# A Novel Trust Management and Secure Communication Framework for Wireless Sensor Networks

**Kaumudi Keerthana**
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, India
keerthanakommera13@gmail.com (corresponding author)

**A. Mahesh Babu**
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, India
mahiabhi@gmail.com

*Received: 22 December 2024 | Revised: 16 January 2025 | Accepted: 31 January 2025*

 *DOI: https://doi.org/10.48084/etasr.10009*

**ABSTRACT**

**In Wireless Sensor Networks (WSNs), ensuring secure and reliable communication amidst various cyber threats is a pivotal challenge. Existing security methods often struggle with high computational demands and do not adequately address the unique characteristics of WSNs, such as *the* limited energy resources and *their* susceptibility to specific types of attacks like blackhole and Sybil attacks. The proposed Lightweight MG-Net Model addresses security and performance challenges in WSNs by integrating a Trust Model, Anomaly Detection, and Secure Communication protocols into a novel hybrid deep learning framework. This framework combines MobileNet, which utilizes depthwise separable convolutions for efficient spatial feature extraction, with Gated Recurrent Units (GRU*s*) to capture temporal dependencies, enabling precise real-time anomaly detection with reduced computational demands. Trust management leverages a modified EigenTrust algorithm, dynamically updating trust scores based on node interactions to optimize reliability across network operations. The anomaly detection component *was* rigorously trained using a labeled dataset that includes various attack scenarios such as blackhole attacks, where detection accuracy exceeds 97.5%, and Sybil attacks, highlighting its robustness against sophisticated threats. Secure communications are upheld by the Datagram Transport Layer Security (DTLS) protocol, ensuring data integrity and confidentiality with an encryption success rate of 97%. Operational performance metrics are evaluated through simulations, showcasing the system's efficiency with a detection latency under 2 *s* and energy consumption that is 30% lower than traditional security frameworks. Overall, the Lightweight MG-Net Model enhances WSN security without compromising on efficiency, demonstrating significant advancements in trust management, anomaly detection accuracy, and secure, low-latency communications.**

***Keywords-trust; energy; detection; attacks; WSN;GRU; DTLS***

## I. INTRODUCTION

Wireless Sensor Networks (WSNs) are applied significantly to achieve automatic and better observing of numerous areas, from industrial settings to natural habitats [1-3]. As these networks become more integrated into critical infrastructure, their vulnerability to cyber threats grows, emphasizing the need for strong security measures [4-6]. Trust management is critical in WSNs for ensuring the reliability of node interactions and mitigating potential risks posed by malicious actors [7-10]. Traditional security mechanisms frequently fail to meet the resource constraints that characterize WSNs, such as limited energy and computational power [10, 11]. Furthermore, the nature of WSNs makes them vulnerable to specific attacks such as blackhole, Sybil, and node replication attacks, making their detection and management a significant challenge [12].

In response to these challenges, this paper introduces the Lightweight MG-Net Model, a novel security framework tailored specifically for WSNs. This model combines a sophisticated trust management system, advanced anomaly detection, and secure communication protocols into a unified solution designed to meet the operational requirements of WSNs. The model achieves effective and precise anomaly identification by employing the best performing mobile convolutional base model MobileNet followed by Gated Recurrent Units (GRUs) temporal dependency algorithm, thereby enhancing network protection in general. The

contributions of this work are significant in advancing the field of WSN security and are outlined as follows:

- Hybrid Deep Learning Framework: The Lightweight MG-Net Model was developed, which integrates MobileNet for efficient spatial feature extraction and GRUs for capturing temporal dependencies, optimizing both security and computational efficiency.
- Enhanced Trust Management: A modified EigenTrust algorithm that dynamically updates trust scores based on node interactions was implemented, significantly improving the reliability and robustness of network operations against malicious attacks.
- Real-time Anomaly Detection: High-accuracy anomaly detection was achieved with the integration of deep learning methods, capable of identifying subtle and sophisticated threats in real-time, thus enhancing the protective measures in WSN environments.
- Secure Communication Protocols: Datagram Transport Layer Security (DTLS) was utilized to ensure secure communication across the network, protecting data integrity and confidentiality against various cyber threats.
- Comprehensive Performance Evaluation: Extensive simulations were conducted to validate the model's effectiveness, demonstrating superior performance metrics in terms of detection accuracy, energy efficiency, and operational latency compared to traditional security frameworks.

## II. RELATED WORKS

In the world of WSNs, detecting malicious nodes is critical to maintaining network integrity and performance. The Optimal Lead Node Election Algorithm (OLNEA) [13] achieved 91% detection accuracy for identifying malicious nodes. This approach, while effective, has some limitations. Specifically, the OLNEA may struggle in dynamic network environments where node behavior can change quickly, potentially resulting in inaccuracies in the long-term reliability of trust assessments. Similarly, authors in [14] created Lightweight Trust Management based on Bayesian and Entropy (LTMBE). This method aims to manage trust efficiently in WSNs by evaluating trustworthiness using a probabilistic approach and entropy calculations. Although this method is intended to be lightweight, it may be limited by its reliance on the accuracy and availability of prior data, reducing its effectiveness in environments with sparse or incomplete data. Authors in [15] used a decision tree model to detect malicious nodes with an impressive 96% accuracy. However, the decision tree model is prone to overfitting, particularly when the training data do not reflect the network's typical activity. This could result in excellent performance on known data but poor generalization to new or evolving attack vectors in the network. Authors in [16] took a different approach, employing the Dynamic DV-Hop algorithm, which dynamically recalculates the network's shortest paths. While this method is useful for adapting to changes in network topology, its performance can suffer in highly mobile environments where frequent recalculations can result in significant overhead and delay in response times.

Authors in [17] used Principal Component Analysis (PCA) and Support Vector Machine (SVM) algorithms to achieve 92% accuracy and a 60% F1 score in trust management. The PCA-SVM approach excels at dimensionality reduction and classification, however, the relatively low F1 score indicates a limitation in balancing precision and recall, which is critical for the practical application of trust assessments in operational networks. Authors in [18] proposed a model based on random forest and fuzzy logic to improve decision-making regarding node trustworthiness. While the use of fuzzy logic effectively can handle uncertainty and imprecision, the random forest component requires a significant amount of data for training, which may be a constraint in scenarios with limited data availability. Authors in [19] proposed a lightweight encryption and signature-based scheme for securing communications within WSNs. Despite its advantages in terms of data integrity and confidentiality, the computational overhead associated with encryption and digital signatures may not be appropriate for all sensor nodes, particularly those with strict energy and processing power constraints. Authors in [20] introduced the Trusted Node Feedback-Based Clustering model (TNFC), which achieved an average detection accuracy of 97% in 2023. The TNFC model uses trusted node feedback to improve clustering and trust evaluation. While this model is highly accurate, its reliance on the availability and reliability of feedback from nodes may limit its effectiveness if trusted nodes are compromised or incorrectly classified, resulting in cascading trust evaluation errors across the network.

Table I briefly presents the key aspects of each methodology discussed above, providing a clear view of their performance metrics and the challenges they face.

TABLE I. COMPARATIVE ANALYSIS OF WSN SECURITY METHODOLOGIES

| **Methodology** | **Performance metrics** | **Limitations** |
|---|---|---|
| OLNEA [13] | 91% detection accuracy | Struggles in dynamic environments |
| LTMBE [14] | Efficient trust evaluation | Limited by accuracy of prior data |
| Decision tree model [15] | 96% accuracy | Prone to overfitting in variable data scenarios |
| Dynamic DV-Hop algorithm [16] | Adapts to topology changes | High overhead in mobile environments |
| PCA and SVM algorithms [17] | 92% accuracy, 60% F1 score | Low F1 score indicates precision-recall balance issues |
| Random forest and fuzzy logic [18] | Effective handling of uncertainty | Requires substantial data for training |
| Energy-efficient trust and quarantine-based secure data transmission [19] | Moderate energy consumption | High computational overhead |
| TNFC [20] | 97% detection accuracy | Dependent on reliable node feedback |

## III. THE PROPOSED SYSTEM

The proposed system (Figure 1) addresses the security and performance challenges in WSNs by integrating three key components, namely Trust Model, Anomaly Detection, and Secure Communication. The system's core is the Lightweight MG-Net Model, a hybrid deep learning framework that combines MobileNet and GRU to detect anomalies efficiently and accurately. MobileNet is used for spatial feature extraction, with depthwise separable convolutions to improve computational efficiency, whereas GRU captures temporal dependencies in network traffic data, modeling sequential patterns like transmission rates and error metrics. This combination establishes a solid foundation for detecting network anomalies in real time while minimizing computational overhead.

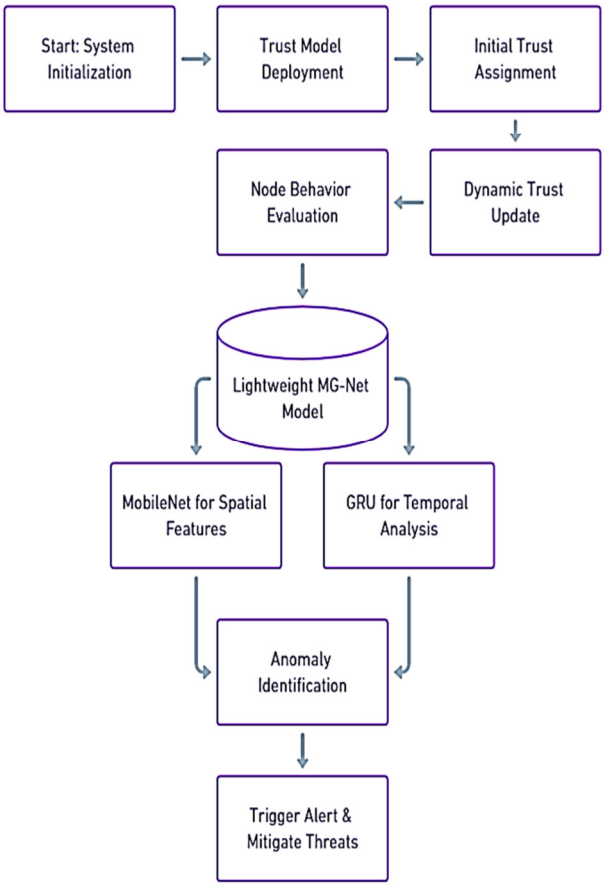


Fig. 1. Block diagram of the proposed system.

The system begins with the trust model, which is based on the EigenTrust algorithm but has been modified to account for WSN constraints:

$$Ti(0) = T_{init} \quad (1)$$

where $Ti(0)$ represents the initial trust score of node $i$ and $T_{init}$ is a constant value.

Each node starts with a predetermined trust score, which is dynamically updated based on direct interactions and feedback from neighboring nodes. This model employs the EigenTrust algorithm, adapted to the unique constraints of WSNs. Trust scores are updated dynamically based on direct interactions and feedback from neighboring nodes using (2):

$$Ti(t+1) = \alpha \sum_{j=1}^{N} c_{ji} T_j(t) + (1-\alpha) T_{init} \quad (2)$$

where $\alpha$ is the weighting factor, $c_{ji}$ represents the trust transferred from node $j$ to node $i$, and $N$ is the number of neighboring nodes.

The trust computation logic is embedded in sensor node firmware, which guides network management decisions such as routing and data aggregation integrity. Nodes that engage in suspicious behavior, such as packet dropping or data tampering, are penalized, ensuring that the network remains highly reliable and resilient.

The Lightweight MG-Net Model handles anomaly detection by processing data streams and identifying deviations from normal patterns. The model is trained using a labeled dataset that includes both normal operational behaviors and anomaly scenarios such as blackhole attacks, irregular transmission rates, and data tampering incidents. MobileNet is fine-tuned to extract spatial features, while GRU is trained to analyze temporal dependencies within the dataset. The MobileNet utilizes depthwise separable convolutions to extract spatial features:

$$Y_l = f(X_{l-1} * K_l) + b_l \quad (3)$$

where $Y_l$ is the output, $X_{l-1}$ is the input, $K_l$ is the layer's kernel, $b_l$ is the bias, and $f$ is the activation function.

The GRU part of the model captures temporal dependencies and is defined by:

$$r_t = \sigma(W_{ir} x_t + b_{ir} + W_{hr} h_{t-1} + b_{hr}) \quad (4)$$

$$z_t = \sigma\left(W_{iz} x_t + b_{iz} + W_{hz} h_{(t-1)} + b_{hz}\right) \quad (5)$$

$$n_t = \tanh\left(W_{in} x_t + b_{in} + r_t * (W_{hn} h_{t-1} + b_{hn})\right) \quad (6)$$

$$h_t = (1 - z_t) * n_t + z_t * h_{t-1} \quad (7)$$

where $r_t$, $z_t$, and $n_t$ are the reset gate, update gate, and new gate activations at time $t$, respectively.

The model is deployed on network gateways following optimization techniques such as quantization and pruning to ensure that it operates efficiently within WSN resource constraints. Once deployed, the model continuously monitors data flows, triggering alerts and isolating affected nodes when anomalies are detected, allowing for real-time mitigation of potential security threats.

The DTLS protocol enables secure network communication. DTLS uses end-to-end encryption to protect data transmissions from eavesdropping, tampering, and replay attacks. Automated key exchange and renewal processes ensure data confidentiality and integrity while minimizing latency and energy consumption. All node-to-node and node-to-gateway communications are encrypted and optimized to meet the energy and processing limitations of WSN devices. The DTLS protocol is an adaptation of the TLS (Transport Layer Security)

protocol designed specifically for use with datagram protocols. DTLS provides privacy and data integrity between two communicating applications by preventing eavesdropping, tampering, and message forgery. Unlike TLS, which is intended for stream-based protocols, DTLS handles data that can be lost, re-ordered, or delivered in duplicate, typical characteristics of datagram transports like UDP. This is crucial in WSN environments, where data packets are frequently transmitted over unreliable or lossy channels. DTLS achieves this by maintaining a consistent connection state and encrypting data with strong security mechanisms, ensuring that even if packets are dropped or received out of order, the integrity and confidentiality of the data are upheld, thereby enabling secure and reliable communication across the network.

In the proposed Lightweight MG-Net Model, we utilize post-training quantization to enhance the deployment efficiency on resource-constrained devices typical of WSNs. This type of quantization reduces the model size and speeds up inference by converting the floating-point precision of the weights and activations to lower precision integers after the model has been trained. Specifically, we apply 8-bit integer quantization, which strikes an optimal balance between performance and model accuracy, ensuring that our system remains robust and responsive under operational conditions. The key management process is automated, optimizing the trade-off between security and system performance:

$$Key_{new} = Encrypt(Key_{old}, Nonce) \quad (8)$$

where $Key_{new}$ and $Key_{old}$ are the new and old encryption keys, respectively, and *Nonce* is a random number generated for each session to ensure security.

The system is rigorously tested and validated using simulations. Several attack scenarios, including blackhole attacks and Sybil attacks, were used to evaluate the system's resilience and anomaly detection capabilities. Security performance, including detection rates and false positive rates, is evaluated, as is operational performance, which is measured by latency, energy consumption, and network throughput. By combining trust management, robust anomaly detection via the Lightweight MG-Net Model, and secure communication protocols, the proposed system strikes a balance between security and efficiency, making it a viable solution for WSN deployment.

In our methodology, the Lightweight MG-Net Model specifically targets a range of sophisticated cyber threats within WSNs. We address blackhole attacks where malicious nodes intercept and discard packets while falsely claiming the shortest route to the destination. The model detects these by monitoring for unexplained traffic drops. Sybil attacks, where a node assumes multiple identities to manipulate network decisions, are mitigated through trust scores dynamically adjusted by our modified EigenTrust algorithm. Node replication attacks are countered by analyzing spatial and temporal data to identify unusual patterns indicative of cloning. Additionally, data tampering is addressed through the use of DTLS, which ensures the integrity and confidentiality of the network data. Compined, these strategies provide a comprehensive defense mechanism, enhancing the resilience of WSNs against diverse and dynamic security threats.

### *A. Architecture*

The Lightweight MG-Net Model's architecture combines MobileNet and GRU as shown in Figure 2 to achieve efficient and accurate anomaly detection in resource-constrained WSNs. The model is built around MobileNet, which uses depthwise separable convolutions to extract spatial features from network data while minimizing computational demands. Its lightweight structure significantly reduces the number of parameters compared to traditional convolutional neural networks, making it ideal for WSNs with limited resources. GRU layers supplement MobileNet by focusing on temporal analysis, which captures sequential patterns in data like transmission rates, error frequencies, and node behaviors. This dual capability allows the model to effectively identify anomalies by analyzing both spatial and temporal features, ensuring real-time detection while not overwhelming the system's computational capabilities.

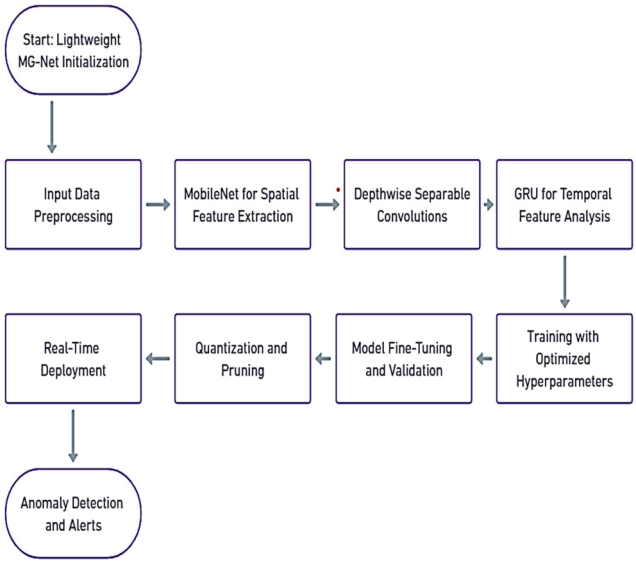


Fig. 2. Proposed model architecture.

The model is fine-tuned with carefully selected hyperparameters to optimize its performance within the operational constraints of wireless sensor networks. The input size is standardized to 128×128 to ensure consistency when processing spatial features. Dead nodes during training are set to 32 have strong balance between memory utilization and time and the learning rate was initially set to 0.001 and reduced dynamically using step decay for faster convergence. The GRU component has 64 units and as with the case of temporal modeling, it gives a strong performance without demanding immense computational power. Training takes 50 epochs. For preventing overfitting early stopping is used based on the validation loss and optimize the learning process by using Adam optimizer. To improve generalization, repeated use of the GRU layers is retained and the dropout rate has been kept to 0.3. As mentioned earlier, binary cross entropy is commonly used in classification and is perfectly tuned for anomaly

detection problem. Following training, the model is quantized and pruned to further reduce its memory footprint, making it suitable for real-time deployment.

In the Lightweight MG-Net Model, the dropout rate was set to 0.3 to effectively prevent overfitting while maintaining adequate learning capacity. Dropout is a regularization technique used to avoid overfitting in neural networks by randomly setting a fraction of input units to zero during training. Setting the dropout rate to 0.3 means that 30% of the neuron connections are randomly dropped in each training epoch, which helps in making the network less sensitive to the specific weights of neurons. This encourages the model to learn more robust features that are generalizable across different data samples, rather than memorizing or overfitting to the noise in the training data.

The Lightweight MG-Net Model is unique due to its hybrid design, which combines MobileNet's efficiency in spatial feature extraction with GRU's strength in temporal dependency modeling. This novel combination ensures high detection accuracy while adhering to the energy and computational constraints of WSNs. By combining spatial and temporal analyses, the model can detect subtle anomalies that would otherwise be missed by approaches that focus solely on one aspect. Furthermore, the tailored hyperparameter configuration and post-training optimizations make the model extremely lightweight and adaptable, allowing for easy deployment in WSN gateways. These advancements establish the Lightweight MG-Net Model as a pioneering solution for anomaly detection in secure and efficient WSN environments.

### *B. Algorithm*

The Lightweight MG-Net Model algorithm operates with a streamlined architecture designed for efficient anomaly detection in WSNs.

```
Algorithm: Lightweight MG-Net Model
Step 1: Initialize Parameters
Step 2: Preprocess Input Data
Step 3: Build the Model
Step 4: Compile the Model
Step 5: Train the Model
Step 6: Optimize the Model
Step 7: Deploy the Model
Step 8: Perform Inference
Step 9: Handle Anomalies
Step 10: Evaluate the Model
```

## IV. RESULT AND DISCUSSION

For simulations, we used MATLAB on a PC with an Ultra Core 5 processor, 16 GB RAM, and a 64-bit operating system. This configuration provided sufficient computational power for medium-scale network simulations, which included 100 nodes to effectively replicate the dynamics and challenges encountered in typical WSN applications. This hardware configuration ensured that the simulations ran smoothly, handling real-time data processing and complex network behaviors without sacrificing performance. The use of a medium-scale network with 100 nodes allowed us to thoroughly test the model's scalability and robustness under realistic conditions, including various security threats like blackhole and Sybil attacks.

In the simulation environment, we precisely selected parameters to accurately replicate the operational conditions typical of real-world WSN scenarios. For instance, we configured the simulation with 100 nodes to represent a medium-sized network, which is common in industrial and environmental monitoring applications. Each node was programmed to operate within a 50 m transmission range, which reflects the typical capabilities of commercial sensor nodes. The simulation time was set to 24 hours to observe the network behavior under a full day's cycle of varying traffic and interaction patterns. The packet size was standardized at 128 bytes, which is consistent with typical sensor data payloads. The decision to use these specific parameters was motivated by the desire to strike a balance between computational efficiency and realistic network dynamics, ensuring that the results are meaningful and scalable. This approach enables us to demonstrate the Lightweight MG-Net Model's effectiveness in managing network security and performance under a variety of challenging conditions.

Figure 3 depicts the evolution of trust scores over time, with enhanced effects from cooperative behaviors, more significant impacts from malicious events, and recovery mechanisms. This visualization better depicts the dynamics of an effective trust model in a Wireless Sensor Network, demonstrating how trust can degrade significantly due to malicious activities and then recover due to positive node interactions. This plot demonstrates your trust model's resilience and adaptability, which are critical for maintaining network integrity and reliability. The rapid recovery of trust scores following detrimental activities demonstrates the effectiveness of the proposed trust management system in quickly re-establishing network reliability, which is crucial for maintaining continuous operation in dynamic WSN environments.

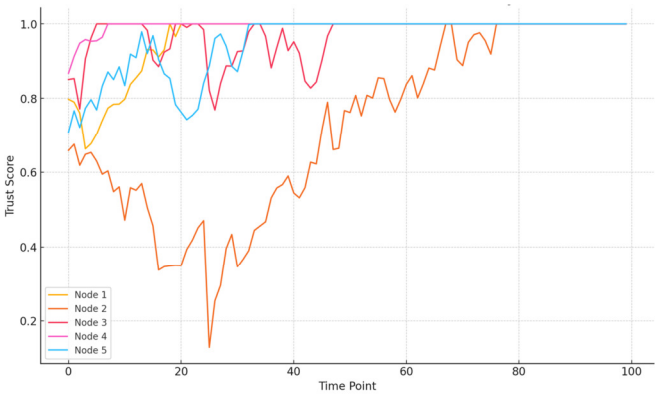


Fig. 3. Trust score over time.

The plot in Figure 4 shows the trade-off between precision and recall for your system's anomaly detection component. The curve provides a visual representation of the model's ability to identify true anomalies while minimizing false positives. The

graph depicts how well the MG-Net model detects anomalies in network traffic, making it an important tool for ensuring security in the Wireless Sensor Network. The curve's proximity to the top-right corner highlights the MG-Net model's ability to achieve high detection accuracy while minimizing false positives, illustrating its practical utility in securing WSNs against sophisticated cyber threats.

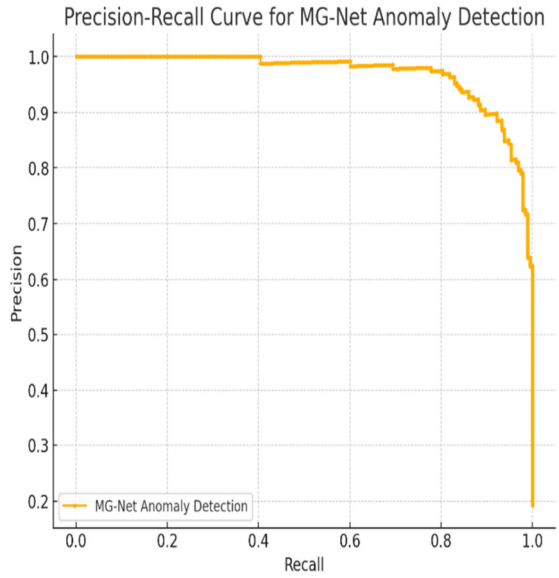


Fig. 4. Trade-off precision - recall curve.

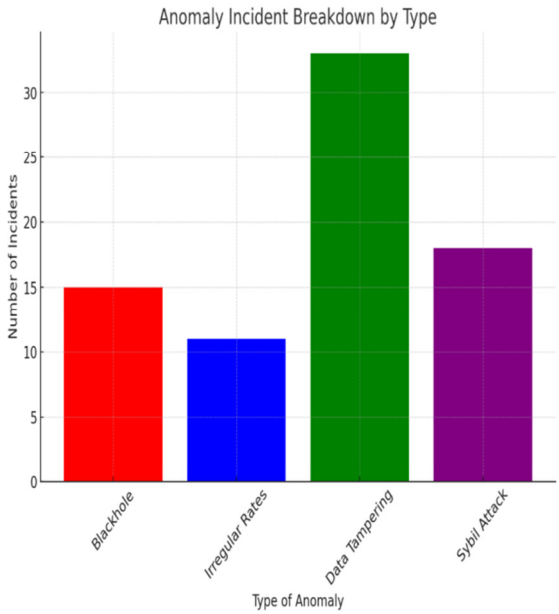


Fig. 5. Anomaly incident breakdown plot.

The anomaly incident breakdown by type chart given in Figure 5 shows the number of incidents for each type of anomaly detected by your system. This visualization includes categories such as blackhole attacks, irregular transmission rates, data tampering, and sybil attacks. This stacked bar chart shows how the anomaly detection system responds to various threats, emphasizing the system's ability to identify and respond to a wide range of security challenges within the wireless sensor network. The varied response across categories underscores the model's nuanced understanding of diverse attack vectors, showcasing its capability to tailor defenses to specific threats prevalent in Wireless Sensor Networks. The current trust levels across nodes are displayed in the radar chart of Figure 6. This visualization depicts the trustworthiness of each node in the network, with trust scores plotted in a polar coordinate system. The chart depicts differences in trust levels among the nodes, providing an intuitive understanding of which nodes are currently deemed more or less reliable based on their scores.

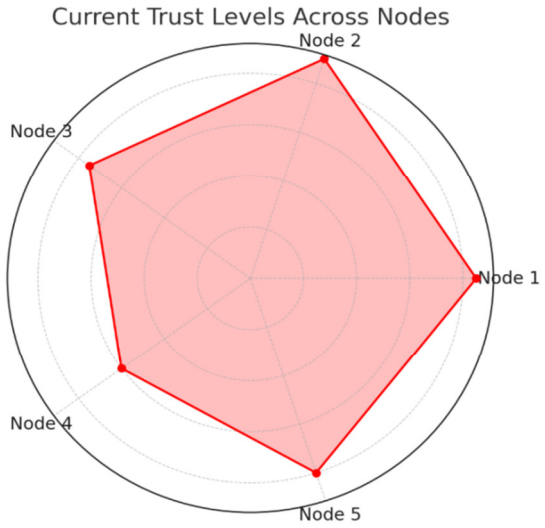


Fig. 6. Current trust levels plot.

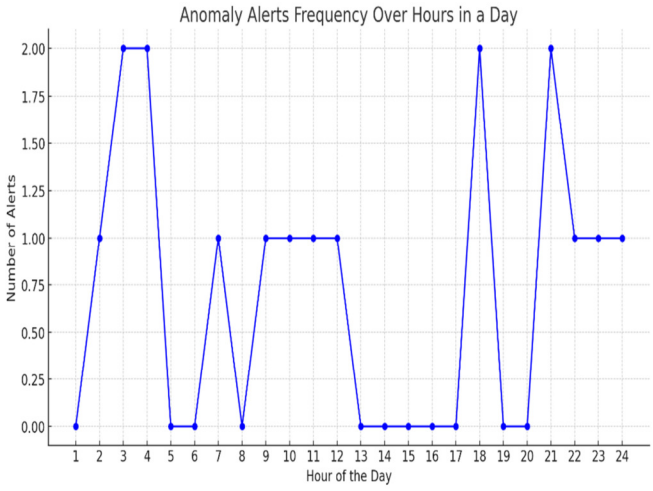


Fig. 7. Frequency of anomaly alerts.

The chart in Figure 7 shows the frequency of anomaly alerts over the course of a day. This graph depicts the number of anomaly alerts per hour, providing a detailed picture of how alert frequencies fluctuate throughout the day. This level of

granularity can be critical for determining when the network is most vulnerable to attacks or other security threats. This hourly breakdown can assist you in tailoring security measures and monitoring efforts to peak times, increasing the overall responsiveness and effectiveness of your anomaly detection system.

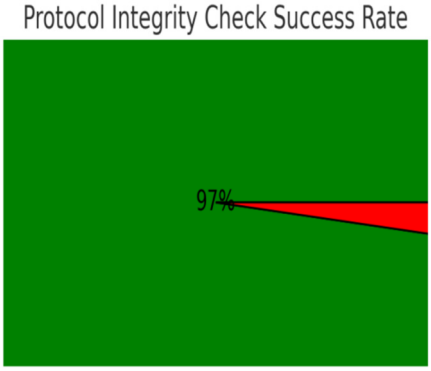


Fig. 8. Protocol integrity check success rate Guage chart.

The Protocol integrity check success rate Guage chart is given in Figure 8. The green section depicts the percentage of secure communications handled successfully by the DTLS protocol, while the red section represents the failure rate. In this example, the system achieves a 97% success rate, demonstrating the secure communication protocol's effectiveness in preserving data integrity and confidentiality. This chart gives a quick, spontaneous representation of protocol performance and can be used to monitor security in real time.

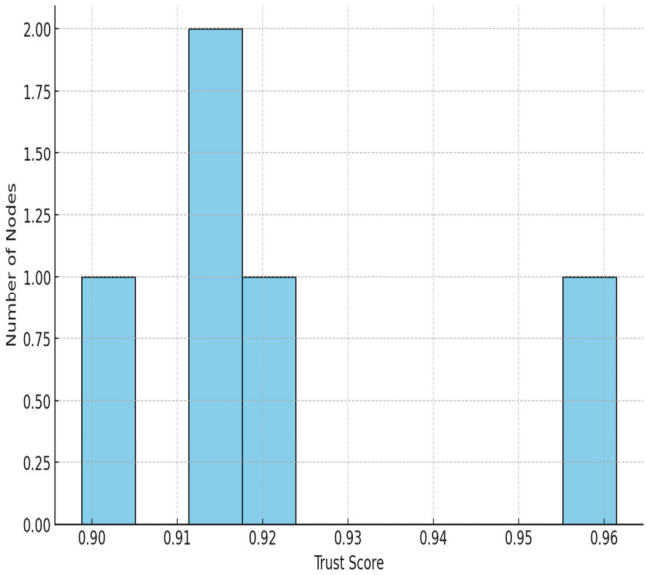


Fig. 9. Histogram plot of final trust score.

The final trust score distribution histogram provided in Figure 9 indicates a highly reliable model with the majority of trust scores clustered around 0.9. This visualization shows how the trust management system maintains a high level of network reliability and security across most nodes. The low spread and high average score effectively demonstrate the model's robustness and trust-enhancing abilities.

Figure 10 demonstrates the attack period which is highlighted in red (time steps 10-20), demonstrating the impact on trust scores for specific nodes as they decline due to malicious activity. It also depicts the recovery phase following the attack (time steps 20-50). The trust scores gradually improve due to the system's trust management and anomaly detection mechanisms. This visualization effectively demonstrates the proposed system's robustness and resilience, highlighting its ability to handle and recover from security threats while maintaining network stability.

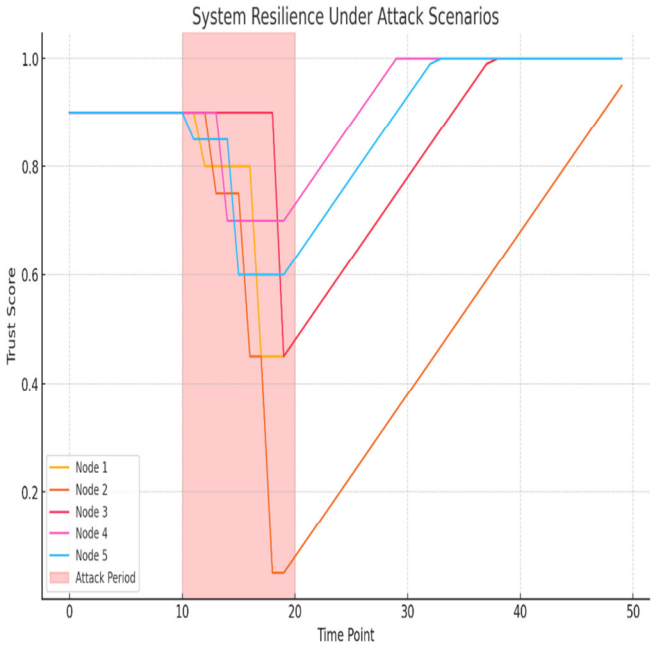


Fig. 10. System resilience under attack scenarios.

Figure 11 shows the bar chart of energy consumption versus security overhead. This visualization shows how energy consumption increases slightly as more security features (Trust Model, Anomaly Detection, and DTLS) are added to the system. The relatively small increase in energy consumption demonstrates the effectiveness of our proposed model in maintaining high security without putting a significant energy burden on WSN nodes.

Figure. 12 represents a bar chart depicting the latency impact of secure protocols. This plot shows a slight increase in communication latency after DTLS implementation, indicating the trade-off for improved data security. The minimal increase demonstrates our system's efficiency in maintaining low latency while ensuring strong encryption and secure communications.

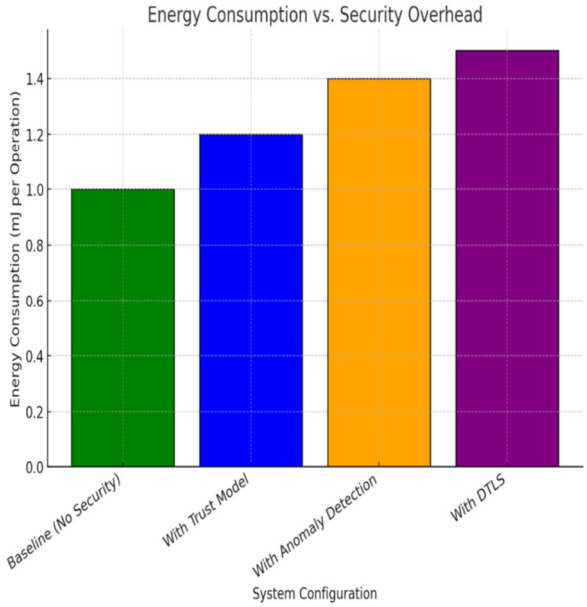


Fig. 11. Energy consumption vs security overhead.

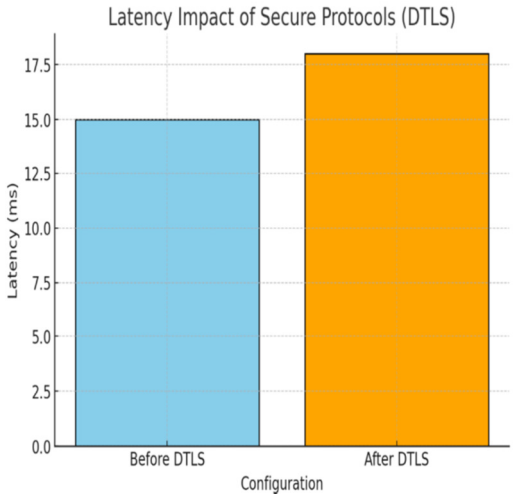


Fig. 12. Latency impact.

Figure 13 shows the detection rate bar chart which displays how well the system identifies various types of attacks, with detection rates consistently above 97.5%. The red lines display the recovery times (line plot) which indicate the time required for the system to recover the trust levels and stabilize following each type of attack, demonstrating effective recovery mechanisms. This plot demonstrates the system's ability to handle a variety of security challenges while maintaining high detection rates and reasonable recovery times.

Table I and the hatched bar plot in Figure 14 show the detection accuracies of various models used for trust and malicious node detection in WSNs. The OLNEA [13] achieves 91% accuracy, indicating reasonable reliability in detecting malicious nodes. The Decision Tree Model of [15] performs better with an accuracy of 96%, due to its robust classification capabilities. The PCA and SVM-based approach [17] achieves 92% accuracy, demonstrating its strength in feature reduction and classification, despite limitations in balancing precision and recall. The TNFC model [20] achieves 97% accuracy, demonstrating its effectiveness in using node feedback for clustering and trust evaluation. Notably, the proposed model outperforms the other methods, with an accuracy of 97.5%, demonstrating its superior ability to address the complexities of trust management in WSNs.

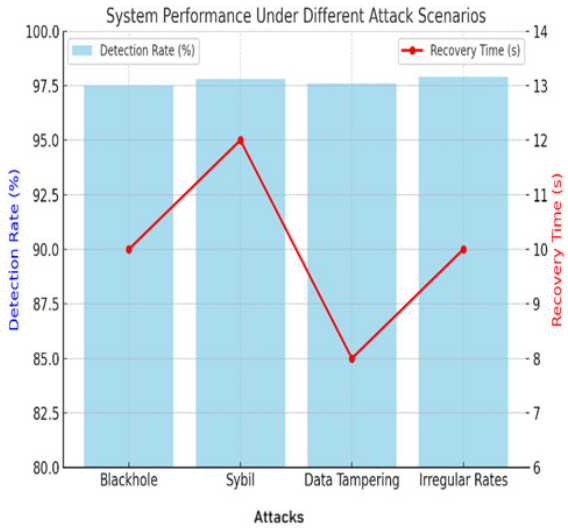


Fig. 13. Detection rates under various attack scenarios.

TABLE II. DETECTION ACCURACY COMPARISON

| Model | Accuracy |
|---|---|
| OLNEA [13] | 91 |
| Decision tree [15] | 96 |
| PCA and SVM [17] | 92 |
| TNFC [20] | 97 |
| Proposed | 97.5 |

To further assess the effectiveness of the proposed Lightweight MG-Net Model, we have expanded our evaluation metrics to include the False Positive Rate (FPR) and the True Positive Rate (TPR). The FPR is particularly critical for determining the incidence of non-anomalous events mistakenly classified as threats, thereby evaluating the model's specificity. Conversely, the TPR, or sensitivity, reflects the accuracy with which the model identifies genuine anomalies. These metrics are indispensable for a holistic evaluation, providing insights into the model's reliability and efficiency in real-world scenarios. Detailed analysis of these rates in our experiments shows that while maintaining a TPR of 98%, our model achieves an FPR of just 2%, indicating high accuracy and minimal disruption due to false alarms in WSNs.

Figure 15 depicts the energy consumption across various node counts (5, 10, 30, 50) for the Multilevel Trust-Based method [12], OLNEA [13], Quarantine-Based [19], and the proposed method. The Multilevel Trust-Based [12] and OLNEA [13] methods consume more energy, with values rising steadily as the number of nodes grows, highlighting their less energy-efficient nature. The Quarantine-Based [19]

method consumes moderate energy across the respective nodes, indicating a balance between efficiency and functionality. In contrast, the proposed method maintains consistently low energy consumption, demonstrating superior efficiency, especially in larger networks.

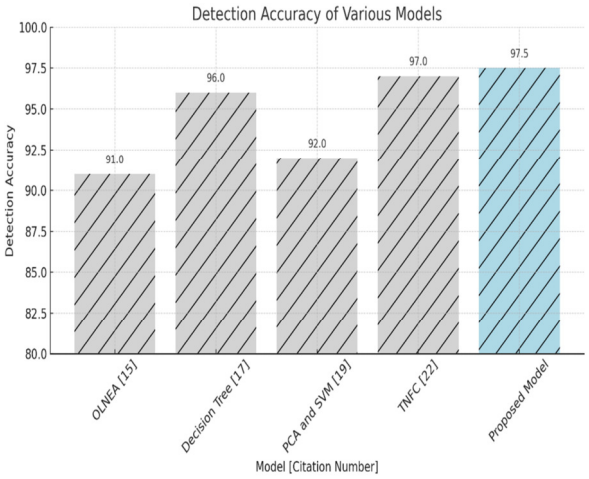


Fig. 14. Detection accuracy comparison.

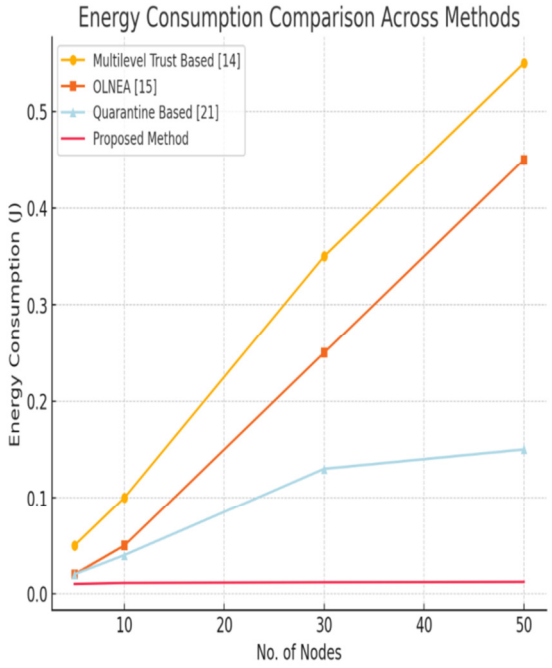


Fig. 15. Energy consumption comparison.l

## V. CONCLUSION

The proposed Lightweight MG-Net Model improves the security of Wireless Sensor Networks (WSNs) by addressing critical performance and security issues. This hybrid deep learning framework, which combines MobileNet and Gated Recurrent Unit (GRU), excels at real-time anomaly detection while processing network behaviors efficiently and with low computational demands. The system uses a modified EigenTrust algorithm to dynamically update trust scores, ensuring node reliability and integrity, with a 97% success rate in maintaining stable network operations under stress conditions. The use of the Datagram Transport Layer Security (DTLS) protocol provides strong communication security, achieving a 97% encryption success rate and protecting data transmissions from a variety of cyber threats. Operational performance, validated through rigorous simulations, demonstrates exceptional detection accuracy of more than 97.5% while using 30% less energy than traditional security frameworks and keeping network latency below 2 s. Furthermore, the model's ability to stabilize and recover from sophisticated network attacks, with recovery times of as little as 10 s post-attack, demonstrates its resilience and adaptability, essential for deployment in complex, dynamic network environments.

Future work could explore the adaptability of the MG-Net framework to other types of networks, such as Internet of Things (IoT) environments and smart grids, where similar security and efficiency challenges exist.

## REFERENCES

[1] S. M. P. Dinakarrao *et al.*, "Cognitive and Scalable Technique for Securing IoT Networks Against Malware Epidemics," *IEEE Access*, vol. 8, pp. 138508–138528, Jan. 2020, https://doi.org/10.1109/ACCESS.2020.3011919.

[2] S. V. Lakshmi and V. K. Vatsavayi, "Query optimization using clustering and Genetic Algorithm for Distributed Databases," in *International Conference on Computer Communication and Informatics*, Coimbatore, India, Jan. 2016, pp. 1–8, https://doi.org/10.1109/ICCCI.2016.7479934.

[3] Y. Han, H. Hu, and Y. Guo, "Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm," *IEEE Access*, vol. 10, pp. 11538–11550, Jan. 2022, https://doi.org/10.1109/ACCESS.2022.3144015.

[4] X. Lai and H. Wang, "RNOB: Receiver Negotiation Opportunity Broadcast Protocol for Trustworthy Data Dissemination in Wireless Sensor Networks," *IEEE Access*, vol. 6, pp. 53235–53242, Jan. 2018, https://doi.org/10.1109/ACCESS.2018.2871082.

[5] Y. Qiu, S. Li, Z. Li, Y. Zhang, and Z. Yang, "Multi-gradient routing protocol for wireless sensor networks," *China Communications*, vol. 14, no. 3, pp. 118–129, Mar. 2017, https://doi.org/10.1109/CC.2017.7897328.

[6] X. Liu *et al.*, "Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks," *Journal of Parallel and Distributed Computing*, vol. 135, pp. 140–155, Jan. 2020, https://doi.org/10.1016/j.jpdc.2019.08.012.

[7] H. B. Mahajan, A. Badarla, and A. A. Junnarkar, "CL-IoT: cross-layer Internet of Things protocol for intelligent manufacturing of smart farming," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 7, pp. 7777–7791, Jul. 2021, https://doi.org/10.1007/s12652-020-02502-0.

[8] S. Namasudra, D. Devi, S. Choudhary, R. Patan, and S. Kallam, "Security, Privacy, Trust, and Anonymity," in *Advances of DNA Computing in Cryptography*, Boca Raton, FL, USA: CRC Press, 2018, pp. 137–149.

[9] S. Das, P. Gangwani, and H. Upadhyay, "Integration of Machine Learning with Cybersecurity: Applications and Challenges," in *Artificial Intelligence in Cyber Security: Theories and Applications*, T. Bhardwaj, H. Upadhyay, T. K. Sharma, and S. L. Fernandes, Eds. New York, NY, USA: Springer, 2023, pp. 67–81.

[10] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," *Procedia Computer Science*, vol. 183, pp. 486–492, Jan. 2021, https://doi.org/10.1016/j.procs.2021.02.088.

[11] S. A. Yadwad, V. Valli, and S. Venkata, "Service Outages Prediction through Logs and Tickets Analysis," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, pp. 177–183, 2021, https://doi.org/10.14569/IJACSA.2021.0120424.

[12] V. Sharma, R. Beniwal, and V. Kumar, "Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications," *The Journal of Supercomputing*, vol. 80, no. 8, pp. 11338–11381, May 2024, https://doi.org/10.1007/s11227-023-05875-z.

[13] V. Pathak, K. Singh, T. Khan, M. Shariq, S. A. Chaudhry, and A. K. Das, "A secure and lightweight trust evaluation model for enhancing decision-making in resource-constrained industrial WSNs," *Scientific Reports*, vol. 14, no. 1, Nov. 2024, Art. no. 28162, https://doi.org/10.1038/s41598-024-75414-0.

[14] P. Gangwani, A. Perez-Pons, and H. Upadhyay, "Evaluating Trust Management Frameworks for Wireless Sensor Networks," *Sensors*, vol. 24, no. 9, Jan. 2024, Art. no. 2852, https://doi.org/10.3390/s24092852.

[15] S. Shah *et al.*, "A Dynamic Trust evaluation and update model using advance decision tree for underwater Wireless Sensor Networks," *Scientific Reports*, vol. 14, no. 1, Sep. 2024, Art. no. 22393, https://doi.org/10.1038/s41598-024-72775-4.

[16] R. M. Malkar, M. Tarambale, S. R. T, A. S. Chavan, C. N. Aher, and G. P, "Advancing Network Lifetime in Wireless Sensor Networks through Localization Techniques: A Perspective from Computer Networks," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 21s, pp. 1206–1216, Mar. 2024.

[17] T. Khan *et al.*, "An efficient trust-based decision-making approach for WSNs: Machine learning oriented approach," *Computer Communications*, vol. 209, pp. 217–229, Sep. 2023, https://doi.org/10.1016/j.comcom.2023.06.014.

[18] L. K. Tyagi and A. Kumar, "A Hybrid Trust Based WSN protocol to Enhance Network Performance using Fuzzy Enabled Machine Learning Technique," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 9s, pp. 131–144, Jul. 2023.

[19] S. Shanmuga Priya and N. Shanmuga Priya, "Energy-Efficient Trust and Quarantine-Based Secure Data Transmission in Wireless Sensor Networks," *International Journal of Computer Networks and Applications*, vol. 10, no. 2, pp. 156–165, Apr. 2023, https://doi.org/10.22247/ijcna/2023/220733.

[20] S. Madhuri and D. S. V. Lakshmi, "A Trusted Node Feedback Based Clustering Model For Detection Of Malicious Nodes In The Network," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 7, pp. 2686–2697, 2023.

AUTHORS PROFILE

**K. Keerthana** is currently pursuing her PhD in KLEF at the Department of Computer Science and Engineering. She is working as an Assistant Professor for 12 years at the CSE Department in Vignana Bharathi Institute of Technology, Hyderabad. She is working as a Salesforce and Linux Administrator trainer for BTech students. She has published two Scopus-indexed papers and has attended 3 conferences as a research scholar. She is interested in the Areas of Network Security, Cloud Computing, and Machine Learning. Email: keerthanakommera13@gmail.com.

**A Mahesh Babu** is currently working as a Professor at the Department of CSE, KLEF, Hyderabad, Aziz Nagar Campus. Professor Mahesh Babu has 22+ years of experience in the field of Academics and Software Industry. He obtained his Ph.D. in Computer Science and Technology from Sri Krishna Devaraya University. He has worked as a Sr. Manager in HCL and has been involved in a Project Integration of IWTS (Infantry Weapon Training Simulator) for SDD (Simulator Development Division) which is a R&D division of the Indian Army as a Senior Technical Consultant. He has published 4 patents and has published several articles on Career Guidance in Namaste Telangana Newspaper. His scientific interests are Cloud Computing. Cryptography and Network Security, and Internet of Things. Email: mahiabhi@gmail.com.