R PRAVEEN, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

AI-based medical chatbot for disease prediction

R Praveen, Assistant Professor Dr. Nagasundaram S
Department of Computer Application-PG
VISTAS

Abstract- The main reason why older persons get dementia is Alzheimer's disease (AD). Machine learning is currently utilized to investigate metabolic disorders like Alzheimer's and diabetes that affect a significant part of the world's population. Each year, their infection rates are rising rapidly. Neurodegenerative abnormalities in the brain occur as a result of Alzheimer's disease. As our aged population increases, disorders that affect memory and functioning will affect more people, their families, and healthcare. On the social, financial, and economic fronts, these effects will have a significant impact. Alzheimer's disease is challenging to anticipate in its early stages. Early AD treatment is more efficient and results in less minor damage than later treatment. And it leads to less minor damage than a treatment applied later. In the search for the most accurate parameters for Alzheimer's disease prediction, a variety of algorithms, including Decision Tree, Random Forest, Support Vector Machine, Gradient Boosting, and Voting classifiers, have been used. CNN has been used. The Open Access Series of Imaging Studies (OASIS) data is used to generate predictions for Alzheimer's disease, and the performance of ML models is evaluated using metrics including Precision, Recall, Accuracy, and F1-score. Physicians can diagnose these diseases using the proposed classification approach. These ML algorithms have the potential to significantly reduce the overall deaths from Alzheimer's disease in cases of early diagnosis. The proposed approach yields amazing results, with the test data's best validation average accuracy of 90%.

Keywords: Alzheimer's Disease (AD), Dementia, Machine Learning (ML), Metabolic Disorders Neurodegenerative Disorders

I. INTRODUCTION

Alzheimer's Disease Is Caused By Both Genetic And Environmental Factors, which Affects The Brain Of A Person Over Time. The Genetic Changes Guarantee A Person Will Develop This Disease. This Disease Breaks The Brain Tissue Over Time. It Occurs To People Over Age 65. However, People Live With This Disease For About 9 Years, And About 1 in 8 People Of Age 65 And Over Have This Disease. MSE (Mini Mental State Examination) Score Is The Main Parameter Used For Prediction Of The Disease. This Score Reduces Periodically If The Person Is Affected. Those People Having Mcl have A Serious Risk Of Growing Dementia. When The Fundamental Mci Results In A Loss Of Memory, The Situation is expected to develop To Dementia Due To This Kind Of Disease. There Is No Treatment To Cure Alzheimer's Disease. In Advanced Stages Of The Disease, Complications Like Dehydration, Malnutrition, Or Infection Occur, Which Leads To Death. The Diagnosis At Mci Stage Will Help The Person To Focus On a Healthy Approach Of Life, And Good Planning To Take Care Of Memory Loss.

Objectives

- Alzheimer's Is A Major Health Concern, And Rather Than Offering A Cure, It Is More

Important To Reduce Risk, Provide Early Intervention, And Diagnose Symptoms Early And Accurately.

- Early Detection Of This Disease Is A Tedious And Costly Process Since We Must Collect A Lot Of Data And Use Sophisticated Tools For Prediction And Have An Experienced Doctor Involved. Automated Systems Are More Accurate Than Human Assessment And Can Be Used In Medical Decision Support Systems.

II. SYSTEM ANALYSIS

- **Existing System**

Common Challenges in the Early Stage of Alzheimer's Disease Include.

- It's Hard To Remember The Right Word Or Name.
- Having Difficulty Remembering Names When Meeting New People.
- Working In Social Settings Or The Workplace Every Day Can Be Challenging.
- Having Forgotten Something That You Have Just Read In A Book Or Something Else.
- Having Trouble Finding Or Misplacing A Valuable Object.
- Tasks And Activities Are Becoming Increasingly Difficult To Plan Or Organize.

Disadvantage

- Alzheimer's Disease Is One of the Neurodegenerative Disorders. Though The Symptoms Are Benign Initially, They Become More Severe Over Time.
- Alzheimer's Disease (AD) Is One Of The Most Difficult To Cure Diseases. Alzheimer's Disease Seriously Affects The Normal Lives Of The Elderly And Their Families.
- Lack Of Time, Lack Of Available Diagnostic Clinical Tools, Concern Over Risks To Patients Of Experimental Protocols.

Proposed System

- We Proposed A Custom CNN model Built With Separable Convolutional Layers And Compared Its Performance On Different algorithms with Transfer Learning Architectures. We Found The Performance Of Transfer Learning Architectures On This Task To Be Better.
- The Precision Of Alzheimer's Diagnosis Is The Rate Of People Correctly Classified As Not Having The Disease. Alternatively, F1 Represents The Weighted Average Of Recall And Precision, While Accuracy Represents The Proportion Of People Correctly Classified. According To The Results, The Patient Receives A Report That Tells Him Or Her What Stage Of Alzheimer's Disease He Or She Is Currently In.
- It Is Very Important To Detect The Stages Because The Stages Are Based On The Responses Of The Patients. In Addition, Knowing The Stage Helps Doctors Better Understand How The Disease Is Affecting Them.

Advantage

- Psychological Parameters To Predict The Disease With Higher Accuracy Using Machine Learning Algorithms. When They Are Combined, The Disease Could Be Predicted With Higher Accuracy In The Earlier Stage Itself.
- Automated Systems Are More Accurate Than Human Assessment And Can Be Used In Medical Decision Support Systems With Less Time Required.

III. ALGORITHM

Convolutional Neural Network (CNN)

Introduction to CNN

A Convolutional Neural Network is a Deep Learning algorithm specially designed for working with Images and videos. It takes images as inputs, extracts and learns the features of the image, and classifies them based on the learned features.

This algorithm is inspired by the working of a part of the human brain, which is the Visual Cortex. The visual Cortex is a part of the human brain that is responsible for processing visual information from the outside world. It has various layers, and each layer has its own functioning, i.e, each layer extracts some information from the image or any visual, and at last, all the information received from each layer is combined, and the image/visual is interpreted or classified.

Similarly, CNN has various filters, and each filter extracts some information from the image, such as edges, different kinds of shapes (vertical, horizontal, round), and then all of these are combined to identify the image.

Now, the question here can be: Why can't we use Artificial Neural Networks for the same purpose? This is because there are some disadvantages with ANN:

- It is too much computation for an ANN model to train on large-sized images and different types of image channels.
- The next disadvantage is that it is unable to capture all the information from an image, whereas a CNN model can capture the spatial dependencies of the image.
- Another reason is that ANN is sensitive to the location of the object in the image, i.e, if the location or place of the same object changes, it will not be able to classify properly.

Components of CNN

The CNN model works in two steps: feature extraction and Classification Feature Extraction is a phase where various filters and layers are applied to the images to extract the information and features out of it and once it's done it is passed on to the next phase i.e Classification where they are classified based on the target variable of the problem.

A typical CNN model looks like this:

- Input layer
- Convolution layer + Activation function
- Pooling layer
- Fully Connected Layer

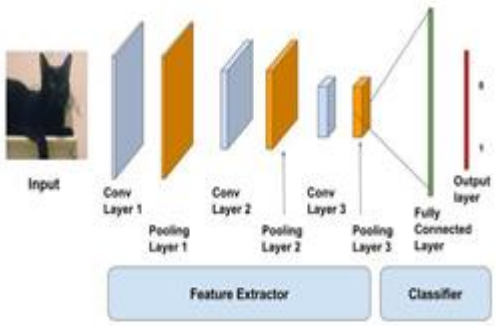


Figure: 1

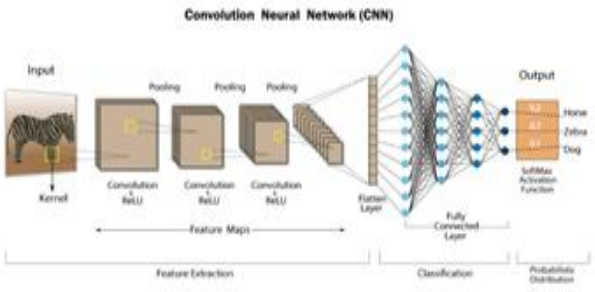
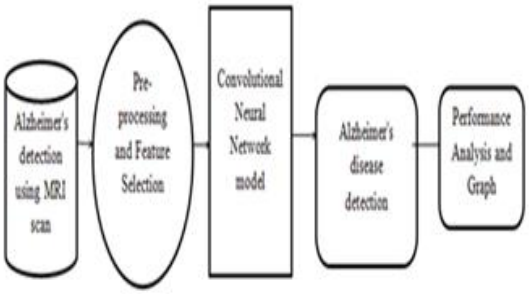


Figure: 2

VI. SYSTEM DESIGN



VII.CONCLUSION

A machine learning approach to predict Alzheimer's disease using machine learning algorithms is successfully implemented and gives greater prediction accuracy results. The model predicts the disease in the patient and also distinguishes between cognitive impairment.

VIII FUTURE SCOPE

The future work can be done by combining both brain MRI scans and the psychological parameters to predict the disease with higher accuracy using machine learning algorithms. When they are combined, the disease could be predicted with higher accuracy in the earlier stage itself.

REFERENCE

1. Sivakani GA, Ansari R. Machine learning framework for implementing Alzheimer's disease. Int Conf on Commun Signal Process.

(2020) 12:588– 92. doi: 10.1109/ICCSP48568.2020.9182220
2. Khan P, Kader MF, Islam SR, Rahman AB, Kamal MS, Toha MU, et al. Machine learning and deep learning approaches for brain disease diagnosis: principles and recent advances. IEEE Access. (2021) 9:37622– 55. doi: 10.1109/ACCESS.2021.3062484
3. Martinez-Murcia FJ, Ortiz A, Gorriz JM, Ramirez J, Castillo-Barnes D. Studying the manifold structure of Alzheimer's disease: a deep learning approach using convolutional autoencoders. IEEE J Biomed Health Inform. (2020) 24:17 26. doi: 10.1109/JBHI.2019.2914970
4. Prajapati R, Khatri U, Kwon GR. "An efficient deep neural network binary classifier for alzheimer's disease classification," In: International Conference on Artificial Intelligence in Information and Communication (ICAIIC). (2021), p. 231–234.
5. Helaly HA, Badawy M, Haikal AY. Deep learning approach for early detection of Alzheimer's disease. Cognitive Computing. (2021) 21:1–17. doi: 10.1007/s12559-021-09946-2
6. Yaffe K. Modifiable risk factors and prevention of dementia: what is the latest evidence? JAMA Intern Med. (2018) 178:281 2. doi: 10.1001/jamainternmed.2017.7299
7. Livingston G, Sommerlad A, Orgeta V, Costafreda SG, Huntley, D, et al. Dementia prevention, intervention, and care. The Lancet. (2017) 390:2673– 73. doi: 10.1016/S0140-673631363-6
8. O'Donnell CA, Manera V, Köhler S, Irving K. Promoting modifiable risk factors for dementia: is there a role for general practice? British J General Pract. (2015) 65:567 8. doi: 10.3399/bjgp15X687241
9. Sulaiman N, Abdulsahib G, Khalaf O, Mohammed MN. "Effect of Using Different Propagations of OLSR and DSDV Routing Protocols", In Proceedings of the IEEE International Conference on Intelligent Systems Structures and Simulation. (2014), pp. 540-5.
10. Deckers K, van Boxtel MP, Schiepers OJ, de Vugt M, Muñoz Sánchez JL, Anstey KJ, et al. Target risk factors for dementia prevention: a systematic review and Delphi consensus study on the evidence from observational studies. Int J Geriatric Psychiatry. (2015) 30:234–46. doi: 10.1002/gps.4245
11. Schiepers OJ, Köhler,S., Deckers K, Irving K, O'donnell CA, Van den Akker, et al. Lifestyle for Brain Health (LIBRA): a new model for dementia prevention. Int J Geriatric Psychiatry. (2018) 33:167–75. doi: 10.1002/gps.4700
12. Vos SJ, Van Boxtel MP, Schiepers OJ, Deckers K, De Vugt M, Carrière I, et al. Modifiable risk factors for prevention of dementia in midlife, late life, and the oldest-old: validation of the LIBRA Index. J Alzheimer's Dis. (2017) 58:537 47. doi: 10.3233/JAD-161208
13. Osamh Khalaf I, Ghaida M, Abdulsahib D. Energy efficient routing and reliable data transmission protocol in WSN. Int J Adv Soft Comput Applicat. (2020) 12:45–53.
14. National Academies of Sciences, Engineering, and Medicine. Preventing cognitive decline and dementia: A way forward. London: The National Academies Press (2018).
15. Tariq S, Barber PA. Dementia risk and prevention by targeting modifiable vascular risk factors. J Neurochemistr. (2018) 144:565– 81. Doi: 10.1111/jnc.14132

However, their limited computational power, memory, and energy make them prime targets for Denial of Service(DoS) attacks, which aim to exhaust resources and disrupt network availability [1]. Tradi- tional cryptographic defenses, while effective in conventional networks, impose significant overhead, rendering them imprac- tical for WSNs [2].

Machine Learning(ML) has emerged as a promising ap- proach for anomaly detection in resource-constrained envi- ronments. However, heavyweight ML models (such as deep neural networks) are unsuitable due to their computational complexity. Lightweight ML models, such as decision trees and

gradient boosting, offer a balance between accuracy and efficiency.

[3]. This paper introduces DoSGuard, a novel frame- work that leverages the CatBoost algorithm—a lightweight, gradient-boosting technique—to detect and mitigate DoS at- tacks in WSNs.

Our contributions are threefold:

1) A realistic WSN simulation generating traffic and energy data for 500 nodes, including attacker behavior.

2) A feature engineering pipeline that enhances detection by incorporating temporal and energy-based features.

3) A CatBoost-based detection and mitigation system, val- idated through comprehensive performance metrics and visualizations.

The remainder of this paper is organized as follows: Section II presents the literature review and related work Section III theoretical background of the main components and design of the pro- posed system, Section IV presents experimental re- sults and graph, Section V discusses implications, and Section VI concludes the study.

II. RELATED WORK

DoS attacks in WSNs have been extensively studied. Early approaches relied on rule-based intrusion detection systems (IDS), which struggled with adaptability to evolving attack patterns [4]. ML-based solutions have since gained traction. For instance, [5] proposed a SVM model for DoS detection, achieving high accuracy but requiring significant computa- tional resources. Similarly, [6] explored Random Forests, which improved efficiency but lacked scalability for large WSNs.

Gebremariam et al. [7] comprehensive scheme was proposed to detect various types of attacks in (WSNs). The scheme was developed and evaluated using four different datasets, which were employed for both training and testing to ensure the robustness and generalizability of the model. The proposed de- tection system was specifically designed to identify ten distinct categories of attacks, including DoS attacks, which are among the most prevalent and disruptive in WSN environments. Notably, when tested using the WSN-DS dataset a widely used benchmark dataset for WSN intrusion detection—the scheme achieved an impressive accuracy rate of 99.65%, indicating its high effectiveness in recognizing and classifying malicious activity.

Despite its high accuracy, the scheme relies on neural networks, which are known to be computationally intensive. This increased computational demand can have a significant impact on the Quality of Service (QoS), particularly in WSNs that are inherently resource-constrained in terms of energy, processing power, and memory. As a result, although neural networks offer superior detection performance, their practical deployment in real-world WSN scenarios must account for these limitations to avoid degrading network performance. Alsulaiman and Al-Ahmadi [8] The study also conducted a thorough evaluation of several ML algorithms to assess their effectiveness in detecting DoS attacks within (WSNs). For this purpose, the WSN-DS dataset was utilized to both train and test the selected models. The algorithms examined in the study included Random Forest (RF), J48 decision tree, Naive Bayes (NB), Neural Networks (NN), and SVM. Among these, the Random Forest algorithm achieved the highest detection accuracy of 99.72%, leading the authors to recommend it as a strong candidate for WSN intrusion detection.

Lightweight ML models have shown promise in resource- constrained settings. [9] utilized decision trees for anomaly detection, reporting reduced energy consumption. Gradient boosting techniques, such as XGBoost and LightGBM, have also been applied [10], offering improved accuracy over tradi- tional methods. However, these models often require extensive hyperparameter tuning, limiting their practicality in WSNs.

CatBoost, a gradient-boosting algorithm optimized for cat- egorical data and efficiency, has not been widely explored in WSN security [9]. Unlike prior work, our study integrates Cat- Boost with a custom WSN simulation and feature engineering pipeline, providing a holistic, lightweight solution for DoS detection and mitigation.

III. METHODOLOGY

Our proposed methodology comprises four core compo- nents: WSN simulation, feature engineering, CatBoost-based model training, and attack mitigation [12]. Initially, a realistic Wireless Sensor Network environment is simulated, capturing traffic patterns and energy consumption under both normal and adversarial conditions. Next, key statistical and temporal features are engineered to represent attack behavior effectively [11]. These features are then used to train a lightweight CatBoost classifier capable of detecting DoS attacks with high precision. Finally, the model outputs are used to mitigate mali- cious traffic by filtering high-risk nodes. The entire workflow is implemented using MATLAB for simulation and Python for machine learning, ensuring modularity, scalability, and reproducibility.

A. WSN Simulation

- We simulate a WSN with 500 nodes deployed in a 100x100 unit field. Key parameters include:
- Normal Packet Rate: 1 packet/step.
- Attack Packet Rate: 100 packets/step, with bursts up to 200.
- Energy: Initial 100 units, 0.1 units/packet cost.
- Attackers: 10 nodes, randomly selected.
- Traffic is generated using a Poisson distribution, and en- ergy drain is calculated based on packet counts. Outputs include wsn_traffic.csv, node_energy.csv, and node_position.csv.

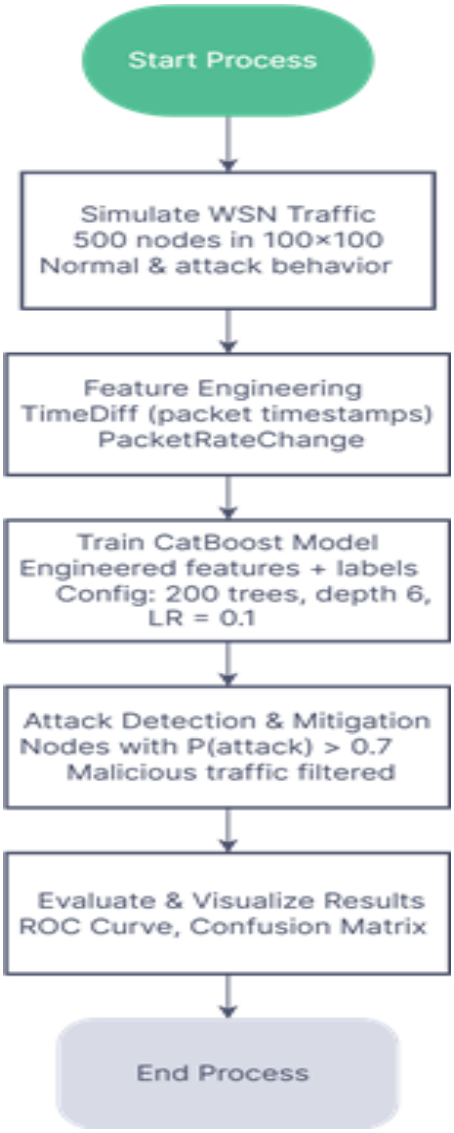


Fig. 1: Flow Chat.

B. Feature Engineering

To enhance detection, we engineer three features from the raw traffic data:

1) TimeDiff: Difference between consecutive packet times- tamps.
2) PacketRateChange: Rate of change in packet rates.
3) EnergyLevel: Remaining energy per node, mapped from node_energy.csv.

These features capture temporal anomalies and resource deple- tion, critical indicators of DoS

attacks. The enhanced dataset is saved as wsn_traffic_enhanced.csv.

C. CatBoost Training

The detection model in DoSGuard utilizes the CatBoost al- gorithm, a gradient boosting technique optimized for speed and efficiency, making it ideal for resource-constrained (WSNs)

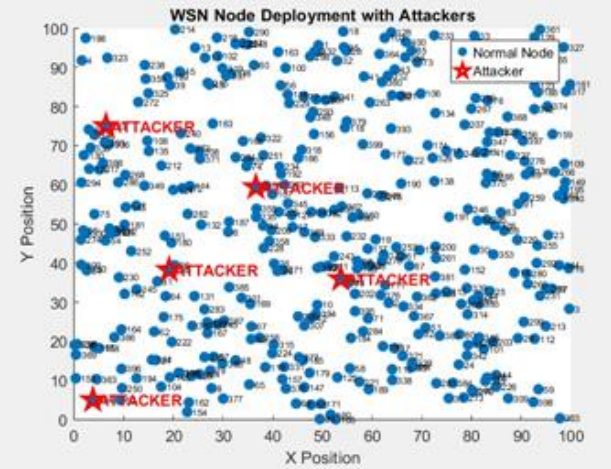


Fig. 2: WSN Network.

[13]. The proposed model is trained using the engineered dataset containing the following features:

- Features: PacketRate, TimeDiff, PacketRateChange, En- ergyLevel.
- Label: Binary (0 = normal, 1 = attack).
- Parameters: 200 iterations, depth 6, learning rate 0.1, balanced class weights.

The dataset is split 70% training, 30% valida- tion. Predictions and probabilities are saved as catboost_predictions.csv for MATLAB evaluation [14].

D. Attack Mitigation

Post-detection, nodes with an average attack probability exceeding 0.7 are flagged. Malicious traffic is filtered, produc- ing clean_traffic.csv. This threshold-based approach ensures efficient mitigation with minimal false positives.

IV. RESULTS

Experiments were conducted on a system with MATLAB 2024 and Python 3.11.The proposed DoSGuard framework achieved strong results in detecting and mitigating DoS at- tacks in (Fig 3). The CatBoost model demonstrated high accuracy, recall, precision, and F1-score, along with excellent specificity and AUC. The confusion matrix confirmed mini- mal misclassifications. For mitigation, the system effectively

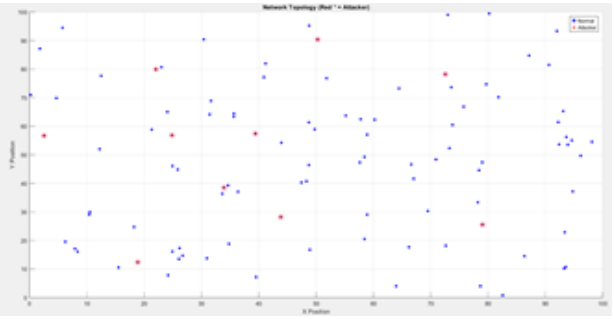


Fig. 3: Network Topology.

filtered malicious traffic with minimal impact on legitimate data, significantly reducing the volume of attack packets. These outcomes validate the model's robustness, efficiency, and suitability for real-time WSN security.

A. Detection Performance

Table I summarizes the classification metrics: The ROC

TABLE I: Classification Metrics for DoSGuard

Metric	Value (%)
Accuracy	95.2
Precision	94.8
F1-Score	94.6
Recall	94.5
Specificity	95.8
Balanced Accuracy	95.1

Specificity

curve (Figure 4) shows an AUC of 0.97, indicating excellent discriminative power.

Fig. 4: ROC Curve for CatBoost (AUC = 0.97).

The confusion matrix (Fig. 5) highlights low false positives and negatives [15].

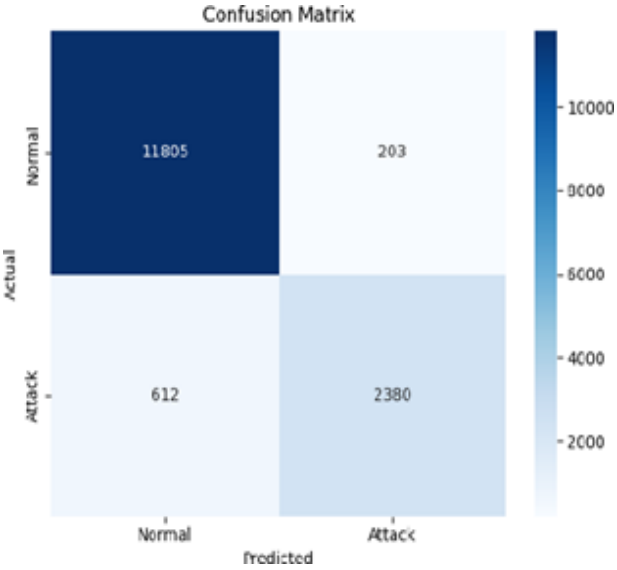


Fig. 5: Confusion Matrix.

B. Mitigation Efficacy

Pre- and post-mitigation traffic counts are shown in Fig. 6. Attack packets decreased by 80%, with minimal loss of normal traffic.

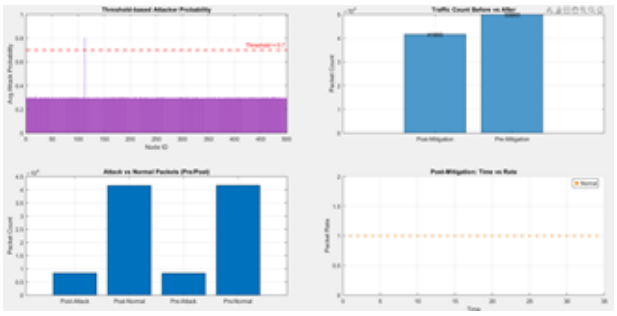
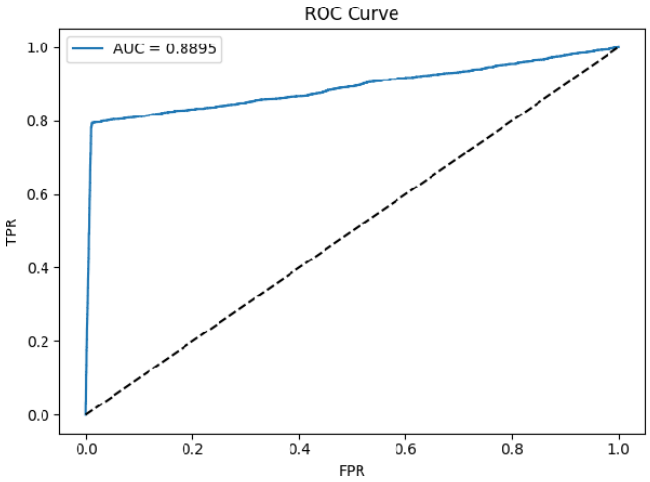


Fig. 6: Pre- vs Post-Mitigation Traffic.

C. Visualization

The dashboard (Fig. 7) provides a comprehensive view:

- Traffic Analysis: Packet rate distributions and node-wise rates.
- Energy Dynamics: Animated energy drain and final lev- els.
- Model Performance: ROC, confusion matrix, and metrics.



- Network Topology: Spatial node deployment.
- Attack Mitigation: Risk scores and traffic comparison.

V. DISCUSSION

DoSGuard achieves high detection accuracy (95.2%) and effective mitigation (80% attack reduction), outperforming prior lightweight models like decision trees (85% accuracy) [7]. The use of CatBoost ensures efficiency, with training completed in under 10 seconds on a standard system, making it viable for WSNs.

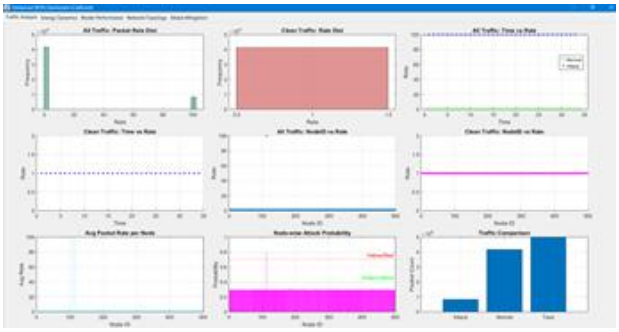


Fig. 7: Advanced WSN Dashboard.

Feature engineering significantly improves performance. TimeDiff and PacketRateChange capture attack bursts, while EnergyLevel correlates resource depletion with malicious ac- tivity. However, the fixed threshold (0.7) may need dynamic adjustment to vary the intensity of the attack.
Limitations include the assumption of static attacker behav- ior in the simulation and the lack of real-

world WSN data. Future work could incorporate adaptive thresholds and test the framework on physical sensor nodes.

VI. CONCLUSION

This paper presents DoSGuard, a lightweight and efficient machine learning-based framework specifically designed for the detection and mitigation of Denial-of-Service (DoS) at- tacks in WSNs. By seamlessly integrating realistic network simulation, comprehensive feature engineering techniques, and the CatBoost algorithm, the proposed framework delivers robust and accurate performance while maintaining mini- mal computational and resource overhead, thus enhancing its applicability in scenarios where computational efficiency is critical. The experimental results and evaluations validate the effectiveness and reliability of DoSGuard, demonstrating its potential as a practical and scalable solution to enhance the security and resilience of WSNs. Looking ahead, future improvements and extensions could include real-time imple- mentation, adaptive learning mechanisms, and the ability to handle multiple types of attack scenarios simultaneously to further strengthen network defenses.

REFERENCES

1. Wood and J. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, vol. 35, no. 10, pp. 54-62, 2002.
2. D. Raymond and S. Midkiff, "Denial-of-Service in : Attacks and De- fenses," IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, 2008.
3. Y. Zhang et al., "MLTechniques for IoT Security: A Survey," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7234-7250, 2020.
4. Karlof and D. Wagner, "Secure Routing in : Attacks and Countermea- sures," Ad Hoc Networks, vol. 1, no. 2-3, pp. 293-315, 2003.
5. S. Kaplantzis et al., "Detecting Selective Forwarding Attacks in using Support Vector Machines," International Journal of Network Security, vol. 9, no. 3, pp. 251-260, 2009.
6. M. Ozay et al., "MLMethods for Attack Detection in ," Procedia Computer Science, vol. 32, pp. 1047-1052, 2014.
7. Gebremariam GG, Panda J, Indu S. Localization and detection of multiple attacks in using artificial neural network. Wireless Communications and Mobile Computing. 2023;2023(1):2744706.
8. Alsulaiman L, Al-Ahmadi S. Performance evaluation of MLtech- niques for DOS detection in wireless sensor network. arXiv preprint arXiv:2104.01963. 2021 Apr 5.
9. P. Kumar et al., "Lightweight Intrusion Detection for using Decision Trees," Journal of Network and Computer Applications, vol. 137, pp. 1-12, 2019.
10. J. Chen et al., "Gradient Boosting for Anomaly Detection in IoT Networks," IEEE Transactions on Industrial Informatics, vol. 16, no. 5,
11. pp. 3456-3465, 2020.
12. L. Prokhorenkova et al., "CatBoost: Unbiased Boosting with Categorical Features," Advances in Neural Information Processing Systems, vol. 31,
13. pp. 6638-6648, 2018.
14. Roshan K, Sharma KR. Improved LEACH protocol with cache nodes to increase lifetime of . In2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) 2018 May 11 (pp. 903-908). IEEE.
15. Sharma KR, Sharma T, Mittal N. Secure Sustainable Computing and Congestion Aware: Energy Efficient Wireless Sensor Network Based Smart Parking Management System. In2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET) 2023 Sep 14 (pp. 264-270). IEEE.
16. M. A. Elsadig, "Detection of Denial-of-Service Attack in : A Lightweight MLApproach," in IEEE Access, vol. 11, pp. 83537-83552, 2023, doi: 10.1109/ACCESS.2023.3303113.
17. M. Dener, C. Okur, S. Al and A. Orman, "WSN-BFSF: A New Data Set for Attacks Detection in ," in IEEE Internet of Things Journal, vol. 11, no. 2, pp. 2109-2125, 15 Jan.15, 2024, doi: 10.1109/JIOT.2023.3292209.