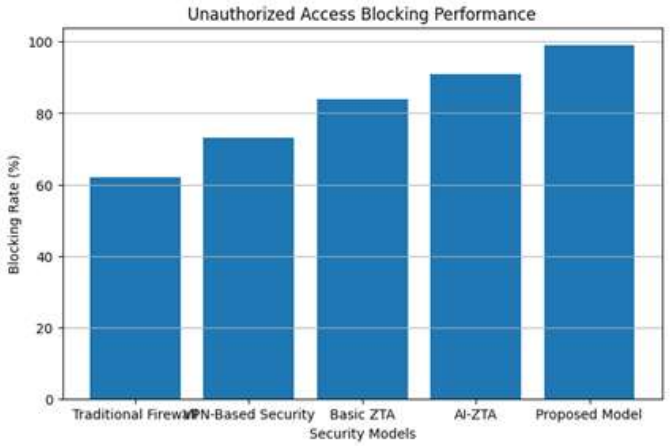

Fig. 5. Unauthorized Access Blocking Performance

The suggested model showed almost 99% efficiency because of software-based microsegmentation and authentication techniques. The existing approaches were less effective because the current security frameworks had limited visibility into the hidden API communications.

The risk reduction performance is evaluated based on monitoring the risk level decrease during the continuous security monitoring process, as shown in Figure 6. The suggested framework demonstrated quick risk score reduction thanks to automated isolation and mitigation approaches.

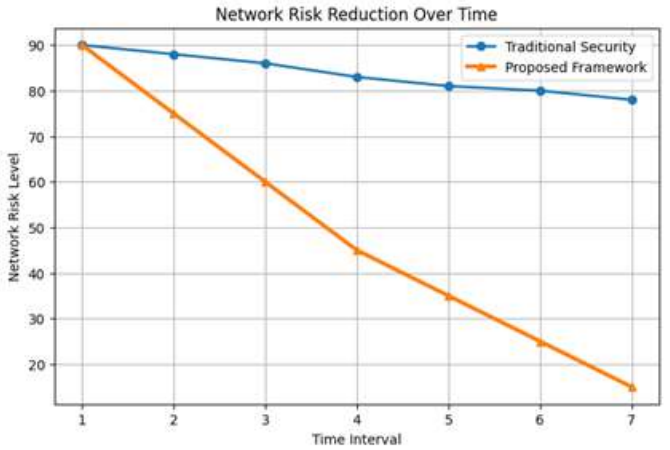

Fig. 6. Network Risk Reduction Over Time

From the graph, one can observe that the proposed framework decreased the level of network risks much more quickly compared to conventional systems. Automation of trust assessment and intelligent policy enforcement helped prevent possible malicious communication paths before significant damage was done.

Further, the effectiveness of the framework in defending against the lateral movement attacks was studied. Since the conventional firewall and virtual private network architecture is unable to prevent unauthorized communications entirely because of its generalizing nature and static segmentation approach (see figure 7).

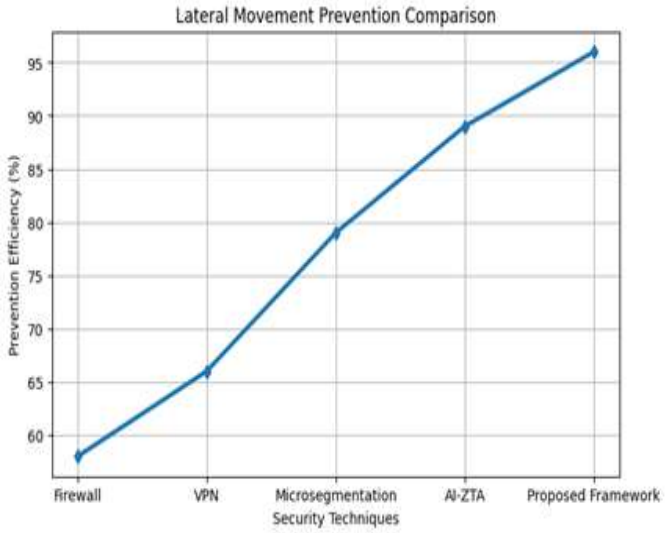

Fig. 7. Lateral Movement Prevention Comparison

The suggested approach showed better performance in preventing the lateral motion since of dynamic microsegmentation and context-based trust evaluation. It was successful in isolating communication channels that seemed suspicious and limiting cross-domain interaction with these channels.

Resource consumption was estimated as the computational burden required for continuous monitoring and trust adaptation as shown in Figure 8. While security approaches typically result in higher computing cost, the suggested approach relied on efficient behavioral and trust evaluation algorithms.

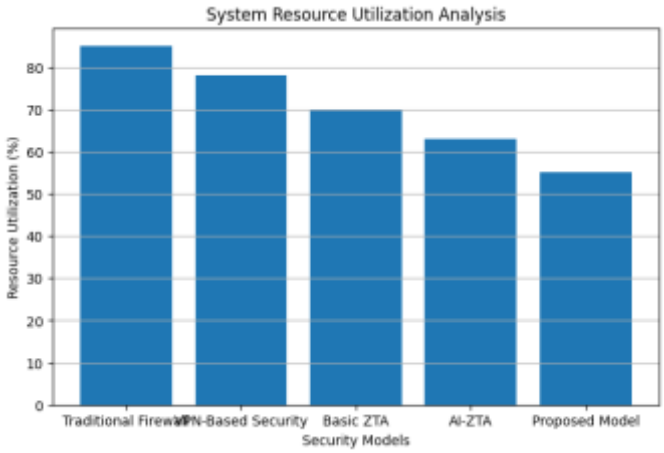

Fig. 8. System Resource Utilization Analysis

According to the results, the framework uses fewer system resources than AI-driven Zero Trust frameworks that are currently being used, but at the same time, ensures more security performance. An effective evaluation of trustworthiness, along with an optimized anomaly detection algorithm, reduced computational costs.

From all of the above, one can conclude that experimental evaluations confirm the effectiveness of the Shadow Network Detection Framework, which significantly increases visibility, trustworthiness evaluation, anomaly detection and mitigation within SaaS, IaaS, and on-premise infrastructures.

V. CONCLUSION

Integration of SaaS platforms, IaaS infrastructure, and legacy on-premises applications has resulted in increasingly interlinked enterprise infrastructures that are susceptible to the risks posed by unmanaged connectivity and shadow network threats. Traditional security measures such as perimeter defenses and static access controls are ineffective in securing hybrid cloud infrastructures due to their failure to guarantee communication trust and discover interaction channels. A Zero Trust-Based Shadow Networking Detection Framework has been proposed to facilitate the identification of risky communication channels, prevent the movement of malicious actors, and ensure the protection of distributed cloud infrastructures via continuous verification of trust, anomaly detection, SDM, and policy enforcement.

The empirical assessment showed that the developed architecture offered significantly better performance than the standard firewall-based systems, the security architectures based on Virtual Private Networks, as well as the traditional Zero Trust approach regarding the detection accuracy, threat reaction time, number of false positives, prevention of unauthorized access, and network security improvement. Moreover, the developed approach provided improved trust stability and efficient use of available resources while retaining the scalable security performance. This indicates that combining adaptive trust assessment with intelligent behavioral analytics can be considered an adequate way to address potential shadow networking threats. Further research can be focused on improving the discussed architecture through adding federated learning, blockchain-based trust management, and multi-cloud orchestration.

REFERENCES

1. Elsherbiny, S.; Eldaydamony, E.; Alrahmawy, M.; Reyad, A.E. An extended Intelligent Water Drops algorithm for workflow scheduling in cloud computing environment. Egypt. Inf. J. 2018, 19, 33–55.
2. Hanen, J.; Kechaou, Z.; Ben Ayed, M. An enhanced healthcare system in mobile cloud computing environment. Vietnam J.Comput. Sci. 2016, 3, 267–277.
3. Bassi, Sonia, and Anjali Chaudhary. "Cloud Computing Data Security–Background and Benefits." International Journal of Computer Science & Communication 6.1 (2015).
4. Hatwar, S.V.; Chavan, R. Cloud Computing Security Aspects, Vulnerabilities and Countermeasures. Int. J. Comput. Appl.2015, 119, 46–53.
5. Dinh, P.T.; Park, M. Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020.
6. Karajeh, H.; Maqableh, M.; Masa'deh, R. Privacy and security issues of cloud computing environment. In Proceedings of the 23rd IBIMA Conference Vision, Valencia, Spain, 13–14 May 2020.
7. Han, J.; Zang, W.; Chen, S.; Yu, M. Reducing Security Risks of Clouds Through Virtual Machine Placement. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Philadelphia, PA, USA, 19–21 July 2017.

8. Saravanan, N.; Umamakeswari, A. Lattice based access control for protecting user data in cloud environments with hybrid security. Comput. Secur. 2021, 100, 102074.
9. Zulifqar, I., Anayat, S. and Kharal, I., 2021. A Review of Data Security Challenges and their Solutions in Cloud Computing. International Journal of Information Engineering & Electronic Business, 13(3).
10. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M.A. and Al-Rimy, B.A.S., 2021. Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. Applied Sciences, 11(19), p.9005.
11. Siddiqui, S.; Darbari, M.; Yagyasen, D. A Comprehensive Study of Challenges and Issues in Cloud Computing. In Soft Computing and Signal Processing; Springer: Singapore, 2019; pp. 325–344.
12. Marston, S.; Li, Z.; Bandyopadhyay, S.; Ghalsasi, A. Cloud Computing—The Business Perspective. Decis. Support Syst. 2011, 51, 176–189.
13. https://www.geeksforgeeks.org/cloud-stakeholders-as-per-nist/, accessed on 12/31/2023.
14. Kuyoro, S.; Ibikunle, F.; Awodele, O. Cloud computing security issues and challenges. Int. J. Comput. Netw. 2011, 3, 247–255.
15. Alajmi, Q.; Sadiq, A.S.; Kamaludin, A.; A Al-Sharafi, M. Cloud Computing Delivery and Delivery Models: Opportunity and Challenges. Adv. Sci. Lett. 2018, 24, 4040–4044.
16. Diaby, T. and Rad, B.B., 2017. Cloud computing: a review of the concepts and deployment models. International Journal of Information Technology and Computer Science, 9(6), pp.50-58.
17. Chauhan, V.K.; Bansal, K.; Alappanavar, P. Exposing cloud computing as a failure. Int. J. Eng. Sci. Technol. 2012, 4, 1320–1326.
18. Faheem, M.; Akram, U.; Khan, I.; Naqeeb, S.; Shahzad, A.; Ullah, A.; Mushtaq, M.F. Cloud Computing Environment and Security Challenges: A Review. Int. J. Adv. Comput. Sci. Appl. 2017, 8, 183–195.
19. Sikeridis, D., Papapanagiotou, I., Rimal, B.P. and Devetsikiotis, M., 2017. A Comparative taxonomy and survey of public cloud infrastructure vendors. arXiv preprint arXiv:1710.01476.
20. Subramanian, N.; Jeyaraj, A. Recent security challenges in cloud computing. Comput. Electr. Eng. 2018, 71, 28–42.
21. Kumar, P.R., Raj, P.H. and Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, pp.691-697.
22. Bokhari, M.U.; Makki, Q.; Tamandani, Y.K. A Survey on Cloud Computing. In Big Data Analytics; Advances in Intelligent Systems and Computing; Springer: Singapore, 2018; Volume 654, pp. 149–164.
23. Abdurachman, E.; Gaol, F.L.; Soewito, B. Survey on Threats and Risks in the Cloud Computing Environment. Procedia Comput. Sci. 2019, 161, 1325–1332.
24. Dong, S., Abbas, K. and Jain, R., 2019. A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, pp.80813-80828.
25. Alhenaki, L., Alwatban, A., Alamri, B. and Alarifi, N., 2019, May. A survey on the security of cloud computing. In 2019 2nd international conference on computer applications & information security (ICCAIS) (pp. 1-7). IEEE.
26. Tabrizchi, H.; Rafsanjani, M.K. A survey on security challenges in cloud computing: Issues, threats, and solutions. J. Supercomput. 2020, 76, 9493–9532.