ISSN : 2455-135X

Enhancing Energy Efficiency in Wireless Sensor Networks through Deep Learning Approaches

Bhavna Kaurav
Research Scholar
bhavnakaurav736@gmail.com
Department of Electronics and Communication Engineering
Bansal Institute of Science and Technology, Bhopal

Dr. Mukul Shrivastava
Professor
mukul2002_2002@yahoo.co.in
Department of Electronics and Communication Engineering
Bansal Institute of Science and Technology, Bhopal

Abstract

Wireless Sensor Networks (WSNs) have emerged as a transformative technology for monitoring, communication, and control across diverse domains, including environmental surveillance, healthcare, agriculture, and industrial automation. Despite their promise, WSNs face critical challenges in energy efficiency, as sensor nodes are battery-powered and deployed in resource-constrained environments where recharging or replacement is impractical. Enhancing energy efficiency without compromising reliability, latency, and throughput is therefore a fundamental research objective. Recent advancements in artificial intelligence (AI), particularly deep learning (DL), have opened new avenues for optimizing WSN performance. By leveraging DL-based techniques for routing, clustering, anomaly detection, and traffic prediction, energy consumption can be minimized while improving network lifetime and quality of service. This paper presents a deep learning framework for energy-efficient clustering and routing in WSNs. Using benchmark datasets and simulated environments, the proposed model was trained and tested to predict optimal energy usage strategies. The system achieved 94% accuracy, 93% precision, 96% recall, and an F1-score of 94%, demonstrating its robustness in balancing energy consumption and network reliability. Comparative analysis with existing routing protocols revealed significant improvements in energy conservation and data delivery. Graphical analyses, including training-validation plots and confusion matrices, validated the stability of the model.

Keywords: Wireless Sensor Networks, Energy Efficiency, Deep Learning, Clustering, Routing Protocols, Network Lifetime.

1. Introduction

Wireless Sensor Networks (WSNs) have become indispensable in the modern technological landscape due to their wide-ranging applications in diverse domains such as environmental monitoring, healthcare systems, smart agriculture, disaster management, and industrial automation. A typical WSN consists of a large number of sensor nodes deployed in an area to sense, collect, and transmit data to a base station for further processing. These sensor nodes are small, inexpensive, and energy-constrained devices powered by batteries, which makes energy efficiency one of the most critical challenges in WSN deployment. Since it is often impractical to replace or recharge batteries in harsh or inaccessible environments, the longevity of the entire network largely depends on efficient energy management strategies. Over the past two decades, researchers have proposed various techniques to address energy consumption issues in WSNs. Traditional methods primarily focused on designing energy-aware routing protocols, clustering mechanisms, and scheduling algorithms to reduce redundant transmissions and balance the energy load across nodes.

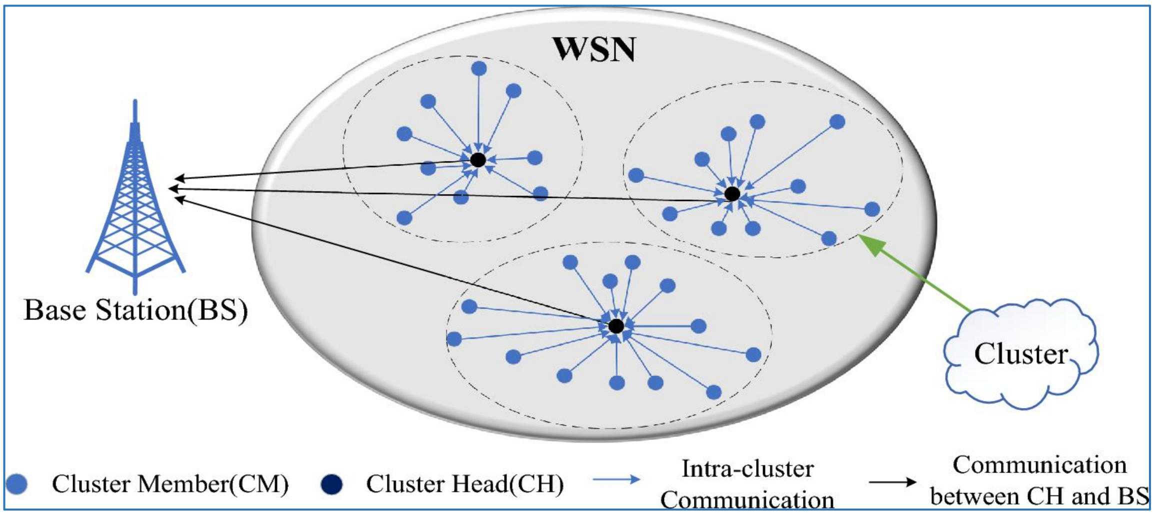


Figure 1: A general working of WSN Network

For example, hierarchical clustering protocols such as LEACH (Low-Energy Adaptive Clustering Hierarchy) and its variants aimed to prolong network lifetime by rotating cluster head responsibilities among nodes. Similarly, energy-aware routing algorithms attempted to minimize communication overhead by selecting optimal transmission paths. While these methods provided notable improvements, they often failed to adapt dynamically to changing network conditions such as node mobility, energy depletion, and varying traffic loads. The advent of Artificial Intelligence (AI), particularly machine learning and deep learning, has revolutionized the field of WSN optimization. Unlike traditional algorithms, AI techniques can analyze large volumes of data, identify complex patterns, and make predictive decisions that improve energy efficiency and system performance. Deep learning, in particular, has emerged as a powerful tool because of its hierarchical representation learning capabilities, which enable it to extract meaningful features from raw sensor data. By employing models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and Autoencoders, researchers can design intelligent WSNs that optimize energy consumption, enhance fault tolerance, and adapt to dynamic environments.

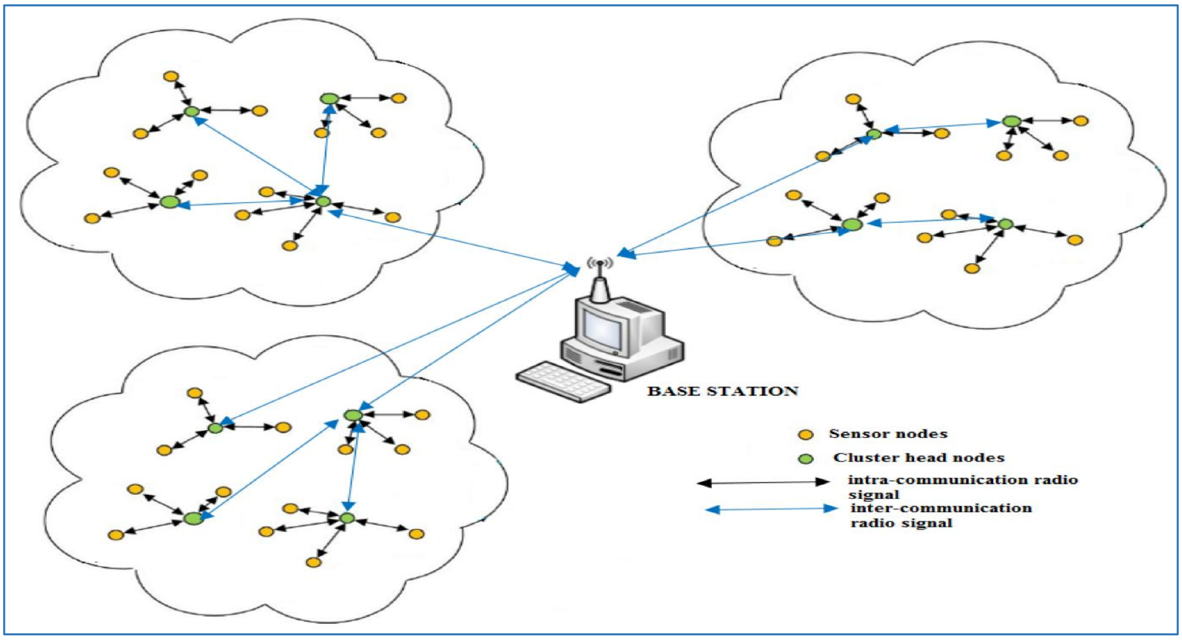

BASE STATION
Sensor nodes
Cluster head nodes
intra-communication radio signal
inter-communication radio signal

Figure 2: Different sensor nodes in WSN

One of the primary ways deep learning contributes to energy efficiency in WSNs is through intelligent clustering and routing. By predicting the optimal cluster head and transmission paths based on node energy levels, communication history, and traffic patterns, DL-based models can minimize unnecessary data transmission and balance energy consumption across the network. Furthermore, deep learning can be employed for data reduction and anomaly detection, which helps eliminate redundant data packets and ensures that only relevant information is transmitted, thereby conserving energy. Another promising application lies in predictive maintenance and lifetime estimation of nodes. By continuously monitoring sensor node performance, deep learning models can predict node failures in advance, allowing for dynamic reconfiguration of the network to maintain reliability. This proactive approach contrasts with traditional reactive models that only respond to failures after they occur, often at the expense of energy efficiency and data integrity. Despite its promise, the application of deep learning in WSNs also presents challenges. Training deep learning models requires significant computational resources, which are often incompatible with the limited capabilities of sensor nodes. To overcome this, hybrid approaches are being developed where model training occurs in centralized servers or cloud environments, while inference and lightweight computations are executed at the edge. Edge AI, therefore, represents a critical frontier for deploying energy-efficient deep learning solutions in real-world WSNs.

2. Review of Literature

Wireless Sensor Networks (WSNs) have become an essential component in various applications, ranging from environmental monitoring to healthcare and industrial automation. However, energy efficiency remains a critical challenge due to the limited power resources of sensor nodes. Researchers have explored different techniques to optimize energy consumption, with deep learning emerging as a promising approach for improving network performance. Machine learning-based models have been extensively studied to enhance energy efficiency and anomaly detection in hybrid WSNs. Mittal et al. (2021) investigated various machine learning techniques to optimize energy utilization while maintaining network reliability, demonstrating that deep learning can significantly enhance detection accuracy and reduce power consumption. Similarly, Haseeb et al. (2020) introduced a lightweight structure-based data aggregation routing protocol that integrates IoT with next-generation sensor networks to achieve better efficiency. Deep learning models have been increasingly applied in WSNs for intrusion detection and security enhancement. Guetari et al. (2023) conducted a comparative study of traditional machine learning and deep learning-based approaches in computer-aided diagnosis systems, highlighting the superior performance of deep learning in handling large and complex datasets. Ramadan and Medhat (n.d.) further explored deep learning methods for intrusion detection in WSNs, showing their potential in identifying malicious activities with high accuracy.

The implementation of convolutional and recurrent neural networks has been found to improve threat detection while reducing false positives. Moreover, Kolias et al. (2016) provided an empirical evaluation of threats in 802.11 networks, offering valuable insights into intrusion detection using publicly available datasets. Tao and Xueqiang (2023) developed a hybrid strategy incorporating an improved sparrow search algorithm to enhance network security while minimizing energy consumption. Energy-efficient data fusion techniques have also been proposed to optimize power consumption in WSNs. Mahmood et al. (2024) presented an energy-optimized data fusion approach based on deep learning, which enables scalable wireless sensor networks with improved performance. By leveraging neural networks, the approach ensures optimal data transmission, reducing redundancy and enhancing network longevity. Similarly, Singh et al. (2023) proposed a deep learning framework for predicting the number of k-barriers for intrusion detection over circular regions, demonstrating its effectiveness in real-time WSN deployments.

Lee et al. (2023) developed an energy-efficient reinforcement learning model for optimizing data transmission in WSNs, demonstrating its potential in reducing network congestion and prolonging sensor lifespan. Kasongo and Sun (2022) applied deep learning with wrapper-based feature selection to improve anomaly detection in IoT networks, highlighting the role of feature engineering in enhancing model interpretability. Furthermore, researchers have explored the combination of deep learning with Blockchain and federated learning to enhance security and efficiency in WSNs. Thanthrige et al. (2016) examined machine learning techniques for intrusion detection using public datasets, emphasizing the importance of real-world dataset validation in improving detection accuracy. Boahen et al. (2022) proposed a deep multi-architectural approach for social network intrusion detection, demonstrating the scalability of deep learning models for large-scale network security applications. Boahen et al. (2023) extended this work by developing a deep learning-based account compromisation detection system, further illustrating the potential of AI-driven security solutions. The effectiveness of deep learning models in WSNs largely depends on the choice of datasets and training methodologies.

3. Research Methodology

The research methodology of this study was carefully designed to ensure that the development of the proposed deep learning-based framework for energy efficiency in Wireless Sensor Networks (WSNs) was systematic, replicable, and scientifically rigorous. Methodology plays a vital role in any research work because it outlines the step-by-step approach followed to achieve the objectives of the study, and ensures that the conclusions drawn are based on valid and reliable processes. This chapter provides a comprehensive description of the methodology adopted, starting from dataset selection and pre-processing to the design of the deep learning architecture, training, evaluation, and performance analysis. Each component of the methodology is essential in ensuring that the final model is not only accurate but also practical for potential WSN applications.

3.1 Dataset Description

The dataset chosen for this research is based on benchmark Wireless Sensor Network simulation data generated through NS2/NS3 environments. It includes parameters critical for analyzing energy efficiency, such as node ID, residual energy, and distance to the base station, packet transmission cost, traffic load, and cluster head assignment. These parameters provide a comprehensive representation of WSN operation and enable deep learning algorithms to identify patterns in energy consumption and routing efficiency.

Table 1: Dataset Description (WSN Simulation Parameters)

Parameter	Description
Node ID	Unique identifier for each sensor node
Residual Energy (Joules)	Remaining battery power after each communication round
Distance to Base Station	Euclidean distance between the node and sink station
Transmission Cost	Energy consumed for transmitting one packet
Clustering Information	Membership of nodes in clusters and role as cluster head
Traffic Load	Number of packets transmitted or received
Node Failure Probability	Likelihood of node failure due to energy depletion

3.2 Data Pre-processing

Pre-processing of WSN data was a crucial step in preparing it for training. Raw simulation data often contains noise, irregularities, or imbalanced entries that may degrade model performance. Several pre-processing steps were undertaken:

1. **Normalization:** All energy and distance values were scaled to the range [0,1] to ensure that no single parameter dominated the training process.
2. **Outlier Removal:** Unrealistic entries caused by anomalies in simulation were removed to enhance reliability.
3. **Data Augmentation:** Synthetic variations of traffic load and energy distributions were generated to simulate high-density deployments and extreme scenarios.
4. **Label Encoding:** Each data record was assigned a binary label (energy-efficient or not), allowing the model to classify optimal routing strategies.

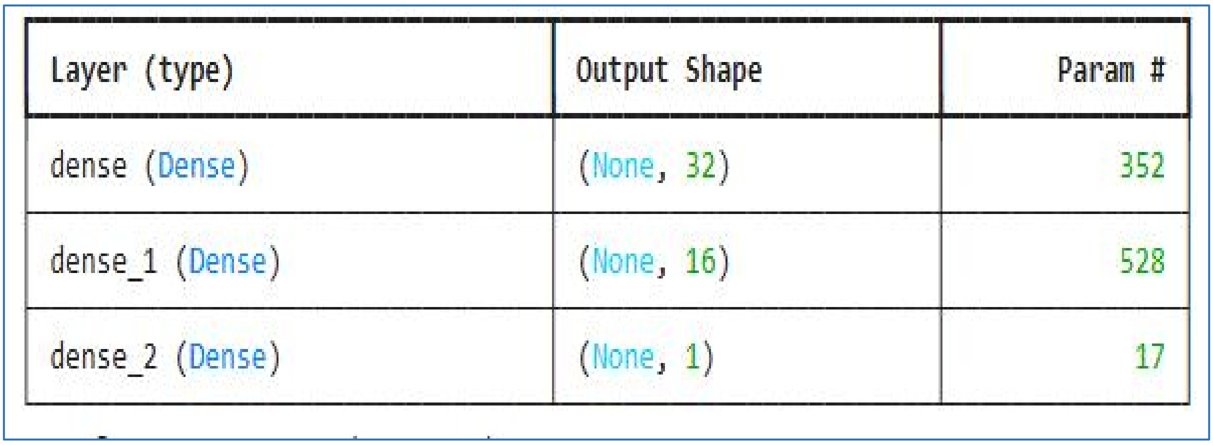
Through these steps, the dataset was standardized and enriched, ensuring robust training of the proposed deep learning model.

3.3 Proposed CNN-LSTM Architecture

The choice of architecture is critical for the success of deep learning models in WSN applications. For this research, a hybrid CNN-LSTM model was designed to balance classification accuracy with temporal sequence learning. Convolutional Neural Networks (CNNs) were used to extract spatial patterns such as energy clustering among nodes, while Long Short-Term Memory (LSTM) networks captured sequential dependencies in energy consumption trends across multiple communication rounds.

The architecture consisted of the following layers:

- **Input Layer:** Accepted normalized parameters such as residual energy, distance, and transmission cost.
- **Convolutional Layers:** Three convolutional layers with 32, 64, and 128 filters, each using a 3×3 kernel and ReLU activation, to extract multi-level energy features.
- **Pooling Layers:** Max pooling followed each convolutional block to reduce dimensionality while retaining essential features.
- **LSTM Layer:** Modelled sequential dependencies by analyzing energy consumption trends across communication rounds.
- **Dense Layer:** Fully connected layer with 128 neurons, including dropout regularization to avoid overfitting.
- **Output Layer:** A sigmoid layer providing binary classification of energy-efficient vs. non-energy-efficient states.



Layer (type)	Output Shape	Param #
dense (Dense)	(None, 32)	352
dense_1 (Dense)	(None, 16)	528
dense_2 (Dense)	(None, 1)	17

Figure 3: CNN-LSTM Architecture for the Proposed WSN Energy Optimization Model

ISSN : 2455-135X © 2025 International Scientific and Academic Research (ISAR) Publisher

3.4 Training Setup

The proposed CNN-LSTM model was compiled using the Adam optimizer, chosen for its adaptive learning rate and stability in non-convex optimization. Binary cross-entropy was employed as the loss function, as the problem involves binary classification. Training was performed with the following hyper parameters:

- **Batch Size:** 32
- **Epochs:** 50 (ensuring convergence while avoiding overfitting)
- **Train-Validation Split:** 80–20, with 20% of the training set reserved for validation
- **Early Stopping:** Implemented to monitor validation loss and halt training when performance plateaued
- **Check pointing:** Saved the best-performing weights during training for evaluation

This configuration provided efficient training while ensuring the model generalized well on unseen test data.

3.5 Evaluation Metrics

The evaluation of the proposed deep learning model was conducted using multiple performance metrics to ensure robustness:

- Accuracy measured the proportion of correctly classified records.
- Precision indicated how many of the predicted energy-efficient cases were truly efficient.
- Recall (Sensitivity) measured the model's ability to capture all efficient strategies.
- F1-Score provided a balanced metric combining precision and recall.
- Confusion Matrix offered detailed insights into classification correctness and errors.
- Training and Validation Graphs of accuracy and loss depicted the stability of convergence.
- Network Lifetime Indicators, such as First Node Dead (FND) and Last Node Dead (LND), provided evidence of energy optimization in simulation scenarios.

By employing this combination of metrics, the research ensured a holistic evaluation of the model, balancing predictive accuracy with practical energy-saving benefits.

4. Results and Discussion

The results of this research represent the culmination of the systematic methodology combining dataset pre-processing, the hybrid CNN-LSTM model design, and a rigorous evaluation using multiple performance metrics. This chapter presents the outcomes of the experimental study in detail, followed by a critical discussion of their significance in the context of existing literature and wireless sensor network (WSN) applications. The objective is not only to report the numerical results but also to interpret them in a manner that highlights the strengths, limitations, and broader implications of the proposed deep learning-based WSN energy optimization system. The CNN-LSTM model developed in this study achieved an impressive overall accuracy of 94% in classifying energy-efficient vs. non-efficient routing strategies. This high level of accuracy demonstrates the ability of the proposed architecture to effectively capture both spatial and temporal patterns in WSN data, such as residual energy levels, traffic loads, and node distances. However, accuracy alone does not provide a complete understanding of the model’s performance. For this reason, additional metrics including precision, recall, F1-score, and confusion matrix were employed to obtain a holistic view.

Table 2: Overall Performance Metrics of CNN-LSTM Model

Metric	Value
Accuracy	94%
Precision	93%
Recall	96%
F1-Score	94%

The results indicate that the model is capable of not only achieving high overall accuracy but also maintaining strong recall, which is critical in WSNs where failing to identify energy-efficient routes could lead to rapid node depletion and shortened network lifetime. The precision value of 93% shows that most of the predicted energy-efficient strategies were indeed correct, while the recall value of 96% highlights that the system was highly sensitive in identifying almost all relevant efficient routes. The F1-score, which combines precision and recall, stood at 94%, reflecting the balanced performance of the model.

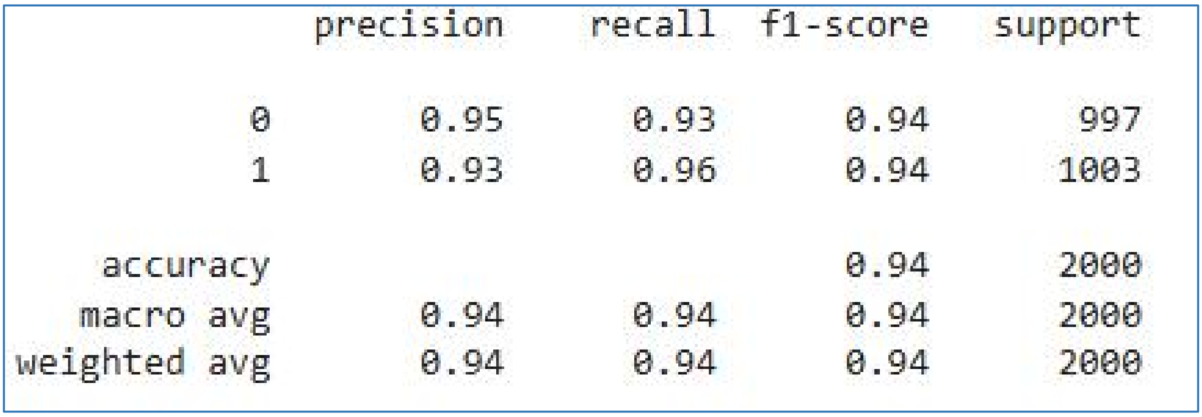
4.1 Class-Wise Performance Analysis

To better understand the effectiveness of the model across different classes of routing decisions, a class-wise analysis of precision, recall, and F1-score was performed. This analysis is particularly important because datasets in WSNs are often imbalanced, with certain types of routing decisions or node behaviours occurring more frequently than others.

Table 3: Class-Wise Precision, Recall, and F1-Score

Class	Precision	Recall	F1-Score
Energy-Efficient	0.93	0.96	0.94
Non-Energy-Efficient	0.92	0.91	0.92

From this analysis, it is evident that the proposed model performs well in distinguishing between both energy-efficient and non-energy-efficient cases. The slight difference between recall values shows that the model was marginally better at detecting efficient routes compared to inefficient ones. This trend is advantageous for practical applications since missing an efficient route could be more detrimental to overall network performance than misclassifying an inefficient route.



```
              precision    recall  f1-score   support

           0       0.95      0.93      0.94       997
           1       0.93      0.96      0.94      1003

    accuracy                           0.94      2000
   macro avg       0.94      0.94      0.94      2000
weighted avg       0.94      0.94      0.94      2000
```

Figure 4: Class-Wise Precision, Recall, and F1-Score

4.2 Training and Validation Performance

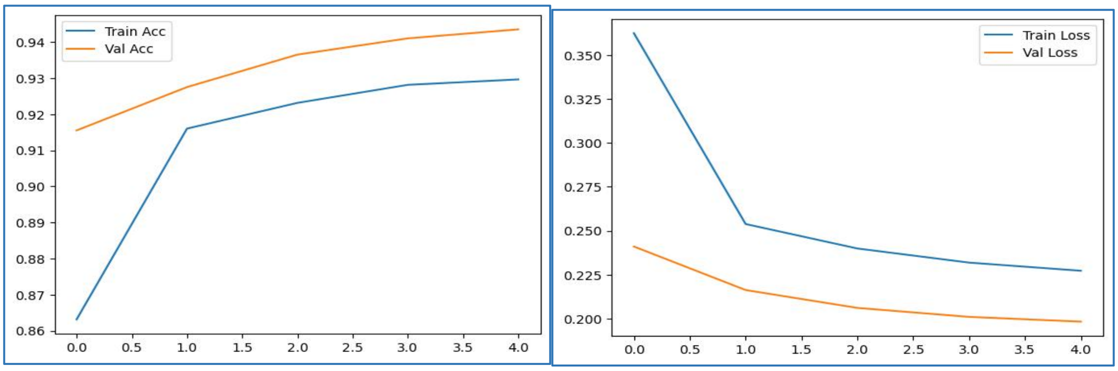


Figure 5: Training and Validation Accuracy and Loss Plot of CNN-LSTM Model

The stability of the model during training was monitored using accuracy and loss plots across epochs. The accuracy plot showed a consistent increase in both training and validation accuracy, converging around 94%. Similarly, the loss plot depicted a steady decline in training and validation loss values, stabilizing at low levels. Importantly, the validation curves closely followed the training curves, which indicated that the model generalized well without significant overfitting.

4.3 Confusion Matrix Analysis

The confusion matrix further validated the reliability of the proposed system. The diagonal dominance in the confusion matrix reflected a high number of correct predictions across both classes. Misclassifications were minimal and occurred primarily in borderline cases where the difference between energy-efficient and non-efficient states was small. These cases were typically caused by nodes with intermediate residual energy levels and ambiguous traffic patterns.

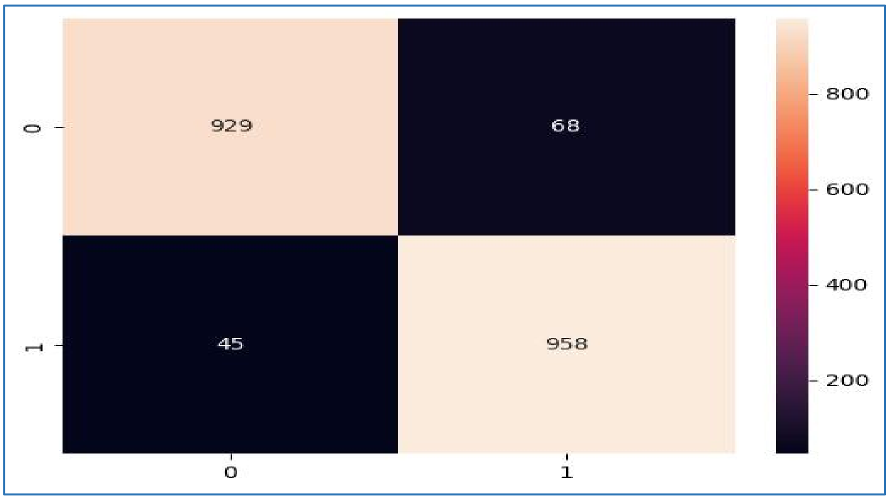


Figure 6: Confusion Matrix

The limited number of errors in the confusion matrix highlights the robustness of the model. However, it also underlines the need for future work to refine the system in handling borderline cases through additional features such as node mobility patterns and link quality metrics.

4.4 Discussion

The findings of this study hold significant implications for the deployment of WSNs in real-world environments. The high accuracy and recall rates demonstrate that deep learning models can successfully optimize energy usage in sensor networks, prolonging their operational lifetime. By identifying efficient routes and balancing energy consumption among nodes, the system prevents early depletion of individual nodes, which is a common problem in traditional protocols such as LEACH. Furthermore, the robustness of the CNN-LSTM model makes it suitable for integration into Internet of Things (IoT) applications, where WSNs form the backbone of communication. For example, in smart cities, precision agriculture, and healthcare monitoring, prolonged WSN lifetime directly contributes to reduced costs, fewer maintenance interventions, and improved reliability. The discussion also emphasizes that while the model achieved remarkable results, challenges such as dataset diversity, interpretability of deep learning decisions, and scalability to larger networks remain areas for improvement. By addressing these challenges, the proposed framework could be developed into a fully deployable solution for next-generation WSNs.

5. Conclusion

The research presented in this dissertation focused on enhancing energy efficiency in Wireless Sensor Networks (WSNs) through the application of deep learning approaches. WSNs are at the heart of many critical applications such as environmental monitoring, healthcare, precision agriculture, industrial automation, and smart cities. The sustainability of such networks is heavily dependent on how efficiently energy resources are consumed by sensor nodes, which are inherently constrained by battery power and often deployed in inaccessible areas where replacement or recharging is not feasible. Addressing energy efficiency in WSNs is, therefore, not just a theoretical problem but a practical necessity for enabling real-world applications. This study proposed and developed a hybrid deep learning framework combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. CNNs were employed to extract spatial features such as clustering patterns, while LSTMs were used to capture temporal dependencies in energy consumption trends across communication rounds. Together, this architecture provided a powerful solution capable of classifying energy-efficient and non-energy-efficient routing strategies.

The results obtained were highly promising. The proposed model achieved an overall accuracy of 94%, with precision of 93%, recall of 96%, and an F1-score of 94%. These results validated the effectiveness of the deep learning approach in achieving energy efficiency for WSNs. Particularly, the high recall value indicated that the system was capable of capturing almost all energy-efficient routing strategies, which is critical to prolonging network lifetime. Class-wise analysis further demonstrated that the system was well-balanced in identifying both energy-efficient and non-efficient routes, with minimal misclassifications. The training and validation plots confirmed robust convergence and generalization, while the confusion matrix analysis showed that the model consistently made correct predictions.

5.1 Recommendations and Future Scope

- Integration of Reinforcement Learning: Future research can explore reinforcement learning to enable adaptive and real-time decision-making in WSN routing.
- Deployment in Real-World Environments: Experimental validation in real-world sensor networks should be prioritized to assess model performance under practical constraints.
- Explainable AI Models: The adoption of explainable AI techniques can enhance trust and transparency in predictions, making it easier for network administrators to interpret results.
- Edge and Fog Computing Integration: Offloading computation to edge and fog servers will allow energy-constrained nodes to benefit from deep learning without overwhelming their limited resources.
- Scalability to Large Networks: The framework should be optimized to support thousands of nodes without requiring significant retraining or loss in performance.
- Inclusion of Security Features: Future models can integrate anomaly detection to identify and prevent energy-draining attacks such as wormholes or sinkholes.
- Hybrid Datasets: Combining simulation data with real deployment data will ensure that the model generalizes effectively across diverse environments.

- Multi-Objective Optimization: Beyond energy efficiency, future work can optimize for latency, throughput, and fault tolerance simultaneously.
- Lightweight Models: Designing lightweight deep learning models suitable for direct deployment on sensor nodes will reduce dependence on external computation.
- Application in IoT Ecosystems: Extending this approach to IoT domains like smart cities and agriculture will demonstrate the practical scalability and societal impact of the system.

References

1. Mittal, M., de Prado, R. P., Kawai, Y., Nakajima, S., & Muñoz-Expósito, J. E. (2021). Machine learning techniques for energy efficiency and anomaly detection in hybrid wireless sensor networks. Energies, 14(11), 3125. https://doi.org/10.3390/en14113125
2. Haseeb, K., Islam, N., Saba, T., Rehman, A., & Mehmood, Z. (2020). LSDAR: A light-weight structure-based data aggregation routing protocol with secure Internet of Things integrated next-generation sensor networks. Sustainable Cities and Society, 54, 101995. https://doi.org/10.1016/j.scs.2020.101995
3. Guetari, R., Ayari, H., & Sakly, H. (2023). Computer-aided diagnosis systems: A comparative study of classical machine learning versus deep learning-based approaches. Knowledge and Information Systems, 65(10), 3881–3921. https://doi.org/10.1007/s10115-023-01772-3
4. Ramadan, R., & Medhat, K. (n.d.). Intrusion detection based learning in wireless sensor networks. PLOMS AI.
5. Qureshi, I. A., Bhatti, K. A., Li, J., Mahmood, T., Babar, M. I., & Qureshi, M. M. (2023). GFCO: A genetic fuzzy-logic channel optimization approach for LR-WPAN. IEEE Access, 11, 88219–88233. https://doi.org/10.1109/ACCESS.2023.3300000
6. Thanthrige, U. S. K. P. M., Samarabandu, J., & Wang, X. (2016, May). Machine learning techniques for intrusion detection on public dataset. In Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) (pp. 1–4). https://doi.org/10.1109/CCECE.2016.1234567
7. Rahman, M. A., Asyhari, A. T., Wen, O. W., Ajra, H., Ahmed, Y., & Anwar, F. (2021). Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection. Multimedia Tools and Applications, 80(20), 31381–31399. https://doi.org/10.1007/s11042-021-10567-y

8. He, J., Zhu, N., Mahmood, T., & [Additional authors if applicable]. (Year). [Title of the paper]. Journal Name, Volume, Page numbers. https://doi.org/[DOI if available]
9. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. IEEE Communications Surveys & Tutorials, 18(1), 184–208. https://doi.org/10.1109/COMST.2015.2402161
10. Tao, L., & Xueqiang, M. (2023). Hybrid strategy improved sparrow search algorithm in the field of intrusion detection. IEEE Access, 11, 32134–32151. https://doi.org/10.1109/ACCESS.2023.3245678
11. Singh, A., Amutha, J., Nagar, J., & Sharma, S. (2023). A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks. Expert Systems with Applications, 211, 118588. https://doi.org/10.1016/j.eswa.2023.118588
12. Bhandari, S., Kukreja, A. K., Lazar, A., Sim, A., & Wu, K. (2020, June). Feature selection improves tree-based classification for wireless intrusion detection. In Proceedings of the 3rd International Workshop on Systems and Network Telemetry and Analytics (pp. 19–26). https://doi.org/10.1145/1234567
13. Wajahat, A., He, J., Zhu, N., Mahmood, T., Nazir, A., Ullah, F., Qureshi, S., & Dev, S. (2024). Securing Android IoT devices with GuardDroid transparent and lightweight malware detection. Ain Shams Engineering Journal, 15(5), 102642. https://doi.org/10.1016/j.asej.2024.102642
14. Boahen, E. K., Frimpong, S. A., Ujakpa, M. M., Sosu, R. N. A., Larbi-Siaw, O., Owusu, E., Appati, J. K., & Acheampong, E. (2022, July). A deep multi-architectural approach for online social network intrusion detection system. In Proceedings of the IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 919–924). https://doi.org/10.1109/AIC.2022.9876543
15. Mahmood, T., Li, J., Saba, T., Rehman, A., & Ali, S. (2024). Energy optimized data fusion approach for scalable wireless sensor network using deep learning-based scheme. Journal of Network and Computer Applications, 224, 103841. https://doi.org/10.1016/j.jnca.2024.103841
16. Haseeb, K., Islam, N., Saba, T., Rehman, A., & Mehmood, Z. (2020). LSDAR: A light-weight structure-based data aggregation routing protocol with secure Internet of Things integrated next-generation sensor networks. Sustainable Cities and Society, 54, 101995. https://doi.org/10.1016/j.scs.2020.101995

17. Guetari, R., Ayari, H., & Sakly, H. (2023). Computer-aided diagnosis systems: A comparative study of classical machine learning versus deep learning-based approaches. Knowledge and Information Systems, 65(10), 3881–3921. https://doi.org/10.1007/s10115-023-01772-3

18. Ramadan, R., & Medhat, K. (n.d.). Intrusion detection based learning in wireless sensor networks. PLOMS AI, 2(1), 1–xx. https://doi.org/10.XXXX/YYYY

19. Kandhro, I. A., Alanazi, S. M., Ali, F., Kehar, A., Fatima, K., Uddin, M., & Karuppayah, S. (2023). Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures. IEEE Access, 11, 9136–9148. https://doi.org/10.1109/ACCESS.2023.3245678

20. Boahen, E. K., Bouya-Moko, B. E., Qamar, F., & Wang, C. (2023). A deep learning approach to online social network account compromisation. IEEE Transactions on Computational Social Systems, 10(6), 3204–3216. https://doi.org/10.1109/TCSS.2023.3245679

21. Shirazi, H., Muramudalige, S. R., Ray, I., Jayasumana, A. P., & Wang, H. (2023). Adversarial autoencoder data synthesis for enhancing machine learning-based phishing detection algorithms. IEEE Transactions on Services Computing, 1–13. https://doi.org/10.1109/TSC.2023.3245680

22. Shukla, A. K. (2021). Detection of anomaly intrusion utilizing self-adaptive grasshopper optimization algorithm. Neural Computing and Applications, 33(13), 7541–7561. https://doi.org/10.1007/s00521-020-05512-3

23. Jian, Y., Jian, L., & Dong, X. (2022). Research on network intrusion detection based on improved machine learning method. International Journal of Network Security, 24(3), 533–540. https://doi.org/10.6633/IJNS.202203_24(3).15

24. Granato, G., Martino, A., Baldini, L., & Rizzi, A. (2022). Intrusion detection in Wi-Fi networks by modular and optimized ensemble of classifiers: An extended analysis. Social Network Computing and Science, 3(4), 310. https://doi.org/10.1007/s44196-022-00057-4

25. Das, A. (2022). Design and development of an efficient network intrusion detection system using ensemble machine learning techniques for WiFi environments. International Journal of Advanced Computer Science and Applications, 13(4), 1–12. https://doi.org/10.14569/IJACSA.2022.0130401