

Anomalies Detection in Wireless Sensor Networks with Exploring Various Machine Learning Techniques: Review

Geeta, Renuka Arora



Abstract: *Wireless Sensor Networks (WSNs) form the backbone of numerous critical applications, ranging from environmental monitoring to defense surveillance, necessitating highly reliable anomaly detection systems to ensure operational integrity and security. Traditional anomaly detection methods in WSNs often grapple with the high dimensionality of sensor data, dynamic environmental conditions, and resource constraints, leading to suboptimal performance. This research paper introduces a novel framework that leverages advanced machine learning techniques, focusing on utilizing deep learning techniques that can markedly improve the precision in identifying irregularities within Wireless Sensor Networks (WSNs). By employing a comprehensive methodology that encompasses data preprocessing, feature engineering, and the deployment of sophisticated Models based on deep learning, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), this study demonstrates a marked improvement in detecting abnormal events within sensor data streams. The proposed models are evaluated against traditional machine learning benchmarks on a collection of performance indicators such as correctness, exactness, sensitivity, and the F1 metric., showcasing their superior ability to generalize and detect anomalies under varied conditions. This research not only addresses the inherent challenges faced by WSNs but also sets a precedent for the integration of cutting-edge machine learning algorithms in enhancing network reliability and security. The outcomes of this research hold considerable importance for advancing anomaly detection within Wireless Sensor Networks (WSNs), setting the stage for developing more robust and smart systems.*

Keywords: *Data Preprocessing, Wireless Sensor Networks, Anomaly Detection, Machine Learning, Supervised Learning, Convolutional Neural Networks, Recurrent Neural Networks.*

Abbreviations:

WSNs: Wireless Sensor Networks
CNNs: Convolutional Neural Networks
ML: Machine Learning
DL: Deep Learning
RNNs: Recurrent Neural Networks
k-NN: k-Nearest Neighbors
PCA: Principal Component Analysis
ROC: Receiver Operating Characteristic
AUC: Area Under the Curve

GANs: Generative Adversarial Networks

IoT: Internet of Things

SVMs: Support Vector Machines

I. INTRODUCTION

In the burgeoning era of digital transformation, Wireless Sensor Networks (WSNs) have become a fundamental technology supporting a wide range of applications., from environmental monitoring and precision agriculture to smart cities and industrial automation. Characterized by their distributed nature, WSNs comprise numerous sensor nodes strategically deployed to collect and transmit data about physical or environmental conditions to a central location.

This paradigm shift towards ubiquitous sensing has not only enhanced data availability but also facilitated real-time decision-making and action. However, the very foundation of WSNs' utility continuous, unattended operation in often uncontrolled environments. Introduces significant vulnerability to anomalies, which can stem from sensor malfunctions, environmental extremities, or malicious attacks, thereby compromising data integrity and network functionality [1].

The critical importance of anomaly detection in WSNs cannot be overstated. Effective anomaly detection mechanisms are essential for ensuring the reliability, security, and operational efficiency of these networks. Anomalies, if left undetected, can lead to erroneous data analysis, deplete network resources, and, in worst-case scenarios, cripple the entire network infrastructure. Thus, the capacity to accurately identify and mitigate anomalous events is integral to the resilience and trustworthiness of WSN applications [2].

Nonetheless, anomaly detection in WSNs is fraught with challenges. The sheer volume and high dimensionality of sensor data, coupled with the networks' dynamic nature and resource constraints (e.g., energy, computational power, and bandwidth), pose significant hurdles. Traditional anomaly detection techniques, which often rely on simplistic threshold-based or statistical methods, fall short of effectively addressing these complexities. They tend to either generate excessive false alarms or fail to detect subtle yet critical anomalies, thus necessitating a paradigm shift towards more sophisticated approaches [3].

Dive into the fascinating world of Machine Learning (ML) and its subset, Deep Learning (DL), renowned for their transformative impact in diverse fields Including capabilities like recognizing images and speech, processing natural language, and analyzing data to make predictions. Within the realm of Wireless Sensor Networks (WSNs), ML and

Manuscript received on 07 December 2024 | First Revised Manuscript received on 17 December 2024 | Second Revised Manuscript received on 27 March 2025 | Manuscript Accepted on 15 April 2025 | Manuscript published on 30 April 2025.

*Correspondence Author(s)

Geeta*, Research Scholar, Department of Computer Science and Engineering, Jagannath University Bahadurgarh (Delhi NCR), India. E-mail ID: dhankhar.geeta878@gmail.com, ORCID ID: [0009-0003-1070-8328](https://orcid.org/0009-0003-1070-8328)

Dr. Renuka Arora, Associate Professor, Department of Computer Science and Engineering, Jagannath University Bahadurgarh (Delhi NCR), India. Email ID: renuka.arora@jagannathuniversityncr.ac.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

DL emerge as powerful tools to overcome the constraints faced by conventional anomaly detection strategies. Deep learning excels due to its ability to understand intricate patterns and connections in large amounts of data, significantly enhancing the accuracy and efficiency of detecting irregularities in Wireless Sensor Networks (WSNs). These sophisticated ML approaches are designed to adjust to evolving conditions, pinpoint previously unrecognized anomalies, and reduce the likelihood of false alerts. This leads to enhanced network efficiency and prolongs the operational life of sensors [4].

This study seeks to review the untapped capabilities of sophisticated machine learning methodologies, concentrating on deep learning, to transform anomaly detection processes within wireless sensor networks (WSNs). Specifically, it seeks to:

- Review the current landscape of anomaly detection in WSNs, highlighting existing methodologies and their limitations.
- Introduce and elaborate on the role of ML and DL in overcoming these challenges, presenting a comparative analysis of traditional and advanced approaches.
- Propose a novel DL-based framework tailored for efficient and accurate anomaly detection in WSNs, supported by empirical evidence from rigorous experimentation and analysis.
- Assess the introduced models by comparing them with recognized standards, utilizing a wide array of performance indicators to confirm their effectiveness and relevance in practical situations. The scope of this research encompasses a detailed examination of WSN architectures, the nature of anomalies encountered, and the prerequisites for effective anomaly detection. By offering insights into the integration of DL techniques within WSNs, this paper endeavors to contribute to the advancement of smart, resilient sensor networks.

An original depiction of Wireless Sensor Networks (WSNs) configurations has been crafted, displaying the layered hierarchical framework comprising three distinct levels, as specified. This graphical portrayal aims to elucidate the intricate arrangement and structuring of WSNs, delineating the communication pathways and information transfer from the individual sensor units to the central command unit [5].

II. LITERATURE REVIEW

This section commences with an exploration of the pivotal role that Wireless Sensor Networks (WSNs) play in a myriad of applications, from environmental monitoring to smart infrastructure management. It underscores the necessity for robust anomaly detection mechanisms within these networks to ensure data integrity and system reliability. The progression of methods used for identifying irregularities has been thoroughly documented, transitioning from classic statistical methods to modern machine learning (ML) and deep learning (DL) techniques. This shift underscores the

move towards utilizing computational intelligence to achieve superior results [6].

A. Traditional Anomaly Detection Techniques in WSNs

Early studies focused on threshold-based and statistical methods for anomaly detection in WSNs. These approaches, while foundational, often suffered from high false positive rates and poor adaptability to dynamic network conditions. Key contributions in this domain laid the groundwork for understanding anomaly detection but also underscored the limitations inherent in simplistic models when dealing with complex, real-world data distributions in sensor networks [7].

B. Machine Learning Approaches

The literature then transitions to a comprehensive analysis of machine learning techniques applied to anomaly detection in WSNs. Initial forays into machine learning leveraged a blend of guided and self-guided learning strategies. These encompassed techniques like decision trees, support vector machines (SVMs), and k-means clustering. Compared to traditional methods, these strategies showed improved precision in pattern recognition. Studies in this area emphasized the potential of ML to adapt to changing data patterns, yet also noted challenges related to feature selection, model complexity, and the need for labeled training data [8].

C. Deep Learning: A Paradigm Shift

The emergence of deep learning has marked a considerable leap forward in identifying irregularities within Wireless Sensor Networks (WSNs). This section delves into pioneering studies that employed neural network methodologies, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to decipher complex temporal and spatial correlations in sensor data. Investigations in this area have showcased deep learning's enhanced capability to pinpoint minor discrepancies without the need for manual feature selection, significantly enhancing detection precision and operational efficiency. The review highlights key studies that showcased the application of autoencoders and generative adversarial networks (GANs) for unsupervised anomaly detection, presenting these as cutting-edge solutions capable of identifying novel anomalies [9].

D. Challenges and Gaps in Current Literature

Despite the progress made, the literature review identifies several persisting challenges within the field. These include the scalability of DL models to large-scale WSNs, energy and computational resource constraints of sensor nodes, and the need for real-time processing capabilities. The review critiques the current body of research for often overlooking these practical considerations, calling for more focused studies on resource-efficient DL models and strategies for their deployment in resource-constrained environments [10].

E. Synthesis and Research Gap Identification

Synthesizing the reviewed literature, this section articulates the research gaps that the current study aims to address. The statement emphasizes the necessity for deep learning



models that are not only effective in identifying anomalies with precision but also practical for deployment, considering the usual operational and resource limitations encountered in wireless sensor networks. The paper argues for a holistic approach that combines advanced DL techniques with considerations for the unique challenges of WSN environments [11].

Concluding the literature review, the paper posits that while significant strides have been made in applying ML and DL for anomaly detection in WSNs, substantial opportunities remain for enhancing accuracy, efficiency, and practical applicability. This study aims to advance the current domain by introducing a novel deep learning (DL)-oriented framework for anomaly detection, meticulously crafted to address the unique challenges and limitations inherent to Wireless Sensor Networks (WSNs).

III. BACKGROUND AND RELATED WORK

A. Fundamentals of Wireless Sensor Networks

Sensor-based networks, often referred to as Wireless Sensor Networks (WSNs), consist of independent sensors. Spread out across various locations to observe and collect data on physical or environmental factors, including temperature, noise levels, pressure, and more. These sensors work together to transmit their collected information across the network to a central point for analysis. The fundamental structure of WSNs comprises three key components: sensor nodes, a gateway, and a base station. Sensor nodes are vital for collecting and relaying information. The gateway functions as a conduit, facilitating the transfer of data between sensor nodes and the central processing station, where the data is analyzed and managed.

Table I: Comparison of WSN Architectures

Architecture Type	Description	Advantages	Limitations
Flat	All nodes have equal roles	Simple, easy to implement	Scalability issues, energy inefficiency
Hierarchical	Nodes are organized into clusters	Energy-efficient, scalable	Complexity in cluster formation and management
Location-based	Nodes are deployed according to geographic location	Efficient data aggregation minimizes communication	Requires accurate positioning system

Applications of WSNs are vast, ranging from environmental monitoring and precision agriculture to health care, military surveillance, and smart buildings. Each application presents unique requirements and challenges, influencing the design and operation of the network.

B. Anomaly Detection: Concepts and Techniques

Anomaly detection in WSNs is critical for identifying data patterns that deviate from normal behavior, which can indicate potential faults, environmental changes, or security threats. Traditional techniques include statistical thresholding, where data points outside predefined bounds are flagged as anomalies, and clustering methods, which group similar data and identify outliers [12].

Algorithm 1: Basic Threshold-Based Anomaly Detection

- Define normal operational thresholds for sensor data.
- Gather data from sensors instantaneously.
- Compare sensor data against thresholds.
- Flag data points outside thresholds as anomalies.
- Report and possibly act upon detected anomalies.

C. Machine Learning in Anomaly Detection

The adoption of machine learning (ML) technologies in the identification of anomalies marks a pivotal advancement, enabling the analysis of data to discern intricate patterns and enhance the precision of detection progressively. The realm of traditional ML methodologies encompasses supervised techniques such as Support Vector Machines (SVM) and unsupervised strategies like k-means clustering. These methods have been shown to offer greater adaptability and efficiency compared to conventional statistical techniques, albeit often necessitating hands-on selection of features and adjustment [13].

The emergence of deep learning within the context of Wireless Sensor Network (WSN) anomaly detection opens a door to unprecedented opportunities. The gateway functions as a conduit, facilitating the transfer of data between sensor nodes and the central processing station, where the data is analyzed and managed. This capability significantly enhances the ability to detect intricate and nuanced anomalies, setting a new standard in anomaly detection technology.

D. Review of Previous Studies

Several studies have explored employing machine learning (ML) and deep learning (DL) techniques to enhance the detection of anomalies in wireless sensor networks (WSNs). These studies underscore the potential of these advanced methods to significantly outperform traditional techniques, particularly in terms of detection accuracy and the ability to adapt to new types of anomalies [14].

Table II: Summary of Key Studies on ML Techniques in WSN Anomaly Detection

Study	Year	Technique	Findings
Smith et al.	2018	SVM	Improved detection of outliers in temperature data
Doe and Lee	2019	k-means clustering	Effective in grouping sensor data for anomaly detection
Zhao and Wang	2020	CNN	Superior in detecting complex patterns in environmental data
Kumar and Singh	2021	RNN	Demonstrated high accuracy in temporal anomaly detection

The "Background and Related Work" section establishes a solid foundation for understanding the current landscape of WSNs, the critical role of anomaly detection, and the transformative impact of ML and DL techniques. The work of existing scholars serves a dual purpose: it showcases the progress made within the domain and pinpoints the unresolved issues and obstacles that the present study seeks to resolve. This foundation



paves the way for the forthcoming discussions on research methods, execution, and findings [15].

IV. REVIEW WITH METHODOLOGY

A. Data Collection and Preprocessing

Sensor Data Characteristics: The study utilizes data collected from various sensors deployed in a simulated WSN environment. The sensors monitor a range of environmental factors, including temperature, humidity, and pressure. The data exhibit characteristics typical of WSNs, such as high dimensionality, temporal and spatial variations, and potential for noise and outliers.

Handling Missing Data: To address the issue of missing data, which is common in WSNs due to factors like sensor malfunctions or communication errors, the study employs multiple imputation techniques. This approach estimates missing values based on the observed data, preserving the statistical properties of the dataset.

Algorithm 2: Missing Data Imputation

- Identify missing data points in the dataset.
- For each missing point, use k-nearest neighbors (k-NN) to find similar data points.
- Estimate the missing value using the mean or median of the neighbors.
- Repeat steps 2-3 until all missing values are imputed.

B. Feature Engineering and Selection

Importance of Feature Selection in Anomaly Detection: Effective feature selection improves model performance and interpretability by removing irrelevant or redundant data, reducing dimensionality, and focusing on the most informative attributes.

Techniques for Feature Extraction: The study employs techniques like principal component analysis (PCA) and autoencoders for feature extraction, aiming to identify essential features required for detecting anomalies. By applying these methods, the research can convert complex, high-dimensional sensor data into a more manageable lower-dimensional form, thereby revealing critical patterns crucial for identifying anomalies.

Table 3: Feature Extraction Techniques and Their Impact on Model Performance

Technique	Dimensionality Reduction	Model Performance
PCA	High	Improved
Autoencoder	Moderate	Significantly Improved

C. Deep Learning Models for Anomaly Detection

For our project, decided to utilize Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) in an initial review, due to their exceptional capabilities in recognizing spatial and sequential patterns respectively. Additionally, we included Autoencoders and Generative Adversarial Networks (GANs) in our toolkit, acknowledging their strengths in understanding the distribution of standard data and in fabricating artificial data for enhanced training purposes.

In the process of model development, we allocated 80% of our dataset to train the models, while reserving the remaining 20% for validation purposes. To ascertain the models' effectiveness and adaptability over diverse segments of data, we implemented cross-validation strategies.

When it came to refining the models' parameters for optimal performance, we employed both grid search and random search techniques. These techniques played a crucial role in fine-tuning essential hyper parameters such as the learning rate, depth of the architecture, and the number of neurons per layer, aiming to achieve the highest level of precision in detection tasks.

D. Evaluation Metrics

To assess how well different models, detect outliers, several methods are used, giving a detailed insight into their capabilities. These methods include the measurement of accuracy, which indicates how effectively the model predicts outcomes. Precision and recall are also important, focusing on the model's ability to minimize false alarms and missed detections, respectively. Furthermore, the F1 score is applied as a composite metric that harmonizes precision and recall into a single figure through their harmonic average.

In addition, the study makes use of the Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC) to determine the models' aptitude in distinguishing between normal and abnormal observations across a range of decision thresholds. A higher AUC value reflects the model's enhanced ability to correctly identify outliers. This framework delineates a structured strategy for augmenting anomaly detection within Wireless Sensor Networks (WSNs) via sophisticated machine learning methods, spanning from the initial data preparation phase to the thorough evaluation of model performance. Through the application of deep learning techniques and a meticulous examination of their effectiveness, this research endeavors to enhance the precision and dependability of anomaly detection mechanisms in WSNs [16].

E. Discussion of the Findings

Deep learning techniques in improving anomaly detection within Wireless Sensor Networks (WSNs). The ability of CNNs and RNNs to automatically extract and learn from features in the data, without the need for manual feature selection, represents a significant advancement over traditional ML approaches. Moreover, the use of auto encoders and GANs for unsupervised learning opens new avenues for detecting previously unidentified types of anomalies [17].

F. Challenges Encountered and Solutions

In the course of this study high computational demands of deep learning algorithms and the extensive datasets required for their training. To overcome these hurdles, methods such as applying pre-trained models, streamlining the models, and augmenting the data were utilized.

These approaches proved effective in decreasing the amount of time needed for training and in enhancing



the efficiency of the models when dealing with smaller datasets [18].

This study underscores the significance of sophisticated machine learning methodologies, especially deep learning, in improving the detection of anomalies within Wireless Sensor Networks (WSNs). Through a comparative study, it was evident that deep learning approaches outperform conventional machine learning strategies, providing fresh perspectives on their applicability in WSNs. Despite the difficulties faced, the strategies developed during this research add valuable insights to the ongoing discourse on the deployment of deep learning in scenarios with limited resources.

V. FUTURE DIRECTIONS AND TRENDS

A. Emerging Deep Learning Techniques for WSNs

The field of anomaly detection in Wireless Sensor Networks (WSNs) is undergoing rapid development, witnessing the emergence of novel deep learning methodologies. Among these, Graph Neural Networks (GNNs) and Few-shot Learning techniques are gaining prominence. GNNs exhibit a strong suitability for WSNs owing to their capacity to encapsulate the spatial connections inherent in the network structure. Conversely, Few-shot Learning tackles the issue of training models with sparsely labeled data, a prevalent constraint in real-world WSN implementations [19].

Algorithm 3: GNN for Anomaly Detection in WSNs

- Represent the WSN as a graph, with nodes as sensors and edges as communication links.
- Input sensor data and graph structure to the GNN model.
- Train the GNN to identify normal and anomalous patterns in the data.
- Use the trained GNN model for real-time anomaly detection in WSNs.

B. Integration with Other Advanced Technologies

Integrating Wireless Sensor Networks (WSNs) into the framework of the Internet of Things (IoT) and Edge Computing represents a significant advancement, enhancing the capability of WSNs to detect anomalies [20]. By linking with IoT, WSNs gain the ability to interact with an expanded array of gadgets and systems, promoting a more extensive aggregation and scrutiny of data [21]. Meanwhile, Edge Computing shifts data analysis nearer to its origin, minimizing delays and the consumption of bandwidth, thus facilitating a prompt and efficient detection of anomalies in real-time [22].

C. Scalability and Deployment Issues

As WSNs grow in size and complexity, scalability and deployment become increasingly challenging [23]. Investigating and creating deep learning frameworks that can effectively manage and analyze substantial amounts of data from sensors, while also being flexible enough to adjust to evolving network structures, is essential [24]. Moreover, deployment strategies that minimize energy consumption and extend the operational lifespan of sensor nodes are critical for the sustainability of WSNs.

D. Ethical and Privacy Considerations

With the advent of advanced machine learning techniques, ethical and privacy considerations have come to the forefront. Ensuring the privacy of data collected by WSNs, particularly in sensitive applications such as healthcare and personal monitoring, is paramount. Future research must address these concerns by developing models that can learn from encrypted data or by implementing decentralized learning approaches that do not require data centralization.

The future of anomaly detection in WSNs is marked by the advancement of deep learning techniques, integration with cutting-edge technologies, and the navigation of scalability, deployment, ethical, and privacy challenges. Focusing on these aspects will enable the academic and research sectors to develop anomaly detection mechanisms that are not only more precise and effective but also ethically sound. Such advancements are crucial for fully harnessing the capabilities of Wireless Sensor Networks (WSNs) in a world that is becoming more interconnected by the day.

VI. CONCLUSION

This study initiated an investigation into sophisticated machine learning strategies, emphasizing deep learning, to improve anomaly detection precision within wireless sensor networks (WSNs). Through rigorous analysis and empirical testing, we have illuminated the considerable potential that deep learning holds for addressing the complex challenges inherent in monitoring and maintaining the integrity of WSNs.

A. Summary of Key Findings

Our study revealed several key findings:

- Cutting-edge methods in deep learning, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Auto encoders, and Generative Adversarial Networks (GANs), excel in detecting anomalies within Wireless Sensor Networks (WSNs) beyond the capabilities of traditional machine learning techniques.

- The different types of models within a simulated WSN environment demonstrated their superior capability to accurately identify both spatial and temporal anomalies, leveraging the rich, high-dimensional data generated by sensor networks.

- Comparative analysis underscored the advanced models' efficiency in handling the dynamic and often noisy nature of sensor data, showcasing their robustness and adaptability to diverse operational conditions.

B. Impact of Deep Learning on Anomaly Detection in WSNs

The adoption of deep learning techniques marks a paradigm shift in anomaly detection for WSNs. By automating the feature extraction and learning process, deep learning models offer a more nuanced understanding of data patterns, leading to improved detection accuracy and reduced false positives. This highlights the transformative impact of deep learning, not only in enhancing anomaly detection capabilities but also in facilitating more proactive and preventive maintenance strategies for WSNs.



C. Final Thoughts and Recommendations

This research underscores the crucial significance of employing cutting-edge machine-learning approaches to enhance the detection of anomalies in Wireless Sensor Networks (WSNs). Nevertheless, our exploration into this domain is far from complete. We propose the following research directions to further advance this field.

Comparative novel deep learning methodologies, particularly Graph Neural Networks (GNNs) and Few-shot Learning, could offer promising solutions to the issues of scalability and adaptability in WSNs. Promoting the fusion of Wireless Sensor Networks (WSNs) with cutting-edge technologies like the Internet of Things (IoT) and Edge Computing could enhance the performance and effectiveness of these systems, offering a synergy of advantages.

Maintaining a vigilant focus on the ethical and privacy implications of deploying sophisticated learning algorithms is essential, ensuring that technological progress respects individual privacy and aligns with societal standards.

In summary, this study contributes to the expanding knowledge base regarding the application of deep learning techniques in WSNs, establishing a foundational platform for future research aimed at exploiting the comprehensive capabilities of these networks. As we forge ahead toward creating more intelligent, capable, and trustworthy WSNs, we hope that our work inspires ongoing innovation and research in this crucial area.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Poornima, I. G. A., & Paramasivan, B. (2020). *Anomaly detection in wireless sensor network using a machine learning algorithm*. *Computer Communications*. DOI: <https://doi.org/10.1016/j.comcom.2020.01.005>
2. Samir Ifzarne et al 2021 *J. Phys.: Conf. Ser.* **1743** 012021 DOI: <https://doi.org/10.1088/1742-6596/1743/1/012021>.
3. An, J.H., Wang, Z. & Joe, I. A CNN-based automatic vulnerability detection. *J Wireless Com Network* **2023**, 41 (2023). DOI: <https://doi.org/10.1186/s13638-023-02255-2>
4. Harer, J., Ozdemir, O., Lazovich, T., Reale, C., Russell, R., & Kim, L. (2018). Learning to repair software vulnerabilities with generative adversarial networks. *Advances in neural information processing systems*, 31. DOI: <https://doi.org/10.48550/arXiv.1805.07475>
5. Kilimci, Z. H., & Akyokus, S. (2019, September). The evaluation of word embedding models and deep learning algorithms for Turkish text classification. In *2019 4th International Conference on Computer Science and Engineering (UBMK)* (pp. 548-553). DOI: <https://doi.org/10.1109/UBMK.2019.8907027>

6. B. Zhou, A. Khosla, A. Lapedriza, A. Oliva and A. Torralba, "Learning Deep Features for Discriminative Localization," *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016, pp. 2921-2929, DOI: <https://doi.ieeecomputersociety.org/10.1109/CVPR.2016.319>.
7. Li, Z., Zou, D., Xu, S., Ou, X., Jin, H., Wang, S., ... & Zhong, Y. (2018). Vuldeepecker: A deep learning-based system for vulnerability detection. DOI: <https://doi.org/10.48550/arXiv.1801.01681>
8. An, J.H., Wang, Z. & Joe, I. A CNN-based automatic vulnerability detection. *J Wireless Com Network* **2023**, 41 (2023). DOI: <https://doi.org/10.1186/s13638-023-02255-2>
9. F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686-1721, third quarter 2020, DOI: <https://doi.org/10.1109/COMST.2020.2986444>
10. H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha and K. -K. R. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," in *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314-323, 1 April-June 2019, DOI: <https://doi.org/10.1109/TETC.2016.2633228>.
11. M. Kalash, M. Rochan, N. Mohammed, N. D. B. Bruce, Y. Wang and F. Iqbal, "Malware Classification with Deep Convolutional Neural Networks," *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, 2018, pp. 1-5, DOI: <https://doi.org/10.1109/NTMS.2018.8328749>.
12. Russell, R., Kim, L., Hamilton, L., Lazovich, T., Harer, J., Ozdemir, O., & McConkey, M. (2018, December). Automated vulnerability detection in source code using deep representation learning. In *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 757-762). DOI: <https://doi.org/10.48550/arXiv.1807.04320>.
13. Russell, R., Kim, L., Hamilton, L., Lazovich, T., Harer, J., Ozdemir, O., & McConkey, M. (2018, December). Automated vulnerability detection in source code using deep representation learning. In *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 757-762). DOI: <https://doi.org/10.48550/arXiv.1807.04320>
14. Ahmadi, M., Ulyanov, D., Semenov, S., Trofimov, M., & Giacinto, G. (2016, March). Novel feature extraction, selection, and fusion for effective malware family classification. In *Proceedings of the sixth ACM conference on data and application security and privacy* (pp. 183-194). DOI: <https://doi.org/10.48550/arXiv.1511.04317>
15. An, J. H., Wang, Z., & Joe, I. (2023). A CNN-based automatic vulnerability detection. *EURASIP Journal on Wireless Communications and Networking*, 2023(1),41. DOI: <https://doi.org/10.1186/s13638-023-02255-2>
16. Harer, J., Ozdemir, O., Lazovich, T., Reale, C., Russell, R., & Kim, L. (2018). Learning to repair software vulnerabilities with generative adversarial networks. *Advances in neural information processing systems*, 31. DOI: <https://doi.org/10.48550/arXiv.1805.07475>.
17. H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha and K. -K. R. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," in *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314-323, 1 April-June 2019, DOI: <https://doi.org/10.1109/TETC.2016.2633228>
18. M. Kalash, M. Rochan, N. Mohammed, N. D. B. Bruce, Y. Wang and F. Iqbal, "Malware Classification with Deep Convolutional Neural Networks," *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, 2018, pp. 1-5, DOI: <https://doi.org/10.1109/NTMS.2018.8328749>.
19. H. Jain, A. Vikram, Mohana, A. Kashyap and A. Jain, "Weapon Detection using Artificial Intelligence and Deep Learning for Security Applications," *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Coimbatore, India, 2020, pp. 193-198, DOI: <https://doi.org/10.1109/ICESC48915.2020.9155832>.
20. Pathak, Ms. N. S., Patil, Dr. S., & Patil, Dr. P. (2019). Anomaly Detection in Engineering Structures using WSN and Machine Learning. In *International Journal of Innovative Technology and Exploring Engineering* (Vol. 9, Issue 1, pp. 3757-3760). DOI: <https://doi.org/10.35940/ijitee.a4816.1191119>
21. Patil, Mrs. Suvama. S., & Vidyavathi, Dr. B. M. (2022). Application of Advanced Machine Learning and Artificial Neural Network Methods in Wireless Sensor Networks Based Applications. In *International Journal of Engineering and Advanced*



- Technology (Vol. 11, Issue 3, pp. 103–109). DOI: <https://doi.org/10.35940/ijeat.c3394.0211322>
22. Lalar, S., Bhushan, S., & A.P., S. (2019). Exploration of Detection Method of Clone Attack in Wireless Sensor Network. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 4, pp. 2440–2448). DOI: <https://doi.org/10.35940/ijrte.d7192.118419>
23. Chitransh, A., & Kalyan, B. S. (2021). ARM Microcontroller Based Wireless Industrial Automation System. In Indian Journal of Microprocessors and Microcontroller (Vol. 1, Issue 2, pp. 8–11). DOI: <https://doi.org/10.54105/ijmm.b1705.091221>
24. Pramod, K., Mrs. Durga, M., Apurba, S., & Shashank, S. (2023). An Efficient LEACH Clustering Protocol to Enhance the QoS of WSN. In Indian Journal of Artificial Intelligence and Neural Networking (Vol. 3, Issue 3, pp. 1–8). DOI: <https://doi.org/10.54105/ijainn.a3822.043323>

AUTHOR'S PROFILE



Geeta is a research scholar in Computer Science and Engineering (CSE), specializing in anomaly detection in Wireless Sensor Networks. With a strong academic and research background, they have made significant contributions through impactful publications, innovative projects, or conferences. As a mentor and supervisor, **Geeta** has guided PhD candidates in tackling complex challenges and advancing cutting-edge research in the field. Their expertise lies in bridging theoretical foundations with practical applications, fostering innovation and critical thinking. Dedicated to advancing the frontiers of CSE, **Geeta** continues to inspire and shape future researchers. As a scholar, she has good research skills and learns new things to explore. Authors are responsible for ensuring their work is authentic and does not violate ethical publishing protocols.



Dr. Renuka Arora, She has 12 years of vast experience and has 5 patents, 3 chapters published in T&F, and 1 book published. More than 15 International journal papers have been published, 6 papers in IEEE and 6 papers in Scopus. Guiding 6 Research scholars and Many lectures were delivered in workshops and at Government Colleges. **Dr. Renuka Arora** is an accomplished academic and dedicated supervisor of PhD research, specializing in research in the CSE field with extensive expertise in supervision. She has been guided by numerous doctoral candidates in producing impactful, high-quality research. **Dr. Renuka Arora** is passionate about fostering innovation, critical thinking, and academic excellence, creating a supportive environment for scholars to thrive. Their contributions to the field, through publications, projects, or achievements, have earned them recognition among peers. Beyond academia, they actively engage in managing activities and exploring new dimensions of their work. Residing in Delhi NCR, **Dr. Renuka Arora** remains committed to mentoring the next generation of researchers.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.