Comprehensive Analysis of Intrusion Detection System: A Cloud Computing Security System

E.Abirami[1], Dr. Sreejith Vignesh B P[2]

[1]Research scholar, Department of computer science, Sri Krishna Adithya college of Arts and Science, Tamil Nadu, India
[2]Research supervisor, Department of computer science ,Sri Krishna Adithya college of Arts and Science, Tamil Nadu, India

Received: 10.07.2024 Revised: 13.08.2024 Accepted: 09.09.2024

ABSTRACT

Cloud computing is an innovative technology that recently presented a flexible model in terms of resource usage. Nonetheless, its broad usage has led to extensive security vulnerabilities about the prevention of versatile cyber threats. Intrusion Detection Systems (IDS) can be seen as an essential component in Cloud Computing security since their main mission is to recognize and respond to threats. IDS technologies for cloud computing security is something that this paper seeks to discuss in detail in relation to tradition and advanced forms of the technology. It looks at the IDS frameworks of dual nature based on the integration of ML, DL, and MO algorithms for better accuracy and efficiency. It also assesses the progressed themes, including the blockchain for secure data exchange and trust management. The study also reveals some of the challenges, namely the computational complexity, scalability, and generalization of the dataset that impede the application of IDS in complex cloud environments. A review of available techniques is provided with emphasis on; efficiency and robustness, and their applicability to practical problems. This research outlines specific opportunities, including the development of lightweight real-time IDS solutions and privacy-preserving methodologies, as well as future research areas for building efficient and scalable IDS architectures. This analysis will help researchers and practitioners to understand the direction of enhancing security systems to improve the integrity of cloud computing systems against emerging security threats.

Keywords: Intrusion Detection System (IDS), cloud computing security, machine learning, feature selection, real-time detection, and cyber threat mitigation.

INTRODUCTION

Cloud Computing (CC) has always been an area of interest for the researchers. When it was thought of cloud in the early years starting from 2008, cloud was defined as an execution unit with fast execution capabilities [1]. Later, with the evolution of cloud and application architecture, cloud started to provides services that are related to infrastructure as well. The cloud has three layers of computation namely Infrastructure as Service (IaaS), Platform as Service (PaaS) and Software as Service (SaaS) [2]. The IaaS involves all the hardware-oriented operations that contains the physical aspects of the cloud. As for example, IaaS will have super end processors, task scheduling units, the negotiator with the client to decide Service Level Agreements (SLAs). Any application to be executed on any infrastructure, requires a platform in terms of operating system and hence PaaS service must be integrated to provide SaaS. Due to increasing number of users on cloud networks, there are several types of security aspects that a cloud is concerned like maintaining the SLA first of all, managing the energy efficacy in the service provisioning and preventing the overload on the execution elements of the cloud like a Physical Machine (PM).

The security framework at any computation platform can be easily segregated into two aspects. The first aspect is user authentication and provisioning of the access control architecture popularity known as Role Based Access Control (RBAC) [3]. The cloud needs to perform RBAC process to make sure that the correct information reaches to the correct person of correct level. However, the first aspect is quite interesting to get focus and researchers from around the world has contributed significantly for the same, but, the proposed work is focused on the second aspect of the security. The second aspect refers to network level security in which the cloud server gets anonymous number of requests per second. Due to advancements in data science, the fruit of knowledge has also produced poisons to the computation models of cloud and they are referred as security attack in this research draft.

Due to high volume of users, it is hard to identify and mark the security attack manually and that even when there are varieties in security attacks. If a cloud fails to identify the risk in the early stage, the consequences could be massive in terms of losses. The intruder may breach into secret accounts and can reveal a lot of information or for the time being the intruder may also misuse it against a specific group of personals. In such a scenario, early detection of security attack or threat can only be done using System Aided Design (SAD). Any SAD architecture consists of two portions namely training and classification. The classification score defines the preciseness of the training. The training aspect involves the data selection suitable to its category in terms of feature and feature vector. This research draft illustrates a modified selection algorithm and improves the overall classification rate for variety of attacks [4].

Attacks in Cloud Computing

Cloud computing is a platform in which virtualized resources are made available as a pay-peruse service, similar to power is distributed in an electrical grid [5]. Websites and web-based applications were set up on a single system prior to this arrangement. The resources were constrained together as a virtual computer with the development of this technology. The benefits of cloud computing for businesses include the ability to connect and collaborate globally without the need to build up additional infrastructure, such as servers, datacenters, and other facilities.

The environment can support a large number of users because it is scalable. The key benefits of switching to this computer paradigm include lower costs, less reliance on staff, resilient scalability, and others [6]. Social networking and other forms of interactive technology are included in cloud computing, although for the most part, cloud computing refers to the utilisation of internet software applications, data management, and computational power. Without investing in additional hardware, employing more employees, or obtaining software licences, cloud computing allows for the dynamic easing of congestion or addition of capabilities. It increases information technology's (IT) potential. Over the past several years, cloud computing has evolved from a potential business idea to one of the IT sectors with the quickest rate of growth. But as more and more information about individuals and companies is kept on cloud servers, concerns over the environment's security are beginning to surface. [7].

CC has revolutionised information processing by providing a technology platform that is affordable, efficient, and scalable. From an administrative standpoint, cloud computing offers greater storage and processing capacity at a lower cost. According to a Market Research Media report, the world's cloud computing 30 percent compound annual growth rate (CAGR) is anticipated for the market, which is projected to reach $270 billion in 2020 [8]. Though, the Cloud-based crimes and assaults against clouds and their users are more challenging to forestall and look into because of aspects that make cloud computing so strong [9].

Although the CC paradigm is not very big, there are many security breaches that are made against different cloud deployment methodologies, posing a substantial risk to users of the cloud. [11]. For instance, a number of attacks such as inundation, wrapper, malicious insertion, side passage, and cryptography man-in-the-middle techniques, and authentication attacks against cloud computing are possible [12].

Table 1. Attacks on the cloud component

Attacks	Protocol vulnerability exploitation	Spoofing	Using VM Migration	Incurring high load	Flooding	Gain access to hypervisor
VM migration	No	No	Yes	Yes	No	No
Cloud Internal DoS	Yes	No	No	Yes	No	No
VM Sprawling	No	No	No	Yes	No	No
Neighbour attacks	No	No	No	Yes	No	No
VM escape	No	No	No	No	No	Yes
Mimicking DoS	No	No	No	No	No	Yes
Economic DoS	No	Yes	No	Yes	Yes	Yes
Application DoS	Yes	No	No	No	No	No

Energy oriented DoS	No	No	No	Yes	No	No

The NSL-KDD dataset also includes the following attacks: the probing attack shown in table 2, Denial-of-service (DOS), Remote to Local (R2L), and User to Root (U2R).

Table 2. Attacks Present in NSL KDD dataset

Attack category	Attack name
DoS	Apache 2, sumurf, Neptune, Back, Teardrop, Pod, Land, Mailbomb, Processtable, UDPstorm
Remote to local (R2L)	WarezClient, Guess_Password, WarezMaster, Imap, Ftp_Write, Named, MultiHop, Phf, Spy, sendmail, SnmpGuess, Worm, Xsnoop, XLOCK
User to root (U2R)	Buffer_Overflow, Httptuneel, Rootkit, LoadModule, Perl, sXterm, Ps, SQLattack
Probe	Satan, Saint, Ipsweep, Nmap, Mscan

DoS and DDoS attack

A denial-of-service (DoS) attack is any event or malicious action that lessens or prevents a cloud's capacity to provide the services and functionalities that users expect [13]. Circulated version of Distributed DoS (DDoS) attacks is referred to as DoS attacks. It uses many network hosts to do more damage damaging consequences for its sufferer [14]. A DoS attack is one that targets a resource or service in the cloud with the intention of temporarily preventing it from offering its regular services.

DoS attacks frequently target the connectivity or capacity of computer networks, which jeopardises the accessibility of cloud services and resources. Generally, DoS attacks occur due to bandwidth restriction, problem in connectivity, exhausting of resources, limitation of exploitation, disruption in processes, corrupted data, and due to physical disruption [15]. A distributed denial of service (DDoS) attack involves the use of many hacked computers to overload a target system with traffic, rendering it inaccessible to its intended users. In cloud computing, DDOS attacks can be classified into several types, based on the nature of the attack and the way it is carried out. Some common types of DDOS attacks in cloud computing are:

- Volume-based attacks: In order to overrun the target system and prevent it from being used by its intended users, these attacks try to overload it with a lot of traffic, such as HTTP requests or network packets.
- Protocol-based attacks: By taking advantage of flaws in the TCP/IP protocol stack and other communication protocols utilised by the target system, these attacks make the system inaccessible and clogged.

R2L (Remote to Local)

An R2L attack is a kind of cyberattack where a hacker uses either stolen login credentials or system weaknesses to obtain unauthorised access to a computer system. The attacker starts from a remote location and gains access to a local system, often with the goal of compromising the target system's data or taking control of the system. R2L attacks are a type of cyber-attack that targets vulnerabilities in a network or application from a remote location, with the goal of gaining unauthorized access to a local system [16]. This type of attack is often carried out by exploiting weaknesses in the security infrastructure of an organization, such as weak passwords or unpatched software, to gain access to sensitive information or disrupt operations [17].

USER TO ROOT (U2R)

U2R (User-to-Root) attacks are a type of cyberattack where an attacker with limited user privileges on a system can escalate their access and gain full administrative control, known as "root" access. This type of attack is considered particularly dangerous because it can occur without the need for an initial compromise of the system and can often go undetected. The attacker first gains access to a system by exploiting vulnerabilities in web applications, phishing emails, or other means, and then leverages that initial access to escalate their privileges. This is often achieved by exploiting weaknesses in system configuration, such as unpatched software, weak passwords, or misconfigured permissions. Once the attacker has gained root access, they have full control over the system and can carry out a variety of malicious activities, such as installing backdoors, stealing sensitive data, or launching further attacks on other systems.

U2R attacks can be prevented by implementing robust security measures, including regularly patching software, using strong passwords, and properly configuring system permissions [18]. Additionally, implementing intrusion detection and prevention systems, as well as conducting regular security audits, can help to detect and prevent U2R attacks [17]. It's also important to educate users on security best practices, such as avoiding phishing emails, not downloading or installing unknown software, and being aware of potential threats. By adopting a comprehensive security strategy, organizations can better protect themselves against U2R attacks and other types of cyber threats. In summary, U2R attacks are a serious threat to the security of systems and networks, and organizations must take proactive measures to prevent and detect them. This includes implementing strong security controls, educating users on best practices, and conducting regular security assessments.

Probe Attack

One kind of cyberattack designed to learn more about the intended system or network is called a probe assault. The attacker uses various tools and techniques to gather information about the network's infrastructure, security measures, and vulnerabilities, with the ultimate goal of finding ways to exploit those weaknesses. In cloud security, probe attacks are particularly dangerous because cloud environments are often large and complex, and attackers can easily hide their tracks. The goal of a probe attack in the cloud is to gain access to sensitive information or compromise systems. Several techniques, including as port scanning, vulnerability scanning, and network mapping, can be used to carry out probe attacks [19]. Finding open ports on a target system is a procedure known as port scanning, which might reveal details about the kinds of services that are operating on that system.

Finding and using known flaws in the target system or network is known as vulnerability scanning. Network mapping involves creating a visual representation of the network's infrastructure, including the devices and services running on it. Once the attacker has gathered information about the target system or network, they can use that information to launch more sophisticated attacks, such as denial-of-service (DoS) attacks, man-in-the-middle (MitM) attacks, or data breaches.

Organisations should use a multi-layered security strategy that incorporates firewalls, intrusion detection and prevention systems, and access restrictions to stop probing attacks. Regular security audits and vulnerability scans should also be performed to identify and address any potential security weaknesses. In network security, probe attacks can be prevented by implementing network segmentation, which involves dividing the network into smaller, separate segments. This helps to limit the scope of a potential breach and makes it more difficult for an attacker to gather information about the entire network.

Organisations should train staff members on security best practises and how to recognise and report possible probing attacks in addition to technological protections. This can help to reduce the risk of a successful probe attack and ensure that employees are prepared to respond quickly if an attack does occur [20]. In summary, probe attacks are a significant threat to cloud and network security, as they provide attackers with the information they need to launch more sophisticated attacks [21]. Entities must to adopt a multipronged security strategy that encompasses intrusion detection and prevention systems, firewalls, access restrictions, and security audits. Additionally, they must to train staff members on security best practises and how to spot and report any probing attacks.

Intrusion Detection System

Intrusion detection is usually referred to the technology and the software applications that monitor the network activities and detect security breaches in terms of malicious activities. Soon after Dorothy Denning work on the initial IDS model presented at SRI international [22], several intrusion detection works were put forth to address the challenges of research industry. The generalized architecture of the IDS system shown in figure 1. included the following components:

- Sensors that gather and collect the data from the system to be monitored.
- Detector which is also known as intrusion detection engine which perform analysis of malicious activities on the data collected from the sensor.
- Knowledgebase is the database that act as a repository for the pre-processed version of the collected information using sensors. It is also annotated for the attack signature, profiles, etc. to help security experts.
- Configuration device is used to share information regarding the current state of the IDS.
- Response Component is the last component of the system that initiates action as and when an intrusion is detected by the system. The generated response can be customised and may or may not involve human intervention.

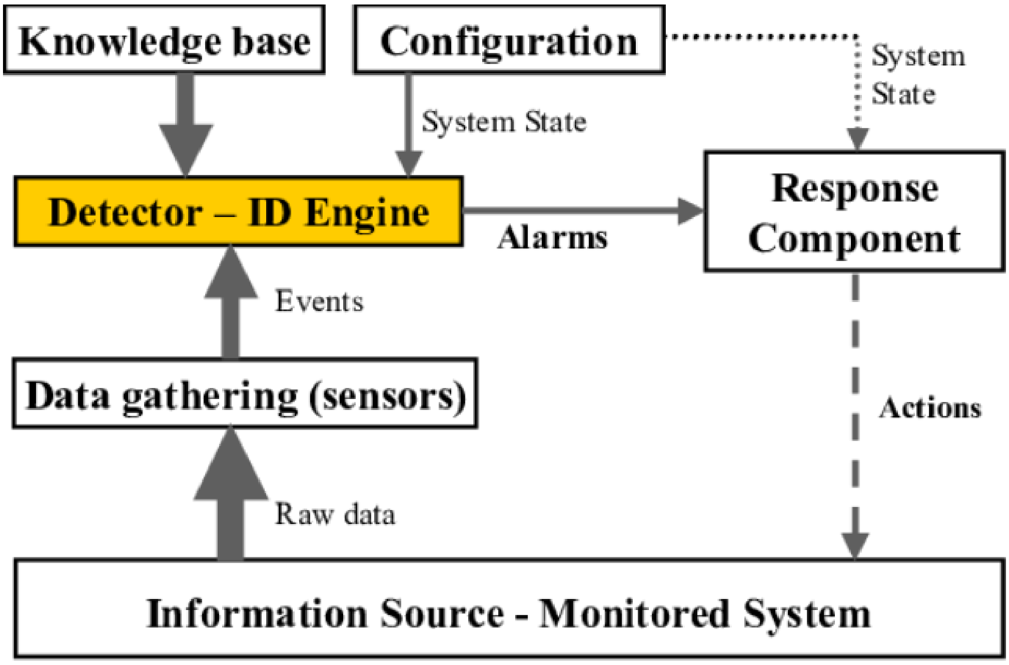

Figure 1. IDS Architecture

These intrusion detection tools or the intrusion detection systems (IDS) are aimed at identifying the security threats in real time scenario and are broadly classified as follows.

- Network based IDS (NIDS) This type of IDS analyses the network packets to identify the suspicious patterns that looks deviated from the usual pattern. As soon as the malicious activity is detected, it generates a predefined action to mitigate the potential threat.
- Host based IDS (HIDS) This type of IDS is installed on an individual computer system and monitors the activity of the specific host computer system. It analyses the behaviour of various processes, user activity and files for the host system to detect any abnormal activity or unauthorized access attempts to the system files. The IDS forms one of the critical component of the cyber security that helps in identifying any security breaches, cyber-attacks, etc.

Comprehensive Analysis of IDS

Intrusion Detection Systems (IDS) are critical components in safeguarding modern computational infrastructures against potential security breaches. IDS methodologies are categorized into signature-based, anomaly-based, and hybrid systems. Signature-based IDS excels at detecting known threats by leveraging a predefined database of attack signatures, whereas anomaly-based IDS identifies deviations from normal network behavior, enabling the detection of zero-day attacks. Hybrid systems amalgamate both approaches to improve detection efficacy.

The efficiency of an IDS depends on its classification mechanism, which involves identifying whether a network activity is benign or malicious. Key challenges in IDS design include high false-positive rates, scalability issues in large networks, and the increasing complexity of attack vectors. The implementation of machine learning and deep learning in IDS has transformed classification mechanisms, providing enhanced accuracy and adaptability. These systems incorporate supervised, unsupervised, and reinforcement learning techniques to automate anomaly detection and signature generation. Table 3 provides a detailed analysis of diverse IDS classification systems, highlighting their underlying techniques, inference, and drawback.

Table 3. Analysis of Diverse IDS Classification System

Reference	Year and Author Name	Purpose	Techniques Used	Inference	Drawback
[23]	Aldallal & Alisa (2021)	Develop a hybrid IDS using SVM and GA to secure	SVM with kernel optimization, Genetic	Achieved improved detection	Higher computational cost due to GA-

		cloud environments.	Algorithm	accuracy using CICIDS2017 dataset with feature selection and optimization.	SVM parallel execution.
[24]	Alzughaibi & El Khediri (2023)	Enhance cloud IDS accuracy using DNN with backpropagation and PSO.	Multi-Layer Perceptron (MLP), Particle Swarm Optimization	Achieved 98.97% binary classification accuracy on CSE-CIC-IDS2018, demonstrating improved performance over related studies.	Limited scalability and dataset generalization to diverse real-world scenarios.
[25]	Chang et al. (2022)	Survey on IDS technologies for fog and cloud computing environments.	Comprehensive review of IDS frameworks and security policies.	Proposed structured guidelines for securing cloud and fog systems, emphasizing software-as-a-service (SaaS) and automation.	Lacks experimental validation of proposed strategies in a live cloud environment.
[26]	Attou et al. (2023)	Develop a DL-based IDS using RF for feature selection and RBFNN for detection in cloud environments.	Random Forest, Radial Basis Function Neural Network	Achieved accuracy >92% and improved MCC from 28% to 93%, validating effectiveness on Bot-IoT and NSL-KDD datasets.	Computationally intensive for real-time intrusion detection.
[27]	Elmasry, Akbulut & Zaim (2021)	Design an integrated CIDS with third-party cloud service to enhance intrusion prediction and reporting.	Enhanced Bagging Ensemble, Deep Learning Models	Demonstrated resilience against cloud attacks with effective modular design and ensemble-based learning techniques.	Dependency on third-party services may raise privacy and trust issues.
[28]	Mohamed & Ismael (2023)	Develop a hybrid IDS for fog-to-cloud IoT environments for real-time attack detection.	Artificial Neural Networks, Genetic Algorithms	Reduced execution time by up to 37.07% on UNSW-NB15 and ToN_IoT datasets while maintaining high accuracy through optimized	Limited generalization across diverse IoT device architectures and environments.

				neural network parameters.	
[29]	2021, Aldallal & Alisa	To propose a hybrid machine learning-based IDS for cloud security	SVM combined with GA, fitness function	Improved accuracy and feature selection, 5.74% higher performance than benchmarks	Limited to datasets like CICIDS2017, KDD CUP 99, and NSL-KDD
[30]	2020, Alkadi et al.	To review cloud intrusion detection and blockchain applications	Review-based analysis	Discusses collaborative NIDS and blockchain for privacy and trust	Lacks experimental validation or detailed quantitative comparison
[31]	2023, Fatani et al.	To enhance IDS for IoT and cloud environments	CNNs for feature extraction, modified GO with WOA	High accuracy in identifying unknown attacks; improved GO performance	Computational overhead due to deep learning and multiple optimizations
[32]	2020, Wang et al.	To design a cloud IDS for high-dimensional, large-scale traffic	Stacked contractive autoencoder (SCAE) + SVM	Reduced computational overhead, better feature extraction, high detection accuracy	Limited to specific datasets; scalability to larger networks untested
[33]	2020, Samriya & Kumar	To address cloud security issues using a hybrid IDS approach	Fuzzy ANN, Spider-Monkey Optimization	Reduced computational time and enhanced accuracy compared to existing hybrid methods	Complexity of iterative clustering and fuzzy updates
[34]	2022, Onyema et al.	To design an IDS for IoT in smart cities using cyborg intelligence	Ensemble learning with AdaBoost, RF, Bayesian Networks	High detection accuracy and low false-positive rates for botnet attacks	Limited scope for other IoT security threats
[35]	2022, Kareem et al.	To develop an FS model for IoT IDS	GTO optimized with BSA	Improved convergence rates, high-quality solutions across datasets	High dependency on metaheuristic parameter tuning
[36]	2020, Kunhare et al.	To improve IDS performance using FS and optimization	PSO, RF for FS, various classifiers	High accuracy and low false-positive rates; reduced feature set	Focused on NSL-KDD; generalization to other datasets untested
[37]	2020, Chkirbene et al.	To create a trust-based IDS for feature selection and classification	TIDCS/TIDCS-A, dynamic feature selection	High accuracy and detection rates, reduced false positives	Increased computational time during trust evaluation and

					updates
[38]	Alkanhel et al. (2023)	Develop a hybrid optimization algorithm for feature selection in IDS for IoT networks.	Grey Wolf Optimization (GW), Dipper Throated Optimization (DTO), GWDTO hybrid algorithm, statistical analysis.	The GWDTO algorithm provides a balance between exploration and exploitation, enhancing classification accuracy and stability in IoT-based IDS.	Potential limitations in scalability for very large datasets or applicability across varied network conditions.
[39]	Disha & Waheed (2022)	Evaluate ML models' performance for IDS using feature selection to handle high-dimensional datasets.	Gini Impurity-based Weighted Random Forest (GIWRF), Decision Tree (DT), Gradient Boosting Tree (GBT), MLP, LSTM, GRU.	GIWRF-DT model significantly improves performance on UNSW-NB 15 and Network TON_IoT datasets, outperforming surveyed methods in F1 score.	Limited exploration of deep learning techniques, which might provide better results with further investigation.
[40]	Dahou et al. (2022)	Enhance IDS performance for IoT environments using deep learning and metaheuristic optimization for feature selection.	Convolutional Neural Network (CNN), Reptile Search Algorithm (RSA), datasets (KDDCup-99, NSL-KDD, CICIDS2017, BoT-IoT).	The RSA-based feature selection combined with CNN improves the performance of IDS in IoT networks compared to other optimization techniques.	The study may have a limited focus on real-time processing and might require significant computational resources.

The reviewed studies are valuable to develop IDS for cloud, fog, and IoT, exploring a variety of state-of-the-art machine learning, deep learning, and optimization. Advanced learning methodologies such as SVM-GA, CNN, and PSO have played significant roles to increase the detection rates, features extraction and reduction and computational time. In many works, to minimize feature space and achieve high detection rates, researchers work on the feature selection step where feature space is reduced; using different datasets including, CICIDS2017, UNSW-NB15 and NSL-KDD. Further improvements in the model efficiency have been achieved with metaheuristic algorithms such as Grey Wolf Optimization (GWO), Reptile Search Algorithm (RSA), and Spider-Monkey Optimization.

Some problems remain in the approach: the computational overhead, scalability, applicability of obtained models to specific datasets only, and real-time considerations. While ensemble learning and advanced optimization methods give higher accuracy, the necessity to use computational resources and parameter setting is a question. Multiple works highlighting IDS in cloud focus on the modularity and integration of the design but there are issues such as trust dependency on third-party services. In addition, the presence of numerous reviews and frameworks for these approaches makes most of them less practical when it comes to testing in various environments since they are not experimentally grounded.

The state-of-art of Intrusion Detection Systems (IDS) for cloud, fog, and IoT environment has identified certain issues that restrict IDS from being implemented. One of the major limitations of current approaches is that they must be adapted to a given dataset and fail to provide good performance at scale or when working with high-dimensional traffic or complex network topologies. Several approaches identified are useful in more homogeneous settings but less applicable in the context of a myriad of IoT devices and smart cities, in particular. Another disadvantage is computational complexity, many deep learning and hybrid optimization algorithms require a lot of computational power, which is inapplicable for IoT and Edge systems.

In addition, third-party cloud-based IDS frameworks pose privacy and trust issues thus; require secure concepts such as blockchain to manage trust and data integrity. Further, there is a lack of effective and efficient real-time intrusion detection, and a majority of the studies are conducted offline and therefore are not quite practically applicable. Lastly, what survey-based frameworks and proposed strategies often lack is a solid experimental proof of their viability, which makes the use of such approaches questionable when addressed to rapidly developing threat scenarios. Closing these gaps calls for improvements in IDS models with low computational and space complexity, and real-time capability for operation in different environments with adequate security features.

CONCLUSION

IDS are essential for the security and reliability of cloud computing against new advanced threats. The strengths of this study include a detailed review of IDS frameworks over time and demonstration of the integration of sophisticated methodologies, including machine learning, deep learning, and metaheuristic optimization to enhance IDS's efficiency and effectiveness of its detection capabilities. Nevertheless, there are issues like computational complexity, growing number of components, and real-time, lightweight solutions. The addition of blockchain for trust and data integrity shows that security can be increased but that implementation in a variety of cloud environments is challenging. Generalization of dataset, privacy concerns, and adaptive learning methods are among the main challenges that still deserve more attention to achieving practical implementation of IDS. Future studies should address the need to design IDS frameworks that are effective at large and operating within resource constraints, and delivering the capacity to rapidly and accurately analyze events in cloud systems that are highly diverse and constantly evolving.

REFERENCE

[1] M. J. Kavis, Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS). John Wiley & Sons, inc, 2014.

[2] T. Guarda, M. F. Augusto, I. Costa, P. Oliveira, D. Villao, and M. Leon, ―The Impact of Cloud Computing and Virtualization on Business,‖ Communications in Computer and Information Science, vol. 1485, pp. 399–412, 2021, doi: 10.1007/978-3-030-90241- 4_31/COVER.

[3] R. S. Sandhu, ―Role-based access control,‖ in Advances in computers, Elsevier, 1998, pp. 237–286.

[4] A. R. Suraj, S. J. Shekar, and G. S. Mamatha, ―A robust security model for cloud computing applications,‖ in 2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), 2018, pp. 18–22.

[5] M. I. Alam, M. Pandey, and S. S. Rautaray, ―A comprehensive survey on cloud computing,‖ International Journal of Information Technology and Computer Science (IJITCS), vol. 7, no. 2, p. 68, 2015.

[6] S. Carlin and K. Curran, ―Cloud computing security,‖ in Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments, IGI Global, 2013, pp. 12– 17.

[7] I. M. Khalil, A. Khreishah, and M. Azeem, ―Cloud computing security: A survey,‖ Computers, vol. 3, no. 1, pp. 1–35, 2014.

[8] Gartner, ―Worldwide Public Cloud End-User Spending,‖ Stamford, 2021. https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecastsworldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021 (accessed Feb. 08, 2023).

[9] R. Buyya, A. Beloglazov, and J. Abawajy, ―Energy-Efficient Management of Data Center Resources for Cloud Computing: A Vision, Architectural Elements, and Open Challenges,‖ Jun. 2010, doi: 10.48550/arxiv.1006.0308.

[10] A. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm, ―What‗s inside the Cloud? An architectural map of the Cloud landscape,‖ in 2009 ICSE workshop on software engineering challenges of cloud computing, 2009, pp. 23–31.

[11] I. S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan, and K. K. R. Choo, ―On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,‖ Journal of Network and Computer Applications, vol. 74, pp. 98-120, 2016.

[12] M. Alotaibi, ―Security to wireless sensor networks against malicious attacks using Hamming residue method,‖ Eurasip Journal on Wireless Communications and Networking, vol. 2019, no. 1, pp. 1–7, Dec. 2019, doi: 10.1186/S13638-018-1337- 5/FIGURES/4.

[13] S. Singh, R. A. Khan, and A. Agrawal, ―Prevention mechanism for infrastructure based Denial-of-Service attack over software Defined Network,‖ International Conference on Computing, Communication & Automation, pp. 348–353, Jul. 2015, doi: 10.1109/CCAA.2015.7148442.

[14] P. Chouhan and R. Singh, ―Security Attacks on Cloud Computing With Possible Solution,‖ International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 1, pp. 92–96, 2016, Accessed: Feb. 08, 2023. [Online]. Available: www.ijarcsse.com

[15] M. Masdari and M. Jalali, ―A survey and taxonomy of DoS attacks in cloud computing,‖ Security and Communication Networks, vol. 9, no. 16, pp. 3724–3751, Nov. 2016, doi: 10.1002/SEC.1539.

[16] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, ―Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects,‖ Electronics 2022, Vol. 11, Page 1502, vol. 11, no. 9, p. 1502, May 2022, doi: 10.3390/ELECTRONICS11091502.

[17] J. Raiyn, ―A survey of Cyber Attack Detection Strategies,‖ Article in International Journal of Security and its Applications, vol. 8, no. 1, pp. 247–256, 2014, doi: 10.14257/ijsia.2014.8.1.23.

[18] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, ―A survey of intrusion detection techniques in Cloud,‖ Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, Jan. 2013, doi: 10.1016/J.JNCA.2012.05.003.

[19] S. Shamshirband, M. Fathi, A. T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescapè, ―Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues,‖ Journal of Information Security and Applications, vol. 55, p. 102582, Dec. 2020, doi: 10.1016/J.JISA.2020.102582.

[20] U. Kumar and B. N. Gohil, ―A Survey on Intrusion Detection Systems for Cloud Computing Environment,‖ International Journal of Computer Applications, vol. 109, no. 1, pp. 975–8887, 2015.

[21] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, and H. Fahmy, ―Monitoring Real Time Security Attacks for IoT Systems Using DevSecOps: A Systematic Literature Review,‖ Information 2021, Vol. 12, Page 154, vol. 12, no. 4, p. 154, Apr. 2021, doi: 10.3390/INFO12040154.

[22] D. E. Denning, ―An Intrusion-Detection Model,‖ IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222–232, 1987, doi: 10.1109/TSE.1987.232894.

[23] Aldallal, A., & Alisa, F. (2021). Effective intrusion detection system to secure data in cloud using machine learning. Symmetry, 13(12), 2306.

[24] Alzughaibi, S., & El Khediri, S. (2023). A cloud intrusion detection systems based on dnn using backpropagation and pso on the cse-cic-ids2018 dataset. Applied Sciences, 13(4), 2276.

[25] 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.

[26] Attou, H., Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., & Almusallam, N. (2023). Towards an intelligent intrusion detection system to detect malicious activities in cloud computing. Applied Sciences, 13(17), 9588.

[27] Elmasry, W., Akbulut, A., & Zaim, A. H. (2021). A design of an integrated cloud-based intrusion detection system with third party cloud service. Open Computer Science, 11(1), 365-379.

[28] Mohamed, D., & Ismael, O. (2023). Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing. Journal of Cloud Computing, 12(1), 41.

[29] Aldallal, A., & Alisa, F. (2021). Effective intrusion detection system to secure data in cloud using machine learning. Symmetry, 13(12), 2306.

[30] Alkadi, O., Moustafa, N., & Turnbull, B. (2020). A review of intrusion detection and blockchain applications in the cloud: approaches, challenges and solutions. IEEE Access, 8, 104893-104917.

[31] Fatani, A., Dahou, A., Abd Elaziz, M., Al-Qaness, M. A., Lu, S., Alfadhli, S. A., & Alresheedi, S. S. (2023). Enhancing intrusion detection systems for IoT and cloud environments using a growth optimizer algorithm and conventional neural networks. Sensors, 23(9), 4430.

[32] Wang, W., Du, X., Shan, D., Qin, R., & Wang, N. (2020). Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. IEEE transactions on cloud computing, 10(3), 1634-1646.

[33] Samriya, J. K., & Kumar, N. (2020, October). A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing. In Materials Today: Proceedings (Vol. 2, No. 1, pp. 23-54). Elsevier.

[34] Onyema, E. M., Dalal, S., Romero, C. A. T., Seth, B., Young, P., & Wajid, M. A. (2022). Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities. Journal of Cloud Computing, 11(1), 26.

[35] Kareem, S. S., Mostafa, R. R., Hashim, F. A., & El-Bakry, H. M. (2022). An effective feature selection model using hybrid metaheuristic algorithms for iot intrusion detection. Sensors, 22(4), 1396.

[36] Kunhare, N., Tiwari, R., & Dhar, J. (2020). Particle swarm optimization and feature selection for intrusion detection system. Sādhanā, 45, 1-14.

[37] Chkirbene, Z., Erbad, A., Hamila, R., Mohamed, A., Guizani, M., & Hamdi, M. (2020). TIDCS: A dynamic intrusion detection and classification system based feature selection. IEEE access, 8, 95864-95877.

[38] Alkanhel, R., El-kenawy, E. S. M., Abdelhamid, A. A., Ibrahim, A., Alohali, M. A., Abotaleb, M., & Khafaga, D. S. (2023). Network Intrusion Detection Based on Feature Selection and Hybrid Metaheuristic Optimization. Computers, Materials & Continua, 74(2).

[39] Disha, R. A., & Waheed, S. (2022). Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. Cybersecurity, 5(1), 1.

[40] Dahou, A., Abd Elaziz, M., Chelloug, S. A., Awadallah, M. A., Al-Betar, M. A., Al-Qaness, M. A., & Forestiero, A. (2022). Intrusion detection system for IoT based on deep learning and modified reptile search algorithm. Computational Intelligence and Neuroscience, 2022(1), 6473507.