A Hybrid Framework for Intrusion Detection and Attack Classification Using Network Security and Data Mining Techniques

OPEN ACCESS

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
Preethi, C. J., et al. "A Hybrid Framework for Intrusion Detection and Attack Classification Using Network Security and Data Mining Techniques." *Shanlax International Journal of Arts, Science and Humanities*, vol. 13, no. 3, 2026, pp. 323–28.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i2-Feb.10299

Mrs. CJ. Preethi
Assistant professor, Department of Computer Application
Thiruthangal Nadar college, Chennai

Mrs. CJ. Manju
Assistant Professor, Department of Computer Application
Thiruthangal Nadar College, Chennai

Dr. K. Somasundaram
Associate Professor, Department of Computer Application
Thiruthangal Nadar college, Chennai

Abstract

The swift growth of cloud platforms, network-based services, and IoT infrastructures has led to an increase in the frequency and sophistication of assaults. Due to their limited classification capabilities and reliance on signature-based methodologies, traditional intrusion detection systems frequently fall short in identifying new threats. This study suggests an integrated method for intrusion detection and attack classification utilising deep learning and intelligent machine learning approaches in order to address these issues. Network traffic data collection, preprocessing, feature extraction and selection, intrusion detection, and multi-class attack categorization are some of the steps that make up the suggested framework. To improve detection accuracy and categorise assaults into groups including Denial of Service (DoS), Distributed DoS (DDoS), Probe, Remote-to-Local (R2L), User-to-Root (U2R), and malware incursions, a hybrid deep learning model is used. In order to facilitate real-time response and mitigation, the system also includes an alert production mechanism. Comparing the suggested integrated model to traditional IDS techniques, experimental results on benchmark intrusion datasets show that it improves classification performance, lowers false positive rates, and increases accuracy. All things considered, the suggested framework offers a scalable and effective way to handle proactive cyber threat management and next-generation network security.

Keywords: Intrusion Detection System, Attack Classification, Cybersecurity, Deep Learning, Machine Learning, CNN-LSTM, Network Traffic Analysis, Feature Selection, DoS Attacks, IoT Security.

Introduction

This proposed model presents innovative deep learning techniques. Here, developing a trustworthy intrusion detection system to assist

in spotting malevolent attempts is the goal. Three methods are used in the development of a deep learning-based solution framework. Adamax, SGD, Adagrad, Adam, RMSprop, Nadam, and Adadelta are among the seven optimiser functions of the first method, which uses a Long-Short Term Memory Recurrent Neural Network (LSTM-RNN). The NSL-KDD dataset is used to assess the model and classify several attacks.[1]The rapid development of Internet of Things (IoT) devices has created a more complicated threat landscape, making it difficult for conventional Intrusion Detection Systems (IDS) to manage the enormous and varied amounts of data produced by IoT networks. This study introduces an innovative IDS for optimised feature selection that combines Quantum-Inspired Particle Swarm Optimisation (QIPSO) with Adaptive Neuro-Fuzzy Inference System (ANFIS).[2]With the most recent developments in information and communication technology, more private user and business data is constantly transmitted over the network, increasing its vulnerability to attacks that could jeopardise data availability, confidentiality, and integrity. Intrusion Detection Systems (IDS) are crucial security tools that may quickly identify malicious activity by examining host-based logs or network traffic.[3]Vehicles and infrastructures can communicate wirelessly thanks to vehicular ad hoc networks, or VANETs. In smart cities and Intelligent Transportation Systems (ITSs), connected cars hold great promise. Enhancing road safety, comfort, driving efficiency, and waiting times is VANET's primary goal.[4]An intrusion detection system (IDS) that can quickly and automatically identify and categorise cyberattacks at the host and network levels is being developed using machine learning techniques. However, a scalable solution is needed since malicious attacks are always evolving and happening in enormous quantities.[5]Due to their ability to identify complex Advanced Persistent Threat (APT) attacks, provenance-based intrusion detection systems (IDSes) have recently become more and more common. To find potentially harmful activity, these IDSes use provenance graphs made from system logs.[6] Although it directly affects the availability of services provided by IoT devices and the privacy of users connected to the network, researchers and business owners place a high priority on IoT network security.[7]Our lives have been profoundly improved in many ways by the advent of innovative technologies like artificial intelligence, cloud computing, big data driven by the Internet, and its highly prized real-world applications that comprise symmetric and asymmetric data distributions.[8]

Related Work

In order to protect contemporary computer networks against malicious activity, unauthorised access, and cyberattacks, intrusion detection systems, or IDS, are essential. Access control and firewalls are no longer adequate security measures due to the explosive rise of cloud computing, Internet-based applications, and IoT-enabled environments. As a result, a lot of research has gone into creating sophisticated methods for attack classification and intrusion detection. The majority of early intrusion detection strategies relied on signature-based approaches, which use pre-established attack patterns. These systems are successful in identifying existing assaults, but they are unable to detect new and emerging threats. Anomaly-based detection techniques, which treat unusual departures from typical network behaviour as possible intrusions, were developed to get around this restriction. However, high false alarm rates are a common problem with anomaly detection.

Proposed System Architecture

The proposed architecture offers an intelligent and integrated framework for efficiently classifying various cyberattack kinds and detecting network breaches. The system integrates machine learning and deep learning approaches to improve detection accuracy, lower false alarms, and facilitate multi-class attack classification in light of the growing complexity of network environments and changing attack patterns.

The architecture's multi-layered structure guarantees effective network traffic data processing from acquisition to ultimate decision-making.

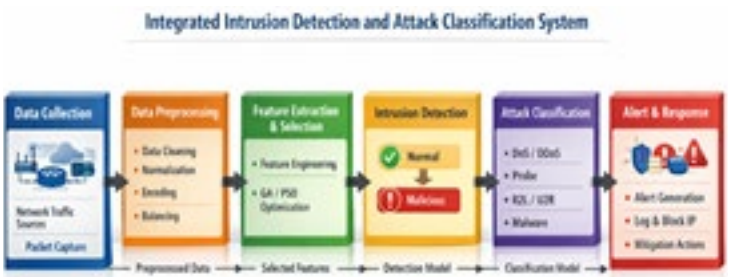

Fig -1 Integrated Intrusion Detection and Attack Classification System

Data Collection Layer

The proposed architecture's initial phase is dedicated to gathering network traffic data from multiple sources, including:

- Routers and switches
- IoT devices
- Cloud servers
- Enterprise networks
- Packet sniffers and monitoring tools

Important details like IP addresses, protocols, ports, packet sizes, and flow statistics are all included in the traffic that has been gathered. For training and validation, standard benchmark datasets like NSL-KDD, CICIDS-2017, and UNSW-NB15 can also be used.

Data Preprocessing Layer

The Noise, missing values, redundant features, and inconsistent formats are common in raw network traffic data. Preprocessing is therefore necessary to enhance model performance. This layer does the following:

- Data cleaning and removal of irrelevant features
- Handling missing or null values
- Feature normalization and scaling
- Encoding categorical attributes (e.g., protocol types)
- Dataset balancing using oversampling/under sampling methods

By doing this, the input data is guaranteed to be appropriate for successful learning.

Feature Extraction and Selection Layer

In order to effectively depict traffic behaviour, significant network features are extracted at this stage. Feature engineering aids in the reduction of computing complexity and dimensionality. The structure uses:

- Statistical feature extraction
- Correlation analysis
- Optimization-based feature selection (GA/PSO)
- Automated deep feature learning

The objective is to choose the most pertinent characteristics that support precise attack classification and intrusion detection.

Integrated Detection and Classification Layer

This is the suggested architecture's central stratum. It combines attack classification and intrusion detection into a single model.

Intrusion Detection Module

The intrusion detection module identifies whether incoming traffic is:

- Normal
- Suspicious
- Malicious

To identify anomalous behaviour, binary classification techniques like Random Forest or Deep Neural Networks are used.

Algorithm

The suggested technique unifies attack classification and intrusion detection into a single framework. It uses machine learning and deep learning techniques to process network traffic data, identify anomalous activity, and categorise assaults into several groups.

Input

Network traffic dataset D
Feature set F
Pre-trained detection model M_d
Pre-trained classification model M_c

Output

Intrusion detection result (Normal / Malicious)
Attack class label (DoS, Probe, R2L, U2R, DDoS, etc.)
Alert generation for identified attacks

Step 1: Data Collection

Capture real-time network traffic packets.
Extract flow-based traffic records.
Store collected data into dataset D.

Step 2: Data Preprocessing

Remove missing values and noise from D.
Normalize numerical features using Min–Max scaling.
Encode categorical attributes (protocol, service type).
Balance dataset using oversampling or under sampling methods.

Step 3: Feature Extraction and Selection

Extract relevant traffic features F.
Apply feature selection techniques (e.g., GA/PSO/Correlation).
Reduce dimensionality for faster computation.

Step 4: Intrusion Detection Phase

For each network instance $x_i \in D$:
Predict intrusion label using detection model:
$y_d = M_d(x_i)$
If y_d=Normal:
Mark traffic as legitimate.
Continue monitoring.
Else if y_d=Malicious:
Forward instance to attack classification module.

Implementations

The development of an intelligent framework that can recognise malicious network activity and accurately categorize attack types is the main goal of the proposed integrated intrusion detection and attack classification system's implementation. To provide reliable cybersecurity monitoring in real-time settings, the system integrates preprocessing, feature engineering, deep learning-based detection, and multi-class classification.

Dataset Implementation

To validate the proposed approach, standard benchmark intrusion detection datasets are used, such as:

- NSL-KDD Dataset
- CICIDS-2017 Dataset
- UNSW-NB15 Dataset

These datasets contain labeled network traffic records representing both normal behavior and multiple attack types including DoS, Probe, R2L, and U2R attacks.

Data Preprocessing Implementation

Missing numbers, irrelevant attributes, and an imbalance between normal and attack records are common in raw network traffic data. Consequently, the following procedures are used to implement preprocessing:

Data Cleaning

- Removal of duplicate entries
- Handling missing or null values

Normalization

Numerical features are normalized using Min–Max scaling:

X^'=(X-X_min)/(X_max-X_min)

This improves learning convergence in deep neural networks.

Encoding

Categorical features such as protocol type and service are converted into numerical form using:

- One-hot encoding
- Label encoding

Conclusion

In order to improve the security of contemporary network settings, this study offered an integrated method for intrusion detection and attack classification. Traditional security measures are unable to identify sophisticated and changing threats due to the growing complexity and frequency of cyberattacks. The suggested framework successfully integrates intelligent intrusion detection, feature extraction, data preprocessing, and multi-class attack categorization into a single system. The architecture correctly classifies many attack types, including DoS, Probe, R2L, U2R, and other network-based incursions, and successfully detects malicious activity. In comparison to traditional intrusion detection techniques, the system increases detection accuracy while decreasing false positive rates by integrating machine learning and deep learning models, especially hybrid architectures like CNN-LSTM. The integrated approach offers dependable performance, real-time

monitoring capability, and improved cybersecurity response, as demonstrated by experimental implementation on benchmark datasets. All things considered, the suggested strategy supports proactive defence against new cyberthreats by providing an effective and scalable solution for next-generation intrusion detection systems.

References

1. A. K. Silivery, R. M. Rao Kovvur, R. Solleti, L. S. Kumar, and B. Madhu, "A model for multi-attack classification to improve intrusion detection performance using deep learning approaches," Measurement: Sensors, vol. 30, Dec. 2023, doi: 10.1016/j.measen.2023.100924.
2. G. Logeswari, J. Deepika Roselind, K. Tamilarasi, and V. Nivethitha, "A Comprehensive Approach to Intrusion Detection in IoT Environments Using Hybrid Feature Selection and Multi-Stage Classification Techniques," IEEE Access, vol. 13, pp. 24970–24987, 2025, doi: 10.1109/ACCESS.2025.3532895.
3. N. Oliveira, I. Praça, E. Maia, and O. Sousa, "Intelligent cyber attack detection and classification for network-based intrusion detection systems," Applied Sciences (Switzerland), vol. 11, no. 4, pp. 1–21, Feb. 2021, doi: 10.3390/app11041674.
4. A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification Approach for Intrusion Detection in Vehicle Systems," Wireless Engineering and Technology, vol. 09, no. 04, pp. 79–94, 2018, doi: 10.4236/wet.2018.94007.
5. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
6. M. Ur Rehman, H. Ahmadi, and W. Ul Hassan, "Flash: A Comprehensive Approach to Intrusion Detection via Provenance Graph Representation Learning," in Proceedings - IEEE Symposium on Security and Privacy, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 3552–3570. doi: 10.1109/SP54263.2024.00139.
7. R. Qaddoura, A. M. Al-Zoubi, H. Faris, and I. Almomani, "A multi-layer classification approach for intrusion detection in iot networks based on deep learning," Sensors, vol. 21, no. 9, May 2021, doi: 10.3390/s21092987.
8. E. Jaw and X. Wang, "Feature Selection and Ensemble-Based Intrusion Detection System: An Efficient and Comprehensive Approach," Symmetry (Basel)., vol. 13, no. 10, p. 1764, Sep. 2021, doi: 10.3390/sym13101764.
9. Ravikumar, D., T. Jaya, S. Harish Kumar, R. Vishal, R. Rokesh, and S. Hariharan. FMNet: A novel hybrid face mask detection using deep learning." In AIP Conference Proceedings, vol. 2463, no. 1, p. 020021. AIP Publishing LLC, 2022.
10. Devi, V., and D. Ravikumar. "Segmentation and Classification of Image Abnormalities in Retinal Fundus using Discrete Wavelet Transforms." International Journal of Recent Technology and Engineering,(IJRTE) 8, no. 4 (2019): 11357-11360.
11. Ravikumar, D., Arun Raaza, V. Devi, and E. Gopinathan. "A genetic algorithm approach for global routing of VLSI circuits." International Journal of Engineering &Technology 7, no. 2.21 (2018): 394-397.
12. Ravikumar, D., and Arun Raaza. "Computational Analysis of Microarray Image.& Jour of Adv Research in Dynamical & Control Systems 9, no. 5 (2017).