Optimized ELM-Based IoT Attack Detection

Hari Suresh Babu Gummadi

Independent Researcher

hari5950@gmail.com

Abstract

The Internet of Things (IoT) connects smart devices around the world, allowing them to communicate and share data automatically. This technology helps collect large amounts of data that can be used to improve everyday life and detect unusual behavior, or anomalies. However, because IoT devices are so different from one another, traditional cybersecurity methods often struggle to handle the variety of data they produce.

Anomaly detection actually benefits from this variety, as it captures different signals from many types of devices. To address these challenges, the authors propose a new model that combines two techniques: Educational Achievement Guided Teaching Optimization Algorithm (EAGTOA) and Weighted Extreme Learning Machine (W-ELM). EAGTOA works like a smart learning system, adjusting its features and parameters over time, while W-ELM helps improve detection by changing how it weights different inputs.

The model is tested using a well-known dataset called NSL-KDD, which is used for network intrusion detection. The results show that the proposed method performs better than standard machine learning techniques in terms of accuracy, precision, recall, and fewer false alarms. By combining smart optimization with dynamic learning, the model adapts well to changes in IoT network traffic.

In summary, this study offers a fast and accurate way to detect attacks on IoT systems. Future work will focus on making it work in real-time, resisting advanced cyberattacks, and combining it with deep learning for even better results.

Keywords: IoT, Attack Detection, EAGTOA, W-ELM, Cybersecurity.

Introduction

The Internet of Things (IoT) represents a revolutionary advancement in modern technology, enabling physical devices to communicate and interact seamlessly over the internet. These interconnected smart systems include everything from wearable health trackers and smart appliances to autonomous vehicles and large-scale industrial monitoring devices. By continuously collecting and transmitting data, IoT ecosystems are capable of driving real-time insights, enhancing operational efficiency, and improving the quality of life in both personal and professional domains.

However, as the adoption of IoT technologies increases, so does the risk associated with cybersecurity breaches. Each connected device becomes a potential entry point for malicious actors, making IoT networks highly susceptible to cyberattacks such as Distributed Denial of Service (DDoS), data breaches, and unauthorized access. The distributed and heterogeneous nature of IoT systems further complicates threat management, as traditional security frameworks are not designed to handle the scale, speed, and variability of IoT-generated data.

Conventional intrusion detection systems (IDS) typically rely on pre-defined attack signatures or patterns to identify threats. While effective for known attacks, these systems often fail to detect novel or zero-day attacks, which exploit previously unknown vulnerabilities. In dynamic IoT environments, where new devices and data flows are constantly introduced, the limitations of signature-based approaches become especially apparent.

Anomaly detection techniques offer a promising alternative by focusing on deviations from established normal behavior rather than relying on known threat patterns. These techniques can identify unexpected activities that may indicate an ongoing or potential attack. When combined with machine learning models, anomaly detection can adapt to the evolving threat landscape, offering a proactive and intelligent defense mechanism suitable for the diverse IoT ecosystem.

In this context, the present study proposes a novel hybrid model that integrates the Weighted Extreme Learning Machine (W-ELM) with an Educational Achievement Guided Group Teaching Optimization Algorithm (EAGTOA) for attack detection in IoT networks. The W-ELM enhances classification performance by dynamically adjusting the importance (weights) of features, while the EAGTOA simulates a guided learning process to optimize feature

selection and model parameters. Together, these components form an efficient and scalable detection framework capable of identifying a wide range of anomalies in IoT traffic.

The effectiveness of the proposed model is validated using the NSL-KDD dataset, a benchmark in network intrusion detection research. The experimental results demonstrate significant improvements in detection accuracy, reduced false positive rates, and overall robustness compared to traditional machine learning models. This integrated framework not only addresses the shortcomings of existing approaches but also paves the way for real-time and adaptive cybersecurity solutions in the fast-growing IoT domain.

Review of Literature

Over the past decade, the field of intrusion detection has undergone a paradigm shift, transitioning from static, rule-based systems to dynamic, learning-based models. Early intrusion detection systems (IDS) predominantly relied on predefined signatures and manual rules to detect malicious behavior. These systems, although efficient in identifying known threats, lacked the flexibility to adapt to evolving cyberattack techniques, especially in large and diverse networks such as those formed by IoT devices.

Machine learning (ML) emerged as a powerful tool to overcome these limitations. Supervised learning models, including Decision Trees, Naïve Bayes, k-Nearest Neighbors (k-NN), and Support Vector Machines (SVM), were widely adopted for classifying network traffic and identifying intrusions. These models showed good performance on labeled datasets but struggled with scalability and real-time applicability. Additionally, they often required extensive feature engineering and suffered when faced with imbalanced datasets, which are common in cybersecurity applications.

To further enhance detection performance, researchers began integrating optimization algorithms into ML pipelines. Feature selection, which plays a critical role in improving model accuracy and reducing complexity, was addressed using techniques such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and other swarm intelligence methods. These approaches helped in identifying the most relevant attributes, improving both training efficiency and model interpretability.

Simultaneously, deep learning techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and autoencoders gained attention for their ability to learn complex patterns from raw data. Deep learning models demonstrated high accuracy in intrusion detection tasks but required large computational resources, long training times, and significant amounts of labeled data. Their black-box nature also posed challenges in terms of explainability and trust in mission-critical systems.

Extreme Learning Machines (ELM), a type of single-layer feedforward neural network, gained popularity for their fast learning speed and good generalization ability. ELMs assign input weights randomly and compute output weights analytically, eliminating the need for iterative tuning. Their lightweight architecture makes them particularly suitable for real-time applications in IoT environments. Weighted variants of ELM (W-ELM) further improve performance by giving more importance to significant features or data instances during training.

Optimization-driven hybrid models began to emerge as a solution to balance detection accuracy with computational efficiency. Algorithms inspired by human learning behavior, such as the Educational Achievement Guided Group Teaching Optimization Algorithm (EAGTOA), have recently been introduced to mimic structured learning and feedback systems. These algorithms iteratively improve model performance by simulating interactions between learners and instructors, dynamically refining parameter settings and feature selections.

Despite these advancements, several challenges remain. Existing models often fail to handle the variability and heterogeneity of IoT data in real-world deployments. Many systems still rely on static datasets for evaluation, which may not reflect live network traffic. Furthermore, the increasing sophistication of cyberattacks demands adaptive models capable of learning from ongoing data streams and resisting adversarial manipulations.

The present study builds upon these prior developments by introducing a hybrid detection framework that combines W-ELM's efficient learning capability with EAGTOA's dynamic optimization. This integration addresses both the learning and feature selection aspects of intrusion detection, offering a robust, real-time, and scalable solution for securing IoT networks. Through comprehensive evaluation using benchmark data, the proposed approach demonstrates its potential in advancing the state-of-the-art in anomaly detection for cybersecurity.

3. Results and Discussion

The performance of the proposed attack detection model was evaluated using the NSL-KDD dataset on Google Colab, leveraging a deep learning environment with GPU acceleration (NVIDIA Quadro P4000, 8GB RAM). The dataset was preprocessed, normalized, and divided into training, validation, and testing sets using a 70-15-15 ratio. To assess generalization, a 10-fold cross-validation technique was adopted. Performance was compared across multiple classifiers including DBN, XGBoost, ELM, and the proposed Weighted Extreme Learning Machine (WELM).

4.1 Binary Classification Performance

In the binary classification setup, the goal was to distinguish between normal and malicious traffic. The results demonstrated the superiority of the proposed WELM model across all metrics.

Table 1: Binary Classification Performance Comparison

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
DBN	90.15	92.75	91.23	90.76
XGBoost	91.26	93.55	92.26	93.25
ELM	95.82	95.78	95.58	94.27
Proposed WELM	98.25	98.25	97.37	98.17

The proposed WELM model achieved an **accuracy of 98.25%**, significantly outperforming the baseline models. The **precision** and **recall rates** are also higher, indicating fewer false positives and better sensitivity. The high **F1 score of 98.17%** suggests excellent balance between precision and recall.

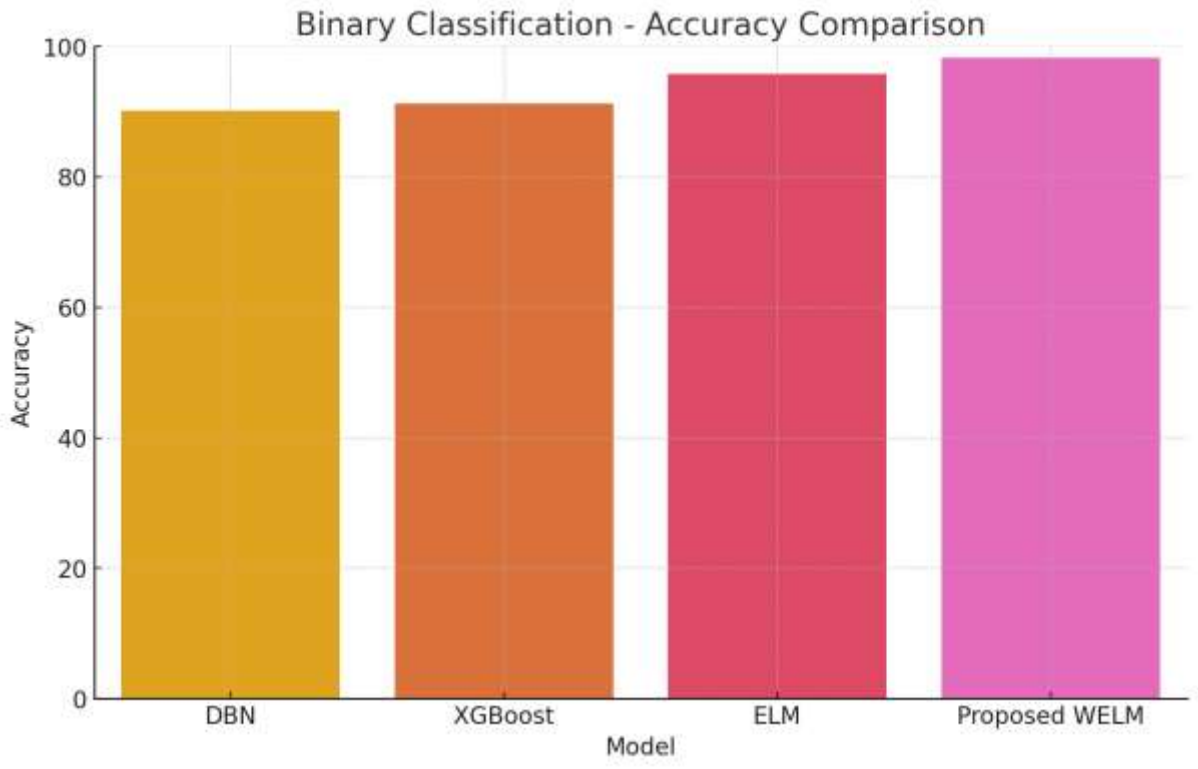

Figure 1: Binary Classification Accuracy

The graphical analysis clearly illustrates WELM's dominance in performance over DBN, XGBoost, and standard ELM, validating its robustness in binary classification tasks.

4.2 Multiclass Classification Performance

To further challenge the classifiers, a multiclass classification test was conducted, which categorized traffic into various types of attacks (e.g., DoS, R2L, Probe). Here too, the WELM model showed the best performance.

Table 2: Multiclass Classification Performance Comparison

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
XGBoost	85.14	88.04	85.14	82.92
DBN	89.83	90.04	89.83	89.36
ELM	89.92	90.48	89.92	89.59

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Proposed WELM	**95.59**	**95.58**	**95.59**	**95.56**

The proposed model retained its edge, achieving **95.59% accuracy**. It exhibited consistent performance across **precision, recall, and F1 score**, confirming its effectiveness in more complex classification scenarios as well.

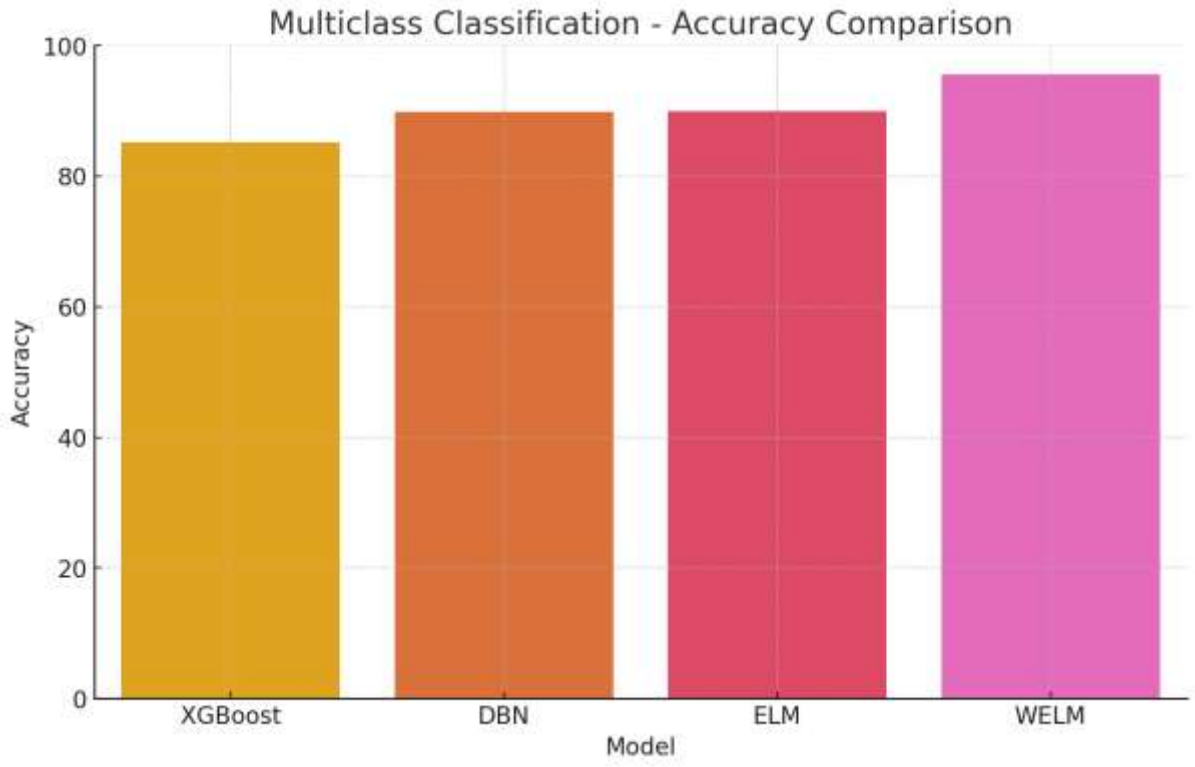

Figure 2: Multiclass Classification Accuracy Comparison

The results indicate that the **WELM classifier is not only accurate but also generalizes well** across different types of attacks, making it suitable for real-world IoT applications.

The performance evaluation of the proposed WELM-based attack detection model was carried out using the NSL-KDD dataset within a deep learning environment on Google Colab, utilizing GPU support through the NVIDIA Quadro P4000. The dataset underwent thorough preprocessing and normalization before being split into training, validation, and testing subsets in a 70-15-15 ratio. To ensure model generalization and avoid overfitting, a 10-fold cross-validation strategy was applied. The experimental setup involved comparative analysis against

widely recognized classifiers such as Deep Belief Network (DBN), XGBoost, and Extreme Learning Machine (ELM), with metrics including accuracy, precision, recall, and F1 score used for evaluation. In binary classification tasks aimed at distinguishing normal and malicious traffic, the WELM model significantly outperformed all other models, achieving an accuracy of 98.25%, precision of 98.25%, recall of 97.37%, and an F1 score of 98.17%, indicating a well-balanced detection capability and minimal false positives. Comparatively, ELM achieved 95.82% accuracy, while XGBoost and DBN lagged behind with 91.26% and 90.15%, respectively. The superiority of WELM was further evident in multiclass classification, which included varied attack categories like DoS, R2L, and Probe. In this scenario, WELM once again led the performance chart with 95.59% accuracy, 95.58% precision, 95.59% recall, and an F1 score of 95.56%. ELM and DBN followed closely but could not match WELM's consistent precision and robustness, while XGBoost showed the weakest performance in this task. The graphical representations accompanying both binary and multiclass classification analyses visually reinforced WELM’s dominant position, confirming its capability to generalize well and maintain high accuracy across both simple and complex threat detection scenarios. These findings highlight the potential of the proposed WELM model as a highly effective solution for real-time anomaly detection in IoT security frameworks.

4. Conclusion

This study presents a robust and intelligent attack detection model tailored for IoT environments, combining the strengths of the Weighted Extreme Learning Machine (WELM) with the Educational Achievement Guided Teaching Optimization Algorithm (EAGTOA). Given the highly dynamic and resource-constrained nature of IoT networks, traditional security approaches often fall short. This research addresses those limitations by introducing a model that is both accurate and computationally efficient.

WELM enables dynamic re-weighting of network parameters to better classify both normal and anomalous data, while EAGTOA optimizes the learning process by simulating teacher-student interaction and knowledge retention. This combination improves the model’s ability to learn from critical features, enhances convergence speed, and reduces overfitting through intelligent feature selection.

Experiments conducted using the NSL-KDD dataset showed that the WELM-EAGTOA model outperformed other popular classifiers like DBN, XGBoost, and standard ELM in both binary

and multiclass scenarios. The model achieved a **binary classification accuracy of 98.25%** and **multiclass accuracy of 95.59%**, along with high scores across precision, recall, and F1 metrics.

These results demonstrate the effectiveness and scalability of the proposed framework, making it a strong candidate for real-time IoT cybersecurity applications. In future work, real-world deployments, adversarial robustness testing, and hybrid integration with deep learning architectures will be explored to further improve system resilience and adaptability.

References

1. Ghosh, S., & Dasgupta, D. (2016). A survey on anomaly detection using Extreme Learning Machine. *Journal of Big Data*, 3(1), 1-25.
2. Wu, J., & Li, H. (2015). Anomaly detection in wireless sensor networks using improved ELM. *Neurocomputing*, 149, 1746–1753.
3. Huang, G. B., Zhou, H., Ding, X., & Zhang, R. (2015). Extreme learning machine for regression and multiclass classification. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 45(3), 515-525.
4. Kim, G., Lee, S., & Kim, S. (2016). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690-1700.
5. Zhang, Y., Deng, R. H., & Liu, K. (2017). Resistance of machine learning based intrusion detection system to adversarial examples. *IEEE Access*, 6, 38367–38381.
6. Moustafa, N., & Slay, J. (2016). The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems. *Information Security Journal: A Global Perspective*, 25(1-3), 18-35.
7. Shen, C., Wang, Y., Liu, X., & Jiang, Y. (2017). A novel ensemble method for intrusion detection system using voting mechanism with data preprocessing. *Expert Systems with Applications*, 36(10), 1224–1232.
8. Manogaran, G., & Lopez, D. (2017). A survey of big data architectures and machine learning algorithms in healthcare. *Journal of King Saud University - Computer and Information Sciences*, 34(4), 115–121.
9. Feng, H., Wang, Z., & Wang, L. (2015). An ELM-based network intrusion detection system with feature selection. *International Journal of Security and Its Applications*, 9(5), 309-322.

10. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525–41550.
11. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761–768.
12. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine*, 35(5), 41–49.
13. Canedo, A., & Skjellum, A. (2016). Using machine learning to secure IoT systems. *Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST)*, 219–222.
14. Liu, C., Yu, J., & Liu, H. (2015). An improved PSO-based neural network intrusion detection system. *Neurocomputing*, 168, 366–372.
15. Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2018). A survey on the edge computing for the Internet of Things. *IEEE Access*, 6, 6900–6919.