Journal of Information Systems Engineering and Management
2025, 10(11s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Intrusion Detection and Prevention: -Network Security in Cloud

Bhoopendra Singh[1], Brijesh Kumar[2]

1 Ph.D Research Scholar, Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, INDIA

[2] Prof. (Dr.) Brijesh Kumar, Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, INDIA

ARTICLE INFO

Received: 14 Nov 2024

Revised: 26 Dec 2024

Accepted: 10 Jan 2025

ABSTRACT

The growing adoption of cloud computing has introduced heightened vulnerabilities to cyber-attacks. Network Intrusion Detection Systems (NIDS) are pivotal in safeguarding cloud computing environments. However, the dynamic and distributed nature of cloud computing imposes challenges on traditional NIDS. This study examines the state of NIDS in cloud computing, their limitations, and potential improvements through machine learning and artificial intelligence. Ensuring NIDS can effectively detect both known and unknown threats is essential for cloud security, warranting ongoing research and innovation.

Keywords: Network Monitoring, Threat Detection. Intrusion Prevention, Data Protection, Cyber security, Virtualization

INTRODUCTION

Cloud computing revolutionizes data storage and management by utilizing remote servers rather than local systems. While it reduces operational costs and enhances flexibility, cloud computing also introduces new security risks, particularly network intrusions. Unauthorized access to networks can lead to data breaches and service disruptions. NIDS play a critical role in mitigating these risks by detecting threats in real-time, surpassing traditional solutions like firewalls and antivirus software. These systems leverage advanced algorithms and machine learning to analyze network traffic and identify anomalies, ensuring secure cloud environments [1]. In cloud computing environments, network intrusions can lead to significant repercussions, such as data breaches, service outages, and the compromise of sensitive information. The necessity of implementing network intrusion detection systems (NIDS) cannot be emphasized enough. These systems are vital for ensuring network security and safeguarding sensitive data stored in the cloud. A key advantage of NIDS in cloud computing is their ability to identify and mitigate potential threats in real-time, providing proactive protection against emerging risks [2]. Ongoing prevalent security devices and application such as firewalls and antivirus are not always effective in identifying advanced cyber threats, making it necessary to have a network intrusion detection system in place. These systems employ sophisticated algorithms and machine learning methods to examine network traffic and detect any unusual or potentially harmful activity. Cloud computing is a revolutionary technology that has transformed the way businesses and individuals store, process, and access data [3]. It allows for the outsourcing of computing resources, enabling users to access applications and store data remotely. However, this shift towards cloud computing has also brought about new security challenges, as data and applications are no longer housed within the traditional network perimeter, making them susceptible to various cyber threats. One of the key security concerns in cloud computing environments is the risk of network intrusion [4]. Network intrusion refers to unauthorized access, misuse, or disruption of a computer network or its resources. With the vast amount of data stored in the cloud, the potential risk of network intrusion is even greater. In response to this growing concern, there have been significant innovations in the field of Network Intrusion Detection Systems (NIDS) to enhance the security of cloud computing environments [5]

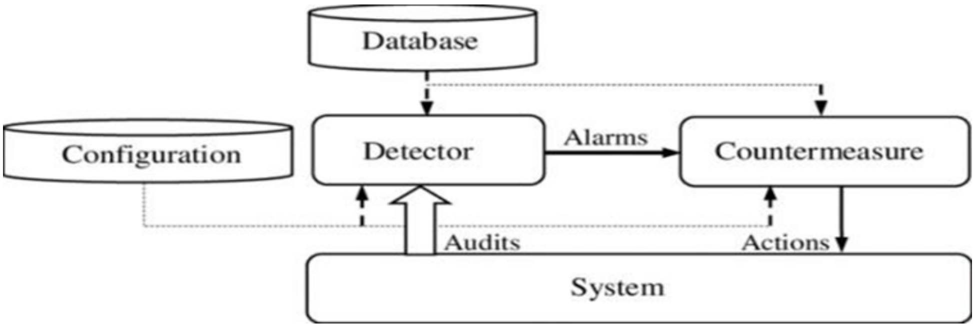

Fig 1: Construction of NIDS diagram

Network Intrusion Detection Systems (NIDS) are designed to oversee network traffic, promptly identifying potential threats by examining patterns and behaviors to uncover any suspicious activity and alert network administrators to possible attacks. Historically, NIDS were deployed as on premise solutions, monitoring network traffic within an organization's infrastructure [6]. The key contributions of NIDS include:

Early detection of attacks: NIDS enable the early identification of security threats and attacks in cloud environments, allowing for swift action to mitigate risks and prevent extensive damage.

Real-time monitoring: By continuously monitoring network traffic, NIDS provide immediate alerts for suspicious activities, enabling rapid responses to limit the impact of potential intrusions.

Scalability: Given the inherently scalable nature of cloud computing, NIDS can adapt seamlessly to changes in network infrastructure, making them well-suited for dynamic cloud environments [7].

Visibility into virtual networks: NIDS offer insight into virtual networks, facilitating the detection of activities within cloud environments, which are often more vulnerable due to their dynamic configurations.

Anomaly detection: Leveraging machine learning algorithms and behavioral analysis, NIDS can identify abnormal network behaviors, effectively detecting new or unknown threats within the cloud. [7-9].

RELATED WORKS

Cloud computing has gained significant popularity in recent years among both businesses and individuals. Offering advantages such as cost efficiency, scalability, and user-friendliness, it is becoming a go-to solution for many organizations' IT requirements. However, alongside these benefits, there are also various security risks to consider [10]. A major challenge in cloud computing is detecting network intrusions. Network intrusion detection involves monitoring and analyzing network traffic to detect unauthorized or malicious activities. In conventional IT setups, this is usually achieved by deploying intrusion detection systems (IDS) at key network entry points [11]. In a cloud computing environment, however, this process becomes more complicated due to the distributed and virtualized nature of the systems. One of the key challenges in detecting network intrusions in the cloud is the limited control over the network infrastructure. Unlike traditional IT setups, where organizations have full control over their network and can enforce stringent security measures, cloud environments often involve shared resources and external management [12]. In a cloud environment, however, the network is shared among multiple users and managed by the cloud service provider. This shared nature makes it challenging for organizations to effectively monitor and control network traffic, increasing the likelihood that intrusions may go undetected. Network Intrusion Detection (NID) is a crucial component of cybersecurity in any computing environment, particularly in cloud computing. As cloud computing continues to grow in popularity, offering convenient and cost-effective data storage and processing solutions, the need for robust intrusion detection becomes even more critical [13]. While cloud computing offers significant convenience, it also presents several challenges, particularly in the area of Network Intrusion Detection (NID). One of the key difficulties in detecting and preventing intrusions in cloud environments lies in the unique architecture of cloud systems. Cloud setups often involve a large, shared pool of resources, such as servers, databases, and networks. This shared infrastructure complicates the process of isolating and monitoring individual users and their activities, making it harder to detect and track potential intrusions effectively [14]. Another significant challenge for Network Intrusion Detection (NID) in cloud environments is the sheer volume of data and traffic. Cloud systems handle vast amounts of data, making it difficult for traditional intrusion detection systems to manage and analyze effectively. With numerous data transactions occurring simultaneously, detecting malicious or abnormal patterns that might signal an intrusion becomes increasingly complex. As a result, network intrusion detection in cloud computing is a relatively new and rapidly evolving field that has attracted considerable attention in recent years [15]. The migration of data and services to the cloud has prompted a reassessment of traditional intrusion detection systems, as the distinct features of cloud environments present new challenges in detecting and preventing network attacks. Unlike traditional networks, cloud environments are highly dynamic and distributed, making it difficult to effectively monitor and safeguard against intrusions. Consequently, the development of new, specialized intrusion detection techniques tailored for cloud computing has become a key priority for researchers and professionals in the field [16].

PROPOSED MODEL

A Network Intrusion Detection System (NIDS) is a vital security tool that identifies and prevents potential network attacks. Since the demand of cloud computing continues to grow and gain widespread popularity, developing an efficient NIDS specifically for cloud environments is becoming essential to protect sensitive data and resources.

A. Construction technique

Developing a Network Intrusion Detection System (NIDS) in a cloud computing environment presents significant challenges due to the cloud's dynamic and distributed nature. In contrast to traditional networks, cloud environments have complex network structures with fluctuating numbers of servers, virtual machines, and network connections. This constant change makes it difficult to deploy and manage traditional NIDS, which are typically built for more stable and static network infrastructures.

$$J = \left(\frac{dJ_i}{dI_i^2} \right) \tag{1}$$

$$di_i^2 = 2 * di * dI_J \tag{2}$$

To develop a Network Intrusion Detection System (NIDS) in the cloud, the first step is to thoroughly understand the cloud infrastructure. This includes gaining knowledge of the various cloud components, such as hypervisors, virtual switches, and virtual networks. It also involves analyzing network traffic patterns, communication protocols, and the behavior of cloud applications and services. Once a clear knowledge of the infrastructure is achieved, further to identify potential attack vectors and vulnerabilities within the cloud environment.

B. Implementation part

Network intrusion detection is a crucial element of security in any computing environment, and its significance is heightened in cloud computing. The cloud's intricate and ever-changing nature, where data is stored and accessed remotely across various locations, exposes it to potential cyberattacks. Consequently, the effective implementation of network intrusion detection in cloud computing is vital to safeguarding the security and integrity of data. This process includes employing a variety of technologies and techniques to monitor network traffic, identify potential threats, and alert administrators about possible security breaches.

$$n_i^2 = \left(\frac{2 * I_m}{J_u} \right) \tag{3}$$

This can be achieved by implementing intrusion detection and prevention systems (IDPS) that continuously monitor network traffic, comparing it to predefined attack signatures and patterns. Additionally, the integration of artificial intelligence and machine learning algorithms can improve anomaly detection, enabling the identification of unusual network traffic patterns that may indicate a potential cyberattack. Shown below in fig-2 is the block diagram.

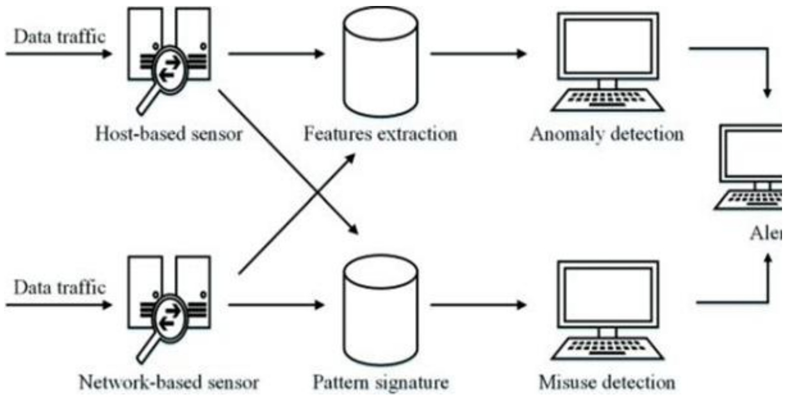

Fig 2: Functional block diagram

A major challenge in implementing network intrusion detection in cloud computing is the dynamic nature of the cloud environment. As cloud resources and applications frequently change, cyber attackers also evolve their techniques and methods to exploit emerging vulnerabilities. Consequently, network intrusion detection systems must be regularly updated and adapted to keep pace with these changes. This can be achieved through continuous monitoring, incorporating threat intelligence, and performing routine vulnerability assessments

C. Functional working model

Network Intrusion Detection (NID) is a key component of network security in cloud computing environments. It is A Network Intrusion Detection (NID) system is a technology designed to monitor network traffic for malicious or suspicious activities, alerting the appropriate personnel when potential intrusions are detected. It combines both hardware and software to analyze network traffic, identifying anomalies or patterns that could indicate a threat. In cloud computing environments, the NID system operates in four main stages: data collection, data analysis, event generation, and response. During the data collection stage, the NID system collects network traffic data from multiple sources, including firewalls, routers, and switches.

$$j''(o) = \lim_{i\to 0}\left(\frac{j(j+i)-j(i)}{i}\right) \qquad (4)$$

$$j'(o) = \lim_{j\to 0}\left(\frac{j^{j+i}-j^{j}}{i}\right) \qquad (5)$$

The collected data is then transferred to the data analysis stage, where it is processed and correlated to identify potential threats. During this stage, the NID system applies several techniques, like “signature-based detection, anomaly-based detection, and rule-based detection”, to examine network traffic for suspicious activities. Signature-based detection matches traffic against known malicious patterns, whereas anomaly-based detection identifies unusual or abnormal behavior in the traffic. Rule-based detection uses predefined rules to identify specific attack patterns.

D. Operating principle

Network Intrusion Detection is a security mechanism designed to analyse, monitor and identify any malicious or unauthorized activity within a computer network. In cloud computing environments, it runs by assessing network traffic and the behavior of network hosts to detect potential threats and anomalies. In the beginning, the operation of Network Intrusion Detection is to gather and assess data from multiple sources, including firewalls, routers, and servers. This data consists of network traffic logs, event logs, and system logs. The collected data is then processed and analyzed through various algorithms and techniques to detect patterns and anomalies that could signal potential threats or unauthorized activities. The operational flow diagram has shown in the following fig.3.

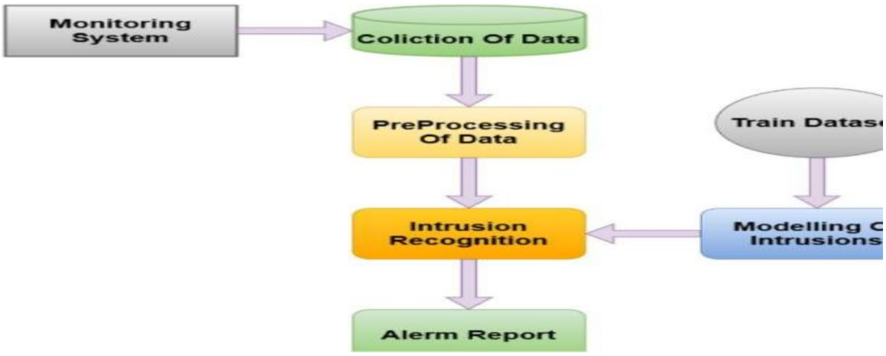

Fig 3: Design flow diagram

The identified patterns and anomalies are matched with established attack signatures and behaviors to detect possible threats. Along with analyzing network traffic, the core function of NID also involves observing the actions of network hosts for any suspicious or unauthorized activities.

$$j(i) = \lim_{j\to 0}\left(\frac{(j^j * j^i) - j^j}{i}\right) \qquad (6)$$

This involves monitoring user activities, file modifications, and system configurations. Any unusual or suspicious behavior is flagged for further investigation. To effectively detect threats in a cloud computing environment, Network Intrusion Detection systems also depend on collaboration and information sharing. This includes exchanging threat intelligence and attack signatures with other systems and platforms, enabling a quicker and more precise response to potential threats.

RESULTS AND DISCUSSION

Analyzing the performance of network intrusion detection in cloud computing environments is vital for maintaining the security of cloud-based systems. The increasing adoption of cloud computing, fueled by its scalability and cost-efficiency, enables organizations to store and process vast amounts of data. However, this convenience also brings the potential for cyber threats, underscoring the need for strong intrusion detection systems to protect cloud infrastructure. The proposed model has been evaluated against the existing "(SNORT) Simple Network Intrusion Detection and Prevention System, (NB-EM) Naive Bayes Expectation Maximization, (AASDD) Attribute –Aware Sequential Data Driven Detection and (ANIDS) Adaptive Network Intrusion Detection System".

I. **Network Traffic**

One of the primary factors influencing the performance of network intrusion detection in cloud environments is the high volume of network traffic. Cloud systems process vast amounts of data, making it difficult to monitor each packet and detect potential threats in real-time. Consequently, intrusion detection systems must possess high computational power to manage large and complex datasets effectively. Another important aspect of performance analysis is the deployment model of the intrusion detection system. Table 1 and figure 4given the comparison of various algorithm for Network Traffic.

NO.OF ROUNDS	SNORT	NB- EM	AASDD	ANIDS	PROPOSED
100	75.53	85.24	78.17	71.52	87.79
200	75.42	85.26	78.00	71.25	87.29
300	75.40	86.14	78.73	71.55	87.41
400	78.50	88.97	82.07	75.06	90.64
500	79.70	90.29	82.80	76.38	91.02

Table.1. Comparative analysis of Network Traffic

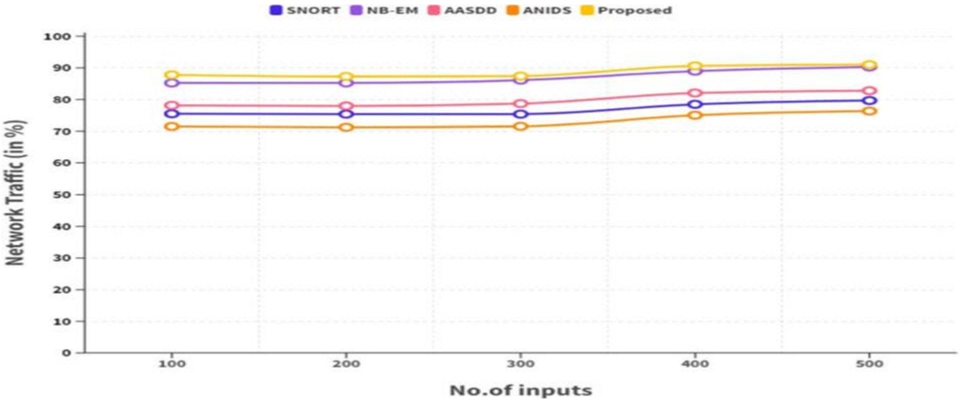

Fig.4: Comparative analysis of Network Traffic

In traditional environments, intrusion detection systems are set up centrally, where all network traffic is directed and monitored from one central point. However, this method is not effective in cloud computing due to the distributed nature of cloud systems. Therefore, intrusion detection systems must be deployed locally within each cloud instance, which creates challenges in managing and coordinating multiple detection systems across the cloud environment.

II. **System Resource Usage**

Network Intrusion Detection (NID) is an essential security mechanism designed to detect and prevent malicious activities on computer networks. As cloud computing continues to grow in popularity, the demand for efficient and effective NID systems has become increasingly critical. Since cloud environments are highly dependent on network connectivity, any intrusion can severely affect the performance and availability of services. To optimize NID performance in a cloud computing environment, several factors must be considered. The first step is to understand the unique characteristics and challenges of cloud computing, including scalability, virtualization, multi-tenancy, and dynamic resource allocation. Table 2 and figure 5 given the comparison of various algorithm for System Resource Usage.

NO.OF ROUNDS	SNORT	NB- EM	AASDD	ANIDS	PROPOSED
100	65.53	75.24	68.17	61.52	77.79
200	65.42	75.26	68.00	61.25	77.29
300	65.40	76.14	68.73	61.55	77.41
400	68.50	78.97	72.07	65.06	80.64
500	69.70	80.29	72.80	66.38	81.02

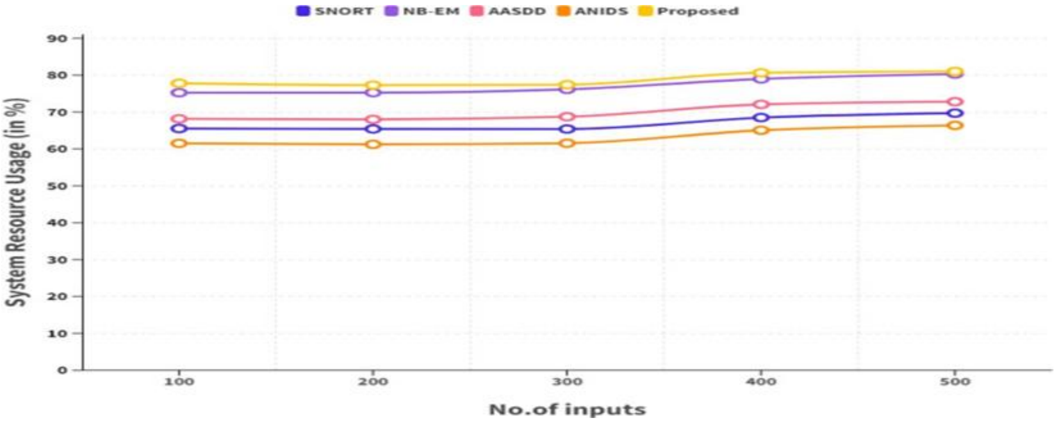

Fig.5: Comparative analysis of System Resource Usage

These factors can greatly influence the performance of NID systems, and optimizing them is essential for achieving high performance. One of the primary strategies for enhancing NID in cloud environments is to take advantage of the cloud's scalability. By leveraging the elastic nature of cloud resources, NID systems can scale up or down according to network traffic volume, ensuring efficient and effective intrusion detection. This also allows NID systems to manage sudden increases in traffic without affecting performance.

III. **Intrusion Detection**

Data masking, or data obfuscation, involves converting sensitive data into an unreadable and meaningless format for anyone who does not have the proper decryption key. This method is employed to safeguard sensitive information, such as personally identifiable details, financial records, and intellectual property, from being accessed by unauthorized individuals. As cloud computing environments increasingly store and process sensitive data, the demand for strong network intrusion detection systems has become even more critical. Network Intrusion Detection Systems (NIDS) are designed to monitor network traffic and identify signs of malicious activity or unauthorized access. Table 3 and figure 6 given the comparison of various algorithm for Intrusion Detection

NO.OF ROUNDS	SNORT	NB- EM	AASDD	ANIDS	PROPOSE D
100	85.53	95.24	88.17	81.52	93.79
200	85.42	95.26	88.00	81.25	93.29
300	85.40	96.14	88.73	81.55	93.41
400	88.50	98.97	92.07	85.06	96.64
500	89.70	100.29	92.80	86.38	97.02

Table.3. Comparative analysis of Intrusion Detection

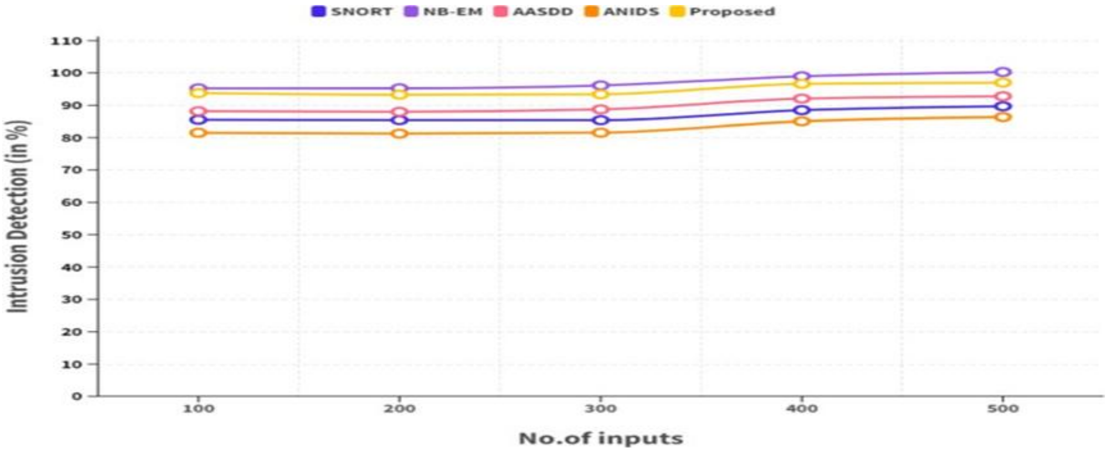

Fig.6: Comparison analysis of Intrusion Detection

They are essential for safeguarding cloud-based systems and data against various cyberattacks. However, the performance of NIDS in cloud environments can be influenced by multiple factors, such as the ever-changing nature of cloud systems, the distributed architecture of cloud networks, and the growing complexity of network traffic. A significant challenge for NIDS in cloud environments is the dynamic nature of cloud networks. In contrast to traditional on premise networks, where the network architecture and traffic patterns tend to remain stable, cloud networks are highly dynamic and constantly evolving. This makes it challenging for traditional NIDS to effectively detect and respond to network intrusions.

IV. **Monitoring authentication**

Network Intrusion Detection (NID) is essential for cybersecurity, as it helps detect and prevent malicious activities within a network. With the rapid growth of cloud computing, the need for robust and reliable NID systems has become even more critical. Cloud environments, characterized by large data volumes, dynamic network configurations, and multiple access points, are highly susceptible to cyber-attacks. Therefore, an efficient and responsive NID system is crucial for protecting the network. A significant challenge in cloud computing is the scalability and performance of NID systems. The unpredictable and constantly evolving nature of cloud network traffic can overwhelm traditional NID systems, making real-time detection difficult. This can result in delayed or missed alerts, thereby increasing the risk of successful cyber-attacks. Table 4 figure 7 given the comparison of various algorithm for Monitoring authentication.

NO. OF ROUNDS	SNORT	NB-EM	AASDD	ANIDS	Proposed
100	69.53	89.24	81.17	65.52	89.79
200	69.42	89.26	81.00	65.25	89.29
300	69.40	90.14	81.73	65.55	89.41
400	72.50	92.97	85.07	69.06	92.64
500	73.70	94.29	85.80	70.38	93.02

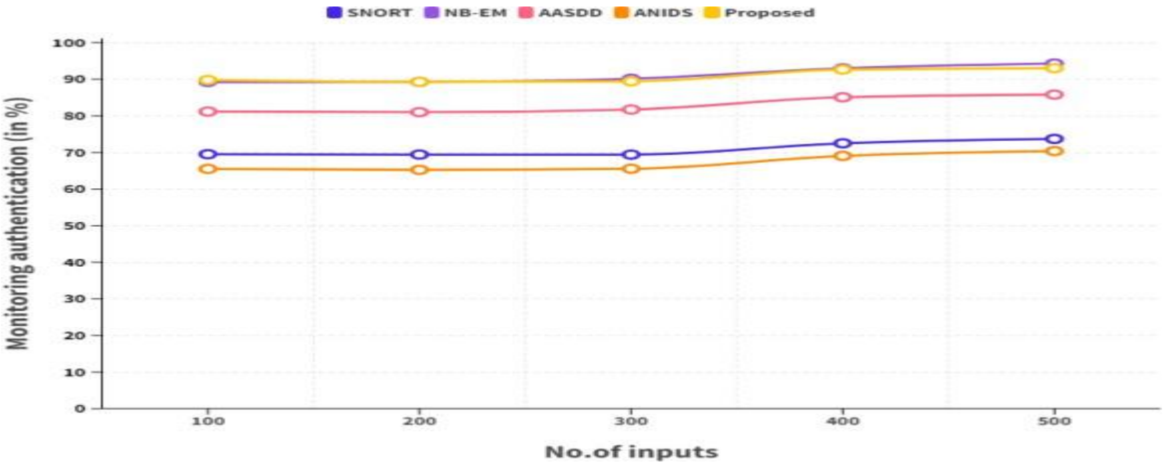

Fig.7: Comparison of authentication

With the advancement of cloud technologies, there have been notable improvements in the performance of NID systems within these environments. A key enhancement in NID performance for cloud computing is the integration of machine learning algorithms. These algorithms are capable of analyzing vast amount of network data to identify patterns of malicious activity, thereby improving detection accuracy and minimizing false positives.

CONCLUSION

In summary, network intrusion detection is a vital component of security in cloud computing environments. As organizations increasingly migrate their operations to the cloud, the risk of cyber-attacks and data breaches grows. Therefore, it is crucial for businesses to adopt robust network intrusion detection measures to safeguard their sensitive data and resources. A primary challenge in cloud-based intrusion detection is the dynamic and distributed structure of the cloud environment. Traditional network security methods may not be adequate in cloud environments, as they are tailored for on-premise networks and cannot manage the scale and complexity of cloud networks. As a result, it is essential to deploy specialized intrusion detection systems specifically for the cloud. Additionally, the integration of machine learning and artificial intelligence technologies has significantly improved the effectiveness of intrusion detection systems. This enables faster and more precise identification of suspicious activities, allowing organizations to respond promptly and mitigate the potential damage from malicious attacks. Additionally, it is crucial for businesses to regularly evaluate and update their network intrusion detection systems to stay ahead of rapidly evolving cyber threats. This involves staying informed about emerging attack methods and vulnerabilities and continuously refining detection algorithms to enhance their effectiveness.

CONFLICT OF INTEREST

The authors declare no conflict of interest

REFRENCES

[1] Javadpour, A., Pinto, P., Ja'fari, F., & Zhang, W. (2023). DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments. Cluster Computing, 26(1), 367-384.

[2] Gupta, K., Jiwani, N., & Afreen, N. (2023). A Combined Approach of Sentimental Analysis Using Machine Learning Techniques. Revue d'Intelligence Artificielle, 37(1).

[3] Sharif, M. H., Gupta, K., Mohammed, M. A., & Jiwani, N. (2022). Anomaly detection in time series using deep learning. International Journal of Engineering Applied Sciences and Technology, 7(6), 296-305.

[4] Lin, H., Xue, Q., Feng, J., & Bai, D. (2023). Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine. Digital Communications and Networks, 9(1), 111-124.Srilatha, D., & Thillaiarasu, N. (2023). Implementation of Intrusion detection and prevention with Deep Learning in Cloud Computing. Journal of Information Technology Management, 15(Special Issue), 1-18

[5] Srilatha, D., & Thillaiarasu, N. (2023). Implementation of Intrusion detection and prevention with Deep Learning in Cloud Computing. Journal of Information Technology Management, 15(Special Issue), 1-18.

[6] V. A. Rajan, T. Marimuthu, G. V. Londhe and J. Logeshwaran, "A Comprehensive analysis of Network Coding for Efficient Wireless Network Communication," 2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA), Imphal, India, 2023, pp. 204-210.

[7] Abd Elaziz, M., Al-qaness, M. A., Dahou, A., Ibrahim, R. A., & Abd El-Latif, A. A. (2023). Intrusion detection approach for cloud and IoT environments using deep learning and Capuchin Search Algorithm. Advances in Engineering Software, 176, 103402

[8] Jain, D. K., Ding, W., & Kotecha, K. (2023). Training fuzzy deep neural network with honey badger algorithm for intrusion detection in cloud environments. International Journal of Machine Learning and Cybernetics, 1-17

[9] Dixit, S., & Hussain, G. (2023). An effective intrusion detection system in a cloud computing environment. In Mobile Radio Communications and 5G Networks: Proceedings of Third MRCN 2022 (pp. 671-680). Singapore: Springer Nature Singapore

[10] Gupta, K., Jiwani, N., Sharif, M. H. U., Datta, R., & Afreen, N. (2022, November). A Neural Network Approach For Malware Classification. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 681- 684). IEEE

[11] Sangaiah, A. K., Javadpour, A., Ja'fari, F., Pinto, P., Zhang, W., & Balasubramanian, S. (2023). A hybrid heuristics artificial intelligence feature selection for intrusion detection classifiers in cloud of things. Cluster Computing, 26(1), 599-612

[12] 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), 1-13

[13] Vinolia, A., Kanya, N., & Rajavarman, V. N. (2023, January). Machine Learning and Deep Learning based Intrusion Detection in Cloud Environment: A Review. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 952-960). IEEE

[14] T. Marimuthu, V. A. Rajan, G. V. Londhe and J. Logeshwaran, "Deep Learning for Automated Lesion Detection in Mammography," 2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA), Imphal, India, 2023, pp. 383-388

[15] Dalal, S., Manoharan, P., Lilhore, U. K., Seth, B., Mohammed alsekait, D., Simaiya, S., ... & Raahemifar, K. (2023). Extremely boosted neural network for more accurate multi-stage Cyber attack prediction in cloud computing environment. Journal of Cloud Computing, 12(1), 14