Brief Report

IMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology
ISSN 2349-3917

2025
Vol.13 No.1:1

Deep Learning-Based Intrusion Detection Systems for Cloud Computing Environments

Nora Schmidt*

Department of Computational Sciences, Technical University of Munich (TUM), Munich 80333, Germany

***Corresponding author:** Nora Schmidt, Department of Computational Sciences, Technical University of Munich (TUM), Munich 80333, Germany; E-mail: schmidtnora01@tum.de

Received date: January 01, 2025, Manuscript No. Ipacsit-25-20918; **Editor assigned date:** January 03, 2025, PreQC No. ipacsit-25-20918 (PQ); **Reviewed date:** January 20, 2025, QC No. ipacsit-25-20918; **Revised date:** January 27, 2025, Manuscript No. ipacsit-25-20918 (R); **Published date:** February 4, 2025, DOI: 10.36648/2349-3917.13.1.1

Citation: Schmidt N (2025) Deep Learning-Based Intrusion Detection Systems for Cloud Computing Environments. Am J Compt Sci Inform Technol Vol.13 No.1:1

Introduction

Cloud computing has revolutionized the digital landscape by providing scalable, flexible, and cost-effective solutions for data storage and processing. However, the increasing dependency on cloud infrastructure has simultaneously amplified concerns related to data privacy, network security, and system vulnerabilities. Traditional Intrusion Detection Systems (IDS) often struggle to cope with the dynamic and distributed nature of cloud environments, where data traffic is massive and continuously evolving. Deep learning, a subset of artificial intelligence, offers a promising approach to enhance intrusion detection by automatically learning complex patterns and identifying anomalies in network behavior. Unlike rule-based or statistical models, deep learning can adapt to emerging threats by continuously training on large datasets, thereby improving the system's ability to detect zero-day attacks and sophisticated cyber intrusions [1].

Description

Deep learning-based intrusion detection systems employ advanced neural network architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Autoencoders to analyze network traffic in real time. These architectures are capable of extracting high-level features from raw input data without the need for manual feature engineering, making them particularly effective in handling the complexity of cloud traffic. For instance, CNNs can detect spatial correlations in packet-level data, while RNNs can capture temporal dependencies in network flows. Autoencoders are frequently used for anomaly detection by learning normal network behavior and flagging deviations as potential intrusions. The IDS can be deployed at different layers of a cloud infrastructure network, hypervisor, or application to provide comprehensive protection against threats such as Distributed Denial-of-Service (DDoS) attacks, insider threats, and malware propagation [2].

Moreover, by leveraging large-scale datasets generated from cloud logs and traffic flows, these models can achieve high detection accuracy and minimize false positives, which have long been a limitation of traditional IDS approaches. Another significant advantage of deep learning-based IDS lies in its adaptability and scalability within multi-tenant cloud environments. Since cloud systems continuously evolve with varying workloads and user demands, an effective IDS must dynamically update its detection model to recognize new attack vectors. Deep learning enables this through transfer learning and continuous model retraining, where knowledge gained from one environment can be applied to another with minimal human intervention [3].

In addition, the use of federated learning in IDS design allows for decentralized model training, where multiple cloud nodes collaboratively improve the detection model without sharing sensitive data, thus preserving user privacy. The integration of deep learning with other emerging technologies, such as edge computing and block chain, further enhances IDS performance by improving response time, decentralizing data analysis, and ensuring integrity in threat intelligence sharing. Despite challenges like computational overhead and data imbalance, ongoing research continues to refine these systems to achieve faster detection rates and better generalization across diverse attack types [4,5].

Conclusion

In summary, deep learning-based intrusion detection systems represent a transformative advancement in safeguarding cloud computing environments. By utilizing neural networks capable of learning from vast and complex data streams, these systems provide enhanced accuracy, adaptability, and resilience against evolving cyber threats. The combination of automation, real-time analysis, and continuous learning makes deep learning approaches superior to traditional IDS models.

Acknowledgement

None

Conflict of Interest

None

References

1. Beam AL, Kohane IS (2018) Big data and machine learning in health care. JAMA 319: 1317–1318

2. Suarez-Albela M, Fernandez-Carames TM, Fraga-Lamas P, Castedo L (2017) A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications. Sensors 17: 1978

3. Kubiak K, Dec G, Stadnicka D (2022) Possible applications of edge computing in the manufacturing industry—systematic literature review. Sensors 22: 2445

4. Heidari A, Navimipour NJ (2021) A new SLA-aware method for discovering the cloud services using an improved nature-inspired optimization algorithm. PeerJ Comput Sci 7: e539

5. Peng D, Yang Q, Yang HJ, Liu H, Zhu Y, et al. (2020) Analysis on the relationship between fisheries economic growth and marine environmental pollution in China's coastal regions. Sci Total Environ 713: 136641