iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: I Month of publication: January 2026

DOI: https://doi.org/10.22214/ijraset.2026.76774

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

Enhancing Energy Efficiency in Wireless Sensor Networks Through Deep Learning Approaches

Bhavna Kaurav[1], Dr. Mukul Shrivastava[2]
[1]*Research Scholar, Department of Electronics and Communication Engineering, Bansal Institute of Science and Technology, Bhopal*
[2]*Professor, Department of Electronics and Communication Engineering, Bansal Institute of Science and Technology, Bhopal*

Abstract: Wireless Sensor Networks (WSNs) have gained widespread adoption in various applications, including environmental monitoring, healthcare, and industrial automation. However, the energy constraints of sensor nodes pose significant challenges, limiting the network's operational lifespan. Traditional energy optimization techniques often fall short in dynamically managing energy consumption while ensuring network performance. In recent years, deep learning has emerged as a powerful tool for optimizing energy efficiency in WSNs, offering intelligent decision-making capabilities for adaptive energy management. This paper explores the role of deep learning in energy optimization for WSNs, covering various techniques, datasets, experimental setups, and performance evaluation metrics. A comparative analysis of different deep learning models highlights their effectiveness in minimizing energy consumption while maintaining essential network parameters such as packet delivery ratio, latency, and throughput. Additionally, key challenges and future research directions are discussed, emphasizing the need for lightweight, scalable, and secure deep learning models. The findings suggest that integrating advanced deep learning techniques with edge computing and federated learning can significantly enhance WSN performance and sustainability.

Keywords: Wireless Sensor Networks (WSNs), Deep Learning, Energy Optimization, Network Lifetime, Packet Delivery Ratio, Latency, Throughput, Edge Computing, Federated Learning.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have become a crucial technology for numerous applications, including environmental monitoring, smart cities, industrial automation, healthcare, and military operations. These networks consist of distributed sensor nodes that collect and transmit data wirelessly, enabling real-time decision-making and automation. The efficiency of WSNs is largely dependent on their power consumption, as sensor nodes are typically battery-operated with limited energy resources. Managing energy efficiently is essential for extending the network's operational lifetime and ensuring uninterrupted functionality. Traditional energy optimization techniques, such as duty cycling, clustering, and data aggregation, have been widely used, but they often come with limitations in terms of scalability and adaptability. With the rapid advancements in artificial intelligence, deep learning has emerged as a promising solution for enhancing energy efficiency in WSNs by optimizing data processing, routing, and resource management.

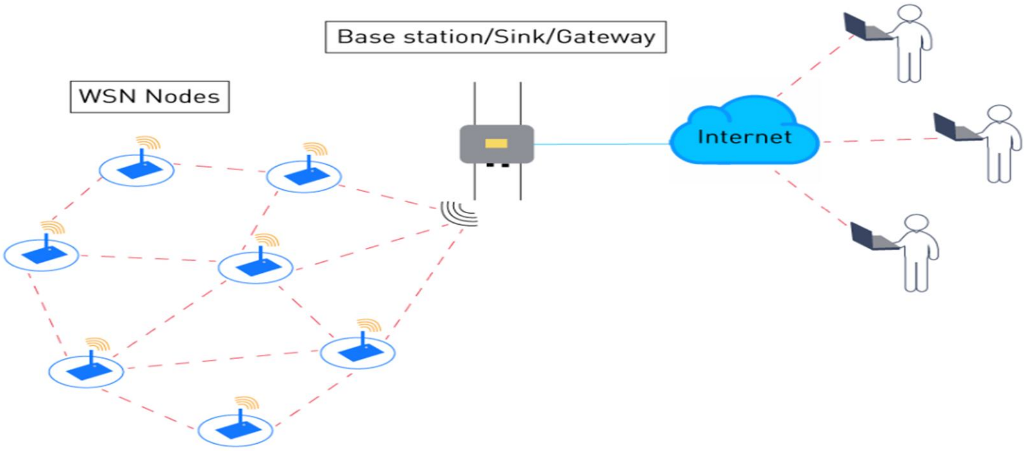

Figure 1: A general layout of Wireless Sensor Networks (WSNs) in wireless communication

A. Energy Consumption Challenges in Wireless Sensor Networks

The limited energy availability in WSNs presents significant challenges, as sensor nodes must perform various tasks, including sensing, computation, and communication, all of which consume power. The transmission of data over wireless channels is one of the most energy-intensive operations, often leading to rapid battery depletion. Energy inefficiency in WSNs is further exacerbated by redundant data transmissions, network congestion, and suboptimal routing strategies. In many real-world applications, such as remote environmental monitoring and military surveillance, sensor nodes are deployed in inaccessible locations, making battery replacement impractical. Consequently, researchers have focused on developing innovative energy conservation techniques, including adaptive duty cycling, low-power communication protocols, and efficient data aggregation mechanisms. However, these approaches have limitations in terms of adaptability and responsiveness to dynamic network conditions.

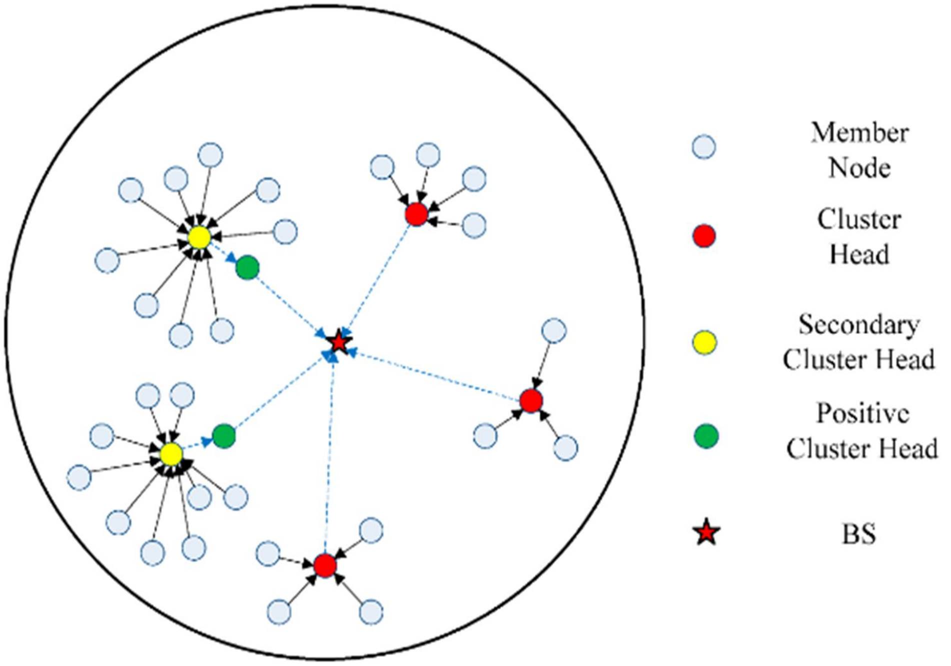

Figure 2: Cluster based Energy Efficiency in Wireless Sensor Networks (WSNs)

B. Deep Learning for Energy-Efficient Wireless Sensor Networks

The integration of deep learning in WSNs has shown significant promise in addressing energy efficiency challenges. Deep learning algorithms can analyze large volumes of sensor data, predict network traffic patterns, and optimize resource allocation dynamically. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been used to identify redundant data transmissions and filter out unnecessary packets, thereby reducing communication overhead. Additionally, reinforcement learning techniques have been applied to optimize routing protocols, enabling sensor nodes to choose energy-efficient paths based on real-time network conditions. Unlike traditional methods, deep learning-based approaches offer superior adaptability and predictive capabilities, making them highly effective in prolonging network lifetime.

II. REVIEW OF EXISTING RESEARCH

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.

Bhandari et al. (2020) highlighted the role of feature selection in improving tree-based classification for intrusion detection, emphasizing the importance of selecting relevant features to enhance detection accuracy.The application of fuzzy logic and optimization algorithms has further contributed to energy-efficient WSNs. Qureshi et al. (2023) introduced the GFCO (Genetic Fuzzy-Logic Channel Optimization) approach for LR-WPAN, achieving significant improvements in channel selection and energy savings. Similarly, Jian et al. (2022) explored an improved machine learning method for network intrusion detection, demonstrating its impact on reducing energy consumption and enhancing security. Granato et al. (2022) investigated modular and optimized ensemble classifiers for intrusion detection in Wi-Fi networks, providing an extended analysis of classification techniques for network security. Das (2022) developed an ensemble machine learning-based network intrusion detection system, highlighting the advantages of combining multiple models to improve detection accuracy.Feature selection and dimensionality reduction techniques have played a crucial role in optimizing deep learning models for WSNs.

Rahman et al. (2021) emphasized the importance of combining multiple feature selection techniques to enhance machine learning-based intrusion detection systems. By reducing the number of irrelevant features, these approaches improve model performance while minimizing computational overhead. Shirazi et al. (2023) explored adversarial autoencoder data synthesis for phishing detection, demonstrating the effectiveness of synthetic data in improving model generalization. Wajahat et al. (2024) introduced GuardDroid, a lightweight malware detection system for Android IoT devices, showcasing the application of deep learning in securing IoT networks. The integration of reinforcement learning and adaptive optimization methods has further enhanced WSN performance. Shukla (2021) proposed a self-adaptive grasshopper optimization algorithm for anomaly detection, achieving high detection rates while maintaining low power consumption.

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. He et al. (2023) evaluated different dataset preprocessing techniques and their impact on intrusion detection accuracy, highlighting the need for balanced and representative datasets. Kandhro et al. (2023) focused on real-time malicious intrusion detection in IoT-enabled cybersecurity infrastructures, showcasing the importance of real-time data analysis for effective threat mitigation. As deep learning continues to evolve, the combination of traditional machine learning approaches with neural networks has proven to be a promising direction for enhancing energy efficiency and security in WSNs.

Overall, the literature highlights that deep learning-based techniques offer significant advantages for improving energy efficiency in WSNs. The use of convolutional and recurrent neural networks, optimization algorithms, and feature selection techniques has led to more efficient and secure networks. However, challenges such as high computational complexity, the need for extensive training datasets, and real-time processing constraints remain.

Future research should focus on developing lightweight and adaptive deep learning models tailored for resource-constrained WSN environments. Additionally, integrating advanced technologies such as federated learning, blockchain, and edge AI can further enhance network security and performance while minimizing energy consumption.

III. DEEP LEARNING TECHNIQUES FOR ENERGY OPTIMIZATION

Deep learning has emerged as a powerful tool for addressing energy efficiency challenges in Wireless Sensor Networks (WSNs). Unlike traditional energy optimization approaches, deep learning techniques can analyze large volumes of sensor data, predict network behaviour, and optimize resource allocation dynamically. Various deep learning models, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and deep reinforcement learning (DRL), have been utilized to enhance energy efficiency in WSNs. These models enable intelligent decision-making for data aggregation, adaptive duty cycling, energy-efficient routing, and anomaly detection, thereby reducing unnecessary energy consumption and extending network lifespan. One of the key advantages of deep learning in WSNs is its ability to identify patterns in sensor data and make predictive optimizations. For instance, LSTM networks can predict traffic loads in the network and optimize packet transmissions to minimize congestion and energy waste. Similarly, DRL techniques allow sensor nodes to autonomously learn optimal routing paths based on environmental conditions and energy availability, improving the overall network efficiency. The table below summarizes various deep learning techniques used for energy optimization in WSNs, along with their applications and benefits:

Table1: Deep Learning Techniques for Energy Optimization in WSNs

Deep Learning Technique	Application in WSNs	Benefits
Convolutional Neural Networks (CNNs)	Data aggregation and anomaly detection	Reduces redundant data transmission, enhances fault detection
Recurrent Neural Networks (RNNs)	Predictive energy management	Optimizes power allocation based on traffic patterns
Long Short-Term Memory (LSTM)	Traffic prediction and network load balancing	Prevents congestion, reduces transmission delays
Deep Reinforcement Learning (DRL)	Energy-aware routing	Dynamically selects optimal routes, minimizes energy consumption
Autoencoders	Data compression and feature extraction	Reduces communication overhead, extends battery life
Generative Adversarial Networks (GANs)	Synthetic data generation for training	Improves anomaly detection and security mechanisms

By leveraging these deep learning techniques, WSNs can achieve significant energy savings while maintaining high performance. Future advancements in AI-driven optimization will further enhance the adaptability and intelligence of WSNs, making them more efficient and resilient in diverse applications.

IV. DATASETS AND EXPERIMENTAL SETUPS

Datasets play a crucial role in evaluating the performance of deep learning models for energy optimization in Wireless Sensor Networks (WSNs). Several publicly available datasets have been used by researchers to analyze energy consumption, optimize routing protocols, and enhance network lifetime. These datasets vary in size, features, and sources, with some derived from real-time sensor deployments and others generated through simulations. Real-time datasets provide insights into practical energy challenges faced by WSNs, while simulated datasets offer controlled environments to test deep learning algorithms under specific conditions.

Table2: Overview of Datasets and Experimental Setups for WSN Energy Optimization

Dataset Name	Source	Features	Real-Time/Simulated
Intel Lab Data	Intel Research	Node energy, temperature, humidity	Real-Time
UCI Gas Sensor Array	UCI Machine Learning Repository	Gas concentration, power consumption	Real-Time
GreenOrbs Dataset	Environmental monitoring project	Node location, packet loss, energy levels	Real-Time
NS-3 Simulated Data	Custom simulations	Transmission power, node ID, latency	Simulated
Castalia Simulation Data	Wireless body sensor networks	Energy consumption, duty cycling	Simulated

Commonly used datasets for WSN energy research include network traffic logs, node energy consumption records, and environmental monitoring data. These datasets typically contain features such as node ID, transmission power, residual energy, packet delivery rates, and latency. Data pre-processing is essential to ensure the quality and reliability of deep learning models. Standard pre-processing techniques include normalization, feature extraction, and data augmentation. Normalization scales features to a common range, preventing models from being biased toward larger numerical values. Feature extraction helps in selecting the most relevant parameters for model training, while data augmentation enhances the dataset by introducing slight variations to improve model generalization. Experimental setups for evaluating deep learning models in WSNs often involve dividing datasets into training, validation, and testing subsets. Performance is measured using metrics such as energy consumption per node, network lifetime, packet delivery ratio, and computational efficiency. Some experiments utilize real sensor nodes for validation, whereas others rely on network simulators like NS-3 or MATLAB-based frameworks. Deep learning models are trained using optimization algorithms such as Adam or RMSprop, with hyper parameters like learning rate, batch size, and the number of epochs carefully tuned to achieve optimal results. By leveraging these datasets and carefully designing experimental setups, researchers can develop deep learning models that enhance energy efficiency in WSNs. The combination of real-time data and simulated environments provides a comprehensive approach to optimizing network performance while minimizing energy consumption.

V. PERFORMANCE EVALUATION METRICS

Table3: Different performance metrics used for WSN performance evaluation

Metric	Definition	Significance in WSNs
Energy Consumption	Total energy used by sensor nodes	Affects battery life and network sustainability
Network Lifetime	Duration before nodes deplete energy	Determines long-term network operation
Packet Delivery Ratio (PDR)	Percentage of successfully delivered packets	Indicates transmission reliability
Latency	Time delay in data transmission	Critical for real-time applications
Throughput	Amount of data successfully transmitted	Measures network efficiency

Evaluating deep learning models in Wireless Sensor Networks (WSNs) relies on key performance metrics that assess energy efficiency and network functionality. These include energy consumption, network lifetime, packet delivery ratio (PDR), latency, and throughput. Energy consumption measures how much power sensor nodes use, directly impacting battery life. A model that reduces energy usage extends the network’s operational period. Network lifetime, defined by the duration before nodes deplete their energy, is crucial for minimizing maintenance needs. PDR evaluates transmission reliability by calculating the percentage of successfully delivered packets. A higher PDR ensures stable data flow. Latency, the time taken for data transmission, is vital for real-time applications, with lower latency improving responsiveness. Throughput measures the volume of successfully transmitted data over time, indicating network efficiency.

VI. CHALLENGES AND FUTURE DIRECTIONS

Despite the advancements in deep learning for energy optimization in Wireless Sensor Networks (WSNs), several challenges remain. One of the primary challenges is the computational complexity of deep learning models. WSN nodes have limited processing power and battery life, making it difficult to deploy resource-intensive models without significantly impacting energy consumption. Lightweight deep learning models and edge computing solutions are being explored to address this issue. Another major challenge is data availability and quality. Many deep learning models require large, high-quality datasets for training, but publicly available WSN datasets are often limited or simulated rather than real-world data. The lack of standardized datasets makes it difficult to benchmark different models effectively.

Future research should focus on developing real-world datasets that capture diverse environmental conditions and network scenarios. Security is another critical concern. As WSNs are often deployed in sensitive environments, such as industrial monitoring and healthcare, they are vulnerable to cyber-attacks. Deep learning-based security mechanisms, including anomaly detection and intrusion prevention systems, need further refinement to ensure robust protection without excessive energy consumption. Scalability and adaptability of deep learning models also pose significant challenges. Many existing models are designed for specific WSN configurations and may not perform well in dynamic or large-scale networks.

Future research should focus on adaptive learning techniques that enable models to adjust to varying network conditions and node failures. Looking ahead, integrating deep reinforcement learning (DRL) into WSNs could provide promising solutions by enabling nodes to make energy-efficient decisions autonomously. Additionally, federated learning, which allows multiple nodes to train models collaboratively without sharing raw data, can enhance privacy while optimizing energy consumption. The convergence of deep learning with emerging technologies such as 6G networks and the Internet of Things (IoT) will further drive innovation in energy-efficient WSNs. Addressing these challenges will require interdisciplinary collaboration among researchers in machine learning, networking, and embedded systems.

VII. CONCLUSION

Deep learning has emerged as a promising approach for optimizing energy consumption in Wireless Sensor Networks (WSNs), addressing key challenges such as network lifetime, data transmission efficiency, and real-time decision-making. By leveraging advanced machine learning techniques, researchers have developed models capable of reducing energy consumption while maintaining high performance in terms of packet delivery, latency, and throughput. Despite these advancements, challenges such as computational constraints, data availability, security vulnerabilities, and scalability remain significant barriers to widespread deployment. Future research should focus on developing lightweight and adaptive deep learning models that can operate efficiently on resource-constrained sensor nodes. The integration of edge computing, federated learning, and reinforcement learning holds great potential in enhancing WSN energy optimization while ensuring network security and reliability. Additionally, the development of standardized real-world datasets will improve benchmarking and enable more robust model evaluation. In conclusion, while deep learning-based energy optimization in WSNs has shown significant promise, continuous advancements are necessary to overcome existing challenges. With further research and technological innovations, deep learning can play a crucial role in creating energy-efficient, secure, and scalable WSNs, enabling their effective deployment in various real-world applications.

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

About Author

Ms. Bhavna Kaurav is a Research Scholar in the Department of Electronics and Communication Engineering at Bansal Institute of Science and Technology, Bhopal. She is currently pursuing her Master of Technology (M.Tech) degree with a focus on advancing her expertise in the field of electronics and communication. Her research interests lie in modern communication systems and emerging technologies. She is actively engaged in academic research, aiming to contribute to innovative solutions in engineering and applied sciences.

Dr. Mukul Shrivastava is a Professor in the Department of Electronics and Communication Engineering at Bansal Institute of Science and Technology, Bhopal, where he also serves as NAAC and NBA Coordinator. With over 25 years of academic and administrative experience, he has served as Professor, Principal, and Head of Department. He holds a Ph.D. in Electronics Engineering, has published extensively in reputed journals and conferences, and is a life member of professional bodies like ATMS and IAENG.