View Reviews

Paper ID

1872

Paper Title

A Deep Hybrid LSTM-Attention Model for Context-Aware Anomaly Detection in IoT Traffic

Reviewer #4

Questions

1. Please write detailed Comment for - Suitability of Title and quality of the abstract. - Adequacy of literature review and proposed methods -Quality of result analysis and conclusion

The title accurately reflects the central theme of the paper and communicates the use of deep learning for context-aware anomaly detection in IoT networks. The abstract is concise and highlights the motivation, the hybrid LSTM-Attention model, and the potential impact. However, it could be further strengthened by mentioning key performance results or comparative gains over baseline models.

The literature review demonstrates a solid grasp of foundational work in anomaly detection and time-series learning in IoT contexts. The authors appropriately reference existing deep learning architectures such as RNNs, LSTMs, and GRUs, and they justify the shift toward attention-enhanced models. That said, the literature section could be more comprehensive by including recent advances (2022–2024) involving transformers, graph-based anomaly detection, or edge computing constraints, which are increasingly relevant to IoT analytics.

The methodology section outlines a hybrid architecture combining LSTM for sequence modeling and attention layers for context enhancement. The modular design is technically sound, and the decision to use attention mechanisms is well-motivated, particularly for variable-length IoT data sequences. However, some important implementation details are lacking:

a) Specifics regarding data preprocessing, input dimensionality, and normalization steps.

b) Detailed architecture design (e.g., number of LSTM layers, attention head configurations).

c) Hyperparameter settings such as batch size, learning rate, and number of training epochs.

The results and analysis section reports key evaluation metrics (accuracy, precision, recall, F1-score), and includes visualizations like confusion matrices and performance trend graphs. The proposed model achieves strong results across the metrics, outperforming several baselines. However, the statistical significance of improvements is not addressed. The addition of confidence intervals, multiple runs, or a significance test would improve the empirical rigor.

The conclusion reiterates the main findings and suggests future directions, such as expanding to other traffic types and exploring real-time deployment. While the conclusion is appropriate, it could be improved by briefly discussing model limitations, such as performance under unseen device behaviors, latency under real-time constraints, or sensitivity to data imbalance.

2. Overall evaluation

This paper addresses a pressing challenge in the domain of IoT cybersecurity and anomaly detection, offering a hybrid LSTM-Attention model that is conceptually well-founded and practically relevant. The modular design reflects an understanding of the sequential and contextual nature of IoT traffic patterns.

As a reviewer with experience in time-series modeling and IoT systems, I found the approach both appropriate and thoughtfully implemented. The use of an attention mechanism complements LSTM’s limitations, and the evaluation results support the model’s effectiveness. However, the presentation could be improved with greater methodological transparency and a stronger comparative narrative.

Additional recommendations include:

a) Enhancing language and grammar for technical clarity.

b) Expanding the baseline comparison to include more recent or transformer-based models.

c) Providing deployment context, including discussion on inference latency, model size, and edge-device feasibility.

Overall, this is a valuable submission with meaningful contributions. With revisions focused on clarity, detail, and analytical depth, the paper can be elevated significantly.

Reviewer #5

Questions

1. Please write detailed Comment for - Suitability of Title and quality of the abstract. - Adequacy of literature review and proposed methods -Quality of result analysis and conclusion

Suitability of Title and Quality of the Abstract:

The title is concise and accurately reflects the core contribution of the paper - a deep learning-based hybrid model integrating LSTM and Transformer components for anomaly detection in IoT traffic. The abstract is well-written and informative, outlining the problem, proposed solution, dataset used (CICIoMT2024), and performance highlights. It effectively communicates the relevance of the work to the current challenges in IoT security.

Adequacy of Literature Review and Proposed Methods:

The literature review is well-researched and cites both foundational and recent works across LSTM, Transformers, federated learning, and IoT-specific security frameworks. It appropriately contextualizes the need for hybrid deep learning models and highlights gaps in current approaches. The use of the CICIoMT2024 dataset adds credibility, as it is both recent and highly relevant.

The methodology is detailed and technically solid. The architecture combines LSTM-based encoders for local temporal features and a multi-head self-attention Transformer layer for capturing global dependencies. The preprocessing pipeline (including sliding windows, normalization, and stratified sampling) is robust and ensures high-quality model training. Algorithm 1 and the architectural diagram enhance clarity.

Quality of Result Analysis and Conclusion:

The experimental results are well-structured, showing comparative performance with existing models (e.g., L2D2), achieving 98.7% accuracy on multi-class classification tasks. The inclusion of a confusion matrix, accuracy graphs, and detailed class-specific performance helps in validating the model's robustness.

Particularly commendable is the analysis of how the attention mechanism aids in separating semantically similar attack classes (like spoofing vs reconnaissance). The conclusion summarizes the contributions effectively, and the future scope - especially in online/federated learning and adaptive thresholding - is timely and relevant.

2. Overall evaluation

This is a well-executed research contribution aligned with the ICDSA 2025 themes in intelligent systems, anomaly detection, and cybersecurity in IoT. The hybrid LSTM-Transformer model presented is innovative and addresses both practical deployment concerns (accuracy, interpretability) and technical challenges (long-range dependencies in time series).

Strengths:

Strong problem motivation rooted in real-world IoT security challenges.

Technical rigor in model architecture, data preprocessing, and experimental validation.

Use of a relevant and rich dataset (CICIoMT2024) with a variety of attack types.

High clarity in writing, with visuals and algorithmic representations aiding understanding.

Areas for Improvement:

The paper would benefit from including training time or computational cost comparisons with baseline models.

Consider discussing the scalability of the model for real-time deployment scenarios more explicitly.

Although performance is well-documented, a brief ablation study (e.g., Transformer-only vs. LSTM-only) would strengthen the architectural justification.