Journal of Soft Computing Paradigm (ISSN: 2582-2640)
www.irojournals.com/jscp/

A Review of Deep Learning Techniques for Intrusion Detection in Cloud Computing

Duraipandian M.

Professor & Head, Department of Information Technology, Hindusthan Institute of Technology Coimbatore, India.

E-mail: durainithi@gmail.com.

Abstract

The rapid expansion of cloud has computing caused numerous security problems, particularly in distributed designs and resource expansion steps. This situation has led to the development of advanced threat detection mechanisms that exceed the standard signature-based systems. The implementation of these new technologies into security operations is complicated by a number of issues, including limited communication. The effective use of dynamic situations presents additional challenges including concept drift, scalability problems, and real-time delays. This review paper highlights the importance of deep learning for improving cloud security, particularly in intrusion detection systems, which are key components of smart cloud security. This study discusses the deep learning techniques currently in use for cloud intrusion detection, analyses new research topics, and focuses on the continuous limitations in the field. These reviewed techniques will improve the accuracy of protecting cloud computing systems from evolving cyber threats.

Keywords: Deep Learning, Cloud Security, Intrusion Detection Systems, Cyber Threats.

1. Introduction

Cloud platforms have developed into the industry standard for providing scalable, on-demand computing services across several application areas. Because of their extensive industry support, companies may deploy apps worldwide without experiencing infrastructure expenditures, thereby accelerating digital transformation. However, cloud computing has different features like multi-tenancy, virtualization, elastic scalability, and distributed architectures, which also present significant security risks. Cloud computing platforms are

DOI: https://doi.org/10.36548/jscp.2025.4.003
Received: 10.11.2025, received in revised form: 08.12.2025, accepted: 23.12.2025, published: 02.01.2026

exposed to advanced cyberattacks because they are more dynamic and complex. Figure 1 illustrates the schematic representation of Intrusion Detection Systems (IDS). Cloud security includes several layers, including access control, encryption, firewalling, and identity management. Intrusion detection has received priority in this research because it can offer continuous, real-time monitoring of cloud workloads and network traffic.

Intrusion detection systems can identify both known and unknown risks during runtime, as security methods that depend on static setups or predefined rules are particularly important for dynamic, multi-tenant cloud environments. Intrusion detection systems (IDS) serve as a protective layer capable of detecting threats and avoid normal security measures as cloud services continually face zero-day attacks, insider threats, and advanced multi-stage intrusions. IDS services will provide distributed deployment, automated threat intelligence integration, and interoperability for companies utilizing multi-cloud and hybrid cloud architectures.

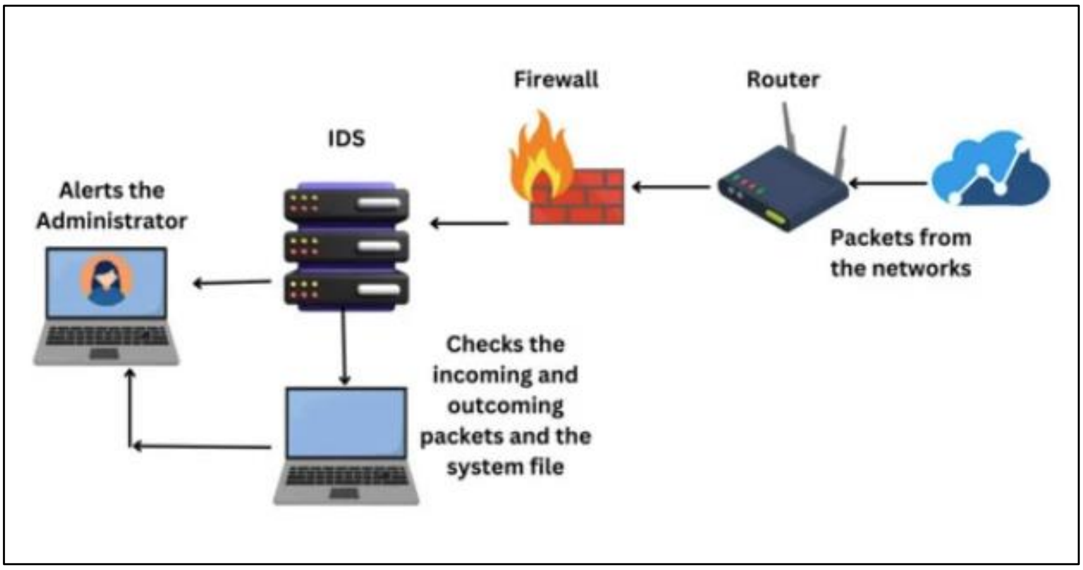
Firewall
Router
IDS
Alerts the Administrator
Packets from the networks
Checks the incoming and outcoming packets and the system file

Figure 1. Schematic Representation of Intrusion Detection System (IDS) [26]

An essential component of cloud security is the intrusion detection system (IDS). IDS is used in cloud systems to detect malicious activities, abnormal behaviour, and restrict unauthorized access. Large-scale workloads, encrypted traffic patterns, zero-day attacks and rapidly changing risks cannot be detected by standard IDS approaches like signature-based and rule-based detection. The need for an automated, intelligent, and flexible IDS that can handle high-dimensional, real-time cloud data will be the primary focus of these limitations [1], [6], [21]. Deep Learning (DL) has been a revolutionary technique in the field of cloud security in recent years. When compared to traditional machine learning methods, Deep Learning models are able to automatically uncover significant patterns from unprocessed data, discover hidden connections, and efficiently generalize across a variety of attack types. Architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, autoencoders, and hybrid deep learning frameworks have achieved advanced performance in identifying network intrusions, DDoS attacks, insider threats, and unusual cloud behavior. Their ability to manage huge quantities of cloud traffic and understand complicated temporal-spatial characteristics is suitable for modern cloud IDS [2], [7], [8].

Despite extensive research on deep learning based intrusion detection, existing studies predominantly focus on model accuracy using isolated datasets, with limited attention to deployment feasibility in real-world cloud environments. There is a lack of comprehensive reviews that critically analyze deep learning models from a cloud-centric perspective, considering scalability, latency, resource consumption, and operational constraints. This study reviews and analyzes deep learning methods for cloud intrusion detection, focusing on deployment-related issues and effectiveness [4], [21].

Objectives

1. Provide an overview of cloud security challenges in intrusion detection.
2. Analyze the deep learning techniques applied to cloud IDS.
3. Summarize existing research trends and models.
4. Identify the key limitations and research gaps.
5. Discuss the future research directions for building scalable, robust, and cloud-native IDS solutions.

This work improves the understanding of how deep learning may enhance cloud security and allows for intelligent, flexible, and dependable intrusion detection systems through an analysis of both practical limitations and technological developments.

2. Literature Review

The research on cloud security with intrusion detection is one of the most studied topics in recent years. Rule-based monitoring and signature-based detection are earlier approaches focused on security techniques that demonstrate high accuracy for known attacks but are unable to detect changing threat patterns and zero-day attacks. Researchers are implementing machine learning methods into cloud-based intrusion detection systems (IDS) to overcome these limitations by creating examples of intelligent security systems. System logs and network traffic are analyzed using a machine learning-based model. Support Vector Machines (SVM), Random Forests (RF), Decision Trees (DT), and clustering algorithms are some of the classifiers utilized by the IDS. The research [1] shows that the ML-based IDS performs better than traditional methods in terms of detection accuracy when it involves anomaly detection in cloud networks. However, these approaches require a significant amount of human feature engineering due to problems with scalability, high-dimensional data, and complex attack patterns.

Deep learning models avoid the requirement for manual features by automatically learning hierarchical representations from raw data. [2] The increase in deep learning adoption for cloud security after 2020 is highlighted, with intrusion detection identified as the dominant application domain. This trend shows the increasing demand for adaptive, real-time, and high-accuracy IDS solutions in dynamic cloud environments. CNNs have been widely adopted for analyzing cloud network traffic due to their ability to capture spatial patterns. The research [8] proposed a CNN-based IDS that achieved superior detection values for both known and zero-day attacks compared to traditional ML classifiers. Similarly, [11] utilized deep CNN models for cloud traffic classification and attack detection, demonstrating improved network performance and reduced false-positive rates. These studies illustrate the effectiveness of CNNs in recognizing complex traffic signatures in cloud infrastructures [15].

The paper [7] surveyed RNN and LSTM-based IDS systems that highlight their ability to model dependencies and predict intrusions proactively. Their results suggest that sequence-aware deep learning models are effective for detecting low, unknown attacks. These unsupervised models learn representations of normal traffic behavior and flag deviations as potential intrusions. The research [4] demonstrated that combining deep autoencoders with data mining techniques reduces false positives while improving detection accuracy. These methods are useful when there is a lack of or insufficient labeled attack data.

Recent research has investigated hybrid and integrated security systems in standalone IDS models. [19] A deep neural network-based intrusion prevention and detection system that can independently reduce threats was proposed to support self-healing cloud infrastructures. Other researchers have combined deep learning with blockchain, cryptographic techniques, and software-defined networking (SDN) to improve trust, durability, and decentralized security management in cloud environments [21]. This literature demonstrates the evolution of unsolved issues. The majority of research utilizes fake or outdated datasets that limit their practical application. Implementing deep learning-based intrusion detection systems (IDSs) in operational security situations is challenging due to their vulnerability to adversarial attacks and frequent lack of interpretability. Additionally, there are still unresolved research issues with concept drift adaptability and scalability across multi-cloud infrastructures [16].

Recent studies have demonstrated that deep learning will improve cloud system intrusion detection. However, for cloud-native IDS systems, additional research on dependability, explainability, scalability, and continuous learning is needed to transform the model from experiments to an adaptable system.

Table 1. Research Gaps

References	Research Focus	Models used	Major Contributions and Findings	Identified Gap
[1]	Machine learning–based cloud security	SVM, RF, Clustering	Demonstrated superior detection accuracy compared to traditional IDS approaches; highlighted an emerging transition toward deep learning–based security mechanisms.	Limited capability to detect complex and zero-day attacks; lacks scalability and adaptability required for dynamic cloud environments.
[2]	Deep learning trends in cloud security	Bibliometric and systematic literature analysis	Identified intrusion detection systems as the most actively researched application of deep learning in cloud security domains.	Provides trend analysis only; does not evaluate model performance, deployment feasibility, or real-time cloud applicability.
[7]	Survey of deep learning–based IDS	CNN, RNN, LSTM, Autoencoders	Highlighted the importance of proactive intrusion detection and temporal feature learning for enhanced cloud security.	Lacks comparative evaluation of models in real cloud environments and does not address deployment challenges such as scalability or latency.

[8]	Intrusion detection in cloud environments	CNN–based IDS	Achieved high detection accuracy, particularly for zero-day attacks, demonstrating the robustness of CNN-based models.	Limited focus on temporal dependencies and high computational cost restricts real-time deployment in large-scale clouds.
[11]	Network traffic classification	Deep CNN	Reduced false positive rates and improved overall network efficiency through effective traffic classification.	Evaluated mainly on standard datasets; lacks validation under real-time cloud traffic and multi-tenant scenarios.
[4]	Anomaly detection in cloud systems	Deep Autoencoders	Enhanced detection accuracy while significantly reducing false alarm rates compared to conventional methods.	Sensitive to threshold tuning and concept drift; limited explainability affects operational trust in cloud IDS.
[19]	Intrusion detection and prevention systems	Deep Neural Network (DNN)	Proposed a self-healing cloud security architecture capable of automated threat detection and response.	Requires large labelled datasets and lacks evaluation against evolving attack patterns in dynamic cloud workloads.
[21]	Cloud-based intrusion detection systems	Machine learning classifiers	Analysed the advantages and limitations of ML-based IDS, highlighting scalability and performance trade-offs.	Does not address deep learning–based solutions or cloud-native challenges such as elasticity, virtualization, and distributed traffic.

3. Role of Deep Learning in Intrusion Detection Systems

3.1 Introduction to Intrusion Detection Systems

Intrusion detection systems (IDS) are important for cybersecurity to detect malicious activity or violations by monitoring network traffic, system operations, and user behavior. Numerous users share resources, virtual machines, and services in cloud settings. IDS protect against cyber attacks and unauthorized access. Compared to traditional systems like static physical infrastructures, cloud systems are dynamic and flexible, creating a significantly larger attack surface that complicates threat detection. Conventional intrusion detection systems depend on strict protocols or predefined signatures to effectively detect known threats. However, new zero-day and adaptive attack techniques pose challenges for these systems. Furthermore, traditional IDS are unable to handle the massive amount, speed, and variability of data generated in cloud environments. This highlights the importance of sophisticated detection systems that utilize effective algorithms to identify complex patterns and adapt to changes in the tech ecosystem of security risks. Deep learning technologies are now recognized for improving detection through learning and increased flexibility for new and diverse cyber threats. [3], [5], [10].

3.2 Types of Intrusion Detection Systems

3.2.1 Signature-Based IDS

Signature-based intrusion detection systems (IDS) are able to detect intrusions when comparing system activity or network traffic to a predefined database of known attacks. These signatures represent characteristics associated with known vulnerabilities, harmful command patterns, malware payloads, and other previously identified risks. Signature-based intrusion detection systems (IDS) are dependable for recognized threat scenarios because of their predictable design that provides high detection accuracy for known assaults and maintains low false-positive rates.

3.2.2 Anomaly-Based IDS

When trying to detect possible intrusions, intrusion detection systems (IDS) create a model of regular system or network behaviour based on anomalies. These systems are highly effective at identifying insider threats, unknown attacks, and highly complex strategies of attack that differ from recognized signatures. In cloud environments, anomaly-based IDS are valuable due to their ability to adapt to diverse workloads and heterogeneous traffic patterns.

3.2.3 Hybrid IDS

The advantages of both signature-based and anomaly-based methods are combined in hybrid intrusion detection systems (IDS) to provide an improved structure. Hybrid intrusion detection systems (IDS) use behavioral analysis and signature analysis to provide high detection accuracy for known attacks while maintaining the capacity to detect unusual and zero-day threats. The adaptability of the system is increased and false positives are decreased using this double layer detection technique.

4. Technologies Enabling Deep Learning-Based IDS

4.1 Cloud Computing Technologies

IDS implementation is made possible by cloud computing technologies like virtualization, containerization, and Software-Defined Networking (SDN). IDS components are dynamically distributed between hosts without affecting cloud services because virtualization allows multiple machines to share physical resources. Microservice-based security modules can be created or relocated based on workload needs, containerization technologies like Docker and Kubernetes significantly improve IDS portability and scalability by providing lightweight solutions.

4.2 Big Data and Streaming Platforms

Large amounts of heterogeneous data such as network traffic, system logs, application logs, and user activity records are produced by cloud infrastructures. Effective intrusion detection requires real-time processing of such high-velocity and high-volume data streams. Large-scale IDS installations are supported by distributed data access, storage, and processing capabilities provided by big data and streaming systems like Apache Kafka, Apache Spark, and Apache Flink.

4.3 GPU and Accelerator Hardware

Intrusion detection deep learning models are computationally complex, when managing high-dimensional cloud data during training in real time. Graphics processing units (GPUs) and specialized accelerators like Tensor Processing Units (TPUs) significantly speed up deep learning workloads by enabling the simultaneous execution of complex neural network operations.

4.4 Cloud Security Datasets

High-quality datasets are required for intrusion detection models to be trained, assessed, and measured. Publicly accessible databases like NSL-KDD, CICIDS, and UNSW-NB15 are frequently used in IDS research because of their availability and labelled attack scenarios. These datasets offer normal metrics for comparative analysis of advanced deep learning-based intrusion detection [23], [24].

5. Trends in Cloud Security Growth

The evolution of cloud security has seen significant developments from 2022 to 2032, with the global market expanding from approximately USD 20.5 billion to a projected USD 148.3 billion, reflecting a compound annual growth rate (CAGR) of 22.5%. This growth underscores the importance of protecting cloud infrastructures against highly advanced cyber threats. Initially, security investments concentrated on Identity and Access Management (IAM) and Data Loss Prevention (DLP), with IAM maintaining its dominant status due to its crucial role in authentication and user identity control, as shown in Fig. 2. As cyber threats evolved, there was a shift toward Security Information and Event Management (SIEM) systems, with a focus on real-time threat detection and response capabilities. The rise of SIEM correlates with the growing use of Intrusion Detection Systems (IDS), which operate as intelligent elements of SIEM environments. These systems enable continuous monitoring, and rapid response to security incidents is essential in handling the complexities of modern cloud data.

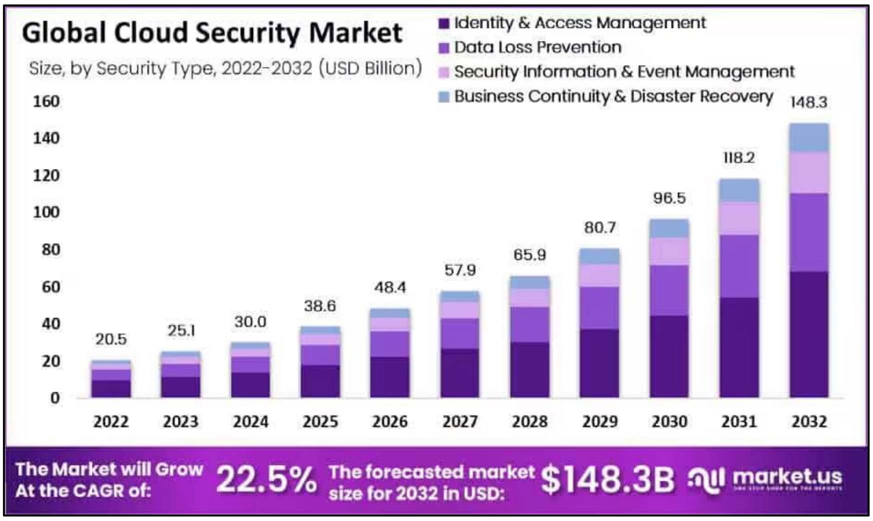

Figure 2. Global Cloud Security Market Growth (2022–2032) by Security Type [27]

The introduction of deep learning into IDS has further improved detection capabilities, as these systems can adapt to new and highly advanced attack patterns. This technological advancement includes models like CNNs for traffic analysis and LSTM networks for sequential log monitoring. Such innovations are fundamental in reducing false positives and improving response times. Moreover, the evolving nature of cloud workloads requires the development of comprehensive security strategies. A larger pattern toward resilience appears in the increasing value of Business Continuity and Disaster Recovery (BCDR) highlighting the importance of rapid recovery and system availability after errors. In the end, the transition from basic security measures to intelligent, integrated security frameworks shows that proactive intrusion detection is now at the core of modern cloud security, improving the overall security posture of cloud infrastructures [22], [24].

Table 2. Comparative Analysis of Deep Learning Models for Cloud IDS

Model	**Strengths**	**Limitations**	**Suitable Attack Scenarios**
CNN [7], [8], [11]	Effective spatial feature extraction; high accuracy for traffic-based attacks	Limited temporal awareness; high computation cost	DDoS, scanning, brute-force
RNN / LSTM [7], [19]	Captures sequential and temporal patterns	Slow training; vanishing gradient (RNN)	Insider threats, slow attacks
Autoencoder [7], [4]	Unsupervised anomaly detection; detects zero-day attacks	High false positives; difficult threshold tuning	Unknown and novel attacks
DNN [19]	Simple architecture; good classification performance	Requires labelled data; less adaptive	Known attack patterns
Hybrid (CNN–LSTM) [7], [11]	Combines spatial and temporal features; high detection accuracy	Complex architecture; high resource usage	Advanced persistent threats
Federated DL [21]	Privacy-preserving; cross-cloud collaboration	Communication overhead; slower convergence	Multi-cloud IDS

In Table 2, a comparative analysis reveals that no single deep learning model is optimal for all cloud intrusion detection scenarios. CNN-based models perform well for network traffic analysis, whereas LSTM-based architectures are more suitable for sequential log and behaviour-based detection. Autoencoders are effective for identifying unknown attacks, but often generate higher false positives. Hybrid models achieve superior detection accuracy by combining complementary features, although at the cost of increased computational complexity. Federated deep learning models address privacy and data-sharing challenges but introduce communication and convergence overheads. These trade-offs highlight the importance of model selection based on deployment constraints and threat characteristics.

6. Discussion On Deep Learning–Based Intrusion Detection in Cloud Computing

This paper highlights the importance of deep learning in improving cloud security through intrusion detection systems (IDS). It illustrates the lack of standard security methods to manage the development of effective defenses against cyber threats and the increasing rise of cloud security-based companies. The review explains the transition from static, rule-based intrusion detection methods to smart, adaptive deep learning-based systems that are essential for monitoring real-time cloud traffic and identifying their abnormalities. Deep learning models such as CNN, LSTM, and autoencoders improve standard machine learning algorithms in intrusion detection methods, providing high accuracy and flexibility by reducing the dependency on manual feature extraction methods. Still, problems exist; most IDS models remain experimental and lack performance generalization due to evaluations on old or fake datasets, leading to a major gap between research and practical application in operational settings. [7], [8], [11].

6.1 Model-Level and Methodological Limitations

This section explains the basic limitations of deep learning-based intrusion detection models, including algorithmic design and learning methods. Deep learning-based intrusion detection systems (IDS) face numerous challenges. Scalability and computational costs are significant challenges that require substantial processing power and memory, leading to delays in real-time cloud systems. Additionally, the lack of transparency in deep learning models affects regulations and emergency responses by reducing confidence among security analysts. The evaluation also highlights threats from adversarial attacks and the effect of concept drift; developing cloud workloads can reduce IDS performance if models are not constantly updated [14], [17].

6.2 Deployment and Operational Challenges

This section discusses the actual challenges that occur when implementing deep learning-based intrusion detection systems in real-world cloud applications.

1. Lack of Realistic and Cloud-Native Datasets

One of the most significant challenges in developing deep learning–based IDS is the lack of up-to-date, real-world cloud security datasets. Most existing datasets, such as NSL-KDD, UNSW-NB15, and CICIDS, are either outdated or generated in controlled laboratory environments. These datasets fail to capture modern cloud characteristics such as container orchestration, microservices, encrypted traffic, multi-tenancy, and elastic resource scaling. As a result, models trained on these datasets often demonstrate high accuracy in experimental settings but perform poorly in real-world cloud deployments. The absence of standardized, cloud-native datasets also makes it difficult to compare IDS approaches fairly across studies [4], [21].

2. Scalability and Real-Time Processing Constraints

Cloud environments generate massive volumes of high-velocity network traffic and log data. Deep learning models, particularly deep and hybrid architectures, require significant computational resources for training and inference. This can introduce latency and hinder real-time intrusion detection, especially in large-scale cloud infrastructures. Deploying IDS at multiple cloud layers, such as network, host, container, and application levels, further amplifies scalability challenges. Ensuring consistent performance while maintaining low latency remains a major obstacle for cloud-based IDS [6], [9].

3. High False Positive Rates in Dynamic Environments

Anomaly-based deep learning IDS often suffers from high false positive rates due to the constantly changing nature of cloud workloads. Legitimate changes in user behavior, application updates, or scaling events may be incorrectly classified as intrusions. High false positive rates increase the operational burden on security analysts, as frequent false alarms require manual investigation, leading to delayed response times and reduced trust in automated intrusion detection systems [13], [18].

4. Concept Drift and Model Degradation

Cloud environments are highly dynamic, with continuous changes in traffic patterns, workloads, and user behaviour. This leads to concept drift, where the statistical properties of input data change over time. Deep learning models trained on previous data can eventually lose efficiency, resulting in lower detection accuracy. IDS models become irrelevant without any options for continuous learning or adaptive retraining. Managing concept drift in real time without compromising system stability is a key research challenge [7], [26].

5. Vulnerability to Adversarial Attacks

Deep learning-based intrusion detection systems depend on malicious attacks that manipulate input data to avoid detection or change training datasets. Effectively developed changes can cause misclassification, allowing malicious traffic to overcome IDS capabilities. Adversarial threats are more serious in cloud systems due to their enormous size and connectivity. An IDS model with a mutually adaptable design remains an open research challenge for the system [9], [12].

5.1 Suitability of Deep Learning Architectures for Cloud Deployment

In the implementation phase, a few deep learning methods are useful for cloud-based intrusion detection systems. Firstly, CNN-based models are scalable for real-time deployment processes and perform continuous evaluations with low latency when combined with GPU. Secondly, RNN and LSTM-based models have high latency, and their increased computational cost makes them unsuitable for cloud traffic situations. Autoencoder-based models are lightweight and efficient, but they generate false positives in different conditions. Lastly, hybrid models improve accuracy by consuming more resources, which affects scalability and leads to high operational costs. Among the deep learning models mentioned, hybrid and CNN-based models are suitable for real-time cloud IDS integrated with edge processing or stream-based analytics [20][25].

7. Conclusion

This review explains how deep learning can transform cloud intrusion detection by integrating a reactive technique with a proactive and smart security architecture. It improves the detection of complex attacks by combining independent feature training, flexible threat detection, and real-time analysis. However, a few key implementation challenges, including scalability limitations, low accessibility, adversarial attacks, and a lack of real cloud-based datasets, must be resolved before using this system in operational cloud systems. Overcoming these problems is important for maintaining the dependability and efficiency of deep learning-based intrusion detection systems (IDS). In the future, the research will focus on explainable AI (XAI), effective training methods for malicious attacks, security-based learning, and energy-efficient models. These features will help to develop scalable, transparent, and adaptable cloud-based intrusion detection systems (IDS) that can protect modern cloud systems from continuous cyber-attacks.

References

[1] Nassif, Ali Bou, Manar Abu Talib, Qassim Nasir, Halah Albadani, and Fatima Mohamad Dakalbab. "Machine Learning for Cloud Security: A Systematic Review." IEEE Access 9 (2021): 20717-20735.

[2] Alzoubi, Yehia Ibrahim, Alok Mishra, and Ahmet Ercan Topcu. "Research Trends in Deep Learning and Machine Learning for Cloud Computing Security." Artificial intelligence review 57, no. 5 (2024): 132.

[3] Hasimi, Lumbardha, Dimitrios Zavantis, Elhadi Shakshuki, and Ansar Yasar. "Cloud Computing Security and Deep Learning: an ANN Approach." Procedia Computer Science 231 (2024): 40-47.

[4] Salem, Israa Ezzat. "Enhancing Cloud Security through the Integration of Deep Learning and Data Mining Techniques: A Comprehensive Review." Periodicals of Engineering and Natural Sciences 11, no. 3 (2023): 176-192.

[5] Gangwani, Divya, Harshal A. Sanghvi, Viral Parmar, Riki H. Patel, and Abhijit S. Pandya. "A Comprehensive Review on Cloud Security using Machine Learning Techniques." Artificial Intelligence in Cyber Security: Theories and Applications (2023): 1-24.

[6] Butt, Umer Ahmed, Muhammad Mehmood, Syed Bilal Hussain Shah, Rashid Amin, M. Waqas Shaukat, Syed Mohsan Raza, Doug Young Suh, and Md Jalil Piran. "A Review of Machine Learning Algorithms for Cloud Computing Security." Electronics 9, no. 9 (2020): 1379.

[7] Sivaprasad Yerneni, K., A. Ravi Teja, K. Sri Harsha, and Y. Naresh Kiran Kumar Reddy. "Towards Proactive Cloud Security: A Survey on ML and Deep Learning-Based Intrusion Detection Systems." J Contemp Edu Theo Artific Intel: JCETAI-116 (2025).

[8] Hizal, Selman, Ünal ÇAVUŞOĞLU, and Devrim AKGÜN. "A New Deep Learning Based Intrusion Detection System for Cloud Security." In 2021 3rd International Congress on Human-Computer Interaction, Optimisation and Robotic Applications (HORA), pp. 1-4. IEEE, 2021.

[9] Qayyum, Adnan, Aneeqa Ijaz, Muhammad Usama, Waleed Iqbal, Junaid Qadir, Yehia Elkhatib, and Ala Al-Fuqaha. "Securing Machine Learning in the Cloud: A Systematic Review of Cloud Machine Learning Security." Frontiers in Big Data 3 (2020): 587139.

[10] Reddy, Premkumar, Yemi Adetuwo, and Anil Kumar Jakkani. "Implementation of Machine Learning Techniques for Cloud Security in Detection of DDoS Attacks." International Journal of Computer Engineering and Technology (IJCET) 15, no. 2 (2024): 25-34.

[11] Garikipati, Venkat, and Veerandra Kumar. "Optimising Traffic Management and Cloud Security in Software Networks Using Advanced Deep Learning Models for Application and Attack Classification." International Journal of HRM and Organisational Behaviour 8, no. 3 (2020): 127-134.

[12] Andi, Hari Krishnan. "Estimating the Role of Blockchain, Deep Learning and Cryptography Algorithms in Cloud Security." Journal of Trends in Computer Science and Smart Technology 3, no. 4 (2021): 305-313.

[13] Vashishth, Tarun Kumar, Vikas Sharma, Kewal Krishan Sharma, Bhupendra Kumar, Sachin Chaudhary, and Rajneesh Panwar. "Enhancing Cloud Security: The Role of Artificial Intelligence and Machine Learning." In Improving security, privacy, and trust in cloud computing, pp. 85-112. IGI Global Scientific Publishing, 2024.

[14] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "Security Enhancement in Healthcare Cloud using Machine Learning." Procedia Computer Science 127 (2018): 388-397.

[15] Alhazmi, Lamia. "Enhancing Cloud Security: Optimisation-based Deep Learning Model for Detecting Denial-of-Service Attacks." International Journal of Advanced Computer Science and Applications 14, no. 7 (2023).

[16] Sokolov, Strahil A., Teodor B. Iliev, and Ivaylo S. Stoyanov. "Analysis of Cybersecurity Threats in Cloud Applications using Deep Learning Techniques." In 2019, 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 441-446. IEEE, 2019.

[17] Prabhu, M., G. Revathy, and R. Raja Kumar. "Deep Learning Based Authentication Secures Data Storage in Cloud Computing." International Journal of Computer and Engineering Optimisation 1, no. 01 (2023): 10-14.

[18] Tiwari, Pradeep Kumar, K. Kannan, Duggineni Veeraiah, Nikhil Ranjan, Jain Singh, Ghalib H. Alshammri, and Awal Halifa. "Security Protection Mechanism in Cloud

Computing Authorisation Model Using Machine Learning Techniques." Wireless Communications and Mobile Computing 2022, no. 1 (2022): 1907511.

[19] Srilatha, Doddi, and N. Thillaiarasu. "Implementation of Intrusion Detection and Prevention with Deep Learning in Cloud Computing." Journal of Information Technology Management 15, no. Special Issue (2023): 1-18.

[20] Bhaskaran, Shinoy Vengaramkode, and Sandesh Achar. "A Study of Evolving Cloud Computing Data Security: A Machine Learning Perspective." International Journal of Professional Business Review: Int. J. Prof. Bus. Rev. 10, no. 3 (2025): 5.

[21] Attou, Hanaa, Azidine Guezzaz, Said Benkirane, Mourade Azrour, and Yousef Farhaoui. "Cloud-Based Intrusion Detection Approach using Machine Learning Techniques." Big Data Mining and Analytics 6, no. 3 (2023): 311-320.

[22] Ţălu, Mircea. "Exploring Machine Learning Algorithms to Enhance Cloud Computing Security." Digital Technologies Research and Applications 4, no. 2 (2025): 33-47.

[23] Shaik, Sajeeda Parveen. "Enhancing Cloud Computing Security Through Deep Learning: An Artificial Neural Network Approach." (2021).

[24] Patell, Jay. "Prospects of Cloud-Driven Deep Learning-Leading the Way for Safe and Secure AI." INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES 8, no. 3 (2020): 10-55083.

[25] Raju, K., N. Ramshankar, J. Anvar Shathik, and R. Lavanya. "Blockchain-Assisted Cloud Security and Privacy Preservation using Hybridised Encryption and Deep Learning Mechanism in IoT-Healthcare Application." Journal of Grid Computing 21, no. 3 (2023): 45.

[26] Diana, Lorenzo, Pierpaolo Dini, and Davide Paolini. "Overview on Intrusion Detection Systems for Computer Networking Security." Computers 14, no. 3 (2025): 87.

[27] Market.us. 2023. “Cloud Security Market Size, Share | CAGR of 22.5%.” October 31, 2023. https://market.us/report/cloud-security-market/.