RESEARCH ARTICLE OPEN ACCESS

Enhancing Cloud Security: A Review of Hybrid Intrusion Detection Approaches

[1]Himanshu Jaiswal, [2]Sreeja Nair, [3]Ritu Ranjani Singh

[1]M.Tech scholar, Department of Computer Science & Engneering AIML, Oriental Institute of Science and Technology

[2]HOD, Department of Computer Science & Engneering AIML, Oriental Institute of Science and Technology

[3]Assistant Professor, Department of Computer Science & Engneering AIML, Oriental Institute of Science and Technology

Abstract: Cloud computing's provision of scalable, flexible, and economical IT services has allowed it to become the backbone of the modern digital infrastructure. With such widespread adoption also comes a whole array of security issues, particularly in detecting and mitigating cyber threats. Intrusion Detection Systems (IDS), being a supportive instrument for cloud security, keep track of system activities to recognize all aberrant behavior. In this paper, we present a structured overview of IDSs for cloud environments, especially focusing on hybrid IDS systems that address the capabilities of signature-based and anomaly-based methods. We then provide an in-depth examination of different types of IDSs according to their operational characteristics and deployments, including host-based IDS, network-based IDS, and hybrid IDS. Recent literature is reviewed, contrasting IDS effectiveness along varying measures including detection accuracy, response time, overhead, and flexibility. An overview of various advanced technologies like machine learning and virtualization that help build more strong IDS frameworks is provided. Load balancing and fault tolerance are considered as complementary measures to ensure the delivery of service quality and the availability of the system in cloud environments. The paper identifies the present challenges and future research avenues that are required to arrive at a resilient, scalable, and intelligent IDS in cloud infrastructures.

Keywords: Cloud security, Intrusion Detection Systems (IDS), Hybrid IDS, Signature-based IDS, Anomaly-based IDS, Host-based IDS

I. INTRODUCTION

Cloud computing is a model for computing resource delivery, like servers, storage, databases, networking, software, and analytics, over the internet, which is also generally called "the cloud," and on a pay-per-use basis. Rather than having to invest in and maintain colossal physical data centers and servers, companies or individuals can simply hire the services of cloud providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform [1]. This mode of working offers unique flexibility, scalability, and cost-efficiency for cloud computing, allowing users to deploy applications in real time, manage a large volume of data, and scale resources up or down according to demand. Cloud computing can take several forms, including three service models-Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)-with each providing various degrees of control and abstraction [2]. In addition, it has deployment models such as public clouds, private clouds, hybrid clouds, and multi-clouds, depending on the degree of security, customization, and integration. By using the cloud, organizations enjoy the ability to accelerate their innovation cycles, reduce complexity in operations, access emerging technologies in artificial intelligence, big data analytics, and Internet of Things ecosystems without heavy investments in in-house infrastructure [3]. However, some new security, privacy, and compliance challenges cloud computing poses will have to be addressed for realizing its full value. Figure 1 illustrates how various cloud-based services—such as storage, management, consulting, and financial services—are accessed by multiple users over the internet.

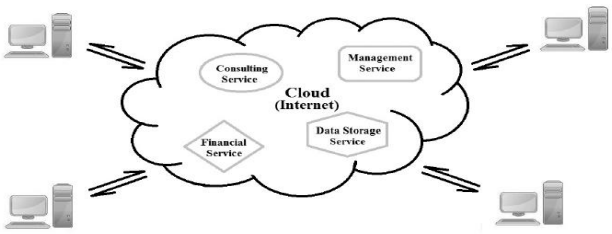

Figure 1 Cloud computing [4]

Cloud computing has quickly emerged as the foundation of contemporary IT infrastructure, providing on-demand access to a variety of services, ranging from storage and computing resources to software platforms. Its intrinsic nature—scalability, elasticity, multi-tenancy, and resource pooling—has rendered it a desirable choice for businesses and individuals. But the same features that make the cloud so robust also provide a huge and intricate attack surface. Distributed by nature, and typically featuring multiple parties, such as CSPs, customers, and third-party vendors, cloud environments contrast with on-premises infrastructure [5]. This dispersed nature can cause the security lines of responsibility to become indistinct and presents challenges in upholding visibility, control, and compliance. Based on the shared-responsibility model used by most CSPs, users need to protect their data and apps, while the provider is in charge of underlying infrastructure.

Too often, users lack the skills or tools to play this role successfully, creating gaps that can be used by attackers. Data leakage, virtual machine escape, misconfigured cloud settings, and unauthorized access are all increasingly prevalent issues, usually due to the misuse of cloud services or poor security practices [6]. Against the backdrop of escalating risks, there is an ever-growing need for sophisticated and proactive defenses that can anticipate and neutralize threats before they inflict substantial losses. Herein lies the role of Intrusion Detection Systems (IDS). IDS are advanced security systems that can analyze network traffic, system logs, and application patterns to look for signs of malicious behavior or policy breaches. Legacy IDS methods, like signature-based detection, work well against established threats but may not catch new or emerging attack vectors [7]. In contrast, anomaly-based IDS will identify unusual behavior that does not conform to a pre-established norm, which makes them more appropriate for catching zero-day attacks and insider threats. Yet they tend to generate greater false-positive volumes, which can bog down security teams and lower overall system performance. To address the limitations of individual approaches, hybrid IDS models have emerged, which combine signature-based and anomaly-based techniques to offer more accurate, adaptive, and scalable security solutions for the dynamic nature of cloud environments [8]. Hybrid systems are capable of detecting a broader range of threats while preserving manageable levels of false alarms. With cyber threats continuously escalating in sophistication, the creation and deployment of hybrid IDS frameworks in cloud environments are becoming crucial not only for defense, but also for fostering trust and resiliency in digital platforms [9].

II. Intrusion Detection Systems

An intrusion detection system (IDS) is a key cybersecurity mechanism that allows continuous monitoring of network traffic and system activity for evidence of suspicious behavior, violations of security policies, or known threats. It takes information from a variety of sources—network packets, system logs, user activities, application behaviors, and so on—and looks for patterns or anomalies that could point to malicious activities, in its quest to figure out if unwanted attacks are occurring [10]. In case of detection, the IDS issues an alert to inform system administrators or security personnel to take timely action to investigate and contain potential threats. With its capability to detect attempts at unauthorized access, acts of cyberattacks, and internal abuses, IDSs are, therefore, an important mechanism for protecting organizational digital assets and maintaining the integrity of the system [11]. It is worth noting that the IDS mainly performs passive traffic monitoring, meaning that it does not block traffic or stop threats by itself. Rather, it is an early-warning system that enhances situational awareness and helps the incident response strategy. An IDS is normally integrated with other components of broader security infrastructure: firewalls, intrusion prevention, and other tools to form a multi-layered and resilient defense against the constantly changing environment of cyber threats [12].

A. Types of Intrusion Detection Systems

There are different types of Intrusion Detection Systems (IDS) working on different functionalities. Signature-Based IDS (SIDS) compared by the behavior of a system with known signatures of attacks and has a very high success rate as far as performance goes; however, it does not account for new or developing threats. Anomaly-Based IDS (AIDS) classify behavior as either positive or negative by comparing it to a knowledge base of established normal modes-their effectiveness comes when dealing with attacks that have not been previously formulated. However, they are susceptible to a large number of false positives. Combining both approaches is termed hybrid IDS: it often combines machine learning into the dynamic of detection. Host-Based IDS (HIDS) run over individual devices to track the internal activities within a system, making it suitable for localized threats or attacks from insiders. On the contrary, network-based intrusion detection systems are set to scan the traffic in the complete network to identify large-scale threats like DDoS denial of service or malware communicating using infected hosts, while this technology can be limited due to encrypted traffic, or problems arising from high volumes of traffic. A layered combo of HIDS and NIDS is usually used for complete protection.

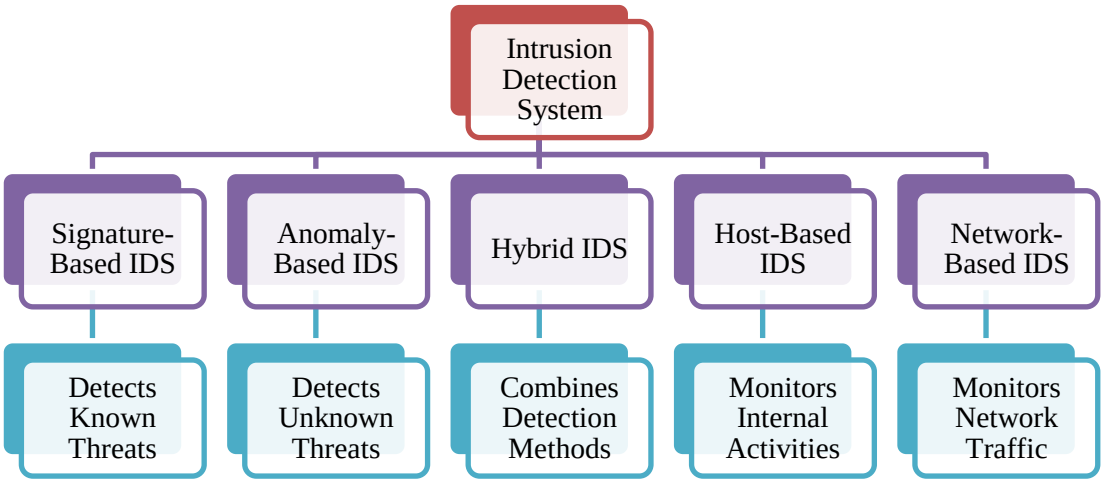

Figure 2 Intrusion Detection Systems Overview

1. Signature-Based Intrusion Detection Systems (SIDS)

The signature-based Intrusion Detection Systems (IDS) work by analyzing incoming network traffic or system behavior by comparing it to an already predefined database of known attack patterns called signatures. These signatures are rules, strings, or identifiable characteristics of specific threats, such as known malware, exploits, or other suspicious activities that have been documented at some point [13]. When the system detects traffic or behavior that matches one of these signatures exactly, the system triggers an alert-to-alert security personnel about a potential intrusion. This method is very efficient for detecting known threats with a very high degree of precision and a low false-positive rate as the system only looks for specific recognized patterns. The biggest downside of signature IDS is that it is entirely dependent on updated threat databases-it may detect attacks that have not been recorded in the database as such, like new, unknown, or even modified attacks [14]. Therefore, this type of IDS may not be useful when it comes to zero-day exploits or advanced evading threats, as it does not work satisfactorily in dynamic environments where continuously changing threat vectors exist.

2. Anomaly-Based Intrusion Detection Systems (AIDS)

An anomaly-based intrusion detection system works by sizing up normal behavior for users, systems, or network traffic, thereafter observing for anything that contradicts this norm. Such contradictions might indicate signs of possible malevolence, for instance, odd login patterns, out-of-place data accesses, or sudden and unanticipated spikes in network traffic [15]. This sort of intrusion detection system is excellent for identifying zero-day attacks and inbound threats that bear no resemblance to any particular signature. The predominant challenge is the high frequency of false positives, which occur when actions that are rightfully termed normal are flagged as malicious. This type of attacks requires much more validation and tuning [16].

3. Hybrid Intrusion Detection Systems (HIDS)

Hybrid Intrusion Detection Systems meld together the advantages of signature-based attack detection with those from anomaly-based techniques to provide a more rounded and adaptable security response. These hybrid systems detect known threats more accurately through signature detection, and they can flexibly deal with unknown threats via anomaly detection, thus minimizing their monitoring blind spots [17]. These systems typically employ machine learning and advanced analytics so that they can improve detection efficiency while working to reduce false alarms. Hybrid IDS finds excellent applications in dynamic environments like the cloud, wherein the inherent diversity and massive amount of data calls for a perfect balance between accuracy, adaptability, and scalability [18].

4. Host-Based Intrusion Detection Systems (HIDS)

An HIDS is a type of intrusion detection system security mechanism that is installed locally on an individual device (such as a server, workstation, or even virtual machine) to look at internal system activity. The system uses indicators such as system logs, file integrity, configuration changes, and application behavior with the intention of detecting unauthorized suspicion or action in the host [19]. Being inside the same device, HIDS can monitor activities which are either not observable from the network, such as unauthorized access to system files, privilege escalation attempts, or unusual behavior of the application, and then detect internal threats, malware infections, and localized attacks against specific machines. Also, the HIDS provide means to maintain compliance in the organization by ensuring that critical files and configurations are not changed or changed only in an authorized way [20]. On the downside, HIDS, deployed on specific devices, are resource-intensive in a large or dynamic infrastructure. Moreover, these have to be updated and tuned frequently for effectiveness.

5. Network-Based Intrusion Detection Systems (NIDS)

Network-Based Intrusion Detection Systems (NIDS) are deployed at strategic points in the network to monitor traffic flowing between devices. The packets collected and analyzed in real-time for network traffic, looking for patterns or behaviors that conform to an attack signature or deviate from what could have been expected. They could determine threats at the network level: DoS attacks, port scanning, man-in-the-middle attacks and command-and-control communications with malware [21]. One of the benefits of NIDS is its ability to obtain a thorough view of network activities, which assists with the detection of coordinated attacks or lateral movement across systems unseen from the host perspective. In cloud or enterprise settings, NIDS are usually placed at the ingress and egress points to observe external connections and east-west traffic within the systems. Though powerful, NIDS are challenged in encrypted traffic or high-volume data flows and typically lack visibility into activities occurring within the encrypted or internal host processes. For that reason, a layered approach is followed, and many companies will use NIDS along with HIDS to ensure that both network and host levels are comprehensively overseen via monitoring [22].

III. Hybrid Intrusion Detection Approaches

Hybrid Intrusion Detection Systems (IDSs) represent a strategic evolution within the field of cyber security that integrates multiple detection techniques, notably signature-based techniques and anomaly-based approaches, in order to create a more adaptive and comprehensive protection scheme. The very essence of hybrid IDS is to avail itself of

the signature method's ability to determine with high accuracy and low false-positive rate the attacks known to it, while anomaly detection can identify attacks which are not known and have either just been introduced or are evolving [23]. In doing so, hybrid IDS circumvent the drawbacks contained within either approach used in isolation. Hybrid systems analyze the normal network activities using machine learning, statistical analysis, and behavioral modeling, aiming to detect any deviations from the normal behavior that could represent malicious behaviors. With this two-layer approach of defending against intruders, the scope and depth of threat detection are achieved through robust attack signature databases. Hybrid IDS are tailored for complex and dynamic environments—such as the cloud—where traditional perimeter defenses are not sufficient because the infrastructure is distributed and virtualized [24].

In cloud environments, hybrid IDS frameworks are tailored for scalability, adaptability, and real-time responsiveness. They can be deployed in various layers such as the network level (monitoring cloud traffic between virtual machines), host level (observing activities of application or system), or directly integrated into the container orchestration platform. Common cloud hybrid IDS design patterns include centralized logging and monitoring tools, distributed sensors across cloud nodes, and AI-driven analytics engines for real-time processing of large volumes of data [25]. Frameworks like Apache Metron, OSSEC, and customized ones based on Snort and Suricata are often adapted and extended to work in cloud-native architectures. Also, they must take into account several cloud-specific challenges such as multi-tenancy, dynamic IPs, encryption, and ephemeral instances. Therefore, hybrid IDS in cloud scenarios must not only be capable of detecting threats but must also continuously adapt to varying threat landscape signatures dictated by the ever-changing topology and usage patterns of cloud workloads [26]. This amalgamation of different techniques and an understanding of architectural design is what defines hybrid IDS as an ever-growing vital element in any cloud security strategy today.

IV. ROLE OF IDS IN CLOUD ENVIRONMENT

An Intrusion Detection System (IDS) is a key element of contemporary cybersecurity infrastructure, which serves to detect, analyze, and react to threats within an information system. It has long been employed in distributed networks, working by continuously tracking network traffic and system activity for any indication of malicious activity, unauthorized access, or policy abuses. It issues alerts—usually called vulnerability analysis warnings—when suspicious activity is noticed, and the alerts are retained for additional analysis or action by system administrators. IDS was first described by Dorothy Denning in 1987, and the technology behind IDS has since made enormous strides [27]. Initially deployed as stand-alone applications on separate computers, IDS has found itself adapting to operate effectively in more advanced and scalable settings, such as virtual machines (VMs) operating on Linux-based platforms, and now cloud computing environments. In current cloud-based infrastructures, with systems being dynamic, scalable, and distributed across several virtual environments, IDS is even more important. Organizations running on the cloud typically have their digital resources watched over and controlled by automated processes, including data storage, software applications, and user interactions. IDS then comes in to play to identify both external and internal threats, like cyberattacks from outside parties and malicious actions by legitimate users who could misuse their access rights. Proper implementation of IDS on cloud systems will involve careful placement and integration. For example, IDS must be placed strategically behind a stateful firewall to examine incoming and outgoing traffic while operating in conjunction with other essential security elements such as antivirus software, access control systems, and authentication protocols. When abnormal activity is sensed—such as unauthorized login attempts, unusual file access, or suspicious data transfers—the IDS can initiate alarms and alerts to inform administrators and possibly trigger a mitigation response. The figure 3 illustrates a cloud-based Intrusion Detection System (IDS) that monitors interactions between cloud users and servers via a network cloud, triggering alerts and alarms in case of suspicious activities.

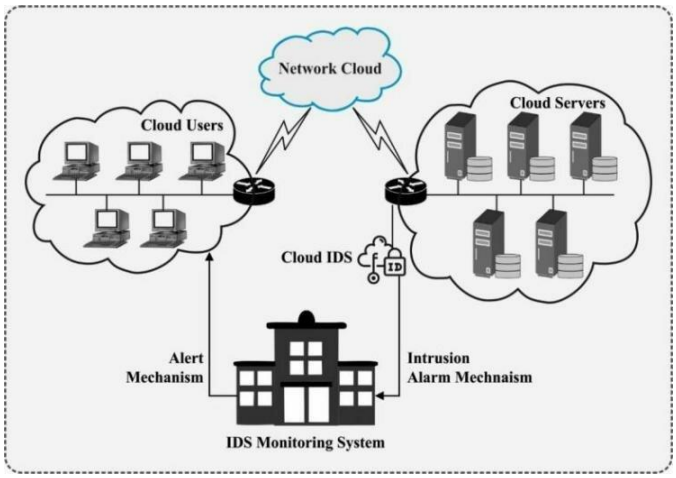

Figure 3 Overview of IDS in Cloud Environment [28]

The difference between an IDS and a firewall is that the former will monitor, control and defend the network infrastructure from both threats and vulnerabilities. Security systems, on the other hand, function as a qualified barrier that allows only types of services, channels, or Port number to get through. As a result, an attacker can get beyond the firewall and target the network and information. It is difficult to halt or identify the source of the attack in such a circumstance. IDS are a critical security aspect in the Cloud Computing systems. Consumers of cloud services rely only on the authentication scheme of the cloud platform. They may need to use IDS in conjunction with other network monitoring technology like as gateways, access restrictions and password protection to monitor and safeguard their fantasy world in the cloud.

V. Challenges, Future Directions, and Research Opportunities

Implementation of the IDS in the cloud would have its own unique challenges due to the distributed, elastic, and multi-tenant nature of cloud infrastructure. One such challenge is

that the user does not have visibility and control of what is happening outside the system infrastructure used directly by the cloud. Security teams maintain direct access to the hardware of on-premises systems; in contrast, cloud service providers manage and abstract the physical infrastructure, limiting the customer's ability to deploy IDS at deeper levels. This implies that maximum monitoring might not be possible, especially in the case of dealing with encrypted traffic or traffic between virtual machines (east-west) within the same cloud instance, which bypasses traditional network monitoring points. The dynamic scaling of cloud resources, for instance, by means of automatically provisioned virtual machines or containers, continues to complicate the need for consistent IDS coverage, given that new instances may come up or go down without securing an immediate security configuration to them. Multi-tenancy-Hosting space is used by numerous users on the same physical infrastructure; therefore, it raises security isolation problem, and if not configured properly, may expose sensitive traffic or lead to cross-tenant attacks, increasing the complexity of deploying an IDS.

Another significant area is data volume and performance; cloud environments can generate very high volumes of traffic and logs, such that there often exist significant computational burdens involved in the real-time processing and analysis of data related to IDS systems. The huge diversity in user behavior and workloads has heightened false positives in the cloud, which deviate from baseline patterns and trigger unnecessary alerts that might overwhelm security teams leading to analysts becoming alert-fatigued and possibly lessen their influence in response. Integration of IDS into heterogeneous cloud platforms contributes to future additions to its already complex environment as each cloud has its own APIs, logging systems, and configurations. Also, integrating data privacy and compliance challenges is induced because IDS may have to inspect data that is sensitive, raising questions about data handling and storage and into whether monitoring practices meet regulatory paradigms. An appropriate cloud-native IDS that is going to be scalable, intelligent, and resourceful in adapting to such dynamic, decentralized architecture clouds with minimum disruption and adequate compliance integrating easily with other security tools will do justice to all these challenges.

Cloud computing continues to face security threats like cyber-attacks; nevertheless, it has been recognized as an important technology with definite benefits in scalability and service flexibility. Within the cloud computing domain, IDSs are instrumental in counteracting these threats, but with a few systematic reviews on their application, especially with respect to a few metascientific analysis methodologies [29], being published-to-date, the impact of IDSs remains seriously unexamined. In recent months, studies were undertaken on hypervisor-based, network-based, machine-learning-based, and hybrid models for yet another classification of IDSs that has investigated such parameters as precision, overhead, response time, and a very few others. It also pointed out several open research issues which attract further study such as intrusion resilience and cost-efficiency [30]. Other reviews stress the need for advanced techniques such as virtual machine and hypervisor introspection and examine the complications posed when simulated data is used for training machine learning models in the case of intrusion detection [31]. Aside from network-related issues, changes in the intrusion detection paradigm, big data, and data mining have received attention in the review [32][33]. In addition, cloud computing presents new opportunities for industries like construction and IoT and augmented reality, while barriers continue to hinder their more widespread adoption [34]. Besides, maintaining performance and service level in cloud environments should be aided by techniques such as efficient resource allocation, scheduling, and load balancing in case of fault tolerance and SLA violations [35][37][38]. Various approaches in cloud security have adopted quite a few other machine-learning methods, with advantages and disadvantages assessed in their capabilities of countering these threats [36].

Table 1 Comparative Analysis of Cloud Computing and Intrusion Detection System (IDS) Studies

Reference	Method	Key Findings	Model	Outcomes
Liu et al. (2022) [29]	Systematic review of 22 IDS papers in cloud	Highlighted IDS types, performance metrics, and gaps in cost-efficiency and resilience	Hypervisor, network, ML-based, and hybrid IDS	Suggested improvement in IDS design for cloud with emphasis on resilience
Lata & Singh (2022) [30]	Review of IDS across cloud models with emphasis on feature selection	Advocated robust feature selection, discussed VMI and HVI techniques	Cloud-specific IDS models with dimensionality reduction	Categorized IDS attack detection capabilities
Chou & Jiang (2021) [31]	Taxonomy of challenges in ML-based NID with dataset focus	Identified 8 key challenges in ML model training for IDS	Real-world dataset recommendation for ML IDS	Suggested future research for scalable, real-data ML IDS
Ozkan-Okay et al. (2021) [32]	Comprehensive overview of IDS technologies and tools	Mapped IDS components and attack types; proposed future research roadmap	Taxonomy and benchmarking of IDS tools	Identified strengths/weaknesses of IDS methods
Salo et al. (2020) [33]	Review of data mining techniques in IDS for big data	Identified effective DMTs and streaming frameworks for large-scale IDS	DMTs, DSFs used in IDS design	Revealed techniques effective for IDS in big data environments

Construction Study [34]	Systematic review of cloud in construction (92 papers)	Cloud as enabler for BIM, IoT, VR/AR in construction; identified adoption barriers	Application integration models in construction	Highlighted future CC applications in construction
Resource Allocation Study [35]	Study of resource allocation and scheduling in cloud	Analyzed pros/cons of resource allocation, load balancing, admission control	Resource management models	Guidelines for better scheduling and load balancing
ML-based Security Review [36]	Review of ML algorithms for cloud security	Compared supervised, unsupervised, semi-supervised, and RL techniques	ML security models in CC (various algorithms)	Performance comparison of ML methods; proposed future directions
Fault Tolerance Review [37]	Survey on fault tolerance mechanisms in cloud	Outlined fault tolerance techniques; stressed need for high availability	Fault-tolerant architectural models	Highlighted gaps in fault tolerance and potential research paths
Load Balancing Review [38]	Analytical review of load balancing techniques in cloud computing	Compared static, dynamic, and nature-inspired LB algorithms; identified research gaps	LB models; fault-tolerant framework	Highlighted operational flow of LB algorithms; proposed future research and framework design

V. CONCLUSION

This study highlights the critical importance of intrusion detection systems in ensuring the security of cloud computing environments, the review considers the unique challenges of threat detection posed by dynamic and distributed infrastructures. Thus, hybrid intrusion detection systems that operate by integrating the advantages of signature-based systems with the anomaly-based class have gained impressive enthusiasm for maximizing detection gotten from the capability of adaptability toward evolving cyber threats. Enhanced integration with fault-tolerance schemes and superior load balancing techniques would further improve the reliability and performance of cloud services. The remaining challenges, such as false positives, monitoring encrypted traffic, dynamic resource management, and compliance with privacy standards, are still important hindrances. Future research should focus on leveraging intelligent algorithms, in particular machine learning and artificial intelligence, to enhance detection rates and operational efficiency. In addition, the construction of real-world datasets, enhancement of IDS scalability, and tackling deployment complexity in multi-cloud and hybrid environments are pertinent to furthering IDS capabilities. Hence, these issues will contribute significantly to the development of robust and agile IDS solutions that would help secure and resilient adoption of cloud computing technologies.

REFERENCES

[1] Berisha, B., Mëziu, E. & Shabani, I. Big data analytics in Cloud computing: an overview. *J Cloud Comp* **11**, 24 (2022). https://doi.org/10.1186/s13677-022-00301-w

[2] Dorsala, M. R., Sastry, V. N., & Chapram, S. (2021). Blockchain-based solutions for cloud computing: A survey. *Journal of Network and Computer Applications*, *196*, 103246. https://doi.org/10.1016/j.jnca.2021.103246

[3] Khan, T., Tian, W., Zhou, G., Ilager, S., Gong, M., & Buyya, R. (2022). Machine learning (ML)-centric resource management in cloud computing: A review and future directions. *Journal of Network and Computer Applications*, *204*, 103405.

[4] hu, Fei & Qiu, Meikang & Li, Jiayin & Grant, Travis & Taylor, Drew & Mccaleb, Seth & Butler, Lee & Hamner, Richard. (2011). A Review on Cloud Computing: Design Challenges in Architecture and Security. Journal of Computing and Information Technology -CIT. 19. 25-55. 10.2498/cit.1001864.

[5] Alsaadi, E. M. T. A., Fayadh, S. M., & Alabaichi, A. (2020, December). A review on security challenges and approaches in the cloud computing. In *AIP Conference Proceedings* (Vol. 2290, No. 1). AIP Publishing. https://doi.org/10.1063/5.0027460

[6] Zulifqar, I., Anayat, S., & Khara, I. (2021). A review of data security challenges and their solutions in cloud computing. *International Journal of Information Engineering and Electronic Business*, *12*(3), 30. DOI: 10.5815/ijieeb.2021.03.04

[7] Akbar, H., Zubair, M., & Malik, M. S. (2023). The security issues and challenges in cloud computing. *International Journal for Electronic Crime Investigation*, *7*(1), 13-32. https://doi.org/10.54692/ijeci.2023.0701125

[8] Ahmad, S., Mehfuz, S., & Beg, J. (2022). Assessment on potential security threats and introducing novel data security model in cloud environment. *Materials Today: Proceedings*, *62*, 4909-4915. https://doi.org/10.1016/j.matpr.2022.03.536

[9] Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), 11. https://doi.org/10.3390/fi14010011

[10] Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). *International*

journal of information security, *22*(5), 1125-1162. https://doi.org/10.1007/s10207-023-00682-2

[11] Abdulganiyu, O.H., Tchakoucht, T.A. & Saheed, Y.K. Towards an efficient model for network intrusion detection system (IDS): systematic literature review. *Wireless Netw* **30**, 453–482 (2024). https://doi.org/10.1007/s11276-023-03495-2

[12] Abbas, S., Naser, W., & Kadhim, A. (2023). Subject review: Intrusion detection system (IDS) and intrusion prevention system (IPS). *Global Journal of Engineering and Technology Advances*, *2*(14), 155-158. https://doi.org/10.30574/gjeta.2023.14.2.0031

[13] Masdari, M., & Khezri, H. (2020). A survey and taxonomy of the fuzzy signature-based intrusion detection systems. *Applied Soft Computing*, *92*, 106301. https://doi.org/10.1016/j.asoc.2020.106301

[14] Zipperle, M., Gottwalt, F., Chang, E., & Dillon, T. (2022). Provenance-based intrusion detection systems: A survey. *ACM Computing Surveys*, *55*(7), 1-36. https://doi.org/10.1145/3539605

[15] Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Applied sciences*, *11*(18), 8383. https://doi.org/10.3390/app11188383

[16] Alem, S., Espes, D., Nana, L., Martin, E., & De Lamotte, F. (2023). A novel bi-anomaly-based intrusion detection system approach for industry 4.0. *Future Generation Computer Systems*, *145*, 267-283. https://doi.org/10.1016/j.future.2023.03.024

[17] Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, *26*(6), 3753-3780. https://doi.org/10.1007/s10586-022-03776-z

[18] Najafli, S., Toroghi Haghighat, A., & Karasfi, B. (2024). Taxonomy of deep learning-based intrusion detection system approaches in fog computing: a systematic review. *Knowledge and Information Systems*, *66*(11), 6527-6560. https://doi.org/10.1007/s10115-024-02162-y

[19] Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems*, *133*, 95-113. https://doi.org/10.1016/j.future.2022.03.001

[20] Sworna, Z. T., Mousavi, Z., & Babar, M. A. (2023). NLP methods in host-based intrusion detection Systems: A systematic review and future directions. *Journal of Network and Computer Applications*, *220*, 103761. https://doi.org/10.1016/j.jnca.2023.103761

[21] Kumar, S., Gupta, S., & Arora, S. (2021). Research trends in network-based intrusion detection systems: A review. *Ieee Access*, *9*, 157761-157779. https://doi.org/10.1109/ACCESS.2021.3129775

[22] Rakas, S. V. B., Stojanović, M. D., & Marković-Petrović, J. D. (2020). A review of research work on network-based scada intrusion detection systems. *IEEE Access*, *8*, 93083-93108. https://doi.org/10.1109/ACCESS.2020.2994961

[23] Thakur, K., Kumar, G. Nature Inspired Techniques and Applications in Intrusion Detection Systems: Recent Progress and Updated Perspective. *Arch Computat Methods Eng* **28**, 2897–2919 (2021). https://doi.org/10.1007/s11831-020-09481-7

[24] Abdulganiyu, O.H., Tchakoucht, T.A. & Saheed, Y.K. Towards an efficient model for network intrusion detection system (IDS): systematic literature review. *Wireless Netw* **30**, 453–482 (2024). https://doi.org/10.1007/s11276-023-03495-2

[25] Heidari, A., Jabraeil Jamali, M.A. Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Comput* **26**, 3753–3780 (2023). https://doi.org/10.1007/s10586-022-03776-z

[26] Ayyagari, M.R., Kesswani, N., Kumar, M. *et al.* Intrusion detection techniques in network environment: a systematic review. *Wireless Netw* **27**, 1269–1285 (2021). https://doi.org/10.1007/s11276-020-02529-3

[27] Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., ... & Kobusińska, A. (2022). A survey on intrusion detection systems for fog and cloud computing. *Future Internet*, *14*(3), 89. https://doi.org/10.3390/fi14030089

[28] Raj, Meghana & Pani, Santosh. (2021). A Meta-analytic Review of Intelligent Intrusion Detection Techniques in Cloud Computing Environment. International Journal of Advanced Computer Science and Applications. 12. 10.14569/IJACSA.2021.0121023.

[29] Liu, Z., Xu, B., Cheng, B., Hu, X., & Darbandi, M. (2022). Intrusion detection systems in the cloud computing: A comprehensive and deep literature review. *Concurrency and Computation: Practice and Experience*, *34*(4), e6646.

[30] Lata, S., & Singh, D. (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. *International Journal of Information Management Data Insights*, *2*(2), 100134.

[31] Chou, D., & Jiang, M. (2021). A survey on data-driven network intrusion detection. *ACM Computing Surveys (CSUR)*, *54*(9), 1-36.

[32] M. Ozkan-Okay, R. Samet, Ö. Aslan and D. Gupta, "A Comprehensive Systematic Literature Review on Intrusion Detection Systems," in *IEEE Access*, vol. 9, pp. 157727-157760, 2021, doi: 10.1109/ACCESS.2021.3129336.

[33] Salo, F., Injadat, M., Nassif, A. B., & Essex, A. (2020). Data mining with big data in intrusion detection systems: A systematic literature review. *arXiv preprint arXiv:2005.12267*.

[34] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.

[35] George, S. S., & Pramila, R. S. (2021). A review of different techniques in cloud computing. *Materials Today: Proceedings*, *46*, 8002-8008. https://doi.org/10.1016/j.matpr.2021.02.748

[36] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing

security. *Electronics*, *9*(9), 1379. https://doi.org/10.3390/electronics9091379

[37] Kumari, P., & Kaur, P. (2021). A survey of fault tolerance in cloud computing. *Journal of King Saud University-Computer and Information Sciences*, *33*(10), 1159-1176. https://doi.org/10.1016/j.jksuci.2018.09.021

[38] Shafiq, D. A., Jhanjhi, N. Z., & Abdullah, A. (2022). Load balancing techniques in cloud computing environment: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 3910-3933. https://doi.org/10.1016/j.jksuci.2021.02.007