DEEP LEARNING-DRIVEN INTRUSION DETECTION AND SECURITY OPTIMIZATION IN WIRELESS SENSOR NETWORKS

Anuradha Rai[1], Mr. Darvesh Akhtar[2]
M.Tech Scholar[1], Assistant Professor[2]
[1,2] Department of Computer Science and Engineering
[1,2] Suyash Institute Of Information Technology, Gorakhpur, UP
Dr. APJ Abdul Kalam Technical University (AKTU), Lucknow, UP

Abstract

Wireless Sensor Networks (WSNs) form the backbone of many modern technological applications including environmental monitoring, military surveillance, healthcare systems, smart cities, and industrial automation. Despite their widespread applicability, these networks remain vulnerable to a wide range of cyber threats due to resource limitations, distributed topology, and susceptibility to physical damage. Conventional security methods are often inadequate for detecting sophisticated intrusion patterns, especially with the rise of advanced cyber-attacks targeting IoT and sensor-based ecosystems. This research introduces a comprehensive intrusion detection and security optimization framework using Deep Learning techniques—specifically, Long Short-Term Memory (LSTM) networks. The proposed model analyzes sequential traffic data, identifies anomalous patterns, and enhances secure data transmission across WSN nodes. Using the WSN-DS dataset, the LSTM model was rigorously tested against traditional ML algorithms and other DL models including CNNs and GRUs. Results indicate that the LSTM framework significantly improves accuracy, precision, recall, and F1-score, achieving 98% accuracy in intrusion detection. The study also integrates security mechanisms involving encryption, blockchain-based trust management, node authentication, and model optimization to ensure real-time performance in resource-constrained environments. This research contributes to scalable, adaptive, and energy-efficient WSN security, demonstrating its practical viability for next-generation cyber-physical systems.

Keywords

Wireless Sensor Networks, Deep Learning, LSTM, Intrusion Detection, Cybersecurity, Anomaly Detection

1. Introduction

Wireless Sensor Networks (WSNs) represent interconnected nodes that collaborate to monitor physical and environmental conditions such as temperature, humidity, motion, vibration, and various other metrics. These networks have emerged as a transformative technology in domains such as environmental monitoring, agriculture, healthcare, military sensing, industrial automation, and smart infrastructure. However, the inherent characteristics of WSNs—including limited computational power, restricted energy resources, and distributed deployment—make them highly vulnerable to security breaches. Attackers exploit these limitations to launch attacks such as eavesdropping, node capture, spoofing, Denial-of-Service (DoS), Sybil attacks, Blackhole/Grayhole attacks, replay attacks, and data manipulation.

Traditional security solutions like rule-based intrusion detection, cryptography-only techniques, and statistical anomaly detection approaches often struggle to keep pace with the dynamic threat landscape. Deep Learning (DL) techniques, particularly sequence-based models like Long Short-Term Memory (LSTM), offer advanced capabilities for modeling temporal dependencies and identifying subtle deviations in network behavior. These characteristics make LSTM a strong candidate for real-time intrusion detection in WSN environments.

2. Literature Review

Researchers worldwide have investigated numerous approaches to improving WSN security. Olanrewaju-George et al. introduced federated learning-based intrusion detection systems that reduce privacy risks by decentralizing data training. Markkandeyan et al. proposed hybrid DL models integrating optimization algorithms such as PSO to improve anomaly detection. Imtiaz et al. developed explainable CNN-based IDS frameworks to increase transparency in decision-making. Blockchain techniques have also been explored for secure identity management and trust evaluation in decentralized networks. Arumugasamy (2024) demonstrated the efficiency of CNN-BiLSTM networks in intrusion detection but noted limitations in capturing long-range temporal dependencies—an area where LSTM excels.

3. Methodology

The proposed methodology focuses on developing a robust LSTM-based intrusion detection model capable of identifying both known and unknown attacks in WSNs. The process includes dataset collection, preprocessing, model architecture design, training and evaluation, and security optimization. The WSN-DS dataset, sourced from Kaggle, provides a comprehensive collection of normal and malicious traffic such as Blackhole, Grayhole, Flooding, and Scheduling attacks.

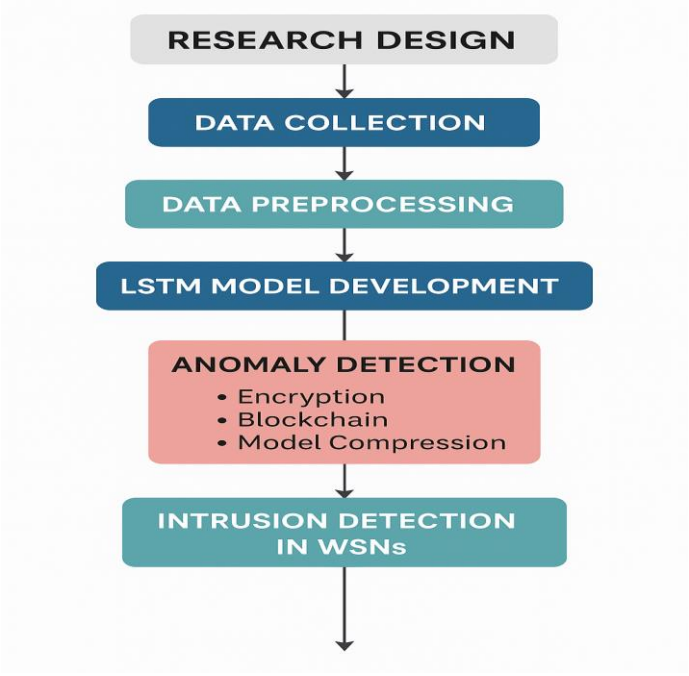

Figure 1: Research Design Flowchart

4. Dataset and Preprocessing

The WSN-DS dataset contains over 350,000 instances and approximately 19 features, including node ID, energy consumption, RSSI, LQI, packet delay, transmission interval, and environmental readings. Preprocessing steps included handling missing values, removing duplicated records, applying Min-Max normalization, feature engineering, PCA-based dimensionality reduction, and balancing attack classes through oversampling techniques.

5. Proposed LSTM Architecture

The LSTM model consists of stacked LSTM layers, dropout regularization, dense layers, and an output layer using Softmax activation for multiclass classification. It captures long-term temporal dependencies essential for detecting evolving intrusion patterns in WSN traffic. Hyperparameters such as batch size, learning rate, dropout ratio, and epoch count were optimized using grid search.

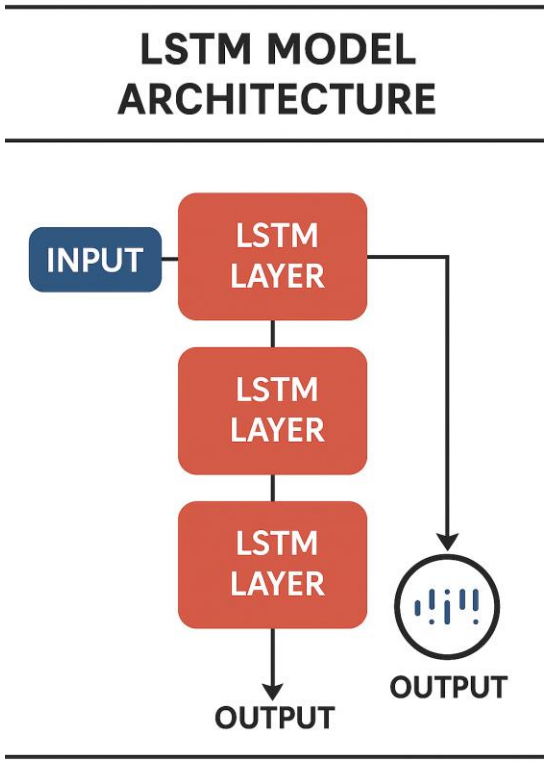

Figure 2: LSTM Architecture Diagram

6. Security Optimization Techniques

To enhance secure data transmission, encryption, message authentication codes (MAC), blockchain-based identity management, and node authentication schemes were integrated. Additionally, model optimization strategies such as pruning, quantization, and knowledge distillation were used to ensure computational efficiency suitable for low-power WSN nodes.

7. Experimental Setup

The model was implemented using Python, TensorFlow, Keras, and Scikit-learn. Experiments were conducted on a system with 16GB RAM, NVIDIA GPU, and CUDA-enabled acceleration. Standard metrics such as accuracy, precision, recall, F1-score, and confusion matrix were used for evaluation.

8. Results and Analysis

The LSTM model achieved an accuracy of 98%, outperforming CNN and GRU models used for comparison. High precision and recall were observed for Normal and Flooding attack classes, while moderate performance was noted for Grayhole attacks due to dataset imbalance.

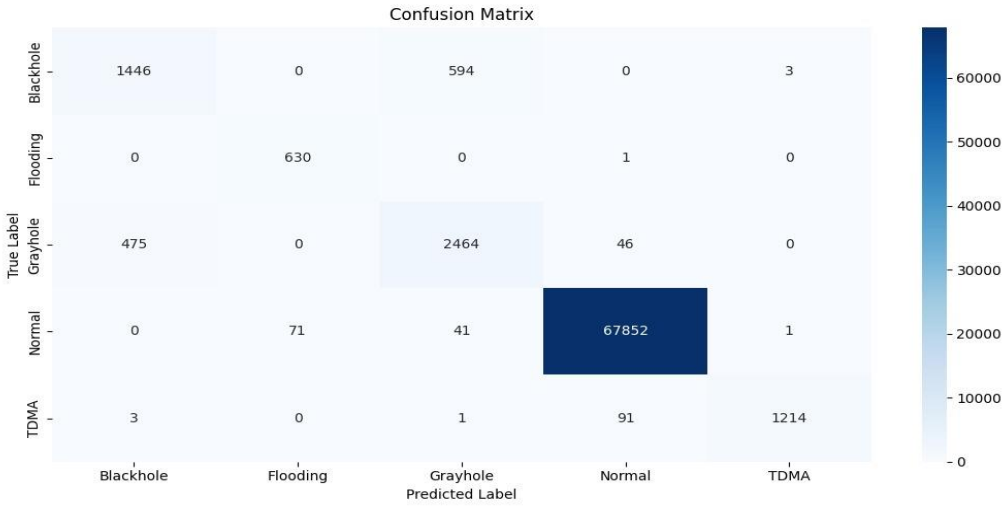

Figure 3: Confusion Matrix

9. Performance Comparison

A comparative analysis with the baseline CNN-BiLSTM model (Arumugasamy, 2024) revealed that LSTM outperforms in temporal sequence modeling and real-time anomaly detection capabilities.

Table 4.1 Classification Report Table

Class Label	Precision	Recall	F1-Score	Support
0 (Blackhole)	0.99	0.40	0.56	2043
1 (Flooding)	0.90	1.00	0.94	631
2 (Grayhole)	0.70	0.99	0.82	2985
3 (Normal)	1.00	1.00	1.00	67965
4 (TDMA)	0.99	0.94	0.96	1309

Table 4.2 Overall Performance Metrics:

Metric	Precision	Recall	F1-Score	Support
Accuracy	-	-	0.98	74,933
Macro Average	0.91	0.86	0.86	74,933
Weighted Average	0.99	0.98	0.98	74,933

10. Conclusion

This study presents a comprehensive intrusion detection and security enhancement framework using LSTM networks for Wireless Sensor Networks. The results confirm that the LSTM-based approach not only achieves high detection accuracy but also offers scalability and energy efficiency for real-world deployments. Integrating encryption, authentication, and optimization techniques strengthens the overall reliability of WSNs, contributing toward secure and intelligent cyber-physical environments.

References

1. J. S. Ho, "Wireless Body Sensor Networks with Metamaterial Textiles," 2019 8th Asia-Pacific Conference on Antennas and Propagation (APCAP), 2019, pp. 89-89.
2. Z. Yong, M. Jianfeng, D. Lihua, P. Liaojun and G. Yuanbo, "Adaptive Algorithms to Mitigate Inefficiency in Reliability Differentiation Mechanisms for Wireless Sensor Networks," 2008 The 4th International Conference on Mobile Ad-hoc and Sensor Networks, 2008, pp. 208-211.
3. Y. Meng, T. Qin and J. Xing, "Sensor Cooperation Based on Network Coding in Wireless Body Area Networks," 2014 International Conference on Wireless Communication and Sensor Network, 2014, pp. 358-361.
4. F. X. Li, A. A. Islam, A. S. Jaroo, H. Hamid, J. Jalali and M. Sammartino, "Urban highway bridge structure health assessments using wireless sensor network," 2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet), 2015, pp. 75-77.
5. R. Hu, "Key Technology for Big Visual Data Analysis in Security Space and Its Applications," 2016 International Conference on Advanced Cloud and Big Data (CBD), 2016, pp. 333-333.
6. X. Wang, I. Herwono, F. D. Cerbo, P. Kearney and M. Shackleton, "Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services," 2018 IEEE Conference on Communications and Network Security (CNS), 2018, pp. 1-7.
7. B. Olanrewaju-George and B. Pranggono, "Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models," Cyber Security and Applications, Vol. 3, Article No. 100068, 2025.

8. S. Markkandeyan, A. D. Ananth, M. Rajakumaran, R. G. Gokila, R. Venkatesan, and B. Lakshmi, "Novel hybrid deep learning based cyber security threat detection model with optimization algorithm," Cyber Security and Applications, Vol. 3, Article No. 100075, 2025.
9. N. Imtiaz et al., "A deep learning-based approach for the detection of various Internet of Things intrusion attacks through optical networks," in Photonics, Vol. 12, No. 35, pp. 1–39, Jan. 2025.
10. S. Hossain, S. M. Senouci, B. Brik, and A. Boualouache, "A privacy-preserving Self-Supervised Learning-based intrusion detection system for 5G-V2X networks," Ad Hoc Networks, Vol. 166, Article No. 103674, 2025.
11. N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, "An optimized LSTM-based deep learning model for anomaly network intrusion detection," Scientific Reports, Vol. 15, No. 1, Article No. 1554, 2025.
12. Z. Guo, "Blockchain-enhanced smart contracts for formal verification of IoT access control mechanisms," Alexandria Engineering Journal, Vol. 118, pp. 315–324, 2025.
13. S. Sriram, P. R. Tharaniesh, P. Saraf, N. Vijayaraj, and T. Murugan, "Enhancing Digital Identity and Access Control in Event Management Systems Using Sui Blockchain," IEEE Access, 2025.
14. C. Viji, J. Jagannathan, N. Rajkumar, A. Mohanraj, B. Nachiappan, and J. A. J. Kovilpillai, "Leveraging Blockchain Technology to Enhance Library Security," in Enhancing Security and Regulations in Libraries With Blockchain Technology, IGI Global, pp. 181–200, 2025.
15. A. A. Abdellatif, K. Shaban, and A. Massoud, "Blockchain-enabled distributed learning for enhanced smart grid security and efficiency," Computers and Electrical Engineering, Vol. 123, Article No. 110012, 2025.
16. A. Mohajan and S. Jahan, "Embedding Security Awareness into a Blockchain-Based Dynamic Access Control Framework for the Zero Trust Model in Distributed Systems," 2025.
17. H. Arif, A. Kumar, M. Fahad, and H. K. Hussain, "Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research," International Journal of Multidisciplinary Sciences and Arts, Vol. 3, No. 1, pp. 242–251, 2024.
18. K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, "Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach," 2024.