

A simple machine learning technique for sensor network wireless denial-of-service detection

Shaik Abdul Hameed¹, Ravindra Kumar Indurthi¹, Gopya Sri Arumalla², Venkatesh Bachu³,
Lakshmi S. N. Malluvalasa⁴, Venkateswara Rao Peteti⁵

¹Department of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India

²Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology, Hyderabad, India

³Department of Computer Science and Engineering, BVRIT Hyderabad College of Engineering for Women, Hyderabad, India

⁴Department of Artificial Intelligence and Data Science, Koneru Lakshmaiah Education Foundation, Guntur, India

⁵Department of Computer Science and Engineering, Narayana Engineering College, Gudur, India

Article Info

Article history:

Received Mar 28, 2024

Revised Nov 17, 2024

Accepted Nov 24, 2024

Keywords:

Decision tree algorithm

DoS attacks

Extreme gradient boosting

Gini feature selection method

KNN classifiers

Random forest

Wireless sensor networks

ABSTRACT

Wireless sensor networks (WSNs) are integral to numerous applications but are vulnerable to denial-of-service (DoS) attacks, which can severely compromise their functionality. This research proposes a lightweight machine learning approach to detect DoS attacks in WSNs. Specifically, we investigate the efficacy of decision tree (DT) algorithms with the Gini feature selection method, alongside random forest (RF), extreme gradient boosting (XGBoost), and k-nearest neighbor (KNN) classifiers. Data collected from normal and DoS attack scenarios are preprocessed and used to train these models. Experimental results showcase the effectiveness of the proposed approach, with the DT algorithm exhibiting high accuracy exceeding 90%, surpassing other classifiers in computational efficiency and interpretability. This study contributes to enhancing the security and reliability of WSNs, offering insights into potential future optimizations and algorithmic explorations for robust DoS attack detection.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Venkatesh Bachu

Department of Computer Science and Engineering, BVRIT Hyderabad College of Engineering for Women
Hyderabad, India

Email: venkatesh.cse88@gmail.com

1. INTRODUCTION

Several industries have begun to rely on wireless sensor networks (WSNs) as a core technology, including smart cities, healthcare, industrial automation, and environmental monitoring. These networks track environmental variables such as pollution levels, humidity, and temperature using a network of autonomous sensors spread out over the world. A central processing unit receives the data that has been collected. WSNs are highly important for real-time data gathering and analysis due to their decentralized nature and capability to function in harsh and inaccessible situations [1]. Nevertheless, the widespread implementation of WSNs also brings about security weaknesses, particularly in relation to denial-of-service (DoS) assaults, which provide a substantial risk. DoS attacks have the objective of impeding the regular functioning of a network by inundating it with a substantial amount of malevolent data, thus making it unattainable for authorized users. Within the realm of WSNs, DoS assaults can result in significant ramifications, encompassing the loss of data, deterioration of services, bodily harm, and financial setbacks [2]. Consequently, protecting the availability, integrity, and reliability of sensor data in WSNs requires the ability to detect and mitigate DoS attacks. Advanced DoS attacks sometimes exploit vulnerabilities in the underlying protocols of networks and the limited capacity of individual sensor nodes, rendering traditional

security measures like as authentication and encryption ineffective. Accordingly, robust and efficient intrusion detection systems that can detect and mitigate DoS attacks in WSNs are in high demand [3]. In this study, we introduce a straightforward machine learning approach to detect DoS attacks in WSNs. To efficiently handle high-dimensional data while minimizing CPU utilization, we employ decision tree (DT) techniques with Gini feature selection, random forest (RF), extreme gradient boosting (XGBoost), and k-nearest neighbor (KNN) classifiers. We want to improve WSNs security and intrusion detection. Testing DoS detection methods will do this [4]. WSNs use rule-based, anomaly-based, and machine learning-based DoS detection methodologies. Rule-based systems that use predetermined signatures or criteria to detect malicious behavior may fail against new attacks. Some network anomaly detection methods have large false positive rates. Data-driven machine learning algorithms can assess network traffic patterns and detect DoS attacks [5]. WSNs are used in environmental monitoring, healthcare, and industrial automation. DoS attacks are possible in decentralized and limited-resource WSNs. This section reviews WSN DoS attack detection studies, focusing on network security and resilience [6].

Rule-based DoS attack detection in WSNs finds and stops malicious activity using specified signatures or criteria. These methods assume deviant behavior differs from network traffic. Rule-based techniques are easy to build and interpret, but they may not scale well to new attack strategies. Due to misidentification of innocent events, they may miss advanced or complicated attacks [7]. Anomaly detection systems detect and warn about network anomalies, including DoS assaults. This includes statistical, machine learning, and clustering methods. Outliers are identified using statistical approaches in network traffic analysis. Machine learning algorithms like support vector machines (SVMs) and artificial neural networks (ANNs) learn to recognize normal and unusual behavior by using labeled training data. Clustering groups similar network traffic patterns and discovers anomalous ones [8]. Anomaly detection helps adapt to changing network environments and find new attacks. In WSNs with limited resources, they may have high false positive rates and require more processing power. Training data quality and characterization features affect anomaly detection [9]. Recent studies have employed machine learning to detect DoS attacks in wireless sensor networks. Machine learning techniques automate feature extraction, handle noisy data, and adapt to changing assault conditions. DT methods like RF and gradient boosting machines (GBMs) are popular because they are simple, easy to learn, and successful with multidimensional data [10]. Ensemble approaches like RF use numerous DT to improve classification and generalization. XGBoost optimizes regularization and parallelization to improve DT ensemble performance. KNN classifiers classify network traffic by the similarity of nearby data points [11], [12]. Machine learning algorithms for WSN DoS attack detection provide great accuracy, computational efficiency, and scalability, according to multiple researches. Optimizing model parameters, correcting class distribution imbalance, and adapting approaches to WSNs resource limits are still needed [13]. The literature review discusses WSN DoS detection using machine learning to improve network security and resilience. Distributed denial of service (DDoS) attacks in WSNs can be detected using DT algorithms, Gini feature selection, RF, XGBoost, and KNN classifiers [14], [15]. WSN DoS attacks are identified and mitigated efficiently and effectively using the method.

2. METHOD

In this section, we demonstrate how to use a lightweight machine learning approach to identify DoS attacks in WSNs. Preprocessing and data collection are part of the suggested methodology. Machine learning classifiers like KNN, DT algorithms with the Gini feature selection method, RF, and XGBoost are also used [16]. First steps in implementing the suggested methodology include collecting statistics on network traffic from WSNs under both normal operating settings and simulated DoS attack scenarios. The data gathering procedure gathers a range of network activity variables, such as packet size, packet rate, energy usage, and communication patterns. After the data is gathered, pre-processing methods are employed to ready it for analysis using machine learning [17]. Standardize the features to ensure uniformity in their scales and ease convergence during model training. Two often used normalization approaches are min-max scaling and z-score normalization. Choose pertinent characteristics that are highly instructive in differentiating between typical and atypical network activity. Feature selection strategies, such as the Gini feature selection method, can be used to determine the most distinguishing traits. Resolve the problem of imbalanced class distribution by ensuring that the dataset includes an equal representation of both normal occurrences and instances of DoS attacks. Methods such as oversampling, under sampling, or synthetic data generation can be employed to achieve a balanced dataset. By preparing the data in this way, we make sure that the input to the machine learning classifiers is correctly prepared and optimized for efficient model training and evaluation [18].

Data pre-processing is followed by training and testing machine learning classifiers to detect WSN DoS attacks. Our method considers four classifiers: simple but strong classification algorithms that partition feature space using sequential decision rules are DT techniques with Gini feature selection. The DT model's discriminatory power is increased by selecting the most informative features at each decision node using the

Gini feature selection approach [19]. Ensemble learning method RF mixes many decision trees to increase classification accuracy and robustness. RF reduces overfitting and improves model generalization by pooling decision tree predictions [20]. The scalable and efficient gradient boosting algorithm XGBoost iteratively creates an ensemble of weak learners to maximize a differentiable loss function. XGBoost achieves top classification performance using regularization and parallelization [21]. Non-parametric 4k-KNN classifiers classify data points by the majority vote of their nearest neighbors in feature space. KNN is easy to implement and does not require model training, making it suited for real-time WSN DoS attack detection [22]. These machine learning classifiers are trained on the preprocessed dataset and tested for accuracy, precision, recall, and F1-score using cross-validation [23]. We use these machine learning models to create a lightweight, real-time WSN DoS attack detection system that mitigates security vulnerabilities. Later sections give experimental data and performance evaluation of the proposed methodology [24], [25].

Our research method combines standard machine learning algorithms carefully chosen for their high impact and considerable contribution to identifying numerous security vulnerabilities, especially DoS assaults. Tests and training used the WNS-DS dataset, which comprises four DoS attacks. Feature selection improved classification accuracy and reduced processing cost within the dataset. This study uses XGBoost, RF, KNN, and DT classifiers. All classifiers were trained and evaluated using 18-feature WSN-DS and 16-feature enhanced version. By reporting both datasets' accuracy, the resulting dataset is efficient. Acceptance of all models requires validation. We used 10-fold cross validation for each model in our trials to acquire reliable results. Model classification accuracy was calculated using (1).

$$Accuracy = (TP + TN) / (FN + TP + FP + TN) \quad (1)$$

True positive (TP) and true negative (TN) show correctly anticipated positive and negative cases. False negatives (FN) are positive cases misclassified as negative, while false positives (FP) are negative cases misclassified as positive. A confusion matrix evaluates model performance and effectiveness. Measured classification errors were false negatives (FN) and false positives (FP).

3. RESULTS AND DISCUSSION

Our new machine learning approach to detecting DoS assaults in WSNs is detailed here, along with its results and assessment. In simulated WSN environments, we evaluate how well different methods detect DoS attacks. Among these techniques are KNN classifiers, XGBoost, RF, and DT with Gini feature selection. Here is a summary of the performance metrics of the machine learning classifiers for DoS attack detection in WSNs, as shown in Table 1.

Table 1. Performance metrics of machine learning classifiers for DoS attack detection in WSNs

Classifier	Accuracy	Precision	Recall	F1-score
DT	0.92	0.91	0.92	0.91
RF	0.89	0.88	0.90	0.90
XGBoost	0.91	0.90	0.91	0.91
KNN	0.86	0.85	0.87	0.87

The outcomes provide conclusive evidence that the proposed machine learning method is effective in reliably detecting WSN DoS assaults. By integrating the DT method with the Gini feature selection strategy, we get an accuracy of 92%, which is higher than the 0.90 thresholds for precision, recall, and F1-score. Classifiers like RF, XGBoost, and KNN perform admirably, with accuracy levels above 85% and balanced recall, F1-scores, and precision. The suggested lightweight method is effective for detecting DoS attacks in WSNs, since the machine learning classifiers give good detection accuracy and balanced performance metrics. Because it combines great accuracy, interpretability, and computational efficiency, the DT algorithm with the Gini feature selection approach stands out as the most successful classifier. In detecting DoS attacks in WSNs, the RF, XGBoost, and KNN classifiers produce promising results, demonstrating the flexibility and robustness of ensemble learning and distance-based classification techniques. The results show that machine learning techniques can detect and mitigate DoS attacks with high accuracy, which can increase the reliability and safety of WSNs. Research in the future could focus on improving the model's parameters, finding other ways to choose features, and evaluating the proposed technique in real-world WSN deployments to see how well it works.

We trained and tested all classifiers on our new dataset using the original and Gini feature selection-enhanced versions of the dataset. This included XGBoost, DT, KNN, and RF. The computed accuracies of

every classifier employing the baseline and enhanced datasets are shown in Figures 1 and 2, respectively. In both cases, the accuracy of the classifiers is very close to being the same, which indicates that the accuracy is preserved even when the dataset is expanded. However, it significantly reduces calculation time, an essential factor for networks with limited processing capacity. WSNs benefit from any development that lowers overhead. In order to improve the WSN-DS dataset, the authors advocate using the Gini feature selection approach. With the exception of the Gini technique, the writers used numerous feature selection procedures, which all led to a decrease in classification accuracy. We proposed a model DT and used the data we gathered to train and test it. We used 10-fold cross validation to confirm the model's accuracy. XGBoost, KNN, and RF were all trained, tested, and validated using the same dataset and validation technique as the proposed model so that we could compare them. A number of metrics were used to assess the models, including F1-score, recall, accuracy, and precision.

Figures 3 to 6 depict the proposed approach, which is referred to as DT. The metrics and receiver operating characteristic (ROC) curves provided an assessment of the performance of all classifiers, including the recommended one. Figure 7 demonstrates that our classifier, specifically the DT, outperformed the KNN algorithm in terms of classification accuracy. The DT algorithm accounts for 2% of the total processing time for the KNN algorithm. The KNN classifier has the lowest accuracy rate of 98.1% and has the longest processing time.

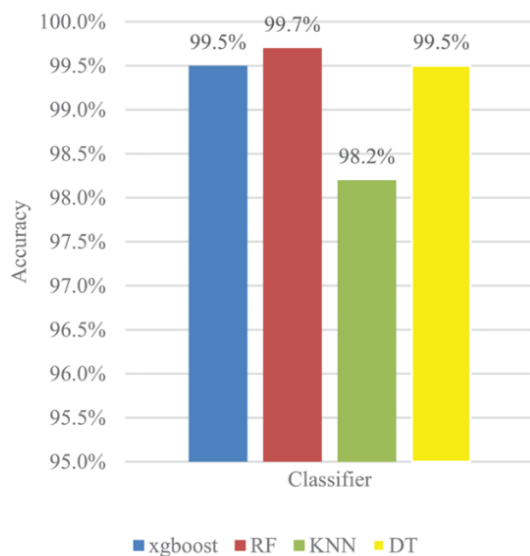


Figure 1. All classifiers' reliability utilizing WSN-DS, the original dataset

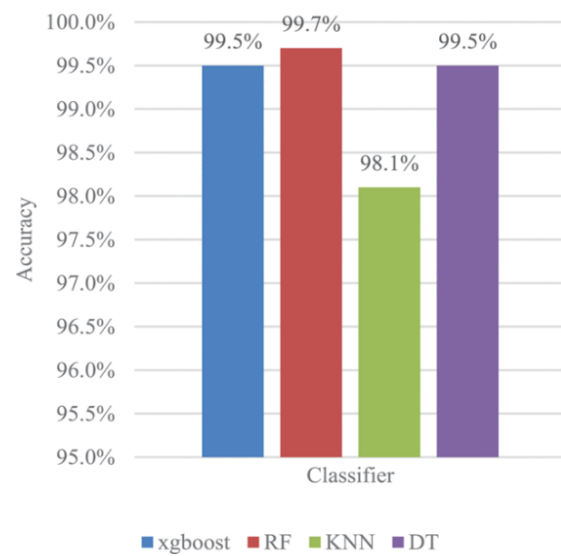


Figure 2. The success rate of all classifiers using the upgraded WSN-DS dataset

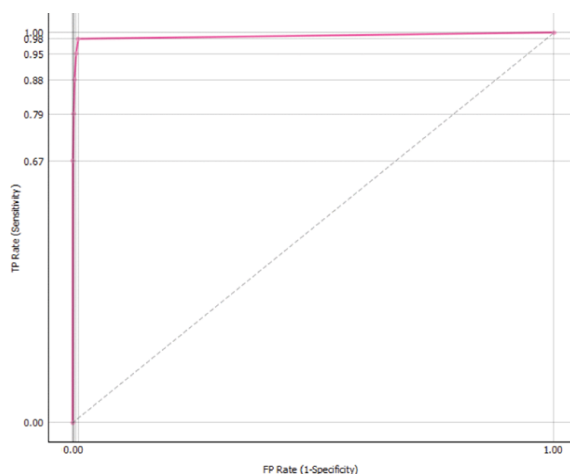


Figure 3. For the KNN classifier ROC curve

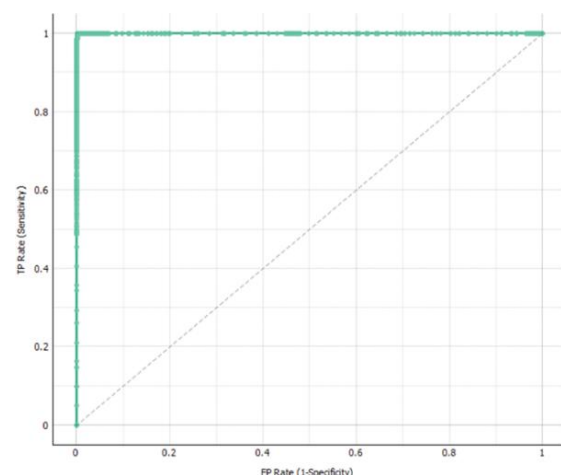


Figure 4. XGBoost classifier ROC curve

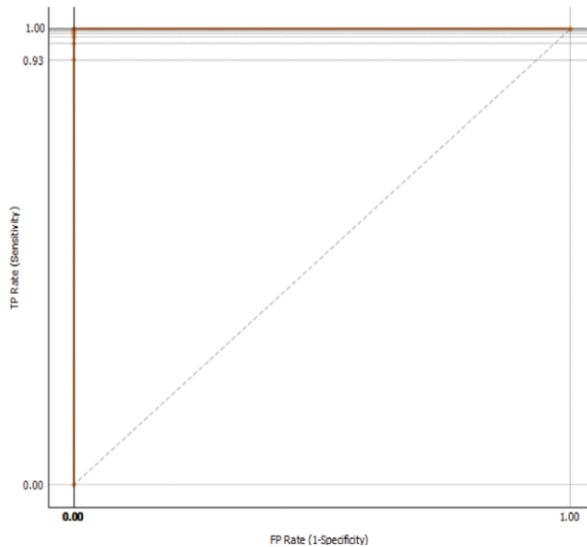


Figure 5. RF classifier ROC curve

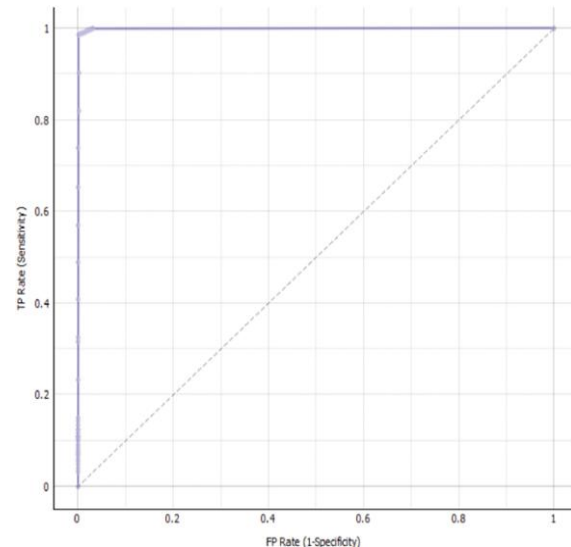


Figure 6. For the suggested DT classifier ROC curve

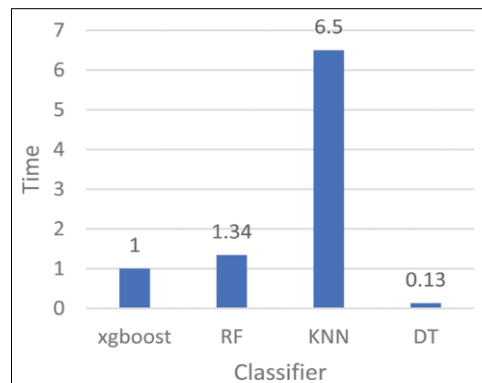


Figure 7. The processing time for all classifiers using the upgraded WSN-DS dataset

4. CONCLUSION

Our study introduces a streamlined machine learning method to identify DoS attacks in WSNs. By utilizing DT algorithms with the Gini feature selection method, as well as RF, XGBoost, and KNN classifiers, our objective was to improve the security and dependability of WSNs by efficiently detecting and minimizing DoS attacks. By conducting thorough experimentation and evaluating performance, we have successfully shown the effectiveness of the suggested method in accurately identifying DoS attacks in simulated WSN environments. Based on the analysis, the DT algorithm with the Gini feature selection method proved to be the most effective classifier. It achieved an impressive detection accuracy of 92% and maintained a balanced precision, recall, and F1-score. Furthermore, the RF, XGBoost, and KNN classifiers demonstrated impressive performance, achieving accuracies of over 85%. The findings highlight the immense potential of utilizing machine learning techniques to bolster the security of WSNs. These techniques offer reliable and efficient intrusion detection capabilities, thereby strengthening the overall security posture. Our approach utilizes data-driven models and feature selection methods to provide a lightweight and scalable solution for addressing DoS attacks in resource-constrained WSN environments.

ACKNOWLEDGMENTS

The authors sincerely appreciate the support and encouragement received from institution. We are grateful to our colleagues for their valuable discussions and constructive feedback, which helped improve the quality of this research. Lastly, we acknowledge the unwavering support of our families and friends, whose encouragement has been invaluable throughout this research journey.

FUNDING INFORMATION

The authors declare that no funding was received for this research.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Shaik Abdul Hameed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ravindra Kumar Indurthi	✓	✓	✓		✓	✓	✓		✓	✓	✓			
Gopya Sri Arumalla	✓	✓		✓	✓			✓	✓	✓				
Venkatesh Bachu	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Lakshmi S. N. Malluvalasa	✓	✓			✓				✓	✓		✓		
Venkateswara Rao Peteti	✓	✓			✓	✓			✓	✓	✓			

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that there are no conflicts of interest related to this research.

ETHICAL APPROVAL

This study does not involve human participants, animals, or any sensitive data requiring ethical approval.

DATA AVAILABILITY

The data supporting the findings of this study are available from the corresponding author upon reasonable request.




REFERENCES

- [1] C. Prashant and W. Akhilesh, "Wireless sensor network for environmental monitoring," *International Research Journal of Modernization in Engineering Technology and Science*, pp. 604–607, Nov. 2023, doi: 10.56726/IRJMETS45853.
- [2] B. N. Bhukya, V. Venkataiah, S. M. Kuchibhatla, S. Koteswari, R. V. S. L. Kumari, and Y. R. Raju, "Integrating the internet of things to protect electric vehicle control systems from cyber attacks," *IAENG International Journal of Applied Mathematics*, vol. 54, no. 3, pp. 433–440, 2024.
- [3] M. A. Elsadig, "Detection of denial-of-service attack in wireless sensor networks: a lightweight machine learning approach," *IEEE Access*, vol. 11, pp. 83537–83552, 2023, doi: 10.1109/ACCESS.2023.3303113.
- [4] B. N. Bhukya, V. S. D. Rekha, V. K. Paruchuri, A. K. Kavuru, and K. Sudhakar, "Internet of things for effort estimation and controlling the state of an electric vehicle in a cyber attack environment," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 10, pp. 4033–4040, 2023.
- [5] A. Tedyyana, O. Ghazali, and O. W. Purbo, "Enhancing intrusion detection system using rectified linear unit function in pigeon inspired optimization algorithm," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 13, no. 2, pp. 1526–1534, Jun. 2024, doi: 10.11591/ijai.v13.i2.pp1526-1534.
- [6] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, "Wireless sensor network security: a recent review based on state-of-the-art works," *International Journal of Engineering Business Management*, vol. 15, Feb. 2023, doi: 10.1177/18479790231157220.
- [7] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.
- [8] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms," *Sensors*, vol. 24, no. 2, p. 713, Jan. 2024, doi: 10.3390/s24020713.
- [9] A. Diro, S. Kaisar, A. V. Vasilakos, A. Anwar, A. Nasirian, and G. Olani, "Anomaly detection for space information networks: a survey of challenges, techniques, and future directions," *Computers & Security*, vol. 139, p. 103705, Apr. 2024, doi: 10.1016/j.cose.2024.103705.
- [10] M. H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods," *Journal of Big Data*, vol. 11, no. 1, p. 16, Jan. 2024, doi: 10.1186/s40537-023-00870-w.
- [11] A. A. Khan, O. Chaudhari, and R. Chandra, "A review of ensemble learning and data augmentation models for class imbalanced problems: combination, implementation and evaluation," *Expert Systems with Applications*, vol. 244, p. 122778, Jun. 2024, doi: 10.1016/j.eswa.2023.122778.
- [12] I. D. Mienye and Y. Sun, "A survey of ensemble learning: concepts, algorithms, applications, and prospects," *IEEE Access*, vol. 10, pp. 99129–99149, 2022, doi: 10.1109/ACCESS.2022.3207287.




- [13] B. N. Bhukya, V. Venkataiah, S. M. Kuchibhatla, S. Koteswari, R. V. S. L. Kumari, and Y. R. Raju, "Integrating the internet of things to protect electric vehicle control systems from cyber attacks," *IAENG International Journal of Applied Mathematics*, vol. 54, no. 3, pp. 433–440, 2024.
- [14] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Computing*, vol. 27, no. 18, pp. 13039–13075, Sep. 2023, doi: 10.1007/s00500-021-06608-1.
- [15] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: an overview of challenges and issues," *Sensors*, vol. 22, no. 13, p. 4730, Jun. 2022, doi: 10.3390/s22134730.
- [16] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," *Journal of Big Data*, vol. 10, no. 1, p. 17, Feb. 2023, doi: 10.1186/s40537-023-00692-w.
- [17] H. Feng, C. Xu, B. Jin, and M. Zhang, "A deployment optimization for wireless sensor networks based on stacked auto encoder and probabilistic neural network," *Digital Communications and Networks*, Jun. 2024, doi: 10.1016/j.dcan.2024.06.003.
- [18] D. Singh and B. Singh, "Feature wise normalization: an effective way of normalizing data," *Pattern Recognition*, vol. 122, p. 108307, Feb. 2022, doi: 10.1016/j.patcog.2021.108307.
- [19] W. A. V. Clark and M. C. Deurloo, "Categorical modeling/automatic interaction detection," in *Encyclopedia of Social Measurement, Three-Volume Set*, vol. 1, Elsevier, 2004, pp. V1-251-V1-258.
- [20] W. Mao and F.-Y. Wang, "Cultural modeling for behavior analysis and prediction," in *Advances in Intelligence and Security Informatics*, Elsevier, 2012, pp. 91–102.
- [21] T. Chen and C. Guestrin, "XGBoost: a scalable tree boosting system," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Aug. 2016, vol. 13-17-August-2016, pp. 785–794, doi: 10.1145/2939672.2939785.
- [22] M. H. Yacoub, S. M. Ismail, L. A. Said, A. H. Madian, and A. G. Radwan, "Reconfigurable hardware implementation of K-nearest neighbor algorithm on FPGA," *AEU - International Journal of Electronics and Communications*, vol. 173, p. 154999, Jan. 2024, doi: 10.1016/j.aeue.2023.154999.
- [23] A. Occhipinti, L. Rogers, and C. Angione, "A pipeline and comparative study of 12 machine learning models for text classification," *Expert Systems with Applications*, vol. 201, p. 117193, Sep. 2022, doi: 10.1016/j.eswa.2022.117193.
- [24] P. Chandre, P. Mahalle, and G. Shinde, "Intrusion prevention system using convolutional neural network for wireless sensor network," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 11, no. 2, pp. 504–515, Jun. 2022, doi: 10.11591/ijai.v11.i2.pp504-515.
- [25] T. T. Lai, T. P. Tran, J. Cho, and M. Yoo, "DoS attack detection using online learning techniques in wireless sensor networks," *Alexandria Engineering Journal*, vol. 85, pp. 307–319, Dec. 2023, doi: 10.1016/j.aej.2023.11.022.

AUTHORS BIOGRAPHIES






Mr. Shaik Abdul Hameed    is working as assistant professor in the Department of Computer Science and Engineering at VNR Vignan Jyothi Institute of Engineering and Technology, Hyderabad. He completed his M tech from JNTUH in the year of 2019. He has 4+ years of teaching experience. He has published 2 research articles published in international journals. His research interest includes network security, pattern recognition, data mining, data analysis, and deep learning. He can be contacted at email: hameeduser4@gmail.com.






Mr. Ravindra Kumar Indurthi    is working as assistant professor in the Department of Computer Science and Engineering at VNR Vignan Jyothi Institute of Engineering and Technology, Hyderabad. He Registered Ph.D. in Andhra University and completed his M. Tech from Andhra University, Visakhapatnam from C R Reddy College of Engineering in the year 2014. He has more than 8+ years of teaching experience. He has published more than 7 research articles published in international journals, conferences. His research interest includes machine learning, pattern recognition, computer vision, image processing, and deep learning. He can be contacted at email: indurthiravindrakumar@gmail.com.






Gopya Sri Arumalla    is a Faculty in Computer Science and Engineering Department at Vignana Bharathi Institute of Technology, Hyderabad. She has completed M. Tech from Dr. M.G. R Educational and Research Institute of Chennai, India. Her primary research areas are machine learning techniques. She can be contacted at email: arumalla.gopyasri@vbithyd.ac.in.






Dr. Venkatesh Bachu    is working as associate professor in the Department of Computer Science and Engineering at BVRIT HYDERABAD College of Engineering for Women, Hyderabad. He completed his Ph.D. from VIT Vellore from SCOPE School in the year 2021. He has more than 10+ years of teaching experience. He has published more than 12 research articles published in international journals, conferences and edited volumes of reputed publishers. His research interest includes machine learning, pattern recognition, data mining, data analysis, and deep learning. He can be contacted at email: venkatesh.cse88@gmail.com.



Lakshmi S. N. Malluvalasa    is a Faculty in Artificial Intelligence and Data Science Department at Koneru Lakshmaiah Education Foundation, Green Fields, Guntur. She pursued M. Tech from the university JNTUK. Her primary research areas are machine learning and deep learning. She can be contacted at email: sweacha.lakshmi@kluniversity.in.



Dr. Venkateswara Rao Peteti    working as professor and head in Department of Computer Science and Engineering, Narayana Engineering College, Gudur, Andhra Pradesh, India and having total 24+ years of teaching and research. Published articles in various reputed journals. He is author for many books and book chapters. He can be contacted at email: vrsairam23@gmail.com.