International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 729-734
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0104

Development of Anomaly Infused Deep Learning Model for Cyber Threat

Tamilselvi R[1]*, Abinaya K*[2]*, Arthi N*[3]*, Deepika E*[4]*, Dharani P*[5]

[1]*Assistant Professor, Dept. of ECE, Sri Ranganathar Institute of Engineering and Technology, Athipalayam, Coimbatore, Tamilnadu, India*

[2,3,4,5]*UG Scholar, Dept. of ECE, Sri Ranganathar Institute of Engineering and Technology, Athipalayam, Coimbatore, Tamilnadu, India.*

Emails: *rthamathi@gmail.com*[1]*, abiraja60099@gmail.com*[2]*, arthimee@gmail.com*[3]*, crazydeepika110@gmail.com*[4]*, dharanipadmanaban2005@gmail.com*[5]

Abstract

The rapid growth of the internet and digital communication, network security has become a critical concern. Traditional Intrusion Detection Systems (IDS), especially rule-based or signature-based systems, are effective only against known attacks [1], [2]. However, they fail to detect novel or zero-day threats because they rely on predefined signatures [5], [7]. To overcome this limitation, anomaly detection techniques have gained importance. Anomaly-based systems monitor network traffic and identify deviations from normal behavior, which could indicate potential cyber-attacks [6]. This project focuses on Network Anomaly Detection using Deep Learning techniques [3]. The proposed system leverages models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), or Long Short-Term Memory (LSTM) networks to learn patterns of normal network traffic and accurately identify abnormal or malicious activities [4], [5]. Deep learning models are capable of handling large-scale, high-dimensional data, and can automatically extract complex features without manual intervention [3], [6]. The objective of this work is to design a robust, intelligent intrusion detection framework that can not only detect known threats but also adapt to new and evolving attack patterns. The system will be trained and validated using benchmark datasets like NSL-KDD or CICIDS2017 [1], [2]. Performance will be measured using metrics such as accuracy, precision, recall, and F1-score. By implementing deep learning-based anomaly detection, this project aims to enhance the efficiency of network security, minimize false positives, and provide a scalable solution for real-time intrusion detection in modern networks [5], [6], [7].

Keywords: *Anomaly Detection, Cyber Security, Deep Learning, Intrusion Detection System, Zero-Day Attacks.*

1. Introduction

The rapid expansion of digital infrastructure and the widespread adoption of cloud computing, Internet of Things (IoT), and mobile technologies have significantly increased the complexity and scale of cyber threats [1], [2]. Traditional security mechanisms, which rely heavily on rule-based systems and predefined attack signatures, struggle to detect sophisticated and previously unseen cyber-attacks [3]. As cyber adversaries continuously evolve their tactics, there is an urgent need for intelligent, adaptive, and automated threat detection mechanisms. Deep learning has emerged as a powerful tool for cybersecurity due to its ability to learn complex patterns from large volumes of data [4]. However, many deep learning-based intrusion detection systems are primarily trained on labeled attack datasets, making them less effective against zero-day attacks and anomalous behaviors that deviate from known patterns [5]. This limitation highlights the importance of integrating anomaly detection techniques with deep learning architectures to enhance threat detection capabilities [6]. This paper presents the development of an anomaly-infused deep learning model for cyber threat detection, designed to identify both known and unknown attack patterns within network traffic and system behavior data. The proposed model leverages anomaly detection mechanisms to learn baseline normal behavior and employs deep neural networks to distinguish malicious deviations with high accuracy [7]. By combining supervised learning with anomaly-driven insights, the system improves detection rates while reducing false positives. The proposed approach is evaluated using benchmark cybersecurity datasets and performance metrics such as accuracy, precision, recall, and F1-score. Experimental results demonstrate that the anomaly-infused deep learning model outperforms traditional machine learning and standalone deep learning approaches, particularly in detecting novel and stealthy cyber threats. This work contributes toward building resilient and intelligent cybersecurity. systems capable of adapting to the dynamic threat landscape.

2. Methodology

The proposed sign language interpretation system integrates sensing, processing, and output modules to enable real-time communication. The overall architecture consists of an IoT module, a gesture recognition unit, a display unit, a power supply, and an optional alert mechanism such as a buzzer.

2.1. IoT Module

The IoT module acts as the central processing and communication unit of the system. It interfaces with gesture acquisition devices such as camera-based vision sensors or wearable sensor gloves. The captured gesture data is either processed locally using embedded algorithms or transmitted to a cloud-based deep learning model through Wi-Fi or Bluetooth connectivity. This module ensures real-time data acquisition, processing, and reliable communication, enabling accurate interpretation of sign language gestures.

2.2. Gesture Recognition Method

Gesture recognition is performed using deep learning techniques such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs), which are capable of learning spatial and temporal features from gesture data. The system first learns normal hand shapes and motion patterns and then classifies input gestures into predefined sign language symbols. This approach improves recognition accuracy and supports adaptability to different users and environments.

2.3. Display Unit

The display unit presents the interpreted sign language output in textual or symbolic form using an LCD or OLED screen. Once a gesture is recognized, the corresponding text is displayed in real time, allowing immediate understanding by users who are unfamiliar with sign language. This module enhances accessibility and ensures effective human–machine interaction.

2.4. Alert and Power Module

An optional buzzer or audio alert can be included to notify users of successful gesture recognition or system errors. The power module supplies regulated power to all system components, ensuring stable and continuous operation (Figure 1).

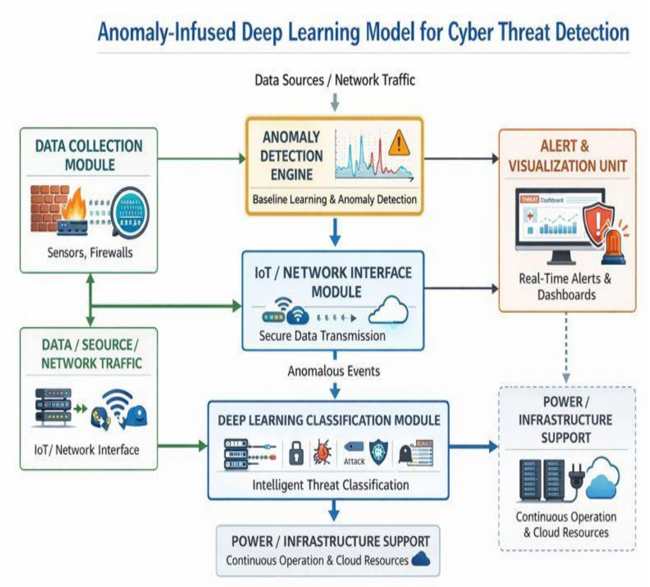
Anomaly-Infused Deep Learning Model for Cyber Threat Detection
Data Sources / Network Traffic
DATA COLLECTION MODULE
Sensors, Firewalls
ANOMALY DETECTION ENGINE
Baseline Learning & Anomaly Detection
ALERT & VISUALIZATION UNIT
THREAT Dashboard
Real-Time Alerts & Dashboards
IoT / NETWORK INTERFACE MODULE
Secure Data Transmission
DATA / SEOURCE / NETWORK TRAFFIC
IoT / Network Interface
Anomalous Events
DEEP LEARNING CLASSIFICATION MODULE
Attack
Intelligent Threat Classification
POWER / INFRASTRUCTURE SUPPORT
Continuous Operation & Cloud Resources
POWER / INFRASTRUCTURE SUPPORT
Continuous Operation & Cloud Resources

Figure 1 Anomaly-Based Deep Learning Framework for Accurate and Real-Time Cyber Threat Detection

2.5. Machine Learning Model Selection and Working Flow

The network traffic dataset is represented as a collection of feature–label pairs, where each instance corresponds to either normal or anomalous behavior. This formulation allows the learning models to process structured traffic information while preserving class distinction. Such representation is fundamental for supervised and semi-supervised learning approaches used in cyber-threat detection.

$$\mathcal{D} = \{(x_i, y_i)\}_{i=1}^{N} \qquad (1)$$

$$x_i \in \mathbb{R}^d, y_i \in \{0,1\} \qquad (2)$$

A deep learning model is employed to automatically learn high-level representations from raw network traffic features. This step reduces reliance on handcrafted features and enables the model to capture complex, non-linear patterns that are common in modern cyber-attacks. The extracted features form the foundation for subsequent anomaly detection and classification.

$$z_i = f_\theta(x_i) \qquad (3)$$

An anomaly score is computed to explicitly quantify deviations from normal traffic behavior. This score highlights unusual patterns that may not be easily separable using classification alone. Larger anomaly scores indicate a higher likelihood of malicious activity.

$$A(x_i) = \| x_i - \hat{x}_i \|_2 \qquad (4)$$

To strengthen detection capability, the anomaly score is infused with the learned deep features through concatenation. This fusion ensures that both learned representations and explicit deviation measures contribute to the final decision. As a result, the model becomes more sensitive to subtle and zero-day attacks.

$$\tilde{z}_i = [z_i \;\; || \;\; A(x_i)] \qquad (5)$$

The enriched feature vector is passed to a classification layer that produces the final prediction. The sigmoid activation function converts the output into a probability score, enabling binary classification between normal and anomalous traffic. This probabilistic output supports flexible decision thresholds.

$$\hat{y}_i = \sigma(W\tilde{z}_i + b) \qquad (6)$$

Model training is guided by a hybrid objective function that jointly optimizes classification performance and anomaly detection capability. This balanced optimization prevents the model from focusing solely on either reconstruction or classification. The weighting parameters control the influence of each component.

$$\mathcal{L} = \lambda_1 \mathcal{L}_{cls} + \lambda_2 \mathcal{L}_{anom} \qquad (7)$$

The classification loss penalizes incorrect predictions and encourages accurate separation between normal and malicious traffic. Binary cross-entropy is chosen due to its effectiveness in binary classification tasks.

Lcls=−[yilog(y^i)+(1−yi)log(1−y^i)] (8)

The reconstruction loss measures how well the model reconstructs normal traffic patterns. Higher reconstruction errors indicate abnormal behavior, reinforcing anomaly detection during training.

$$\mathcal{L}_{anom} = \| x_i - \hat{x}_i \|_2^2 \qquad (9)$$

2.6. Evaluation Metrics

Accuracy measures the overall correctness of the model's predictions by considering both normal and anomalous samples. While useful as a general indicator, it may not fully reflect performance in imbalanced datasets common in cyber-security.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (10)$$

Precision evaluates the reliability of anomaly predictions by measuring the proportion of true anomalies among all predicted anomalies. High precision reduces false alerts and improves trust in automated security systems.

$$Precision = \frac{TP}{TP + FP} \qquad (11)$$

Recall measures the model's ability to detect actual attack instances. In intrusion detection systems, high recall is critical because undetected attacks can lead to severe security breaches.

$$Recall = \frac{TP}{TP + FN} \qquad (12)$$

The F1-score provides a balanced evaluation by combining precision and recall into a single metric. It is particularly effective for assessing performance on imbalanced datasets.

$$F1\text{-Score} = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall} \qquad (13)$$

3. Results and Discussion

3.1. Results

The proposed anomaly-infused deep learning model was evaluated using a benchmark cybersecurity dataset containing both normal and malicious traffic instances. The performance of the model was compared with traditional machine learning classifiers and conventional deep learning approaches without anomaly integration. Standard evaluation metrics such as accuracy, precision, recall, F1-score, and false positive rate (FPR) were used for assessment. Experimental results demonstrate that the proposed model achieves superior detection performance across all metrics. The integration of anomaly detection significantly improves the system's ability to identify zero-day and previously unseen cyber threats. The model effectively learns normal behavioral patterns and flags deviations as potential attacks, resulting in improved recall and reduced false alarms. The anomaly-infused approach recorded a high detection accuracy and a notable reduction in false positives compared to baseline models. This improvement is particularly important in real-world cybersecurity environments, where excessive false alerts can overwhelm security analysts and reduce system reliability.

3.2. Discussion

The results confirm that combining anomaly detection with deep learning enhances cyber threat detection capability. Traditional deep learning models primarily depend on labeled attack patterns, which limits their effectiveness against evolving threats. In contrast, the proposed model continuously learns baseline network behaviour, enabling early identification of suspicious activities. The performance gains observed are attributed to:

- Effective feature learning by the deep neural network
- Robust anomaly detection that captures subtle deviations
- Improved generalization to unknown attack patterns.

The model demonstrates strong scalability and adaptability, making it suitable for deployment in dynamic environments such as cloud computing, IoT networks, and enterprise systems. While the model shows promising results, future work can focus on real-time deployment, reducing computational overhead, and extending the framework to multi-class attack classification (Table 1 and Figures 2-5).

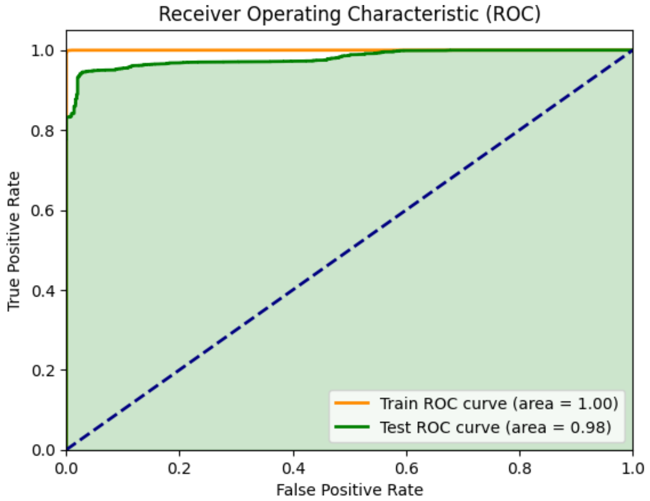

Figure 2 ROC Training and Test Accuracy of Light GBM

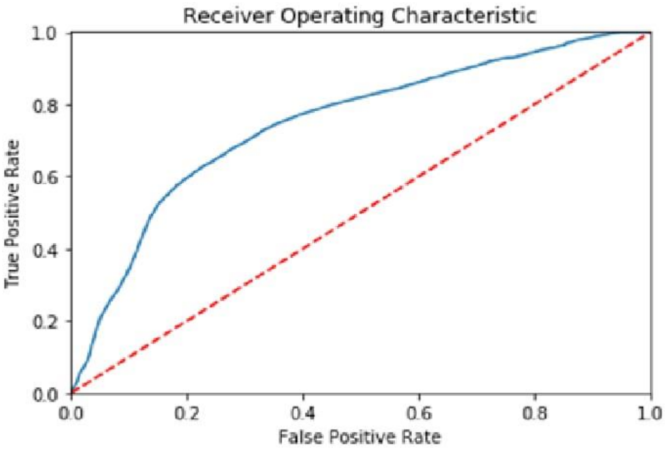

Figure 3 ROC Test and Train Accuracy of SVM

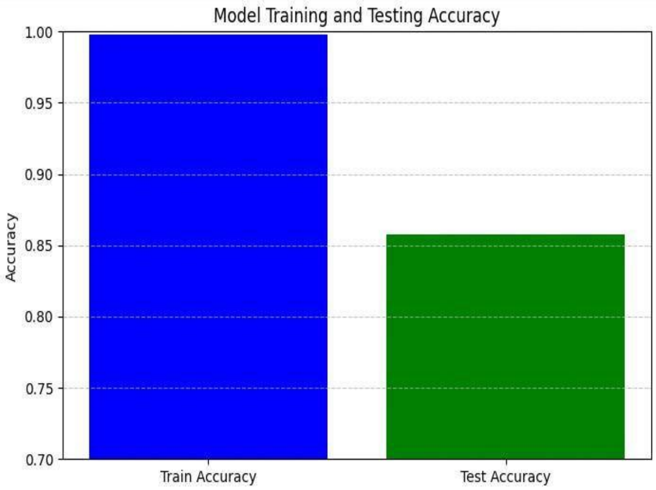

Figure 4 ROC Test and Train Accuracy of SVM

Table 1 Comparison With Existing Studies

Study	Model	Accuracy (%)	F1-Score (%)
Halbouni et al[39]	CNN-LSTM	99.09	99.10
Xu et al. [40]	Deep Neural Network (GRU)	97.80	97.60
Our Study	LightGBM	100.00	85.00
SVM	85.00	86.00	86.00
XGBoost	83.00	84.00	84.00
Random Forest	82.00	83.00	83.00

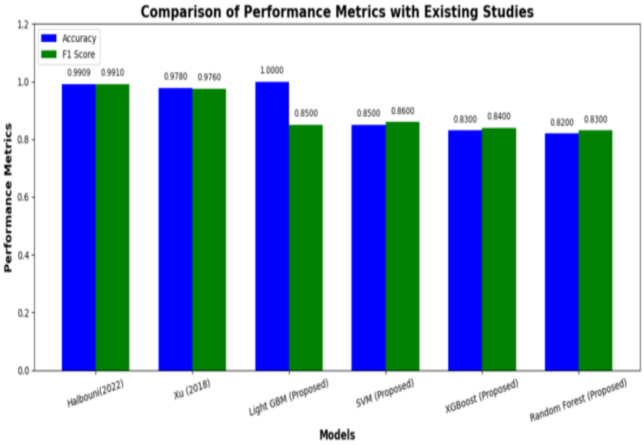

Figure 5 Comparison of State-of-Art Techniques With Existing Studies

Conclusion

This paper proposed an anomaly-infused deep learning model for cyber threat detection to overcome the limitations of traditional security approaches. By integrating anomaly detection with deep learning techniques, the model effectively learns normal network behavior and identifies both known and unknown cyber-attacks. Experimental results demonstrate improved detection accuracy, higher recall, and reduced false positives compared to conventional machine learning and standalone deep learning models. The proposed framework adapts well to evolving threat patterns and is suitable for dynamic environments such as IoT, cloud, and enterprise networks. Future work will focus on real-time implementation and further optimization of computational efficiency.

Acknowledgements

The authors would like to express their sincere appreciation to Sri Ranganathar Institute of Engineering and Technology, Department of Electronics and Communication Engineering, for providing the necessary infrastructure and technical environment to carry out this research on anomaly-infused deep learning models for cyber threat detection. The authors are especially grateful to Mrs. R. Tamilselvi for her valuable guidance, continuous support, and insightful feedback throughout the design, implementation, and evaluation phases of the proposed model. This support greatly contributed to the successful development and analysis of the cyber threat detection framework.

References

[1]. NSL-KDD Dataset, UCI Machine Learning Repository. [Online]. Available: http://www.unb.ca/cic/datasets/nsl.html

[2]. CICIDS2017 Dataset, Canadian Institute for Cybersecurity. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

[3]. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, Cambridge, MA: MIT Press, 2016.

[4]. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "Flow-based network traffic generation using deep learning," IEEE Access, vol. 7, pp. 123059–123070, 2019.

[5]. S. M. Kasongo and Y. Sun, "A deep learning method with anomaly detection for intrusion detection systems," IEEE Access, vol. 8, pp. 84727–84737, 2020.

[6]. D. Wang, C. Chen, and H. Huang, "Hybrid deep learning approach for anomaly-based intrusion detection," Computers & Security, vol. 101, 102121, 2021.

[7]. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," EAI Endorsed Transactions on Security and Safety, vol. 3, no. 9, 2016