A Deep Learning-Based Intrusion Detection System for Securing Cloud Computing Environments Against Emerging Cyber Threats

- Maria Theresa Reyes, Department of Information Technology, Mapua University, Manila, Philippines

The increasing reliance on cloud computing for critical business operations has made cloud environments a prime target for cyber attacks. Traditional intrusion detection systems often struggle to keep pace with the evolving threat landscape and the complexity of cloud infrastructures. This research paper proposes a novel deep learning-based intrusion detection system specifically designed to secure cloud computing environments against emerging cyber threats. The proposed system leverages the power of deep neural networks to accurately identify and classify malicious activities in real-time, enabling prompt response and mitigation measures. The research methodology involves the collection and preprocessing of a diverse dataset encompassing various types of cloud-based attacks, such as distributed denial-of-service (DDoS), insider threats, and advanced persistent threats (APTs). The dataset is used to train and validate a deep learning model, employing state-of-the-art architectures such as convolutional neural networks (CNNs) and long short-term memory (LSTM) networks. The model is optimized through rigorous hyperparameter tuning and cross-validation techniques to ensure high accuracy and generalization capabilities. The proposed intrusion detection system is evaluated through extensive experiments and benchmarked against existing solutions, demonstrating superior performance in terms of detection accuracy, false positive rates, and real-time responsiveness. The study presents a comprehensive analysis of the system's ability to adapt to new attack patterns and its scalability in handling large-scale cloud environments. The findings of this research have significant implications for enhancing the security posture of cloud computing environments. By leveraging deep learning techniques, the proposed intrusion detection system offers a proactive and intelligent approach to detecting and mitigating cyber threats, reducing the risk of data breaches and ensuring the confidentiality, integrity, and availability of cloud-based assets. This research contributes to the advancement of cybersecurity in the cloud computing era, providing a robust and adaptable solution to safeguard organizations against the ever-evolving threat landscape.

References

[1] K. Alwasel, Y. Li, P. P. Jayaraman, S. Garg, R. N. Calheiros, and R. Ranjan, “Programming SDN-native big data applications: Research gap analysis,” *IEEE Cloud Comput.*, vol. 4, no. 5, pp. 62–71, Sep. 2017.

[2] M. Abouelyazid, “Forecasting Resource Usage in Cloud Environments Using Temporal Convolutional Networks,” *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 5, no. 1, pp. 179–194, Nov. 2022.

[3] M. Yousif, “Cloud-native applications—the journey continues,” *IEEE Cloud Comput.*, vol. 4, no. 5, pp. 4–5, Sep. 2017.

[4] M. Abouelyazid and C. Xiang, “Architectures for AI Integration in Next-Generation Cloud Infrastructure, Development, Security, and Management,” *International Journal of Information and Cybersecurity*, vol. 3, no. 1, pp. 1–19, Jan. 2019.