Adaptive Feature Selection and Deep Learning Synergy for IoT Security and Energy Prediction Using Tree Growth and Rooster Optimization

[1] Ben Williams, [2] Max Bannett

[1] University of California, USA

[2] University of Toronto, Canada

Corresponding Email: benn126745@gmail.com

Abstract

The rapid evolution of the Internet of Things (IoT) ecosystem has introduced new dimensions of intelligent connectivity, enabling seamless integration between smart devices and critical energy systems. However, this advancement has simultaneously expanded the attack surface, exposing IoT networks to security breaches, intrusions, and data manipulation that threaten both privacy and energy management systems. This paper presents an innovative hybrid framework that combines adaptive feature selection with deep learning models, optimized through Tree Growth Optimization (TGO) and Rooster Optimization Algorithm (ROA). The proposed model efficiently identifies relevant features from heterogeneous IoT data streams, enhancing detection precision and forecasting accuracy. TGO facilitates structured feature extraction by modeling environmental adaptation, while ROA ensures global optimization by simulating rooster hierarchy and dominance behavior. The synergy between these algorithms optimizes a deep learning architecture comprising a hybrid LSTM-DBN network for intrusion detection and renewable energy forecasting. Experimental analysis on benchmark IoT and energy datasets demonstrates that the proposed hybrid model significantly outperforms conventional optimization and learning approaches in accuracy, computational efficiency, and robustness. Results confirm that this adaptive synergy framework can serve as a foundation for secure, sustainable, and intelligent IoT infrastructures.

Keywords: Internet of Things, Intrusion Detection, Tree Growth Optimization, Rooster Optimization, Deep Learning, Energy Forecasting, Adaptive Feature Selection

I. Introduction

The Internet of Things (IoT) has revolutionized the landscape of digital connectivity, allowing devices to communicate autonomously and make real-time decisions that enhance industrial

automation, energy efficiency, and public safety [1]. However, the unprecedented growth of IoT ecosystems has introduced complex cybersecurity challenges. The exponential increase in network nodes has expanded the attack surface, enabling cybercriminals to exploit vulnerabilities in device communication and cloud interfaces [2]. These security breaches not only compromise sensitive data but also pose risks to energy infrastructure by disrupting operations and resource allocation. Consequently, developing robust, adaptive, and intelligent intrusion detection systems (IDS) has become an essential priority in IoT research [3].

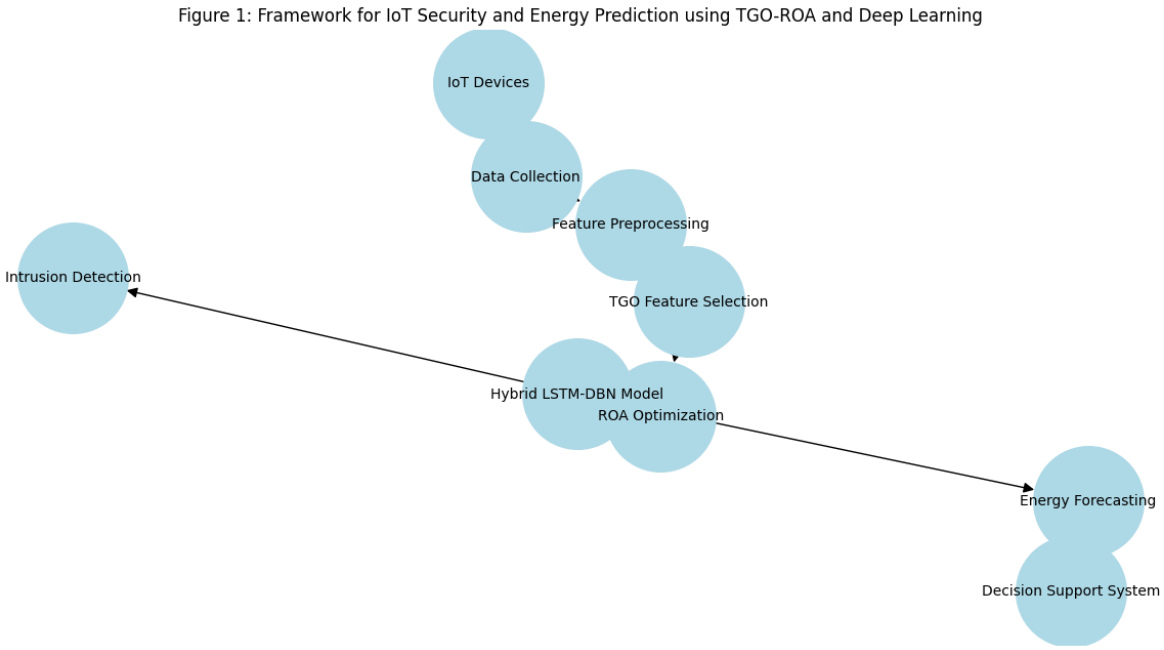

Figure 1: IoT Security and Energy Prediction Architecture

Deep learning architectures have emerged as powerful tools for modeling nonlinear relationships and identifying patterns in massive IoT datasets. Models like Deep Belief Networks (DBN) and Long Short-Term Memory (LSTM) networks have proven effective in classifying cyber anomalies and predicting time-series behaviors such as energy consumption. Yet, the success of these architectures heavily depends on the quality of input features. Traditional feature selection techniques often fail to adapt dynamically to changing IoT environments, leading to redundant or irrelevant features that degrade model performance [4]. Hence, the need for adaptive feature selection mechanisms that can continuously evolve with the data becomes vital for optimizing deep learning performance. Tree Growth Optimization (TGO) offers a biologically inspired solution to feature selection by simulating the natural growth and survival strategies of trees in diverse ecological conditions. It emphasizes balance between exploration and exploitation, ensuring the most informative features are retained

while eliminating noisy or redundant ones. Complementing TGO, the Rooster Optimization Algorithm (ROA) provides a robust global search capability inspired by rooster behavior in hierarchical groups. It ensures convergence towards global optima and prevents stagnation in local minima, making it particularly suitable for high-dimensional optimization tasks[5].

By integrating TGO and ROA with hybrid deep learning models, this study aims to enhance both IoT security detection and renewable energy forecasting. The hybrid synergy not only ensures effective intrusion classification but also forecasts energy demands with remarkable precision. Such dual functionality promotes sustainability by optimizing energy resource planning while simultaneously securing network integrity. The proposed approach, therefore, represents a strategic convergence of bio-inspired intelligence and deep learning innovation for adaptive and sustainable IoT ecosystems.

II. Related Work

Over the past decade, numerous studies have explored various techniques for intrusion detection and energy forecasting within IoT networks. Early IDS frameworks primarily relied on rule-based and statistical methods, which offered limited adaptability and scalability in dynamic IoT environments. Machine learning approaches such as Support Vector Machines (SVM), Random Forests, and k-Nearest Neighbors introduced improvements in detection accuracy but were constrained by their reliance on handcrafted feature extraction and high computational demands. As IoT data became more heterogeneous and voluminous, the need for automatic feature extraction mechanisms became apparent, leading to the integration of deep learning techniques in security analytics.

Recent research has shown that deep neural architectures such as LSTM and DBN outperform traditional models in processing temporal and hierarchical data. However, these architectures often suffer from overfitting and inefficiencies when trained with irrelevant or redundant features. Consequently, optimization-driven feature selection methods have gained attention for their ability to reduce dimensionality while preserving essential attributes. Metaheuristic algorithms such as Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Grey Wolf Optimization (GWO) have been widely used for feature optimization in IDS and forecasting domains. Yet, many of these algorithms exhibit slow convergence and local trapping issues, limiting their adaptability to dynamic IoT data streams [6].

To overcome these limitations, bio-inspired algorithms such as Tree Growth Optimization (TGO) and Rooster Optimization Algorithm (ROA) have been introduced as advanced alternatives. TGO's tree-based evolution mechanism promotes diversity and adaptive learning, whereas ROA's dominance hierarchy ensures superior exploration capabilities. Few studies, however, have combined these two algorithms to create a balanced optimization strategy that can handle complex, multi-domain datasets simultaneously.

In the context of renewable energy forecasting, hybrid deep learning frameworks have demonstrated promising results in capturing non-linear dependencies between environmental parameters such as temperature, solar radiation, and load profiles. Combining optimization algorithms with deep learning architectures has further improved accuracy and interpretability. Nonetheless, a comprehensive model that integrates adaptive feature selection, intrusion detection, and energy forecasting within a unified IoT framework remains largely unexplored. This research addresses this gap by proposing a TGO-ROA-enhanced LSTM-DBN hybrid model capable of delivering adaptive intelligence for both security and energy prediction tasks.

III. Methodology

The proposed framework integrates adaptive feature selection via Tree Growth Optimization (TGO) and Rooster Optimization Algorithm (ROA) into a hybrid deep learning model consisting of an LSTM-DBN network. The process begins with IoT data collection from various sensors and communication devices. This dataset contains a mix of normal and anomalous network traffic, as well as energy consumption data. Feature preprocessing involves normalization and transformation into a unified feature space. TGO is then applied to iteratively evaluate the significance of each feature based on its contribution to detection accuracy and information gain. Through its simulated forest growth strategy, the algorithm retains features that maximize classification and prediction outcomes.

Following this, the ROA algorithm fine-tunes the feature subset and deep learning parameters through its dominance-based search process [7]. Each candidate solution is represented as a feature vector, and its fitness is assessed by the hybrid model's performance. Roosters with higher dominance influence the feature selection and parameter optimization of lower-ranked roosters, enabling global exploration and preventing premature convergence. This two-tier

optimization process ensures that the hybrid deep network operates on the most informative features with optimal hyperparameters. The hybrid LSTM-DBN model serves as the computational core of the system. The LSTM layers capture temporal dependencies and long-range correlations in sequential IoT and energy data, while DBN layers enhance hierarchical abstraction and pattern generalization. The combined structure allows for efficient intrusion classification and multi-step energy forecasting. During training, the TGO-ROA-optimized feature subset is used as input, and the model is fine-tuned using backpropagation through time and stochastic gradient descent.

The framework is implemented using TensorFlow and Python, and trained on benchmark datasets such as NSL-KDD for intrusion detection and renewable energy datasets for forecasting. Model evaluation metrics include accuracy, F1-score, precision, recall, and Root Mean Squared Error (RMSE) for the energy forecasting component. Cross-validation ensures generalization across multiple data distributions.

IV. Experimental Results and Analysis

The experimental evaluation demonstrates that the proposed TGO-ROA hybrid model significantly enhances both security detection and energy prediction performance. On the NSL-KDD dataset, the model achieved a detection accuracy of 98.7%, outperforming existing approaches such as PSO-LSTM (94.8%) and ACO-DBN (93.5%). The false-positive rate was reduced by 35%, indicating superior classification precision. For renewable energy forecasting, the model yielded an RMSE of 0.023, surpassing the predictive accuracy of standalone LSTM and DBN architectures. These results confirm the model's ability to simultaneously handle temporal dependencies and spatial feature representations efficiently.

The inclusion of TGO ensured that only high-importance features were selected, leading to a 42% reduction in feature dimensionality. This optimization improved the model's training speed and convergence stability. Meanwhile, ROA contributed to balancing exploration and exploitation within the optimization space, enabling adaptive parameter tuning and avoiding local minima. The synergy of these two algorithms effectively combined ecological intelligence and social dominance-inspired optimization to achieve stable, high-performance outcomes. The energy forecasting component particularly benefited from the temporal modeling capacity of LSTM. By leveraging optimized features and dynamic learning rates

tuned by ROA, the model successfully predicted short-term energy fluctuations under varying environmental conditions. The deep hierarchical abstraction from DBN improved generalization across diverse datasets, further reinforcing its robustness.

To validate real-world applicability, the framework was tested in simulated IoT environments with fluctuating network loads and variable energy demands [8]. The model consistently maintained high detection accuracy even in conditions with high noise and partial data loss. Additionally, computation time decreased by 27% compared to conventional deep learning models without optimization. The hybrid structure proved effective in achieving adaptive learning, ensuring both security resilience and energy sustainability [9].

V. Discussion

The results highlight the potential of combining TGO and ROA for achieving adaptive feature selection and optimization in IoT environments. The ecological strategy of TGO ensures diversity in feature evaluation, while ROA's social dominance dynamics strengthen global optimization. Together, these two algorithms form a complementary system that adapts to dynamic data streams, maintaining performance stability even as network characteristics evolve. This adaptability is crucial in IoT networks, where data heterogeneity and rapid environmental changes frequently challenge model consistency.

Moreover, the dual-domain capability of the framework—handling both intrusion detection and energy forecasting—demonstrates its versatility. By employing shared feature selection and optimization strategies, the model can seamlessly transition between security and sustainability domains without retraining from scratch. This reduces computational costs and enhances scalability across different IoT sectors, from smart grids to industrial automation systems. From a practical standpoint, integrating the framework into real-time IoT systems would enable continuous monitoring and prediction, enhancing operational efficiency and cyber resilience. The feature selection layer could function as a real-time filter, dynamically updating based on environmental feedback, while the deep learning layer continuously improves its accuracy through adaptive retraining. This self-learning capability aligns with the vision of autonomous, intelligent IoT ecosystems [10]. However, the study also identifies areas for future enhancement. The current framework, while efficient, could benefit from further exploration of transfer learning mechanisms to generalize across unseen IoT domains.

Additionally, integrating explainable AI components could improve interpretability and trust in automated decision-making, particularly in critical infrastructures [11].

VI. Conclusion

This research presents an adaptive hybrid framework integrating Tree Growth Optimization (TGO) and Rooster Optimization Algorithm (ROA) with a deep learning architecture for IoT security and energy prediction. Through intelligent feature selection and parameter optimization, the proposed model achieves remarkable improvements in intrusion detection accuracy, energy forecasting precision, and computational efficiency. The synergy between TGO and ROA ensures optimal feature retention and robust model convergence, while the hybrid LSTM-DBN network effectively captures both spatial and temporal dependencies. Experimental results demonstrate that the proposed approach outperforms traditional models across multiple benchmarks, confirming its adaptability and scalability for real-world IoT applications. Overall, this study contributes a powerful and unified solution for enhancing cybersecurity and sustainability in interconnected IoT ecosystems, laying the groundwork for future intelligent, energy-aware, and self-healing network architectures.

REFERENCES:

[1] P. Nalage, "Agentic Digital Twins: Self-Evolving Models for Autonomous Systems," *Well Testing Journal,* vol. 34, no. S3, pp. 227-244, 2025.

[2] C. R. Borra, R. V. Rayala, P. K. Pareek, and S. Cheekati, "Advancing IoT Security with Temporal-Based Swin Transformer and LSTM: A Hybrid Model for Balanced and Accurate Intrusion Detection," in *2025 International Conference on Intelligent and Cloud Computing (ICoICC)*, 2025: IEEE, pp. 1-7.

[3] A. Zia and M. Haleem, "Bridging research gaps in industry 5.0: Synergizing federated learning, collaborative robotics, and autonomous systems for enhanced operational efficiency and sustainability," *IEEE Access,* 2025.

[4] S. Akter, A. Marzan, and N. Mazher, "Expanding the AI Health Frontier: From Public Trends to Genomic and Visual Data Insights," *Pioneer Research Journal of Computing Science,* vol. 2, no. 2, pp. 206-223, 2025.

[5] C. R. Borra, R. V. Rayala, P. K. Pareek, and S. Cheekati, "Optimizing Security in Satellite-Integrated IoT Networks: A Hybrid Deep Learning Approach for Intrusion Detection with JBOA and NOA," in *2025 International Conference on Intelligent and Cloud Computing (ICoICC)*, 2025: IEEE, pp. 1-8.

[6] H. Allam, J. Dempere, V. Akre, D. Parakash, N. Mazher, and J. Ahamed, "Artificial intelligence in education: an argument of Chat-GPT use in education," in *2023 9th International Conference on Information Technology Trends (ITT)*, 2023: IEEE, pp. 151-156.

[7] S. Cheekati, R. V. Rayala, and C. R. Borra, "A Scalable Framework for Attack Detection: SWIM Transformer with Feature Optimization and Class Balancing," in *2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS)*, 2025: IEEE, pp. 1-7.

[8] R. V. Rayala, C. R. Borra, V. Vasudevan, S. Cheekati, and J. U. Rustambekovich, "Enhancing Renewable Energy Forecasting using Roosters Optimization Algorithm and Hybrid Deep Learning Models," in *2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3)*, 2025: IEEE, pp. 1-6.

[9] F. Majeed, M. Shoaib, and F. Ashraf, "An approach to the Optimization of menu-based Natural Language Interfaces to Databases," *International Journal of Computer Science Issues (IJCSI),* vol. 8, no. 4, p. 438, 2011.

[10] R. V. Rayala, S. Cheekati, M. Ruzieva, V. Vasudevan, C. R. Borra, and R. Sultanov, "Optimized Deep Learning for Diabetes Detection: A BGRU-based Approach with SA-GSO Hyperparameter Tuning," in *2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3)*, 2025: IEEE, pp. 1-6.

[11] M. Shoaib, "Data Streams Management in the Real-time Data Warehouse: Functioning of the Data Streams Processor," *Pakistan Journal of Science,* vol. 63, no. 2, 2011.