PAPER ID: 20260201014

An AI-Driven Intrusion Detection and Prevention Framework for Secure Cloud Environments

Abhishek[1] and Dr. Gaurav Aggarwal[2]

[1]Research Scholar, Department of Computer Science & Engineering, Jagannath University, Delhi NCR, Bahadurgarh

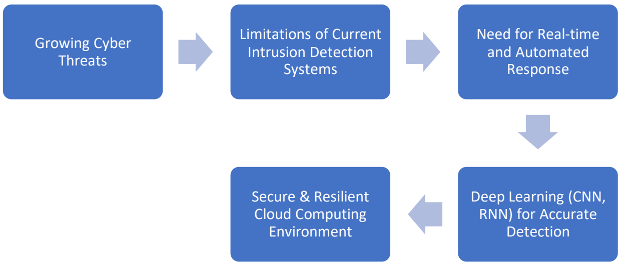
[2]Professor, Department of Computer Science & Engineering, Jagannath University, Delhi NCR, Bahadurgarh

Abstract: The rapid adoption of cloud computing has significantly increased the exposure of cloud environments to sophisticated cyber intrusions and security threats. Traditional intrusion detection and prevention systems often fail to address the dynamic, large-scale, and heterogeneous nature of cloud infrastructures. To overcome these limitations, this paper proposes an intelligent deep learning–based framework for intrusion recognition and avoidance in cloud environments. The proposed framework integrates advanced deep neural network models to automatically learn complex patterns from high-dimensional network traffic data, enabling accurate detection of both known and zero-day attacks. Feature extraction and classification are optimized using deep architectures such as convolutional and recurrent neural networks to enhance detection accuracy while minimizing false positives. In addition, an adaptive response mechanism is incorporated to proactively mitigate detected threats, ensuring real-time intrusion avoidance without degrading system performance. Experimental evaluation on benchmark intrusion datasets demonstrates that the proposed framework outperforms traditional machine learning and signature-based approaches in terms of detection accuracy, precision, recall, and response time. The results confirm the effectiveness of deep learning in strengthening cloud security by providing a scalable, intelligent, and robust intrusion recognition and avoidance solution.

Keywords: Intrusion Detection System (IDS), Intrusion Prevention System, Cloud Computing Security, Deep Learning, Intelligent Security Framework

Introduction

In recent years, deep learning has emerged as a powerful tool for enhancing cybersecurity. Unlike rule-based methods, deep learning models can learn representations from raw data and identify subtle patterns that indicate abnormal behavior. Techniques have shown promising results in intrusion detection research. The integration of deep learning into intrusion detection and prevention frameworks for cloud computing offers a robust solution to evolving cyber threats. By leveraging big data analytics and cloud log monitoring, deep learning-based IDPS can provide accurate classification, anomaly detection, and proactive defense strategies. This research focuses on designing and analyzing a deep learning-driven intrusion detection and prevention framework, aiming to strengthen cloud security, reduce false alarms, and improve response times against sophisticated cyberattacks.The motivation behind this research stems from the increasing volume and sophistication of cyberattacks targeting cloud computing environments. As businesses migrate critical applications and sensitive data to cloud platforms, attackers exploit vulnerabilities at different layers, such as virtualization, networking, and storage. Reports indicate that cloud-based security incidents are on the rise, with significant financial, operational, and reputational consequences for organizations. For instance, breaches in healthcare and financial sectors not only lead to monetary losses but also compromise sensitive personal data, raising ethical and regulatory concerns. Conventional intrusion detection systems rely heavily on predefined rules and signatures, making them ineffective against unknown or zero-day attacks. Moreover, with the dynamic scaling nature of cloud systems, the sheer volume of traffic and user activities makes manual monitoring impractical. This necessitates intelligent, automated, and adaptive security solutions. Deep learning offers unique capabilities such as feature learning, pattern recognition, and anomaly detection from large-scale data, making it an ideal candidate for cloud intrusion detection and prevention.


Growing Cyber Threats
Limitations of Current Intrusion Detection Systems
Need for Real-time and Automated Response
Deep Learning (CNN, RNN) for Accurate Detection
Secure & Resilient Cloud Computing Environment

While deep learning-driven intrusion detection and prevention frameworks show great promise, several challenges hinder their adoption and effectiveness in cloud computing. One of the primary challenges is the availability and quality of datasets. Public intrusion detection datasets such as KDDCup99, NSL-KDD, and UNSW-NB15, although widely used, are often outdated, imbalanced, or lack real-world diversity. Training deep learning models on such datasets may not generalize well to modern cloud attack scenarios. Another challenge lies in the computational and storage overhead. Deep learning models require significant resources for training and inference. Deploying complex models in cloud environments may strain resources and increase latency, which is critical for real-time intrusion prevention. Additionally, high false positive rates can overload administrators with alerts, reducing the practical utility of IDPS systems. The dynamic nature of cloud environments poses further complications. Cloud infrastructures are elastic, multi-tenant, and distributed, leading to constantly changing traffic patterns and security contexts. Designing models that adapt to these variations without compromising accuracy remains a major hurdle. Moreover, attackers are increasingly employing adversarial techniques to manipulate deep learning models, making them misclassify malicious behavior as benign. Data privacy and regulatory compliance also present challenges. Deep learning models often require access to large amounts of user and system data, raising concerns about confidentiality and compliance with regulations such as GDPR and HIPAA. Ensuring privacy-preserving intrusion detection while maintaining model effectiveness is a complex task. Finally, the lack of interpretability in deep learning models makes it difficult for security analysts to understand the reasoning behind detection results. Black-box models limit trust and adoption in mission-critical cloud applications. Addressing these challenges requires innovative approaches in data collection, model design, computational efficiency, adversarial robustness, and explainable AI.This research holds significant importance in the domain of cloud security. With the rapid adoption of cloud computing across industries, ensuring a secure environment is not only a technical necessity but also a business imperative. A successful deep learning-driven intrusion detection and prevention framework has the potential to transform the way organizations defend against cyber threats in dynamic and complex cloud infrastructures. First, this research contributes to improving detection accuracy and reducing false alarms. By leveraging deep learning techniques, the framework can distinguish between normal and abnormal behaviour more effectively than traditional rule-based systems. This ensures faster response to genuine threats while minimizing unnecessary administrative interventions. Second, the study is significant for its proactive defense mechanism. Unlike conventional IDS that only detect intrusions, the proposed framework incorporates prevention strategies, ensuring that malicious activities are blocked in real time. This enhances resilience and reduces the risk of service disruption. Third, the research aligns with the growing need for intelligent, scalable, and adaptive security solutions. As cloud environments expand and evolve, static security models become insufficient. The integration of deep learning provides adaptability, allowing the framework to learn from new data and stay ahead of emerging threats. From a broader perspective, this research also holds significance in terms of compliance and trust. Enterprises handling sensitive data must adhere to strict security regulations. By adopting advanced intrusion detection and prevention systems, organizations can demonstrate regulatory compliance and build trust with customers. Furthermore, the findings of this research are not limited to cloud environments alone. The insights and methodologies can also be extended to other domains such as edge computing, Internet of Things (IoT), and 5G networks. Thus, the study contributes not only to academic knowledge but also to real-world applications, shaping the future of secure computing infrastructures.

Contribution, Objectives, and Research Methodology

This research makes significant contributions toward the design and implementation of an intelligent deep learning–driven intrusion detection and prevention framework for cloud computing environments. It proposes a novel and comprehensive framework that integrates multiple deep learning architectures to achieve both accurate intrusion recognition and proactive intrusion avoidance, addressing the limitations of existing systems that primarily focus on detection alone. By leveraging advanced models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and autoencoders, the framework demonstrates enhanced detection accuracy across diverse attack categories, including zero-day exploits and complex multi-vector intrusions. The proposed approach incorporates real-time automated prevention mechanisms to mitigate malicious activities without degrading system performance, thereby ensuring continuous protection in dynamic cloud environments. To address practical data challenges, the research emphasizes handling imbalanced and noisy datasets through preprocessing, data augmentation, and adversarial training techniques, improving robustness and generalization to real-world scenarios. Scalability and adaptability are evaluated under varying workloads and traffic patterns, confirming the framework’s suitability for large-scale cloud infrastructures. Additionally, the study explores explainable AI techniques to enhance interpretability and trust, enabling security analysts to understand and validate model decisions. Beyond cloud computing, the framework exhibits potential adaptability to emerging domains such as IoT, edge computing, and 5G-enabled networks. Motivated by the growing inadequacy of traditional security mechanisms in combating sophisticated cyber threats, this research aims to develop a robust, adaptive, and intelligent intrusion detection and prevention solution. The research methodology follows a systematic and data-driven approach encompassing an extensive literature review, benchmark dataset selection (including NSL-KDD, CIC-IDS2017, CSE-CIC-IDS2018, and UNSW-NB15), comprehensive data preprocessing, deep learning model design, training, optimization, and performance evaluation. The framework is trained using high-performance computing resources with optimization techniques such as dropout, batch normalization, and hyperparameter tuning, and is evaluated using standard metrics including accuracy, precision, recall, F1-score, AUC-ROC, false alarm rates, execution time, and scalability. Comparative analysis with conventional machine learning and existing deep learning models validates the superiority of the proposed framework, while cross-validation and multi-dataset testing confirm its generalizability and effectiveness in real-world cloud computing environments.

Conclusion

This research presented an intelligent deep learning–based Intrusion Detection and Prevention System (IDPS) tailored for secure cloud computing environments. By integrating advanced deep learning architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Auto encoders, the proposed hybrid framework effectively addresses sophisticated cyber threats targeting the confidentiality, integrity, and availability of cloud resources. The study demonstrated that leveraging multiple deep learning models enhances real-time threat detection accuracy while significantly reducing false positive rates compared to traditional IDS/IPS approaches. A comprehensive comparative analysis with existing intrusion detection and prevention models validated the superiority of the proposed framework in dynamic and distributed cloud settings. Furthermore, the research addressed cloud-specific security challenges, including scalability, multi-tenancy, virtualization, and efficient resource utilization, ensuring adaptability across various cloud service models such as IaaS, PaaS, and SaaS. The inclusion of practical deployment considerations—such as lightweight model optimization, real-time monitoring integration, and compliance with cloud security standards highlights the industrial applicability of the proposed solution. Overall, this work contributes both theoretically and practically to the advancement of intelligent cloud security systems, providing a robust foundation for next-generation intrusion detection and prevention mechanisms.

Future Scope

While the proposed framework demonstrates promising results, several avenues remain open for future research and enhancement. Future work may explore the integration of federated learning to enable privacy-preserving collaborative intrusion detection across distributed cloud environments. The incorporation of reinforcement learning techniques could further enhance adaptive response mechanisms, allowing the system to autonomously evolve against emerging and zero-day attacks. Additionally, extending the framework to support edge and fog computing environments can improve security coverage for latency-sensitive cloud applications. Further optimization using lightweight and explainable AI (XAI) models would improve transparency, interpretability, and trustworthiness of intrusion detection decisions. Real-world deployment and testing on large-scale cloud platforms with live traffic data can further validate the robustness and scalability of the framework.

References

1. Ali, M., Raza, A., Akram, M. A., Arif, H., & Ali, A. (2025). Enhancing IOT Security: A review of Machine Learning-Driven Approaches to Cyber Threat Detection: Enhancing IOT Security: A review of Machine Learning-Driven Approaches to Cyber Threat Detection. *Journal of Informatics and Interactive Technology*, *2*(1), 316-324.
2. Saeed, M. M. (2025). An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption. *IEEE Access*.
3. Rahmati, M., & Pagano, A. (2025, July). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities. In *Informatics* (Vol. 12, No. 3, p. 62). MDPI.
4. Maheswaran, N., Bose, S., Gokulraj, G., Anitha, T., Shruthi, T., & Vijayaraj, G. (2025, January). Intrusion Prevention System in SDN Environment for 6G Networks Using Deep Learning. In *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)* (pp. 53-61). IEEE.
5. Karan, D., & Ryan, B. (2024). Deep Learning-Powered Intelligent Decision Support Systems for Cloud Security.
6. Samriya, J. K., Kumar, S., Kumar, M., Wu, H., & Gill, S. S. (2024). Machine learning based network intrusion detection optimization for cloud computing environments. *IEEE Transactions on Consumer Electronics*.
7. Potluri, S. (2024). A Deep Learning-Driven Framework for Detecting Anomalous Data Breaches in Distributed Cloud Storage Infrastructures. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *5*(3), 80-87.
8. Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. *Artificial intelligence review*, *57*(5), 132.
9. Alzubi, J. A., Alzubi, O. A., Qiqieh, I., & Singh, A. (2024). A blended deep learning intrusion detection framework for consumable edge-centric iomt industry. *IEEE Transactions on Consumer Electronics*, *70*(1), 2049-2057.
10. Hiregowja Kumara, S. (2023). *Machine Learning Driven Network Protection in Cloud Computing Environments* (Doctoral dissertation, Dublin, National College of Ireland).
11. Al-Ghuwairi, A. R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A., & Algarni, A. (2023). Intrusion detection in cloud computing based on time

series anomalies utilizing machine learning. *Journal of Cloud Computing*, *12*(1), 127.

12. RM, B., & MK, J. K. (2023). Intrusion detection on AWS cloud through hybrid deep learning algorithm. *Electronics*, *12*(6), 1423.
13. Upadhyay, U., Kumar, A., Roy, S., Rawat, U., & Chaurasia, S. (2023, November). Defending the cloud: Understanding the role of explainable ai in intrusion detection systems. In *2023 16th International Conference on Security of Information and Networks (SIN)* (pp. 1-9). IEEE.
14. Saxena, D., Gupta, I., Gupta, R., Singh, A. K., & Wen, X. (2023). An AI-driven VM threat prediction model for multi-risks analysis-based cloud cybersecurity. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(11), 6815-6827.
15. Maddali, R. (2022). Enhancing Data Security with Machine Learning-Driven Threat Detection. *Zenodo, doi*, *10*.
16. Jayalaxmi, P. L. S., Saha, R., Kumar, G., Conti, M., & Kim, T. H. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. *IEEe Access*, *10*, 121173-121192.
17. RM, B., K Mewada, H., & BR, R. (2022). Hybrid machine learning approach based intrusion detection in cloud: A metaheuristic assisted model. *Multiagent and Grid Systems*, *18*(1), 21-43.
18. Dash Karan, M. S. (2022). AI-Driven Cloud Computing: Enhancing Scalability, Security, and Efficiency.
19. Mahendar, A., & Chatrapati, D. K. S. (2022). Detection and prevention of cyber attacks on cloud-based data centers using machine learning. *International Journal of Computing and Digital Systems*, *12*(1), 1063-1070.
20. Bangui, H., & Buhnova, B. (2021). Recent advances in machine-learning driven intrusion detection in transportation: Survey. *Procedia Computer Science*, *184*, 877-886.
21. Javeed, D., Gao, T., Khan, M. T., & Ahmad, I. (2021). A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT). *Sensors*, *21*(14), 4884.
22. Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. *IEEE Access*, *9*, 101574-101599.
23. Chou, D., & Jiang, M. (2021). A survey on data-driven network intrusion detection. *ACM Computing Surveys (CSUR)*, *54*(9), 1-36.