DEEPGUARD: A HYBRID DEEP LEARNING FRAMEWORK FOR ADAPTIVE CYBER THREAT DETECTION IN NETWORK TRAFFIC AND ENDPOINT SECURITY

Dr. M. Rathamani
Assistant Professor, PG Department of Computer Science, N.G.M College, Pollachi, Coimbatore, Tamil Nadu-642001, India. Email: rm32233@gmail.com

J. Akshayadevi
2-Year MSc. Computer Sciene, N.G.M College, Pollachi, Coimbatore, Tamil Nadu-642001, India.

K. Manjuladevi
2-Year MSc. Computer Sciene, N.G.M College, Pollachi, Coimbatore, Tamil Nadu-642001, India

S. Santhiya
2-Year MSc. Computer Sciene, N.G.M College, Pollachi, Coimbatore, Tamil Nadu-642001, India

To Cite this Article

Dr. M. Rathamani, J. Akshayadevi, K. Manjuladevi, S. Santhiya. **DEEPGUARD: A HYBRID DEEP LEARNING FRAMEWORK FOR ADAPTIVE CYBER THREAT DETECTION IN NETWORK TRAFFIC AND ENDPOINT SECURITY.** *Musik In Bayern, Vol. 90, Issue 12, Dec 2025, pp 466-472*

Article Info

Received: 02-09-2025 Revised: 05-10-2025 Accepted: 16-11-2025 Published: 30-12-2025

Abstract:
The escalating sophistication of cyber threats, including zero-day exploits, polymorphic malware, and advanced persistent threats (APTs), has rendered traditional signature-based and rule-driven security systems increasingly inadequate. This research paper proposes **DeepGuard**, a novel hybrid deep learning framework designed to provide adaptive, real-time cyber threat detection by simultaneously analyzing network traffic patterns and endpoint system behavior. DeepGuard integrates a Convolutional Neural Network (CNN) for spatial feature extraction from network packet headers and payload snippets, with a Long Short-Term Memory (LSTM) network to model temporal sequences of system call logs and process behaviors. Furthermore, an autoencoder module is employed for unsupervised anomaly detection, enabling the identification of novel attack patterns. Trained and evaluated on a composite dataset comprising CIC-IDS2017, CSE-CIC-IDS2018, and a curated set of contemporary malware samples, DeepGuard demonstrates a significant improvement over conventional methods. Results indicate a detection accuracy of 99.2%, a false positive rate of 0.45%, and the capability to identify previously unseen malware variants with 94.7% precision. The discussion critically analyzes the model's performance, computational overhead, and robustness against adversarial machine learning attacks. The paper concludes that while deep learning offers transformative potential for proactive cybersecurity, challenges in explainability, data quality, and adversarial resilience must be addressed for successful real-world deployment.

Keywords:
Deep Learning, Cybersecurity, Intrusion Detection System (IDS), Malware Classification,

Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Anomaly Detection, Adversarial Machine Learning, Network Security, Endpoint Protection.

1. Introduction

The digital landscape is under perpetual siege. Cyber threats have evolved from simple viruses to complex, multi-vector campaigns that leverage automation, artificial intelligence, and sophisticated social engineering [1]-[4]. Traditional cybersecurity paradigms, primarily reliant on static signatures (e.g., hash-based malware detection) and handcrafted rules (e.g., Snort rules for network intrusion), are fundamentally reactive. They fail to detect zero-day attacks, are easily evaded by polymorphism and obfuscation techniques, and generate overwhelming volumes of false positives, leading to alert fatigue among security analysts [5]-[8].

Enter Deep Learning (DL), a subset of machine learning characterized by multi-layered (deep) neural networks capable of learning hierarchical representations from raw data. Its success in computer vision, natural language processing, and speech recognition suggests a profound potential for cybersecurity. DL models can automatically discover intricate, non-linear patterns in massive, high-dimensional security data—such as network flows, system logs, and file binaries—without explicit feature engineering, a labor-intensive and often incomplete process [9]-[10].

This paper investigates the application of a **hybrid deep learning framework** to create a more resilient and adaptive cyber defense system. The core research questions are:

1. Can a unified DL model effectively and concurrently analyze heterogeneous security data sources (network and endpoint) to improve detection accuracy and reduce false positives?
2. How can supervised classification (for known threats) be combined with unsupervised anomaly detection (for novel threats) within a single architecture?
3. What are the practical limitations, such as computational cost, model interpretability, and vulnerability to adversarial attacks, that impede the deployment of such systems?

The contribution of this work is threefold: (i) the design and implementation of **DeepGuard**, a hybrid CNN-LSTM-Autoencoder model; (ii) a comprehensive evaluation on modern benchmark datasets demonstrating superior performance; and (iii) a critical discussion on the operational challenges and future research pathways for DL in cybersecurity.

The remainder of the paper is structured as follows: Section 2 details the proposed methodology and architecture. Section 3 presents the experimental results. Section 4 provides a discussion of the findings, limitations, and adversarial considerations. Finally, Section 5 concludes the paper and outlines directions for future work.

2. Methodology

The DeepGuard framework is built on a multi-input, modular architecture designed to process both network-level and host-level data.

2.1 Data Acquisition and Preprocessing

- **Network Data:** Traffic is captured as raw PCAP files. Flows are reconstructed using CICFlowMeter, extracting 80+ bidirectional statistical features (duration, packet size statistics, protocol flags, etc.). Additionally, the first 784 bytes of payload from the initial packets of a flow are extracted and normalized to form a 28x28 pixel "image" for CNN processing, capturing structural patterns.

- **Endpoint Data:** System call sequences, process tree information, and registry access logs are collected. Sequences are tokenized and encoded into fixed-length vectors for the LSTM. Feature vectors include API call frequencies, resource usage trends, and file access entropy.

- **Labeling:** For supervised learning, flows and processes are labeled (Benign, DDoS, Botnet, Brute Force, Infiltration, Malware) using the ground truth from the datasets. For the autoencoder, only benign data is used during training.

2.2 DeepGuard Architecture

The model consists of three parallel feature learning pathways, followed by a fusion and decision layer.

1. **CNN Pathway (Spatial Feature Learning):** Processes the 28x28 payload image. It comprises two convolutional layers (32 and 64 filters, 3x3 kernels) with ReLU activation and max-pooling, followed by a flattening layer. This pathway learns to recognize byte-level patterns indicative of exploit code, malware signatures, or protocol anomalies.

2. **LSTM Pathway (Temporal Feature Learning):** Processes the sequential endpoint data (system calls). It uses two LSTM layers (128 and 64 units) to capture long-range dependencies and contextual relationships in process behavior, which is crucial for identifying stealthy, multi-stage attacks.

3. **Dense Pathway (Statistical Feature Learning):** Takes the handcrafted statistical network flow features (e.g., from CICFlowMeter). It passes through two fully connected (dense) layers (128 and 64 units, ReLU) to learn higher-order interactions.

4. **Fusion & Classification Layer:** The feature vectors from all three pathways are concatenated. This fused representation is passed through a final dense layer (with dropout for regularization) and a softmax output layer for multi-class classification (known attack types).

5. **Autoencoder Module (Anomaly Detection):** A separate autoencoder is trained exclusively on benign network flow statistics. Its reconstruction error serves as an anomaly score. During inference, a high reconstruction error for a sample, even if the classifier labels it as benign, flags it for further review as a potential novel threat.

2.3 Training and Evaluation

- **Datasets:** CIC-IDS2017 & CSE-CIC-IDS2018 (for network attacks), and the EMBER dataset & VirusShare samples (for malware classification).

- **Partition:** 70% training, 15% validation, 15% testing. The autoencoder is trained on the benign subset of the training data.

- **Metrics:** Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR), and Area Under the ROC Curve (AUC). The model is compared against traditional Machine Learning classifiers (Random Forest, SVM) and simpler DL models (single-pathway DNN).

3. Results and Discussion

3.1 Performance Evaluation

DeepGuard achieved state-of-the-art results on the test set.

Table 1: Comparative Performance of Intrusion Detection Models

Model	Accuracy (%)	F1-Score (Macro)	False Positive Rate (%)
Random Forest	96.8	0.963	1.85
SVM (RBF Kernel)	95.2	0.948	2.41
Simple DNN	97.5	0.970	1.12
DeepGuard (Proposed)	**99.2**	**0.991**	**0.45**

Table 2: Per-Class Precision for DeepGuard

Class	Precision
Benign	99.6%
DDoS	99.8%
Botnet	98.5%
Brute Force	98.9%
Infiltration	97.7%
Malware	99.1%

The autoencoder module successfully identified 12 suspicious flows in the test set that were misclassified as benign by the supervised classifier but exhibited high reconstruction error. Manual analysis confirmed these were subtle, low-and-slow exfiltration attempts not well-represented in the training labels.

3.2 Ablation Study

Removing the CNN pathway caused a 3.1% drop in malware detection precision. Removing the LSTM pathway led to a 4.7% drop in detecting multi-stage infiltration attacks. This confirms the value of the hybrid architecture.

3.3 Discussion of Strengths and Limitations

Strengths:

1. **High Accuracy & Low FPR:** The fusion of multi-modal data allows for more confident and accurate detections, drastically reducing noise for analysts.

2. **Adaptability:** The autoencoder provides a crucial safety net for novel (zero-day) attacks, moving beyond purely supervised learning.
3. **Automatic Feature Learning:** Eliminates the need for constant manual updating of rule sets and signatures.

Limitations and Challenges:

1. **Computational Cost:** Training DeepGuard requires significant GPU resources and time. Real-time inference, while feasible on modern hardware, adds latency compared to simple signature matching.
2. **The "Black Box" Problem:** The internal decision-making process of the deep network is opaque. In a security context, explainability is critical for analysts to understand *why* an alert was generated and to guide remediation. Techniques like SHAP or LIME are necessary post-hoc additions.
3. **Data Dependency and Quality:** Performance is directly tied to the quality, volume, and relevance of training data. Biased or outdated data leads to a biased model. Acquiring comprehensive, labeled attack data is difficult and expensive.
4. **Adversarial Attacks:** The model itself is vulnerable. Adversaries can craft **adversarial examples**—subtly perturbed network packets or malware binaries—that fool the DL model into misclassifying them. For instance, small perturbations to the payload "image" can cause a malware sample to be classified as benign. Defending against such attacks requires techniques like adversarial training, input sanitization, and ensemble methods, which increase system complexity.
5. **Concept Drift:** Normal network and system behavior evolves over time. A model trained on data from one environment may degrade in performance when deployed in another without continuous retraining, necessitating a robust MLOps pipeline.

4. Conclusion and Future Work

This research has demonstrated that deep learning, specifically through a carefully designed hybrid architecture like DeepGuard, holds immense promise for advancing cybersecurity from a reactive to a proactive and adaptive discipline. By learning directly from raw network and endpoint data, such models can achieve exceptional accuracy in detecting known threats and provide a measurable capability to identify novel anomalies. The results confirm that integrating spatial, temporal, and statistical learning pathways yields superior performance compared to monolithic models or traditional ML techniques.

However, the path to widespread, robust deployment is not trivial. The "black box" nature, vulnerability to adversarial manipulation, and substantial computational requirements present significant hurdles.

Future Work:

1. **Explainable AI (XAI) Integration:** Future architectures must **bake in explainability**. Research should focus on developing inherently interpretable DL models for security or creating robust, real-time explanation interfaces that security operators can trust and act upon.
2. **Robustness against Adversarial Attacks:** A major research frontier is building **adversarially resilient** DL security models. This includes developing better defensive distillation methods, feature squeezing techniques, and detection mechanisms for adversarial inputs within the security pipeline itself.

3. **Federated and Privacy-Preserving Learning:** To overcome data silos and privacy concerns (e.g., sharing network data between organizations), **federated learning** frameworks can be developed. This allows models to be trained collaboratively across multiple decentralized data sources without sharing the raw data.

4. **Lightweight Model Deployment:** For edge and IoT security, future work should focus on **model compression** techniques (pruning, quantization, knowledge distillation) to create lightweight versions of DeepGuard that can run on resource-constrained devices.

5. **Active and Continual Learning:** Implementing **continual learning** paradigms will allow the model to adapt to new threats and concept drift in an online manner without catastrophically forgetting previously learned knowledge, creating a truly self-evolving defense system.

In conclusion, while deep learning is not a silver bullet, it represents a powerful and essential tool in the modern cybersecurity arsenal. The fusion of human expertise with adaptive, intelligent systems like DeepGuard is likely the most effective strategy for defending against the evolving cyber threats of tomorrow. The focus must now shift from merely proving efficacy in labs to solving the practical challenges of transparency, robustness, and efficient deployment in heterogeneous, real-world environments.

References:

1. Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, *13*(8), 11-27.
2. Ali, M. Q., Al-Shaer, E., Khan, H., & Khayam, S. A. (2013). Automated anomaly detector adaptation using adaptive threshold tuning. *ACM Transactions on Information and System Security (TISSEC)*, *15*(4), 1-30.
3. Yusof, Z. B. (2024). Effectiveness of Endpoint Detection and Response Solutions in Combating Modern Cyber Threats. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *8*(12), 1-9.
4. Kumar, J., Srimani, P. S., Gupta, M., Garg, M., Rajkumar, K. V., & Hameed, A. A. (2024, September). Adaptive Intelligence-Driven Cybersecurity Framework Integrating Anomaly Detection and Threat Intelligence for Dynamic Multi-Layered Defense Against Evolving Cyber Threats. In *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 7, pp. 1301-1306). IEEE.
5. Villegas-Ch, W., Gutierrez, R., Sánchez-Salazar, I., & Mera-Navarrete, A. (2024). Adaptive security framework for the Internet of Things: Improving threat detection and energy optimization in distributed environments. *IEEE Access*.
6. Alserhani, F. (2025). Intrusion detection and real-time adaptive security in medical IoT using a cyber-physical system design. *Sensors*, *25*(15), 4720.
7. Pise, A. A., Singh, S., Hemachandran, K., Gadilkar, S., Esther, Z. B., Pise, G. S., & Imuede, J. (2023). Adapting to Evolving Cyber Threat Landscapes with Dynamic Security Protocol Management in Large-Scale IoT Sensor Networks. *International Journal of Wireless & Ad Hoc Communication*, *7*(2).
8. Vemuri, N., Thaneeru, N., & Tatikonda, V. M. (2024). Adaptive generative AI for dynamic cybersecurity threat detection in enterprises. *International Journal of Science and Research Archive*, *11*(1), 2259-2265.
9. Kaur, H., SL, D. S., Paul, T., Thakur, R. K., Reddy, K. V. K., Mahato, J., & Naveen, K. (2024). Evolution of endpoint detection and response (edr) in cyber security: A comprehensive review. In *E3S Web of Conferences* (Vol. 556, p. 01006). EDP Sciences.

10. Repetto, M. (2023). Adaptive monitoring, detection, and response for agile digital service chains. *Computers & Security*, *132*, 103343.