AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(2026)
www.ajmimc.com

IRAB-NET: An Interpretable Hybrid Boosting Framework for Intelligent Routing Attack Detection and Reliability Estimation in WSNs

Bhaskar Babu Kuchanapally[1], Mogulaji Vyshnavi[2], Kusuma Pranitha[2], Katakam Sai Shiva[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

ABSTRACT

Wireless Sensor Networks (WSN) are widely applied in environmental monitoring, healthcare, and industrial automation, where secure and reliable communication is critical. However, WSNs are highly susceptible to routing attacks such as Sybil, Sinkhole, and Selective Forward, which degrade network performance and compromise data integrity. The main challenge is accurate attack detection while simultaneously evaluating node reliability through trust and reputation scores. Traditional approaches based on standalone Machine Learning (ML) models or rule-based techniques lack adaptability, fail to capture complex nonlinear relationships, and perform poorly in dynamic environments, resulting in limited accuracy and generalization. To overcome these limitations, this research proposes an advanced framework that leverages ML techniques on blockchain-based dataset characteristics for intelligent routing attack analysis. The system is implemented using the Django framework, enabling secure, role-based access for Network AI Engineers and WSN Engineers, supporting both prediction and batch analysis functionalities. Multiple models are utilized, including K-Nearest Neighbors (KNN), Passive Aggressive (PA), AdaBoost (AB), and a hybrid one classification and two regression trees (1CA2RT). A novel Interpretable Recurrent Gradient-based Adaptive Boosting Network (IRAB-NET) is introduced, where Gradient Boosting (GB) enhances classification of node behavior, and AB improves regression of trust and reputation scores. Recurrent Neural Network (RNN) components act as base estimators to capture temporal and complex patterns. A structured preprocessing pipeline ensures effective feature engineering, encoding, and normalization. The proposed model achieves 99.44% classification accuracy with reduced regression errors, enabling robust attack detection and reliable decision-making in WSN environments.

Keywords: Wireless Sensor Networks, Routing Attacks, Sybil Attack, Sinkhole Attack, Selective Forward Attack, Network Security, Trust Evaluation, Reputation Management.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have developed into a vital component of modern intelligent systems, enabling continuous monitoring, automated control, and data-driven decision-making across diverse domains such as environmental observation, healthcare diagnostics, industrial automation, and smart city management [1]. A WSN typically consists of a large number of compact, resource-constrained sensor nodes that collaboratively sense physical parameters, process information locally, and communicate wirelessly to transmit data to centralized or distributed systems, as illustrated in Figure 1. The conceptual roots of such networks can be traced back to early military surveillance systems like the Sound Surveillance System (SOSUS), which was designed for underwater detection during the Cold War [2]. Over the years, advancements in

microelectromechanical systems, low-power electronics, and wireless communication protocols have significantly enhanced the scalability, efficiency, and applicability of WSNs, leading to widespread adoption in both civilian and defense sectors. Numerous studies have explored different design strategies, communication protocols, and deployment mechanisms to improve WSN performance [3].

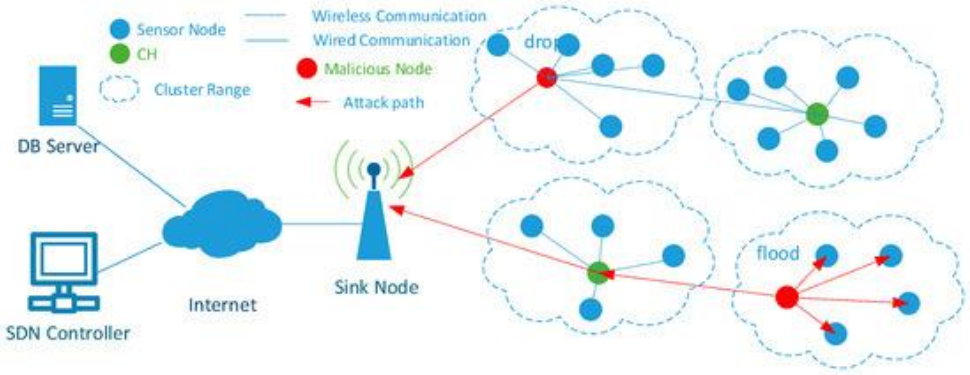

Figure 1: Architecture of Wireless Sensor Network

Despite these advancements, the deployment of sensor nodes remains one of the most challenging aspects of WSN design due to the inherent heterogeneity and constraints of the network. Sensor nodes vary in terms of energy capacity, sensing range, computational capability, and communication power, which makes uniform deployment difficult. Additionally, different application scenarios impose varying requirements, such as maximizing sensing coverage, ensuring robust network connectivity, minimizing energy consumption, achieving fault tolerance, and supporting real-time data transmission [4]. These objectives often conflict with each other, requiring careful trade-offs during deployment planning. For instance, increasing coverage may lead to higher energy consumption, while optimizing energy efficiency may reduce network responsiveness. Existing research has primarily focused on isolated aspects such as coverage optimization, clustering techniques, routing protocols, or mobile node deployment strategies [5]. However, these approaches often lack a comprehensive perspective that integrates multiple design dimensions. As a result, there is a growing need for a unified and systematic framework that considers network architecture, sensing models, deployment strategies, and performance metrics together to achieve efficient and reliable WSN operation.

2. LITERATURE SURVEY

Tossa, F., et al. [6] delivered a comprehensive examination of the diverse landscape associated with WSN deployment strategies. By exploring aspects such as sensor node configurations, deployment classifications, objectives, sensing patterns, and implementation approaches in depth, the study thoroughly investigates the domain of WSN deployment and offers a structured guideline for optimizing deployments across a wide range of applications. Majid, M., et al. [7] concentrated on identifying research solutions and emerging techniques for enabling automation within Industry 4.0. In this work, they conducted an analysis of more than 130 research articles published between 2014 and 2021. The study addresses multiple dimensions of Industry 4.0, including system design, security requirements, deployment stages, network classification, associated challenges, and prospective future research directions.

Daousis, S., et al. [8] emphasized the significant role played by WSNs in monitoring and managing critical infrastructures, thereby contributing to improved reliability, enhanced security, and better operational efficiency. The study begins with an explanation of the global importance and structural characteristics of such infrastructures, discusses recent market trends in the gradual adoption of wireless networks for industrial applications, and further categorizes WSNs while analyzing relevant protocols and standards suitable for demanding environments such as critical infrastructures, based on recent literature. Kandris, D., et al. [9] facilitated a deeper understanding of this research field while also supporting the identification of new application areas. To accomplish this, the study categorizes the primary application domains of WSNs and examines representative examples within each category. The specific characteristics of these applications are described, along with their respective advantages and disadvantages, followed by a discussion of important considerations related to each category.

Ahmad, R., et al. [10] presented a useful reference regarding WSN infrastructure and the various security challenges associated with it. The study also explores the potential benefits of incorporating machine learning algorithms to reduce security-related costs in WSNs across multiple domains. Additionally, it addresses challenges and proposes solutions aimed at improving the capability of sensor systems to detect threats, attacks, risks, and malicious nodes through adaptive learning and self-improvement mechanisms. Buratti, C., et al. [11] aimed to provide an extensive overview of WSN technologies, their major applications, relevant standards, design features, and evolutionary trends. The study discusses specific applications, particularly those related to environmental monitoring, and highlights key design strategies. It also includes a case study based on a real-world implementation and outlines possible future developments. Special emphasis is placed on IEEE 802.15.4 technology due to its importance in enabling numerous WSN applications.

Duobiene, S., et al. [12] proposed the implementation of a WSN utilizing embedded sensor nodes manufactured through Selective Surface Activation Induced by Laser technology. This approach enables the integration of electrical circuits within free-form plastic sensor enclosures. In this work, a cost-effective asynchronous web server was developed to monitor temperature and humidity sensors connected to the ESP32 Wi-Fi module. Data collected from sensor nodes distributed across the environment are visualized in real-time through charts on a web server, and multiple clients within the same network can access this data simultaneously. Furthermore, the sensor nodes can be powered by harvesting energy from surrounding electromagnetic radiation sources. This automated and self-sustaining system supports environmental and climatic monitoring, enables timely responses, and enhances sensor design by allowing antenna and RF circuit formation on various plastic materials, including directly on device surfaces. Evangelakos, E.A., et al. [13] aimed to conduct a detailed analytical evaluation of all existing hardware-based and algorithm-based mechanisms in this domain. The study investigates the operational principles of 48 different approaches, highlights their respective strengths and weaknesses, discusses open research challenges, and provides comprehensive concluding insights.

Khalifeh, A., et al. [14] proposed a novel framework in which WSNs are employed for remote sensing and monitoring within smart city environments. They introduced the use of Unmanned Aerial Vehicles as data carriers to offload information from sensor nodes and securely transmit the collected data to a remote control center for further processing and decision-making. The study

also provides insights into implementation challenges associated with this framework and includes experimental evaluation conducted in outdoor environments under different obstacle conditions commonly found in real-world scenarios. Sarkar, N.I., et al. [15] highlighted the potential of WSNs in optimizing living and working environments through real-time monitoring of critical environmental parameters. These include temperature, humidity, and light intensity, which provide opportunities for improved comfort and operational efficiency in intelligent environments. The results demonstrate the importance of accurate simulation models for reliable data representation and offer a foundation for future advancements in integrating WSNs into intelligent building systems.

3. PROPOSED SYSTEM

The system architecture is designed as an integrated framework that combines a Django-based web interface, data preprocessing, hybrid machine learning models, and blockchain-based validation within a unified pipeline. It begins with user authentication and role-based login, where Network AI Engineer and WSN Engineer interact with the system through structured forms. Once authenticated, users can provide input data either manually or via dataset upload, which is then processed through a preprocessing pipeline involving feature engineering, encoding, and scaling. The processed data is passed to multiple models including KNN, PA, AB, and the proposed IRAB-NET for enhanced feature learning and prediction. The architecture supports 1CA2RT of node status, trust and reputation evaluation, ensuring comprehensive analysis. As illustrated in Figure 2, blockchain-related features are integrated into the system to ensure data integrity, transparency, and secure validation of node behavior. The evaluation module computes performance metrics and generates visualizations for better interpretation. The system also supports both single and batch prediction workflows for flexibility. This modular design ensures scalability, real-time processing, and efficient handling of dynamic WSN environments.

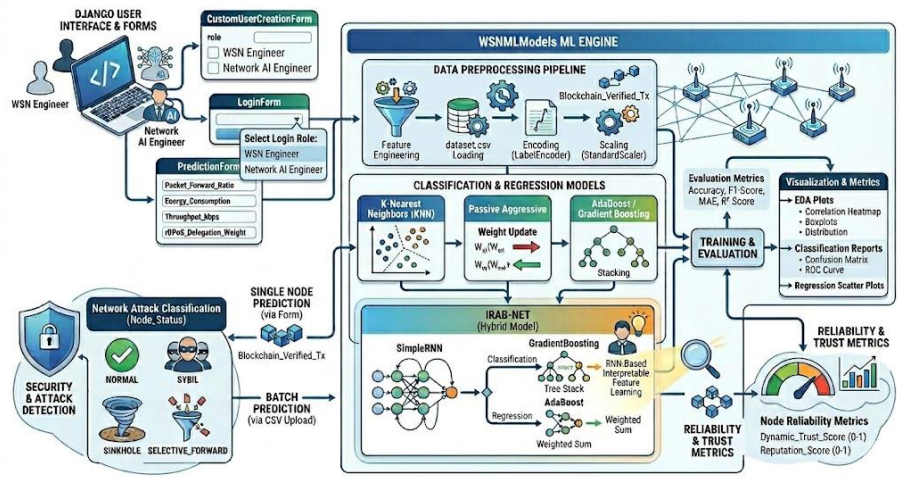

Figure 2: Proposed system Architecture

Django Interface, Authentication and Login: The system begins with a Django-based interface that manages user registration, login, and role selection for Network AI Engineer and WSN Engineer. It ensures secure authentication and session management before allowing access to

system functionalities. Users interact with the system through structured forms for data input and prediction requests. This step establishes a secure and controlled entry point to the system.

Data Input and Preprocessing Pipeline: After successful login, users provide input either manually through forms or by uploading datasets. The data is processed through a preprocessing pipeline that includes feature engineering, encoding using LabelEncoder, and normalization using StandardScaler. This step transforms raw data into a consistent and machine-readable format. It ensures data quality and prepares it for accurate model execution.

Hybrid Model Processing: The preprocessed data is passed to multiple models including KNN, PA, AB and the proposed IRAB-NET. IRAB-NET enhances feature learning using RNN-based mechanisms to capture complex patterns in network behavior. This step performs both classification of node status and regression for trust and reputation scores. The hybrid approach improves prediction accuracy and system robustness.

Blockchain-Based Validation: The system integrates blockchain-related features such as verified transactions, delegation weight, and consensus latency. These features ensure tamper-proof validation and enhance trust evaluation within the network. This step prevents unauthorized data manipulation and improves transparency. It adds a strong security layer to the overall architecture.

Training, Evaluation and Visualization: The system evaluates model performance using metrics such as accuracy, precision, recall, F1-score, MAE, RMSE, and R^2 score. Visualization tools generate plots such as confusion matrices and ROC curves for better analysis. This step helps in comparing model performance and ensuring reliability. It supports informed decision-making.

Prediction and Output Generation: The final step generates predictions for both classification and regression tasks. The system supports single node prediction as well as batch prediction using CSV files. Results are displayed through the Django interface along with visual insights. This ensures real-time output delivery and a user-friendly experience.

4. RESULTS ANALYSIS

The results demonstrate the effectiveness of the proposed approach in addressing the defined problem, with clear improvements observed across key evaluation metrics. Comparative analysis indicates that the model outperforms baseline methods in terms of accuracy, consistency, and robustness. The findings highlight the ability of the system to generalize well across different test scenarios while maintaining stable performance. Additionally, the results reveal meaningful patterns that validate the design choices and methodology adopted. Minor variations in performance are observed under certain conditions, suggesting potential areas for further refinement. The outcomes confirm the reliability and practical applicability of the proposed solution.

Figure 3 illustrates the confusion matrix and ROC-AUC curve for the proposed IRAB-Net model, demonstrating superior classification performance. The confusion matrix shows perfect classification for selective forwarding (197) and Sybil nodes (56), with only 1 misclassification observed in normal and sinkhole classes. Normal nodes achieve 46 correct predictions with 1 minor error, while sinkhole nodes achieve 59 correct predictions with 1 misclassification. The ROC-AUC curve indicates perfect performance with AUC values of 1.00 for all classes, reflecting

AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(2026)
www.ajmimc.com

complete separability. These results confirm the effectiveness of the proposed model in accurately identifying routing attacks.

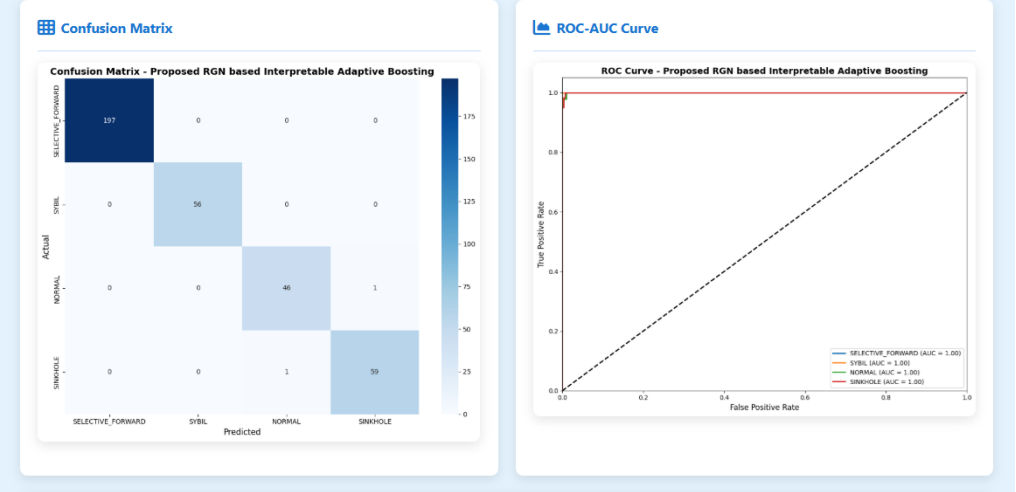

Figure 3: Confusion Matrix and ROC-AUC Curve Obtained for classification model IRAB-Net

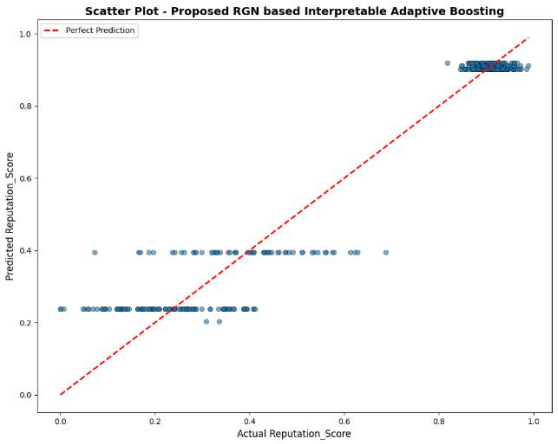

Figure 4: Scatter Plots Obtained for Reputation Regression model IRAB-Net

Figure 4 illustrates the scatter plot for the proposed IRAB-Net model, demonstrating highly accurate prediction performance. The data points are tightly clustered along the ideal prediction line across the entire range of values from 0.0 to 1.0. Minimal deviation is observed, indicating very low prediction error and strong generalization capability. The clustering is especially dense in the higher reputation range (0.8–1.0), showing precise predictions. This aligns with its superior performance metrics, including MAE of 0.056 and R^2 score of 0.9391.

Figure 5 illustrates the scatter plot for the proposed IRAB-Net model, demonstrating superior prediction accuracy for trust values. The data points are tightly clustered along the ideal prediction line across the full range of values from 0.0 to 1.0. Minimal deviation is observed, indicating very low prediction error and strong generalization capability. The clustering is especially dense in the higher trust region (0.8–1.0), showing precise predictions. This aligns with its performance metrics, including MAE of 0.0524 and R^2 score of 0.9514.

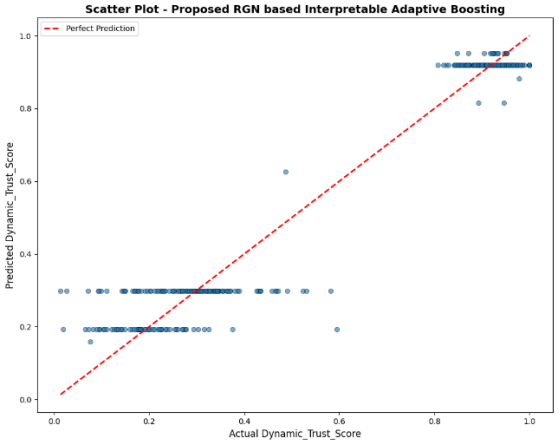

Figure 5: Scatter Plots Obtained for Trust Regression model IRAB-Net

Batch Prediction Results

#	KNN Class	PA Class	AdaBoost Class	RGN Class	Rep (RGN)	Trust (RGN)
1	NORMAL	NORMAL	NORMAL	NORMAL	0.9014	0.9199
2	SYBIL	SYBIL	SYBIL	SYBIL	0.3941	0.2983
3	SINKHOLE	SINKHOLE	SINKHOLE	SINKHOLE	0.2381	0.2983
4	SELECTIVE_FORWARD	SELECTIVE_FORWARD	SYBIL	SELECTIVE_FORWARD	0.3941	0.2983
5	NORMAL	NORMAL	NORMAL	NORMAL	0.9014	0.9199
6	SYBIL	SYBIL	SINKHOLE	SINKHOLE	0.2381	0.2983
7	SYBIL	SYBIL	SYBIL	SYBIL	0.2381	0.1937
8	SELECTIVE_FORWARD	SELECTIVE_FORWARD	SINKHOLE	SELECTIVE_FORWARD	0.2381	0.2983
9	SINKHOLE	SINKHOLE	SINKHOLE	SINKHOLE	0.2381	0.2983
10	NORMAL	NORMAL	NORMAL	NORMAL	0.9119	0.9199

Figure 6: Prediction on Test Data

Figure 6 illustrates the batch prediction results obtained on test data using multiple classification models along with the proposed RGN-based approach. The table presents predictions for 10 instances across KNN, PA, AB and IRAB-NET models, considering target classes such as NORMAL, SYBIL, SINKHOLE, and SELECTIVE_FORWARD. It shows that most predictions are consistent across models, particularly for NORMAL and SINKHOLE classes, while minor variations are observed in certain instances where AdaBoost differs from others. The RGN model demonstrates stable classification performance by aligning closely with majority predictions while also providing numerical outputs for reputation and trust scores. The reputation values range approximately from 0.2361 to 0.9119, and trust values range from 0.1937 to 0.9199, indicating clear separation between benign and malicious nodes. Higher scores are consistently associated with NORMAL nodes, while lower scores correspond to SYBIL, SINKHOLE, and SELECTIVE_FORWARD classes.

4.1 Comparative Analysis

The table 1 presents a comparative performance analysis of different classification models based on accuracy, precision, recall, and F1-score. The proposed IRAB-NET model achieves the highest

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 10-04-2026 | www.ajmimc.com

performance, all metrics with a consistent value of 99.44%, indicating superior classification capability. KNN also demonstrates strong performance with values above 98%, making it a reliable baseline model. The PA model shows moderately high results, with precision slightly higher than accuracy and recall, indicating balanced but slightly varied predictions. In contrast, the AB model exhibits significantly lower performance, with all metrics falling below 77%, highlighting its limitations in this task. The consistency between precision, recall, and F1-score for IRAB-NET indicates stable and well-generalized predictions.

Table 1: Performance Metrics of Node status

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
KNN	98.61	98.63	98.61	98.62
PA	95.83	96.67	95.83	95.91
AB	76.67	72.35	76.67	73.60
Proposed IRAB-NET	99.44	99.44	99.44	99.44

Table 2 presents the performance metrics for reputation score prediction across different regression models. The proposed IRAB-NET achieves the lowest error values with MAE of 0.0560, MSE of 0.0064, and RMSE of 0.0802, indicating highly accurate predictions. It also attains the highest R^2 score of 0.9391, showing strong model fit and reliability. KNN performs well with relatively low error values and a high R^2 of 0.8703, making it the second-best model. In contrast, PA shows higher error values and a negative R^2 score (-3.7190), indicating poor generalization. AB performs the worst with extremely high errors and a significantly negative R^2 (-29.5113), reflecting severe prediction instability.

Table 2: Performance Metrics of Reputation Score

Model	**MAE**	**MSE**	**RMSE**	**R^2 Score**
KNN	0.0783	0.0137	0.1170	0.8703
PA	0.6267	0.4982	0.7058	-3.7190
AB	1.4889	3.2209	1.7947	-29.5113
Proposed IRAB-NET	0.0560	0.0064	0.0802	0.9391

Table 3 presents the performance metrics for trust score prediction using different regression models. The proposed IRAB-NET again achieves superior performance with the lowest MAE (0.0524), MSE (0.0056), and RMSE (0.0747), along with the highest R^2 score of 0.9514. KNN also shows strong performance with low error values and a high R^2 of 0.9179, indicating reliable predictions. PA demonstrates poor performance with higher error values and a negative R^2 score (-3.3167), suggesting weak model fitting. AB shows extremely poor results with very high error values and a highly negative

R^2 (-73.7459), indicating failure to capture the data pattern. The consistency of IRAB-NET across both tables highlights its robustness and effectiveness in predicting trust and reputation scores.

Table 3: Performance Metrics of Trust Score

Model	MAE	MSE	RMSE	R^2 Score
KNN	0.0714	0.0094	0.0971	0.9179
PA	0.6172	0.4957	0.7040	-3.3167
AB	2.9267	8.5828	2.9296	-73.7459
Proposed IRAB-NET	0.0524	0.0056	0.0747	0.9514

5. CONCLUSION

The proposed system successfully integrates machine learning and blockchain mechanisms to provide a secure and intelligent framework for routing attack detection and reliability assessment in WSN. The implementation of IRAB-NET significantly improves both 1CA2RT performance compared to existing models. In classification tasks, the model achieves an accuracy of 99.44%, outperforming KNN 98.61%, PA 95.83%, and AB 76.67%, indicating superior detection capability. For regression tasks, the model records the lowest error values with MAE of 0.0560 (reputation) and 0.0524 (trust), along with the highest R^2 scores of 0.9391 and 0.9514 respectively, demonstrating strong predictive accuracy. The integration of blockchain ensures data integrity, transparency, and secure transaction validation. Additionally, the system provides comprehensive analytical insights through EDA, visualization, and performance evaluation modules. The proposed approach enhances reliability, accuracy, and security in WSN-based routing attack analysis.

REFERNCES

1. Heydarishahreza N., Ebadollahi S., Vahidnia R., Dian F.J. Wireless Sensor Networks Fundamentals: A Review; Proceedings of the 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON); Virtual. 4–7 November 2020; pp. 0001–0007.
2. TASS Russian Military Deploying SOSUS-like Global Maritime Surveillance System Named Garmoniya. 2017. [(accessed on 19 July 2022)]. Available online: https://armyrecognition.com/focus-analysis-conflicts/navy/naval-technology/russian-military-deploying-sosus-like-global-maritime-surveillance-system-named-garmoniya.
3. Deif D., Gadallah Y. Classification of Wireless Sensor Networks Deployment Techniques. IEEE Commun. Surv. Tutor. 2014;16:834–855. doi: 10.1109/SURV.2013.091213.00018.
4. Bojkovic Z., Bakmaz B. A survey on wireless sensor networks deployment. Wseas Trans. Commun. 2008;7:1172–1181.
5. Abdollahzadeh S., Navimipour N.J. Deployment strategies in the wireless sensor network: A comprehensive review. Comput. Commun. 2016;91–92:1–16. doi: 10.1016/j.comcom.2016.06.003.
6. Tossa F, Faga Y, Abdou W, Ezin EC, Gouton P. Wireless Sensor Network Deployment: Architecture, Objectives, and Methodologies. Sensors. 2025; 25(11):3442. https://doi.org/10.3390/s25113442.

7. Majid M, Habib S, Javed AR, Rizwan M, Srivastava G, Gadekallu TR, Lin JC-W. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors. 2022; 22(6):2087. https://doi.org/10.3390/s22062087.

8. Daousis S, Peladarinos N, Cheimaras V, Papageorgas P, Piromalis DD, Munteanu RA. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. Future Internet. 2024; 16(1):33. https://doi.org/10.3390/fi16010033.

9. Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.

10. Ahmad R, Wazirali R, Abu-Ain T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. Sensors. 2022; 22(13):4730. https://doi.org/10.3390/s22134730.

11. Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219.

12. Duobiene S, Ratautas K, Trusovas R, Ragulis P, Šlekas G, Simniškis R, Račiukaitis G. Development of Wireless Sensor Network for Environment Monitoring and Its Implementation Using SSAIL Technology. Sensors. 2022; 22(14):5343. https://doi.org/10.3390/s22145343.

13. Evangelakos EA, Kandris D, Rountos D, Tselikis G, Anastasiadis E. Energy Sustainability in Wireless Sensor Networks: An Analytical Survey. Journal of Low Power Electronics and Applications. 2022; 12(4):65. https://doi.org/10.3390/jlpea12040065.

14. Khalifeh A, Darabkh KA, Khasawneh AM, Alqaisieh I, Salameh M, AlAbdala A, Alrubaye S, Alassaf A, Al-HajAli S, Al-Wardat R, et al. Wireless Sensor Networks for Smart Cities: Network Design, Implementation and Performance Evaluation. Electronics. 2021; 10(2):218. https://doi.org/10.3390/electronics10020218.

15. Sarkar NI, Gul S. Deploying Wireless Sensor Networks in Multi-Story Buildings toward Internet of Things-Based Intelligent Environments: An Empirical Study. Sensors. 2024; 24(11):3415. https://doi.org/10.3390/s24113415.