Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches

Sina Ahmadi
National Coalition of Independent Scholars (NCIS), Seattle, WA, USA

***Abstract*—This research study comprehensively analyzes network intrusion detection in cloud environments by examining several approaches. These approaches have been explored and compared to determine the optimal and appropriate choice based on specific conditions. This research study employs a qualitative approach, specifically conducting a thematic literature analysis from 2020 to 2024. The research material has been exclusively obtained via Google Scholar. The traditional approaches identified in this research include anomaly-based and signature-based detection, along with innovative technologies and methods such as user behavior monitoring and machine learning. The findings of these studies demonstrate the effectiveness of conventional methods in known threat detection. They also struggle to identify novel attacks and understand the need for hybrid approaches that integrate the strengths of both. In this research study, the authors have addressed challenges such as privacy compliance, performance scalability, and false positives, highlighting the importance of continuous monitoring, privacy-preserving technologies, and real-time threat intelligence integration. This study also highlights the importance of stakeholder buy-in and staff training for the successful implementation of a network intrusion detection system (NIDS), especially when determining the evolving nature of cyber threats. This study concludes by defining a balanced approach combining new and old methodologies to offer an effective defense against diverse cyber threats in cloud environments. The future scope of NIDS in cloud environments has also been discussed, including enhancing privacy compliance capabilities and integrating AI-driven anomaly detection to meet emerging threats and regulatory requirements.**

Keywords*—*Cloud networking; cloud security; firewall; intrusion detection; NIDS

I. Introduction

In the changing landscape of cloud computing, the attraction of rapid development, scalability, and cost savings is undeniable. However, shared resources and a dynamic environment exacerbate the weaknesses of this system. Traditional security measures must avoid the ever-evolving attack landscape. Therefore, the robust and adaptable NIDS plays a vital role in the defense system, which protects critical infrastructure and sensitive data [1]. The article presents a detailed analysis of various customized NIDS approaches, especially for the cloud environment. The complexities of anomaly-based, signature-based, and behavior-based detection systems are carefully examined in an organized manner, analyzing their effectiveness in finding and reducing threats within the dynamic cloud environment. The primary objective of this analysis is to gain a comprehensive understanding of the merits and drawbacks of each approach by incorporating and utilizing the latest advancements in the field, as well as recent research and industry best practices.

This systematic and detailed examination provides a detailed overview of anomaly-based, signature-based, and behavior-based NIDS approaches in the cloud system. Furthermore, a comprehensive analysis is conducted to identify the strengths, weaknesses, and perfect cyber threat scenarios for every approach in a systematic manner. Furthermore, organizations carefully examine emerging trends and predict the potential future direction of threats in cloud systems. This article also aims to provide a practical direction for applying and optimizing this system within the cloud environment. By integrating our relative analysis with real-world case research and best practices, readers will acquire practical insights into implementing effective breach detection strategies customized to their cloud architecture and security needs. This article explores the concepts of scalability, resource optimization, and integration with existing security systems. This will aid individuals utilizing cloud services to stay protected from new threats and ensure the resilience of their systems in the face of evolving cyber risks.

II. Literature Review

A. Evaluating the Effectiveness of NIDS Approaches

Network intrusion detection systems have become very common in cloud environments. It is a detection system that is installed on a virtual switch. Additionally, NIDS primarily analyzes and monitors network traffic to detect unauthorized access or unusual activity. The effectiveness of such systems has been researched in prior studies [3]. According to the researchers, NIDS mainly works by detecting data packets for particular behaviors and patterns indicative of an attack. It can also identify and alert network administrations to attacks, including unauthorized access, viruses, and port scanning. Fig. 1 depicts a typical network intrusion detection system.

A prior study [4] shows that NIDS can effectively ensure cloud security. It helps prevent network attacks and detect vulnerabilities within the cloud, such as unsecured networks or outdated software. Another benefit is its ability to protect a company's essential data through its alert system. Real-time monitoring can also be done using NIDS, and security personnel can quickly respond to cloud attacks. Lastly, NIDS helps companies comply with network security regulations like GDPR or HIPAA. Fig. 2 shows the effectiveness of NIDS.

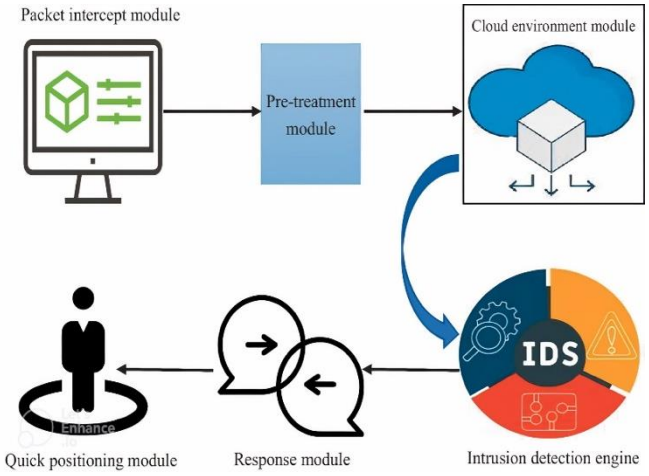

Fig. 1. Network intrusion detection system [2].

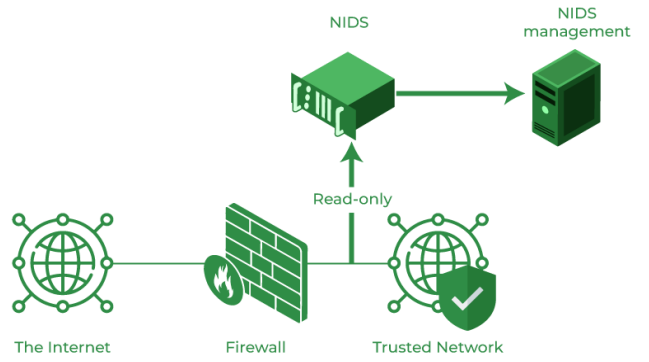

Fig. 2. Effectiveness of NIDS [5].

B. Implementing NIDS Solutions in Cloud Environments

Network intrusion detection system solutions can be implemented in cloud environments using different detection methods. For example, signature-based detection is a common technique in this regard. According to study [6], signature-based detection compares traffic passing throughout the network against attack patterns or already known signatures. These patterns are predefined and linked with different attacks. When the incoming traffic matches a pattern of attack, it is detected instantly, and an alert is sent to the network administrator. However, this method is effective only in the case of detecting known attacks.

Another method is centered on anomaly-based detection. This approach detects anomalous network traffic that deviates from the usual network behavior. An alert is sent to the network administrator when any activity is outside the expected range. This method is very beneficial in detecting known and unknown attacks. However, it can also give false positives. Hybrid detection is another method that combines anomaly-based and signature-based detection. According to a prior study [7], this approach uses both methods to detect the attacks and has high levels of accuracy.

C. Exploring Emerging Trends in Cloud-Native NIDS Technologies

Many new trends are emerging in intrusion detection in cloud environments. These trends are improving how companies approach cloud security. The most common trend is using artificial intelligence (AI) to enhance the capabilities of NIDS technologies. According to study [8], AI helps NIDS evaluate large network traffic data. This way, threats and attacks are detected more efficiently and accurately. Machine learning is also being used in this area to improve a company's NIDS and reduce the level of false positives.

Another trend is the use of microservice architectures and containerization in NIDS. They mainly help companies improve the security of their cloud-based environments. According to study [9], companies utilize advanced NIDS to match the current infrastructure when microservices and containers are used. Real-time detection of threats is carried out with the help of these techniques. Thus, mitigating risks is done more quickly while ensuring highly granular security controls for companies.

D. Integration Matters: Leveraging Cloud Platforms for Enhanced NIDS

Integrating a cloud environment with NIDS provides many advantages to a company's security system [10]. Cloud platforms mainly offer improved services and infrastructure that will enhance the abilities of traditional NIDS. The primary advantage is using cloud-based techniques and services to improve threat detection. In this case, advanced analytics enhance the accuracy of intrusion detection. These analytics can assist companies greatly in improving the effectiveness of their NIDS without using any updated hardware.

Cloud platforms also offer easy integration with different security systems. This provides the ease of implementing an improved security system in companies. According to study [11], the system improves if security information and event management (SIEM) is used in NIDS. It enhances its ability to detect attacks. The IT infrastructure of the company is also improved in this way. The use of third-party solutions and APIs also enhances network security. Companies can develop new strategies with the help of these solutions and improve their cloud-based NIDS.

E. Protecting Data and Meeting Regulations: Balancing Privacy and Compliance in Cloud-based NIDS

Complying with regulatory regulations is crucial when it comes to cloud-based NIDS. Companies need to ensure compliance with relevant regulations to overcome privacy issues. Cloud-based NIDS mainly analyzes and processes network traffic data, including private data. Thus, it is essential to use strong security measures for data protection. According to [12], different regulations, such as CCPA, HIPAA, and GDPR, can be implemented in this case. These regulations require companies to implement strong security practices to protect the cloud environment.

The use of data encryption and anonymization is also another robust approach. By anonymizing and encrypting an individual's personal information using solid passwords, companies can reduce the risk of external attacks. According

to [13], these encryption protocols can help a company manage its security measures while meeting regulatory requirements. The use of data handling procedures is also essential in this case. When a company uses cloud-based NIDS, it is necessary to understand how the traffic data is processed and stored. Gaining consent from users is also required in this case. These specific rules ensure the utmost protection of the data.

F. Future Directions and Challenges for NIDS in Cloud Environments

Various innovative methodologies are emerging in cloud computing and its associated NIDS. For example, the needs of companies are changing, and advanced technologies are being developed accordingly. According to study [14], one primary future direction is using machine learning and AI techniques in NIDS to improve its ability to detect threats. Since cybersecurity attacks are becoming very common these days, these technologies can help companies monitor their security systems in real time.

Furthermore, several challenges are linked to the use of advanced NIDS. According to study [15], the primary concern is to ensure the high levels of efficiency of the NIDS. This is due to the high volume of traffic in cloud systems, which poses challenges in their management. It is essential to ensure high-performance optimization and scalability levels to overcome the challenges of using NIDS. Thus, using advanced technologies and intelligent tactics can significantly help a company.

G. Identified Gaps

While the literature review thoroughly examines cloud-based NIDS techniques, there are several notable gaps worth addressing. First, a deeper analysis of the specific challenges and limitations of each NIDS approach would provide valuable insights into their practical implementation and effectiveness in real-world cloud environments, especially considering the ever-evolving nature of cyber threats. Additionally, the review lacks discussion on the potential impacts of emerging technologies, such as quantum computing, on the efficacy of NIDS systems. Understanding how these advancements may influence threat detection and mitigation strategies is crucial for ensuring the long-term security of cloud-based systems. Furthermore, there is a notable absence of emphasis on the socio-technical aspects of NIDS implementation, including user acceptance, organizational culture, and the human element in cybersecurity operations. Exploring these aspects would offer a more comprehensive understanding of the challenges and opportunities associated with deploying NIDS in cloud environments, ultimately informing more effective security strategies.

III. Problem Definition

In the unique landscape of cloud computing, the assimilation of NIDS creates complex challenges. Organizations encounter an intricate interplay of factors that affect the security of their sensitive data and infrastructure when they transition their systems to a cloud environment. Given the changing threats and technological advancements, the main problem lies in recognizing and applying practical NIDS approaches customized for cloud environments.

A. Complexity of Cloud Environments

Cloud networks show unquiet characteristics, including various network topologies, fluctuating workloads, and shared resources in study [16]. The traditional NIDS is designed for fixed on-site setups, which may need to be revised to adjust to the unique nature of the cloud system. As a result, this difference often leads to problems in an organization's ability to detect and address problems effectively. The constant changes in cloud setups make it difficult to use traditional NIDS. Thus, novel solutions that can adequately adjust to these changes are needed. In addition, the rapid growth and distribution of resources in cloud setups make it even harder for traditional NIDS systems to keep up. For instance, if organizations want to solve these challenges, they would need a revolution towards NIDS solutions that can smoothly combine with cloud systems while maintaining high detection efficiency and responsiveness.

B. Diverse Threat Landscape

The different threat systems present a significant challenge to the effectiveness of NIDS in cloud systems [17]. Cyber threats range from well-known attacks with a signature that is easily accessible to new and unknown viruses and attacks that constantly change their appearance, continuously evolving and posing further risks. Network intrusion detection systems detect known and unknown attacks while reducing false positives and negatives to zero. Maintaining this balance is essential to avoid consuming the security teams with false alarms while confirming that the main threats are solved. Thus, NIDS solutions customized for cloud environments must be quick and sophisticated, accurately differentiating between normal network activities and dangerous behavior to enhance overall threat detection capabilities and effectively reduce security risks. When comparing the performance of signature-based, anomaly-based, and hybrid detection methods (see Table I), it becomes evident that the hybrid approach demonstrates the highest true positive rate at 95%. This indicates its superior capability in accurately identifying intrusions while maintaining a low false positive rate, making it a promising option for enhancing network security.

Table I shows NIDS detection rates.

TABLE I. NIDS Detection Rates

Methodology	True Positive Rate (%)	False Positive Rate (%)
Signature-based	90	5
Anomaly-based	85	8
Hybrid Detection	95	3

C. Adaptability and Scalability

In cloud setups, it is essential for NIDS to have the capability to adapt and scale up [18]. These systems must handle different amounts of work and changes to how the network is set up. They should be able to identify and address security threats and adapt to the cloud setup changes, which is significant for keeping security strong without impeding

performance or causing problems. As the cloud system has changed significantly, NI and DS must adjust quickly and adequately to secure data. Moreover, the cost of a cloud setup is irrelevant.

D. Integration with Cloud-Native Technologies

Connecting the NIDS with cloud-native technologies is very important to identify and stop the challenges in cloud setups. This entails utilizing cloud-based APIs to enhance the capabilities of the NIDS in terms of monitoring and protecting network traffic. However, these tools can be complex to make NIDS perform effectively because each cloud platform performs differently. In addition, continuously monitoring network traffic in containers increases the challenges. To deal with these challenges, organizations must engage in proactive thinking over effective strategies and ensure the implementation of robust security measures. Connecting NIDS with cloud-native technologies is complex; however, it is also essential for ensuring security against online threats in cloud setups.

E. Privacy and Compliance

It is essential to ensure that the NIDS is good at identifying the challenges and problems in the system while following the rules correctly [19]. Additionally, NIDS needs to be able to monitor network traffic and identify threats without breaking the laws and regulations. This means using techniques to hide sensitive data while still identifying threats. It is essential to work according to the laws. Organizations must understand privacy laws and rules and set up robust NIDS systems to protect data privacy and network security. They can reduce risks and protect their network by focusing on data privacy and security. Privacy protection score can be determined using Eq. (1).

$$Privacy\ Protection\ Score = \frac{Data\ Encryption\ Level\ x\ Compliance\ Adherence}{Data\ Sensitivity} \quad (1)$$

IV. Methodology / Approach

A. Research Design

This study used qualitative research methodology to obtain positive and accurate outcomes and to explore and compare different approaches regarding network intrusion detection in cloud-based networks. Qualitative research methodology can be defined as a research methodology that integrates social sciences and other disciplines to understand and explore diverse perceptions, behaviors, and experiences of different people and groups. This approach helps understand the benefits and complexities of the NIDS methodologies in a cloud network. The objective of this study was to gain valuable insights into the research conducted by different authors using qualitative research methods to enable a comparative analysis of different NIDS approaches.

B. Research Setting and Participants

The research setting encompassed different cloud environments, such as hybrid, private, and public clouds. The included participants are researchers who conducted a study on network intrusion detection in cloud environments and the different approaches they used. All the researchers are highly qualified experts who have conducted in-depth research on this topic. The majority of participants consisted of IT professionals, cloud architects, and cybersecurity experts who possessed comprehensive knowledge about cloud environments, their complexities, and their benefits.

C. Data Collection

The study's data collection process began with a systematic search on Google Scholar, using keywords such as "network intrusion detection," "NIDS in cloud environments," and "cloud-based network security." These keywords were meticulously chosen to retrieve scholarly articles, reports, and publications pertinent to network NIDS within cloud environments. By employing this approach, the study aimed to capture a wide array of literature covering various aspects of NIDS methodologies within cloud networks. The selection of specific search terms and their variations ensured a thorough exploration of relevant research material, facilitating a comprehensive understanding of the topic. Through this systematic search strategy, the study aimed to gather diverse perspectives and insights to inform its analysis and conclusions effectively. This rigorous approach to data collection contributes to the study's credibility and enhances its potential to yield valuable insights into NIDS approaches in cloud environments.

D. Data Analysis

To conduct data analysis for this research study, thematic analysis was employed to analyze the qualitative data obtained from the literature review. The data was categorized systematically to identify relevant patterns, themes, and insights regarding emerging trends and challenges related to NIDS approaches within cloud networks. The key findings and data were explored regarding the comparative analysis of different NIDS methodologies in cloud environments. Moreover, thematic analysis played an integral role in identifying discrepancies and commonalities among the findings from the literature review. The analysis process was iterative, ensuring a comprehensive examination and enhancing the reliability and credibility of the study's conclusion. The thematic analysis of qualitative data obtained from the literature review on NIDS approaches within cloud networks bolstered a comprehensive explanation of the identified themes and their direct relevance to the study's aims. Each theme was carefully elucidated with detailed descriptions, supported by specific examples and evidence from the literature. By delving deeper into the nuances of each theme, the analysis aims to offer a nuanced understanding of the challenges, emerging trends, and best practices in NIDS methodologies within cloud environments. Furthermore, the relevance of each theme to the overarching research objectives was explicitly discussed, highlighting how insights derived from these themes contribute to addressing the research questions and advancing knowledge in the field of cloud security. This approach ensures that the analysis not only identifies key findings but also contextualizes them within the broader scope of the study, enhancing the overall quality and significance of the research.

E. Ethical Considerations

The ethical considerations in this research study during the literature review evaluation were centered on the use of academic materials and ethical sourcing. All papers selected from Google Scholar followed the ethical standards, which ensured the acknowledgment of the author's work and the appropriate citation. Biases and conflicts in the literature chosen were also accounted for and acknowledged in the analysis. Moreover, efforts were made to represent the selected research studies' findings accurately and maintain the integrity of this research.

V. Results and Discussion

A. Traditional Approaches Effectiveness

The traditional NIDS techniques, including signature-based and anomaly-based detection, have presented the changing effectiveness of cloud systems [20]. Signature-based detection, which is very efficient in detecting attacks, has faced limitations in finding zero-day threats due to its fixed nature. On the other hand, anomaly-based detection shows the promise to identify the contrasts from normal behavior but often suffers from high false positives, particularly in dynamic cloud environments. Hybrid detection approaches, which combine the advantages of both signature-based and anomaly-based methods, offer enhanced range and reduce false positives compared to conventional approaches. Studies have shown that the hybrid detection system can accomplish accurate favorable rates of almost 95% or higher while maintaining lower false positives, which makes it a practical choice for cloud system breach detection.

B. Challenges and Opportunities in Emerging Approaches

New techniques to detect cloud system breaches are emerging, like machine learning, tracking user behavior, and cloud-specific technologies. Machine learning, especially LSTM networks, has accurately spotted dangerous threats [21]. However, it takes time to understand how these methods work, and in certain situations, additional data is needed before they can be used. Monitoring user behavior can help in detecting anomalous activities performed by individuals within the system. Conversely, it is complex to set up since it needs a lot of user information. Although cloud-specific technologies use aspects of cloud systems to detect breaches, there is a need for enhanced regulations and mechanisms to govern access privileges. Combining the new methods can make the cloud system safer by identifying the recent changes in the system that may jeopardize the integrity of the data. Even though there are challenges, such as understanding how these methods work, new approaches to identifying breaches can help protect the cloud system from potential threats? Thus, it is imperative that we consistently research and enhance these methods to make them even better at safeguarding cloud systems.

C. Comparative Analysis of NIDS Approaches

Comparing old and new approaches to detecting violations shows which is good or bad. Traditional methods work effectively in dealing with known information; however, attacks can be missed nowadays, leading to sensitive data loss. New techniques, such as using intelligent algorithms or observing user behavior, can detect more types of attacks. However, these procedures require meticulous setup and necessitate assistance in comprehending user perspectives and safeguarding data confidentiality [22]. Combining old and new methods can create a favorable balance that detects more threats while minimizing errors. It is also important to consider the dynamic nature of threats and evaluate the effectiveness of the measures in ensuring data security. Traditional approaches might require increased speed to detect emerging attacks; however, innovative methods can adapt and evolve in response to evolving threats. Combining old and new methods strengthens organizations against different cyber threats. Organizations can use the latest technology to stay ahead and keep their data and systems safe from threats.

D. Adapting to an Evolving Threat Landscape

In the context of evolving threats, NIDS must understand the importance of adaptability to changing tactics and emerging attack vectors. Cyber threats are evolving; thus, their complexity also keeps growing, making it imperative for NIDS to stay proactive and vigilant when identifying and mitigating potential risks. Moreover, it is necessary to continuously monitor emerging threats and update the threat intelligence feeds and configurations of NIDS. This is the best way to develop innovative attack methods and vulnerabilities. The effectiveness and agility of NIDS in cloud-based networks can be enhanced by implementing automated systems and integrating real-time threat intelligence for instant threat detection and response.

E. Addressing False Positives

As cloud environments advance, it is essential to minimize false positives to maintain effective intrusion detection [23]. False alarms can easily be mitigated by using SIEM solutions, integrating real-time threat intelligence feeds, and using NIDS parameters. Threat intelligence and detection thresholds are essential in filtering out known benign activities, helping organizations reduce the impact of false positives on organizational operations. Therefore, organizations can focus on ongoing monitoring and analysis of false positive incidents to extract valuable insights and refine NIDS configurations. It is also helpful in improving the overall detection accuracy.

F. Ensuring Performance and Scalability

Suppose an organization wants a high level of performance and scalability in cloud-based networks. In that case, it needs to optimize NIDS configurations and focus on using distributed detection architectures. Organizations can also distribute detection workloads in multiple instances or nodes to efficiently manage workloads without affecting detection efficacy at any cost. Thus, integrating cloud-based technologies and optimizing detection algorithms can enhance the scalability and performance of network intrusion detection strategies.

In addition, the performance of NIDS in cloud environments can be enhanced by focusing on resource allocation and effective capacity planning. Performance bottlenecks may arise from fulfilling future workload demands and concentrating on the overall growth of these strategies. Thus, performance and scalability can be enhanced by

implementing auto-scaling mechanisms based on predefined thresholds to adjust resource allocation due to workload patterns and network traffic changes. Undoubtedly, performance testing is crucial for obtaining valuable insights regarding the effectiveness of NIDS configurations and identifying areas for optimization. Table II details resource allocation in various cloud services and their costs, aiding organizations in understanding usage patterns and budgeting. For instance, $50 for 1000 GB storage shows storage needs, $100 for 500 GB computing reflects computational demands, and $20 for 100 GB network bandwidth stresses connectivity significance.

TABLE II. RESOURCE ALLOCATION

Cloud Service	Resource Allocation (GB)	Cost ($)
Storage	1000	50
Computing	500	100
Network Bandwidth	100	20

G. Privacy and Compliance Considerations

Regulatory compliance standards and data privacy are paramount in cloud-based intrusion detection [24]. In this case, the primary anonymization techniques, such as tokenization and encryption, help protect the sensitive information of organizations and their associated users. Thus, these techniques effectively aid in detecting intrusion. It is also necessary for organizations to ensure compliance with regulations such as PCI DSS, HIPAA, and GDPR, which implement strict data security and privacy requirements. Identity and access management (IAM) systems are implemented to enhance data privacy and limit access to organizational data by granting permissions to specific and authorized users only. Moreover, employees must be educated regarding data privacy policies and regulations, and security awareness practices must be promoted to handle sensitive information. Regular audits must be conducted to ensure ongoing compliance with regulatory requirements. Table III outlines compliance costs for GDPR, HIPAA, and PCI DSS, emphasizing the financial commitment required for regulatory adherence. For instance, $10,000 for GDPR signifies investments in data protection, $15,000 for HIPAA reflects patient information security, and $12,000 for PCI DSS highlights payment data protection expenditures, aiding resource allocation and compliance prioritization.

TABLE III. COMPLIANCE COSTS

Regulation	Compliance Cost ($)
GDPR	10,000
HIPAA	15,000
PCI DSS	12,000

H. Hybrid Approach Advantages

A hybrid approach combines both traditional and innovative NIDS methodologies, enabling it to combine the advantages of both methods for intrusion detection in cloud environments [25]. By combining anomaly-based and signature-based detection strengths, hybrid systems can achieve higher detection accuracy while minimizing false positives. Additionally, integrating adaptive and self-learning hybrid systems with machine learning and AI technologies results in enhanced accuracy and efficiency that can be improved over time. The hybrid approaches have several advantages, such as flexibility and scalability, allowing them to adjust their intrusion detection systems to meet the specific cloud environment. This ability will enable organizations to adjust detection strategies based on workload demands and emerging threats. Eq. (2) can help in calculating detection accuracy.

$$\frac{True\ Positives+True\ Negatives}{True\ Positives+True\ Negatives+False\ Positives+False\ Negatives}\ x\ 100\% \quad (2)$$

I. Organizational Implementation Challenges

The implementation of NIDS in a cloud system can result in several challenges [26]. Organizations must overcome these challenges to deploy and manage NIDS successfully. The biggest challenges are the complications of cloud architecture and the varied range of available platforms and services. Careful management and planning are required for NIDS's compatible and active implementation in multiple cloud environments. Organizations also face resource allocation challenges, including allocating storage spaces for the placement of NIDS without affecting the system and adequate allocation of computing resources. Additionally, the implementation and management of NIDS are greatly influenced by factors such as staff training and skill development. Thus, it is beneficial for organizations to invest in training programs, considering the constantly changing nature of cyber threats and the difficulty of NIDS technologies. It will help organizations ensure that the workers have the skills to accurately monitor, configure, and respond to any security incident. Getting stakeholder buy-in and support is essential to overcome the resistance hindering progress and ensure the proper implementation of NIDS. Collaboration and alignment of aims can be boosted during the implementation process by reaching stakeholders from different levels and departments within the organization.

VI. CONCLUSION

Cloud computing is the most used system nowadays; however, data security in cloud computing is one of the most critical concerns. The rising reliance of organizations on cloud environments for communication, storage, and data computation has led to a growing demand for a robust security system such as NIDS. The main focus of this article is to examine NIDS mechanisms explicitly created for security in a cloud environment. In a time where cloud computing offers scalability, cost-effectiveness, and agility, the shared responsibility model focuses on providing active steps to secure data from breaches. In the constantly changing cloud architecture, old-style security models must be more robust to tackle security threats. For this reason, it has become essential to use anomaly-based, signature-based, and emerging behavior-based threat detection systems, as they help organizations boost their data security in the cloud. Considering information from recent studies, the article seeks to equip stakeholders with a concise overview of limitations,

strengths, and future predictions about different NIDS methodologies. Organizations can quickly detect the difficulties in cloud security with the help of this comparative analysis. The findings of this study will also help them boost strong defenses in this constantly changing threat landscape. Moreover, technologies are evolving continuously, necessitating a corresponding adaptation in strategies to protect data confidentiality.

VII. Future Scope

The future scope of NIDS in cloud environments includes the potential for further innovations and advancements to address emerging challenges quickly and effectively. A significant future development is using machine learning and AI in NIDS frameworks. With these technologies, the abilities of NIDS can be enhanced to detect and respond to different types of threats in real-time, which, in turn, improves the network's overall security. Furthermore, AI-driven anomaly detection mechanisms can be integrated into the future to enhance organizations' visibility into their cloud networks. The future of NIDS in cloud environments also includes exploring innovative approaches to enhance compliance and privacy capabilities. As technology evolves, the associated threats also increase, necessitating an increase in NIDS solutions. For this purpose, privacy-preserving technologies like homomorphic encryption can be incorporated by organizations in the future. The future scope of NIDS also includes exploring advanced threat intelligence integration and collaboration mechanisms. Moreover, NIDS can access various threat intelligence sources by building solid relationships and information-sharing initiatives with industry fellows, cybersecurity organizations, and government agencies.

Additionally, advancements in cloud computing infrastructure and networking technologies offer opportunities for NIDS to evolve further. The integration of software-defined networking (SDN) and network functions virtualization (NFV) can enable more agile and dynamic intrusion detection mechanisms. However, the adoption of edge computing and fog computing paradigms presents new challenges and possibilities for NIDS deployment and management at the network edge. Thus, by leveraging these emerging technologies, NIDS can adapt to the changing landscape of cloud environments, providing enhanced security and resilience against evolving cyber threats. Future research and development in these areas promises to shape the future of NIDS in safeguarding cloud-based systems.

References

[1] M. A. Hossain and M. S. Islam, "Ensuring network security with a robust intrusion detection system using ensemble-based machine learning," Array, p. 100306, 2023.

[2] X. Wang, "Fast Localization Model of Network Intrusion Detection System for Enterprises Using Cloud Computing Environment," 2 August 2023. [Online]. Available: https://link.springer.com/article/10.1007/s11036-023-02176-w.

[3] S. Krishnaveni, S. Sivamohan, S. S. Sridhar and S. Prabakaran, "Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing," Cluster Computing, pp. 1761-1779, 2021.

[4] M. Khan and M. Haroon, "Detecting Network Intrusion in Cloud Environment Through Ensemble Learning and Feature Selection Approach," SN Computer Science, p. 84, 2023.

[5] GeeksforGeeks, "Intrusion Detection System (IDS)," 6 December 2023. [Online]. Available: https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

[6] T. Zaidi, "A Network Intrusion Based Detection System for Cloud Computing Environment," 2021.

[7] A. Sharon, P. Mohanraj, T. E. Abraham, B. Sundan and A. Thangasamy, "An intelligent intrusion detection system using hybrid deep learning approaches in cloud environment," International Conference on Computer, Communication, and Signal Processing, pp. 281-298, 2022.

[8] A. K. Sangaiah, A. Javadpour, F. Ja'fari, P. Pinto, W. Zhang and S. Balasubramanian, "A hybrid heuristics artificial intelligence feature selection for intrusion detection classifiers in cloud of things," Cluster Computing, pp. 599-612, 2023.

[9] J. Flora, "Improving the security of microservice systems by detecting and tolerating intrusions," IEEE International Symposium on Software Reliability Engineering Workshops , pp. 131-134, 2020.

[10] J. C. S. Sicato, S. K. Singh, S. Rathore and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," Journal of Information Processing Systems, pp. 975-990, 2020.

[11] G. González-Granadillo, S. González-Zarzosa and R. Diaz, "Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures," Sensors, p. 4759, 2021.

[12] L. R. Dubs, "Cloud Computing: Security and Privacy Challenges," Doctoral Dissertation, 2020.

[13] J. V. Bibal Benifa and G. Venifa Mini, "Privacy based data publishing model for cloud computing environment," Wireless Personal Communications, pp. 2215-2241, 2020.

[14] M. P. Bharati and S. Tamane, "NIDS-network intrusion detection system based on deep and machine learning frameworks with CICIDS2018 using cloud computing," International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), pp. 27-30, 2020.

[15] H. M. El Masry, A. E. Khedr and H. M. Abdul-Kader, "Challenges and opportunities for intrusion detection system in cloud computing environment," Journal of Theoretical and Applied Information Technology, pp. 3112-3129, 2020.

[16] S. S. Chauhan, E. S. Pilli, R. C. Joshi, G. Singh and M. C. Govil, "Brokering in interconnected cloud computing environments: A survey," Journal of Parallel and Distributed Computing, pp. 193-209, 2019.

[17] M. Ozkan-Okay, R. Samet, Ö. Aslan and D. Gupta, "A comprehensive systematic literature review on intrusion detection systems," IEEE Access, pp. 157727-157760, 2021.

[18] H. Attou, M. Mohy-eddine, A. Guezzaz, S. Benkirane, M. Azrour, A. Alabdultif and N. Almusallam, "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing," Applied Sciences, p. 9588, 2023.

[19] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, pp. 1-22, 2019.

[20] S. Lata and D. Singh, "Intrusion detection system in cloud environment: Literature survey & future research directions," International Journal of Information Management Data Insights, p. 100134, 2022.

[21] I. Shingari, "Critical analysis of genetic algorithm based IDS and an approach for detecting intrusion in MANET using data mining techniques," January 2012. [Online]. Available: https://www.researchgate.net/figure/An-example-of-a-traditional-Intrusion-Detection-System_fig1_272719886.

[22] S. M. S. Bukhari, M. H. Zafar, M. Abou Houran, S. K. R. Moosavi, M. Mansoor, M. Muaaz and F. Sanfilippo, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," Ad Hoc Networks, p. 103407, 2024.

[23] Z. Liu, B. Xu, B. Cheng, X. Hu and M. Darbandi, "Intrusion detection systems in the cloud computing: A comprehensive and deep literature

review," Concurrency and Computation: Practice and Experience, p. 6646, 2022.

[24] P. Lalitha, R. Yamaganti and D. Rohita, "Investigation into security challenges and approaches in cloud computing," Journal of Engineering Sciences, 2023.

[25] K. Samunnisa, G. S. V. Kumar and K. Madhavi, "Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods," Measurement: Sensors, p. 100612, 2023.

[26] T. Nathiya and G. Suseendran, "An effective hybrid intrusion detection system for use in security monitoring in the virtual network layer of cloud computing technology," Data Management, Analytics and Innovation: Proceedings of ICDMAI 2018, pp. 483-497, 2019.