A Hybrid Deep Learning Framework for High-Precision Intrusion Detection in Cloud Infrastructure

Dr S Boopalan, Postdoctoral Research Scholar, Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia. sribalulohith@gmail.com
Dr Sudhakar K, Department of AI & DS, Nitte Meenakshi Institute of Technology (NMIT), Nitte (Deemed-to-be University), Bengaluru, Karnataka, India. . ksudhakar.cs@gmail.com

Abstract: With the dynamic nature of cloud computing environments, which involves multiple tenants and large-scale data processing, they are becoming more vulnerable to advanced forms of cyber-attacks. It becomes difficult to detect zero-day attacks, multi-stage intrusions and other evolving threats by traditional Intrusion Detection System (IDS) approaches, which rely on signature and rule-based methods. Even though various studies show that deep learning algorithms like CNN, LSTMs and Transformers perform well, each of them has weaknesses like high false positive rate, lack of robustness against adversarial examples, low explainability and scalability issues. In order to resolve these problems, this paper introduces a new Hybrid Deep Learning IDS Approach combining CNN-based spatial feature extraction, LSTM temporal dependency modeling, Transformer attention mechanism, adversarial training and explainable AI techniques. The main focus is not only to enhance IDS precision but also to make it suitable for real-time implementation within cloud environment. Implementation methods based on benchmark datasets, such as CICIDS2017, CSE-CICIDS2018, UNSW-NB15 and NSL-KDD datasets, are also considered. This work creates a basis for the upcoming implementation and validation steps in further research.
Keywords: Intrusion Detection System, Cloud Security, Deep Learning, CNN, LSTM, Transformer, Explainable AI, Adversarial Learning.

Introduction

Fast development of cloud computing technology has revolutionized the process of delivering digital services by offering scalable, flexible, and affordable computing capabilities. However, growing complexity and dynamism of cloud architectures have increased the number of potential attack surfaces for cyber attackers considerably. Modern cloud networks produce tremendous amounts of heterogeneous traffic, use encrypted communications, and have several tenants working at the same time, which makes intrusion detection very difficult. Conventional intrusion detection systems are based on signatures and manually constructed rules, which limits their capability to detect novel attacks and intrusions. Deep learning approaches seem to be more promising since they can automatically learn hierarchical representations of raw traffic data. Nevertheless, current solutions still have some problems with scalability, false positives, and efficiency in real clouds.

Motivation

The network traffic generated by cloud infrastructures is massive and constantly fluctuates in terms of workloads and attacks. Traditional IDS architectures lack the necessary flexibility to detect advanced persistent threats (APTs), zero-day attacks, and multi-stage attacks in particular. Moreover, the increasing use of secure communication channels has limited the ability of packet inspection methods to detect attacks. Consequently, there is a need for intelligent IDS systems that can learn from attacks both in space and time. They should be highly robust and interpretable at the same time. These considerations call for the development of a deep learning framework incorporating different learning strategies.

Problem Statement

Even though there have been many breakthroughs regarding the application of deep learning in intrusion detection, there are still some challenges that these intrusion detection solutions must

overcome. The presence of high false-positive rates is a burden on the workload of security experts and reduces their confidence in using automated techniques to detect intrusions. A lot of algorithms fail in detecting infrequent attacks because of the problem of class imbalance in cybersecurity data. Additionally, there are threats of adversarial attacks on deep learning models, which makes it possible for them to bypass detection systems.

Table 1. Limitations of Existing IDS Approaches

Existing Approach	Strengths	Limitations
Signature-based IDS	High accuracy for known attacks	Unable to detect zero-day attacks
Machine Learning IDS	Learns attack patterns automatically	Requires manual feature engineering
CNN-based IDS	Effective spatial feature extraction	Limited temporal understanding
LSTM-based IDS	Captures sequential attack behavior	Computationally expensive
Transformer-based IDS	Models long-range dependencies	Requires large training datasets
Hybrid IDS	Combines multiple strengths	Increased architectural complexity

Research Objectives

It is necessary to note that the main aim of the work presented is the development of an intelligent intrusion detection system which would be able to increase the precision of detection of intrusion and decrease the number of false alarms at the same time. Moreover, the framework should be able to identify zero-day attacks, have a good robustness against adversarial attacks and be able to provide explainable decision making.

Proposed Hybrid IDS Framework

The proposed architecture uses a combination of deep learning modules to leverage the power of each individual component. First of all, a CNN based module will perform the task of extracting features using spatial and structural information from the network traffic. The feature vector obtained through the first module will be fed into the next module of LSTM which will learn the temporal behaviour from the sequences. Further, a transformer-based attention module will be used to find globally significant traffic patterns along with event interactions. A module for adversarial training will be used to make the model resistant to evasion attacks and manipulated traffic. Finally, techniques from explainable AI will be incorporated for interpretation of predictions made by the model.

Table 2. Proposed Hybrid IDS Modules

Module	Function	Expected Benefit
CNN Feature Extractor	Extract spatial traffic features	Improved pattern recognition
LSTM Module	Learn temporal attack sequences	Better sequential modeling
Transformer Attention Module	Capture global dependencies	Improved contextual understanding
Adversarial Training Module	Generate robust representations	Resistance against evasion attacks
Explainable AI Module	Provide interpretable predictions	Increased analyst trust
Final Classifier	Perform attack classification	High precision detection

System Architecture

In the proposed pipeline for an IDS system, the first step involves collecting the data from the network traffic and performing some pre-processing tasks such as missing value handling, duplicate removal,

feature normalization, and encoding. After that, the processed traffic data is fed into the CNN model to extract the spatial features from the data. Further, temporal features are extracted from the data using LSTM models after which self-attention mechanisms are performed by using Transformer models that can extract long-range contextual relationships. The final step involves classification of intrusions after adversarial defense of the IDS system.

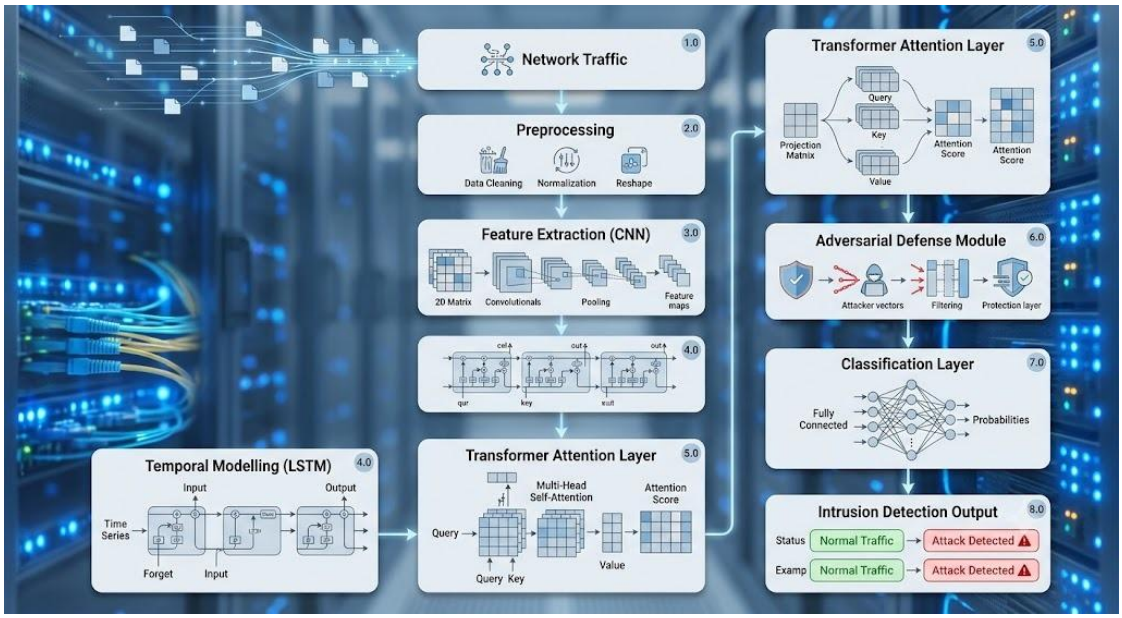

Fig1: Architecture Diagram

Dataset Selection and Preprocessing

In the initial implementation stage, benchmark datasets on cybersecurity that consist of CICIDS2017, CSE-CICIDS2018, UNSW-NB15, and NSL-KDD will be used. The above datasets are characterized by diverse attacks scenarios and cloud network traffic characteristics. In the preprocessing process, missing values will be suitably dealt with, duplicates will be deleted, and categorical features will be encoded by label encoding approaches. Normalization of feature will help achieve model stability in the training process, and class imbalance will be addressed through approaches like SMOTE and GAN data augmentation.

Table 3. Benchmark Datasets

Dataset	Year	Number of Records	Attack Categories
NSL-KDD	2009	1,48,517	DoS, Probe, R2L, U2R
UNSW-NB15	2015	2,57,673	9 attack categories
CICIDS2017	2017	2.8 Million	14 attack categories
CSE-CICIDS2018	2018	16 Million	Multiple modern attacks

Preliminary Implementation

In the initial implementation phase, the feasibility of the suggested framework will be established through the use of simple model architectures. In terms of the CNN architecture, it will have three convolution layers, followed by ReLU activations and max pooling layers to extract features from the data. For the LSTM structure, it will have 64 hidden layers that help in extracting sequential relations from the network traffic flows. In addition, there will be the introduction of a Transformer layer with multi-head self-attention mechanisms for better modeling of the context interactions.

Expected Performance Metrics

This will be achieved through the realization of an accuracy greater than 98% and a precision, recall, and F1 score of more than 97%. Moreover, the goal of this system is to ensure that the false positives generated are less than 2%, hence reducing the work of the analysts and increasing confidence in such automated detection systems.

Expected Contributions

The most significant contribution of the research paper is the introduction of a novel architecture for a hybrid deep learning system incorporating aspects such as spatial features extraction, temporal modeling, attention, adversarial robustness, and explainable artificial intelligence all together into one system. This architecture will enhance the capability of detecting zero-day attacks, minimize false alarms, and increase the interpretability of the decision process related to cybersecurity.

Future Work

In the future research efforts will involve federated learning systems to achieve privacy-preservation collaboration among tenants of different clouds. Explainable AI techniques will be used to increase transparency of machine learning models, while the scalability in production deployments will be evaluated through real-time deployments. Another research direction will be cross-cloud generalization and privacy-preserving intrusion detection approaches.

Conclusion

In this paper, we introduce a Hybrid Deep Learning Intrusion Detection System framework that will seek to solve some of the problems encountered in the initial phase of this study. Through the combination of CNN-based feature extraction, LSTM-based temporal modeling, Transformer-based attention modeling, adversarial learning, and Explainable AI (XAI), the suggested framework will strive to implement precise intrusion detection in a cloud environment. This current paper will lay down the groundwork for future experiments and optimizations to be carried out at other conferences.

References

1. Teyou, Gael & Junior, Momo Ziazet. (2019). Convolutional Neural Network for Intrusion Detection System In Cyber Physical Systems. 10.48550/arXiv.1905.03168.
2. Ferrag, Mohamed Amine & Maglaras, Leandros & Moschoyiannis, Sotiris & Janicke, Helge. (2019). Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study. Journal of Information Security and Applications. 50. 10.1016/j.jisa.2019.102419.
3. Ravi, Vinayakumar & Kp, Soman & Poornachandran, Prabaharan. (2017). Applying deep learning approaches for network traffic prediction. 2353-2358. 10.1109/ICACCI.2017.8126198.
4. Shone, Nathan & Tran Nguyen, Ngoc & Vu Dinh, Phai & Shi, Qi. (2018). A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence. 2. 41-50. 10.1109/TETCI.2017.2772792.
5. Mambwe Sydney, Kasongo & Sun, Yanxia. (2019). A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2905633.
6. Verkerken, Miel & D'Hooge, Laurens & Wauters, Tim & Volckaert, Bruno & De Turck, Filip. (2021). Towards Model Generalization for Intrusion Detection: Unsupervised Machine

Learning Techniques. Journal of Network and Systems Management. 30. 10.1007/s10922-021-09615-7.

7. Patil, Shruti & Varadarajan, Vijayakumar & Mazhar, Siddiqui & Sahibzada, Abdulwodood & Ahmed, Nihal & Sinha, Onkar & Kumar V C, Satish & Shaw, Kaialsh & Kotecha, Ketan. (2022). Explainable Artificial Intelligence for Intrusion Detection System. Electronics. 11. 3079. 10.3390/electronics11193079.
8. K V K, C., Reddy, V.L. Deep learning-based intrusion detection for cloud environments using Modified Stacked Bidirectional Gated Recurrent Unit. Discov Computing 29, 159 (2026). https://doi.org/10.1007/s10791-026-10020-4
9. Chen, S., Feng, X. A novel intrusion detection framework using hybrid deep learning to detect IIoT cloud environments attacks. Sci Rep 16, 11666 (2026). https://doi.org/10.1038/s41598-025-15419-5
10. Padma Priya, N., Mohanbabu, G. Intrusion detection with HACDT-Net and TRBM-Net using a hybrid deep learning framework with enhanced sampling techniques. Sci Rep 16, 11799 (2026). https://doi.org/10.1038/s41598-026-41422-5