iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72191

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

A Machine Learning Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids

Dr. M.V. Vijaya Saradhi[1], Mende Puja[2], B Anjali[3], Lavudya Harshitha[4], Karre Bharadwaj[5]
[1]*Dean, Professor-CSE Department & ACE Engineering College*
[2, 3, 4, 5]*Student, CSE Department & ACE Engineering College*

Abstract: ***The expanding dependence on remote sensor systems (WSNs) inside microgrids has underscored the basic require for strong security components, given their helplessness to different cyber-attacks . This study introduces a machine learning-based cyberattack detection model tailored for WSNs in microgrids, utilizing a comprehensive dataset from Kaggle. Our demonstrate coordinating a assorted set of calculations, counting Convolutional Neural Systems (CNN), Detached Forceful Classifiers, Arbitrary Timberland Classifiers, and XGBoost Classifiers, to guarantee tall exactness and productivity in recognizing peculiarities. By nourishing the framework with organize information, it can precisely classify the organize state as either typical or beneath one of three particular assault sorts: grayhole, blackhole, or flooding assault. This multifaceted approach not as it were upgrades the discovery .***

Keywords: Wireless Sensor Networks, Cyber Attack Detection, Machine Learning, CNN, Passive Aggressive Classifier, Random Forest, XGBoost, Microgrids, Security

I. INTRODUCTION

As the worldwide vitality segment shifts towards renewable and decentralized control frameworks, microgrids have ended up fundamental for effective vitality administration and dispersion. Remote Sensor Systems (WSNs) play a pivotal part in real-time checking, control, and mechanization inside these microgrids. Be that as it may, their dependence on open communication channels makes them profoundly vulnerable to cyber-attacks, which can lead to control disturbances, operational disappointments, and money related misfortunes. Assaults such as grayhole, blackhole, and flooding can compromise arrange astuteness, coming about in postponed information transmission, framework disappointments, and indeed framework power outages.

WSNs in microgrids are defenseless to advanced cyber- attacks like grayhole, blackhole, and flooding assaults, which can seriously affect operations and cause budgetary misfortunes. Conventional security arrangements battle to distinguish and relieve these dangers due to their energetic and advancing nature. A machine learning-based discovery show is required to upgrade the flexibility and security of microgrids. The venture points to create a machine learning-based cyber assault location demonstrate for WSNs in microgrids. By leveraging progressed calculations like CNN, Detached Forceful Classifier, Irregular Timberland, and XGBoost, the show will precisely distinguish and classify cyber dangers, guaranteeing the dependable operation of microgrids. In any case, the reliance of WSNs on open communication channels makes them exceedingly helpless to cyber dangers, posturing noteworthy security dangers. Cyber-attacks focusing on WSNs in microgrids can disturb information transmission, control framework controls, and lead to operational disappointments.

Among the foremost common and harming cyber-attacks are grayhole, blackhole, and flooding assaults. These assaults compromise arrange keenness by specifically dropping, rerouting, or overpowering information parcels, which can result in deferred or misplaced communication between basic lattice components.

The results of such security breaches run from minor benefit intrusions to total framework power outages, driving to extreme money related misfortunes and jeopardizing the unwavering quality of vitality conveyance. In spite of the developing risk scene, conventional security components frequently battle to identify and relieve these modern assaults due to their energetic nature and advancing assault designs.

The essential objective of this venture is to create a machine learning-based cyber assault location demonstrate custom- made particularly for WSNs working inside microgrids. The demonstrate is outlined to distinguish and classify cyber dangers with tall precision by leveraging progressed machine learning calculations. The chosen algorithms— Convolutional Neural Systems (CNN), Inactive Forceful Classifier, Irregular Timberland, and XGBoost—each play a unmistakable part in upgrading the location handle. CNN is especially viable in include extraction and design acknowledgment, making it appropriate for analyzing organize activity inconsistencies.

©IJRASET: All Rights are Reserved

The Inactive Forceful Classifier guarantees fast adjustment to modern assault designs, empowering real-time danger discovery. Improves decision-making precision by combining different choice trees.XGBoost, known for its effectiveness and versatility, advance reinforces the model's prescient capabilities by minimizing untrue positives and making strides classification execution. By joining these machine learning strategies, the proposed location show points to altogether make strides the security system of WSNs in microgrids. It'll not as it were distinguish cyber dangers with tall exactness but moreover adjust to developing assault designs, guaranteeing ceaseless and solid microgrid operation.

The effective execution of this show will offer assistance moderate security dangers, avoid disturbances in vitality conveyance, and upgrade the generally strength of microgrids against cyber-attacks. [1]

II. LITERATURE SURVEY

Security analysis for cyber-physical systems against stealthy deception attacks

([Author(s):] Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang, IEEE, 2013) [1] The security issue in the state estimation problem is investigated for a networked control system (NCS). The communication channels between the sensors and the remote estimator in the NCS are vulnerable to attacks from malicious adversaries.

Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators

([Author(s):] Pajic, Miroslav, James Weimer, Nicola Bezzo, Oleg Sokolsky, George J. Pappas, and Insup Lee, 2017) [2] Examines the growing number of security-related incidents in control systems. Highlights high-profile cyber-attacks on critical infrastructures, including the Maroochy Water breach. Proposes attack-resilient state estimation techniques to enhance system security.

Resilient Distributed Control in the Presence of Misbehaving Agents in Networked Control Systems

([Author(s):] Zeng, Wente, and Mo-Yuen Chow, IEEE, 2014) [3] Studies consensus-reaching problems in networked control systems (NCS) with misbehaving agents. Proposes a reputation-based resilient distributed control algorithm for leader-follower consensus networks. Discusses the effectiveness of this method in mitigating the impact of malicious agents.

Resilient Control of Networked Control Systems with Stochastic Denial of Service Attacks

([Author(s):] Sun, Hongtao, Chen Peng, Taicheng Yang, Hao Zhang, and Wangli He, Neurocomputing, 2017) [4] Focuses on resilient control of NCS under Denial of Service (DoS) attacks, modeled as a Markov process. Examines the interaction between attack and defense strategies. Introduces a control framework that mitigates the effects of packet dropouts due to cyber-attacks. [2] [3]

III. PROBLEM STATEMENT

The critical problem addressed in this study revolves around the vulnerability of wireless sensor networks (WSNs) within microgrids to various sophisticated cyber-attacks, such as grayhole, blackhole, and flooding attacks.These attacks can severely disrupt the operation of microgrids, leading to significant operational and financial losses. Traditional security mechanisms often fall short in effectively detecting and mitigating such attacks due to their complexity and the dynamic nature of cyber threats. Therefore, there is a pressing need for an advanced, efficient, and accurate cyberattack detection model specifically designed for WSNs in microgrids, leveraging the capabilities of machine learning algorithms to enhance the resilience and security of these critical infrastructure systems. [4]

A. Objectives

1) This venture points to create a machine learning-based cyberattack location show particularly for Remote Sensor Systems (WSNs) inside microgrids.
2) The demonstrate is outlined to precisely and productively identify cyber dangers by analyzing organize activity and recognizing inconsistencies.
3) It centers on recognizing grayhole, blackhole, and flooding assaults, which can disturb organize communication and compromise security.
4) Progressed machine learning calculations such as Convolutional Neural Systems (CNN), Detached Forceful Classifiers, Irregular Timberland Classifiers, and XGBoost Classifiers are coordinates to upgrade discovery exactness.
5) By leveraging these calculations, the framework reinforces the security system of microgrids, guaranteeing early discovery

and relief of potential dangers.

6) The demonstrate makes a difference keep up the nonstop and solid operation of microgrids by anticipating cyberattacks that may lead to benefit disturbances.

7) This extend contributes to shielding basic foundation from advanced cyber dangers and improves the flexibility of microgrid systems.

IV. PROPOSED SYSTEM

The proposed framework for identifying cyber assaults in remote sensor systems (WSNs) inside microgrids utilizes a mix of progressed machine learning calculations, particularly Convolutional Neural Systems (CNN), Detached Forceful Classifiers, Arbitrary Timberland Classifiers, and XGBoost Classifiers. This show is planned to analyze and learn from information designs in organize activity, as given by the dataset facilitated on Kaggle. By contributing real-time or chronicled arrange information into the framework, the demonstrate

A. System Architecture

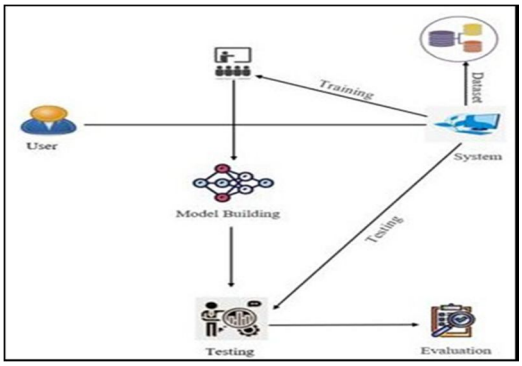


Fig 1. System Architecture

B. Convolutional Neural Network (CNN)

Convolutional Neural Systems (CNNs) are profound learning models outlined for preparing organized framework information, such as pictures. They comprise of convolutional, pooling, and fully associated layers, which extricate various leveled highlights from crude data. Convolutional layers identify designs like edges and surfaces, whereas pooling layers diminish spatial measurements, making strides in productivity. This permits CNNs to exceed expectations in picture recognition, question discovery, and classification. A key advantage of CNNs is their capacity to naturally learn highlights, killing manual highlight building. Progressed models like AlexNet, VGGNet, and ResNet have accomplished beat performance in vision tasks. CNNs are moreover broadly utilized in discourse acknowledgment, restorative imaging, and independent frameworks, making them an effective device in AI applications. [5]

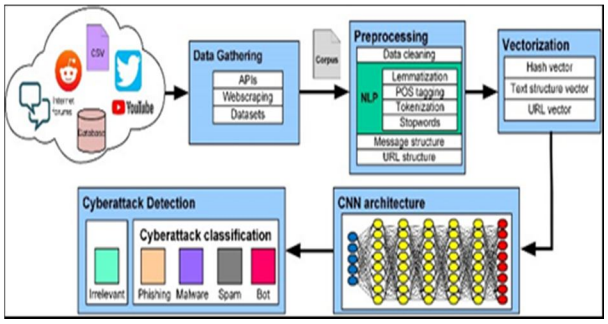


Fig.2 Convolutional Neural Network

C. *Passive Aggressive Classifiers*

Inactive Forceful classifiers are online learning calculations utilized for twofold classification assignments. They point to play down classification mistake whereas adjusting to modern information incrementally. Not at all like conventional bunch learning calculations, Inactive Forceful classifiers upgrade their show parameters consecutively, making them reasonable for scenarios with gushing information or restricted memory assets. These classifiers work by altering their choice boundaries based on the rightness of their expectations, with forcefulness controlled by a hyperparameter. They are especially valuable for real- time applications where information arrives persistently, such as content classification, spam discovery, and estimation investigation. [6]

D. *Random Forest Classifiers*

Random Forest classifiers are ensemble learning methods based on decision tree models. They operate by constructing a multitude of decision trees during training and outputting the mode of the classes (classification) or mean prediction (regression) of individual trees. Each tree is trained on a random subset of the training data and features, promoting diversity among the trees and reducing overfitting. Random Forests are known for their robustness, scalability, and ability to handle high-dimensional data with complex interactions. They are widely used for tasks like classification, regression, feature importance ranking, and anomaly detection in various domains. [7]

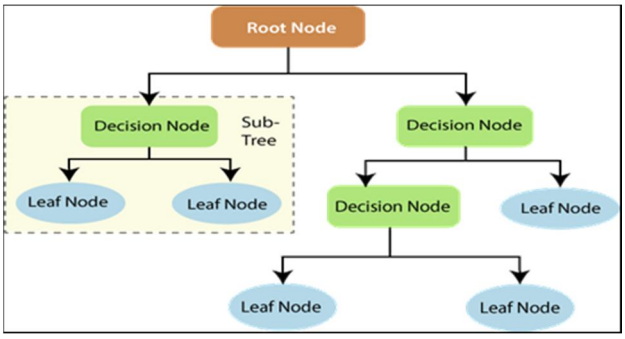


Fig 3: Random Forest Classifiers

E. *XGBoost Classifiers*

XGBoost (Extreme Gradient Boosting) could be a versatile and proficient use of slope boosting machines. It consecutively builds an ensemble of weak learners (ordinarily choice trees) to reduce a user-specified misfortune work. XGBoost utilizes a regularization term within the objective function to control demonstrate complexity and prevent overfitting. It utilizes a disseminated and parallel computing system, making it reasonable for large-scale datasets and computationally intensive tasks. XGBoost has picked up notoriety due to its uncommon execution, including classification, regression, ranking, and anomaly detection.

H. Tianfield, “Data mining-based cyber-attack detection,” [8].

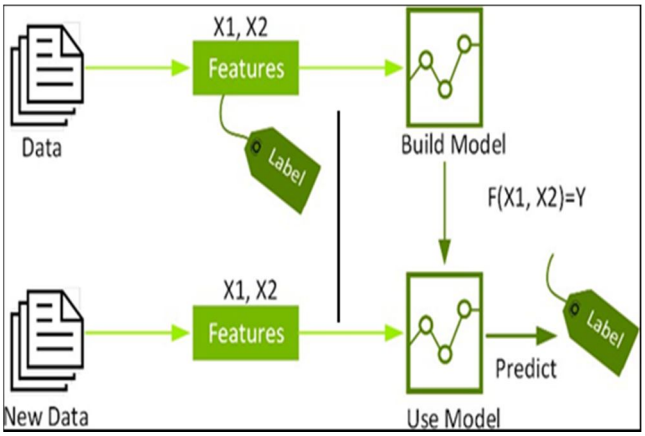


Fig 4: XGBoost Classifiers

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

V. METHODOLOGY

A. Input Data

The first step involves gathering relevant data necessary for attack detection. This data is collected from various network traffic logs, intrusion detection systems, and publicly available cybersecurity datasets. The data should contain both normal and attack traffic instances, ensuring diversity for effective model training.

B. Preprocessing

The preprocessing step is essential for preparing the data for the model. This involves steps such as resizing images, normalizing pixel values, and augmenting the dataset to ensure robustness. Augmentation techniques such as rotation, flipping, and zooming are used to generate a diverse set of images from the original dataset. This helps the model generalize better. Preprocessing also includes removing noise from the images, ensuring that the data is clean and ready for feature extraction.

C. Data Splitting

In this step, the dataset is divided into training and testing sets. The training set is used to teach the model how to identify patterns, while the testing set is used to evaluate the performance of the trained model. A typical split is 70% training data and 30% testing data, though this can vary based on the specific dataset and the requirements of the project. Ensuring a balanced dataset across different classes is also important to prevent any class imbalance issues.

D. Model Selection and Training

This step involves, the implementation of multiple machine learning algorithms to enhance the accuracy of cyberattack detection. The system integrates Convolutional Neural Networks (CNN) for recognizing complex patterns in network traffic data, Passive Aggressive Classifiers for quick adaptation to evolving threats, Random Forest Classifiers for robust decision-making through ensemble learning, and XGBoost Classifiers for optimizing performance by handling imbalanced data effectively.

E. Model Evaluation

After training, the performance of the models is evaluated using various metrics, including accuracy, precision, recall, and F1-score. A confusion matrix is used to provide a detailed breakdown of classification performance, while cross-validation techniques are applied to prevent overfitting and ensure the reliability of the model in real- world scenarios. The best-performing model is selected based on these evaluation metrics.

F. Deployment and Testing

Once the model achieves optimal performance, it is deployed into a real-time environment where it processes incoming network traffic and classifies it as either normal or under attack. To ensure the robustness of the system, rigorous testing is conducted, including unit testing to verify the functionality of individual components, integration testing to assess the interaction between different modules, and system testing to evaluate overall performance under various attack scenarios.

VI. RESULTS



Fig 6.1 Registration

©IJRASET: All Rights are Reserved

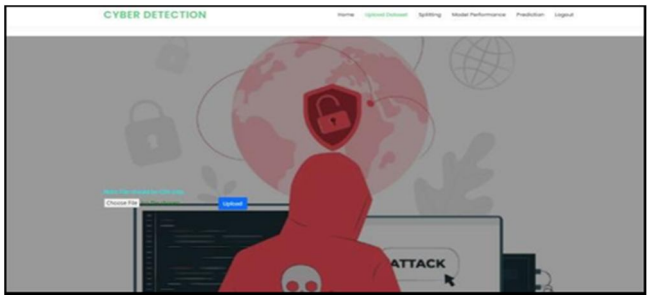


Fig 6.2 Upload data

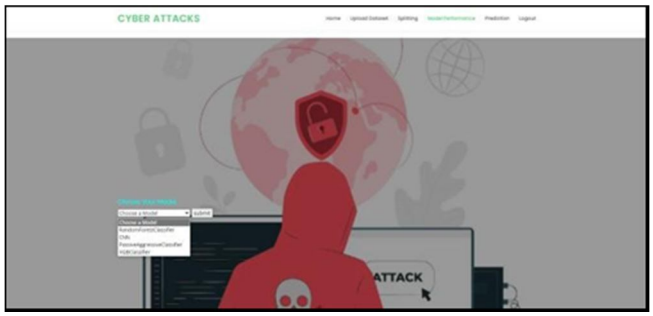


Fig 6.3 Train Model

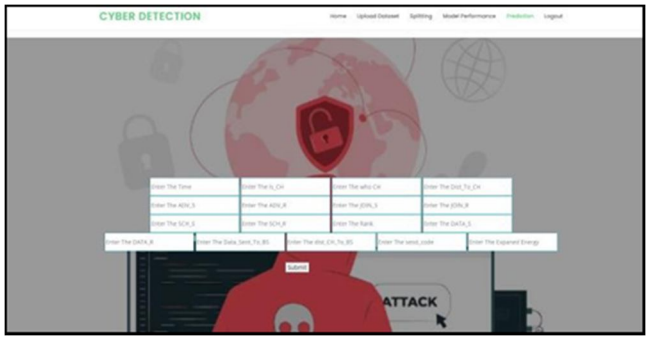


Fig 6.4 Output

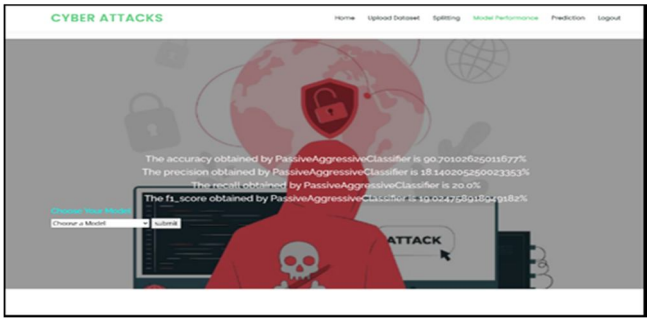


Fig 6.5 Accuracy Prediction

The image provided is from a "CYBER DETECTION" interface, likely related to detecting anomalies or attacks in a wireless sensor network (WSN) or IoT-based network.

Here's an explanation of each input field:

1. Enter The Time: Timestamp of the event or packet transmission.
2. Enter The Is_CH: Flag indicating whether the node is a Cluster Head (CH).
3. Enter The who CH: Identifier of the Cluster Head associated with this node.
4. Enter The Dist_To_CH: Distance from the node to its Cluster Head.
5. Enter The ADV_S: Advertisement packet sent by the source node.
6. Enter The ADV_R: Advertisement packet received by the node.
7. Enter The JOIN_S: Join request sent by a node to become part of a cluster.
8. Enter The JOIN_R: Join request received by the Cluster Head.
9. Enter The SCH_S: Schedule packet sent by the CH.
10. Enter The SCH_R: Schedule packet received by the node.
11. Enter The Rank: Ranking metric used for CH selection or routing.
12. Enter The DATA_S: Data packets sent by the node.
13. Enter The DATA_R: Data packets received by the node.
14. Enter The Data_Sent_To_BS: Amount of data sent from node or CH to the Base Station (BS).
15. Enter The dist_CH_To_BS: Distance from the Cluster Head to the Base Station.
16. Enter The send_code: Possibly an identifier or security token associated with the transmission.
17. Enter The Expanded Energy: Energy expended during communication or sensing operations.

These parameters are typically used to detect malicious activity or abnormalities in data communication, such as sinkhole, Sybil, or selective forwarding attacks in WSN or IoT systems.

VII. ANALYSIS OF SYSTEM PERFORMANCE

Technology plays a crucial role in modern advancements, enabling innovation in computing, automation, and communication. One of the key aspects of any technological solution is scalability, which ensures that systems can handle increasing workloads efficiently without compromising performance. Alongside scalability, efficiency is essential, as it focuses on maximizing productivity while minimizing resource wastage and operational costs. Additionally, cost efficiency is a critical factor, ensuring that businesses and individuals achieve optimal results with minimal expenses while maintaining quality and effectiveness. Another vital aspect is user experience, which enhances interaction by ensuring ease of use, accessibility.

A. Technology Comparison Table

Paper Title	Technology Used	Detection Techniques
A Machine Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids	Machine Learning, Deep Learning	Anomaly Detection, Intrusion Detection Systems (IDS), Pattern Recognition
Cybersecurity in Microgrids: A Review of Machine Learning Approaches	ML, Neural Networks	Supervised & Unsupervised Learning
Anomaly Detection in Wireless Sensor Networks for Smart Grids	AI, Data Mining	Clustering, Statistical Analysis
Deep Learning-Based Intrusion Detection in Smart Microgrid Systems	Deep Learning (CNN, LSTM)	Network Traffic Analysis
Secure Wireless Sensor Networks: A Cybersecurity Approach	Cryptographic Methods, AI	Signature-Based Detection, Hybrid IDS

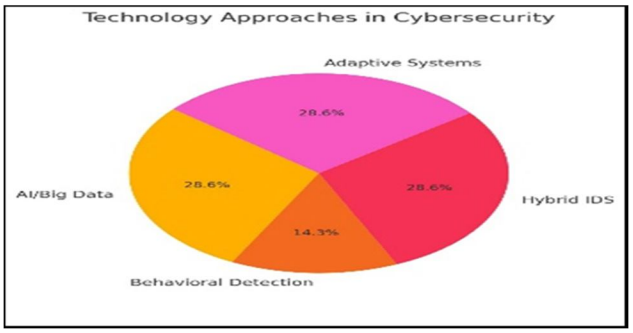


Fig 7.1 Technology approaches in Cybersecurity

Paper Title	Scalability	Computational Resource Requirements
A Machine Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids	High	Requires GPU, Cloud Processing
Cybersecurity in Microgrids: A Review of Machine Learning Approaches	Medium	Can run on standard CPUs
Anomaly Detection in Wireless Sensor Networks for Smart Grids	Medium	Requires moderate processing power
Deep Learning- Based Intrusion Detection in Smart Microgrid Systems	High	Needs pre-trained models and large datasets
Secure Wireless Sensor Networks: A Cybersecurity Approach	High	Scalable cryptographic processing
AI-Driven Cyber Threat Detection for Smart	High	Cloud-based and scalable
Hybrid Intrusion Detection Systems for IoT- Enabled Smart Grids	Medium	Works on edge devices and cloud
Adaptive Cybersecurity Framework for Wireless Sensor Networks	High	Real-time adaptive computing

9.2 Scalability Comparison Table

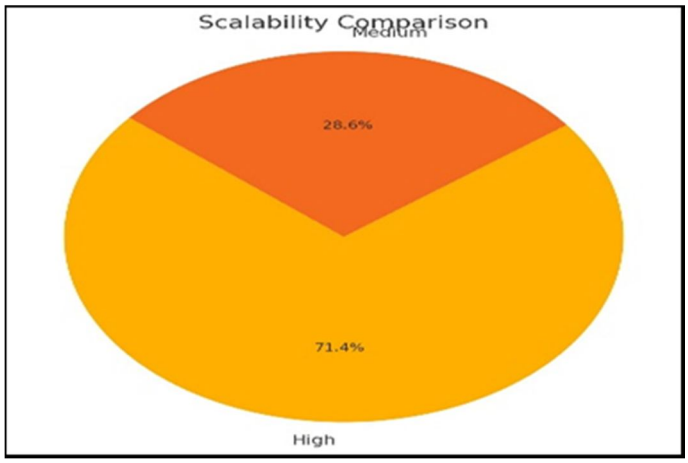


Fig 7.2 Scalability Comparison

B. Efficiency (Accuracy & Performance) Comparison

Paper Title	Accuracy	Speed
A Machine Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids	High (90 %+)	Fast
Cybersecurity in Microgrids: A Review of Machine Learning Approaches	Medium(80-85%)	Moderate
Anomaly Detection in Wireless Sensor Networks for Smart Grids	Medium(80-85%)	Moderate
Deep Learning- Based Intrusion Detection in Smart Microgrid Systems	High(90%+)	Fast
Secure Wireless Sensor Networks: A Cybersecurity Approach	High(90%+)	Real-Time
AI-Driven Cyber Threat Detection for Smart Grid Networks	High(90%+)	Real-time

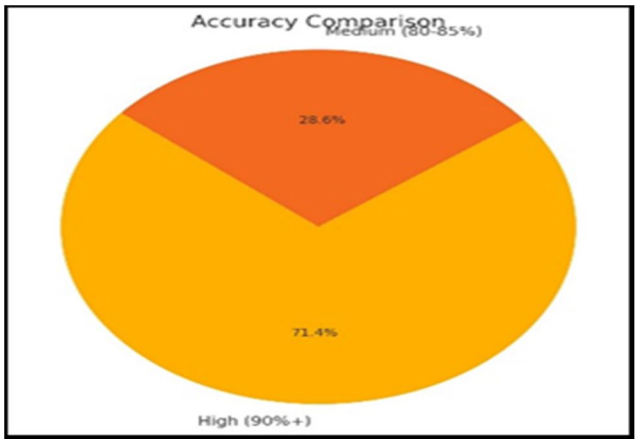


Fig 7.3 Accuracy Comparison

C. Cost Efficiency Comparison

Paper Title	Cost Efficiency	Hardware Requirements
A Machine Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids	Medium	GPU, Cloud Processing
Cybersecurity in Microgrids: A Review of Machine Learning Approaches	High	Low-cost computing
Anomaly Detection in Wireless Sensor Networks for Smart Grids	Medium	Minimal hardware
Deep Learning- Based Intrusion Detection in Smart Microgrid Systems	Low	Pre-trained model dependency
Secure Wireless Sensor Networks: A Cybersecurity Approach	Medium	High cryptographic processing costs
AI-Driven Cyber Threat Detection for Smart Grid Networks	Medium	Cloud and high-performance computing
Hybrid Intrusion Detection Systems for IoT-Enabled Smart Grids	High	Works with edge computing
Adaptive Cybersecurity Framework for Wireless Sensor Networks	Medium	AI-powered edge devices

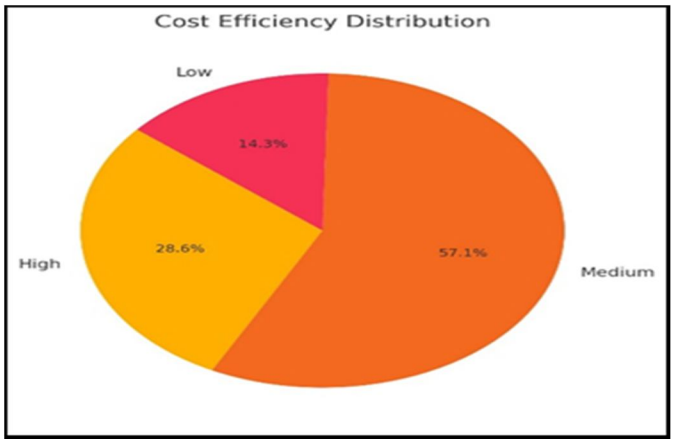
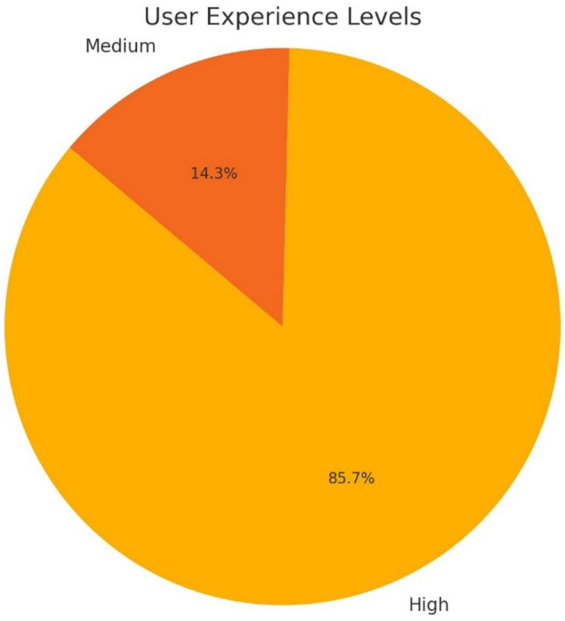


Fig 7.4 Cost Efficiency Distribution

D. User Experience Comparison

Paper Title	Cost Efficiency	User Experience
Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids	High	Moderate
Cybersecurity in Microgrids: A Review of Machine Learning Approaches	High	High(Explanable AI)
Anomaly Detection in Wireless Sensor Networks for Smart Grids	Medium	Moderate
Deep Learning- Based Intrusion Detection in Smart Microgrid Systems	Medium	Low(Black-box AI)
Secure Wireless Sensor Networks: A Cybersecurity Approach	High	High (Security-focused AI)
AI-Driven Cyber Threat Detection for Smart Grid Networks	High	Moderate
Hybrid Intrusion Detection Systems for IoT-Enabled Smart Grids	High	High (Hybrid Explainable AI)
Adaptive Cybersecurity Framework for Wireless Sensor Networks	High	Very High (Self-Adaptive AI)



VIII. CONCLUSION

The proposed system extraordinarily identifies cyberattacks in WSNs inside microgrids employing a combination of CNN, Detached Forceful Classifiers, Arbitrary Woodlands, and XG Boost.

It goes past conventional strategies by identifying unpretentious deviations rather than depending exclusively on known assault marks, tending to dangers like grayhole, blackhole and flooding. CNNs empower effective highlight extraction to reveal complex assault designs and irregularities in organize activity. Detached Forceful Classifiers rapidly adjust to modern assaults by overhauling choice boundaries with approaching information.

Irregular Woodlands upgrade exactness through numerous choice trees, decreasing wrong positives.

XGBoost progresses decision-making and minimizes classification mistakes, optimizing by and large execution.

This collaboration guarantees exact, real-time cyber danger location and fortifies microgrid security.

The versatile learning demonstrate underpins progressing advancement, dealing with advancing assault procedures.

By moving past rule-based frameworks, it empowers proactive, brilliantly defense instruments.

Eventually, the demonstrate contributes to independent, self-sustaining cybersecurity in basic foundation.

IX. FUTURE ENHANCEMENTS

1) Reinforcement Learning for Adaptive Detection: Implement reinforcement learning techniques to enable the system to dynamically adapt and improve its cyberattack detection capabilities over time.

2) Deep Learning-Based Anomaly Detection: Integrate advanced deep learning architectures, such as autoencoders, to enhance the identification of novel and complex attack patterns.

3) Blockchain for Secure Event Logging: Leverage blockchain technology to create a secure, tamper-resistant logging system that ensures the integrity and trustworthiness of network event records.

4) Decentralized Collaborative Defense: Develop a decentralized framework where sensor nodes share real- time threat intelligence, improving the system's resilience against sophisticated and coordinated cyberattacks.

5) Edge Computing for Faster Threat Detection: Utilize edge computing to process cyber threat data locally on WSN nodes, reducing latency and improving response time for attack mitigation.

6) Federated Learning for Privacy-Preserving Security Models: Apply federated learning to train cyberattack detection models across multiple microgrids without directly sharing sensitive network data.

7) AI-Driven Intrusion Response Mechanisms: Integrate AI-driven response systems to automate countermeasures, such as isolating compromised nodes or rerouting traffic to minimize attack impact.

8) Multi-Modal Data Analysis for Enhanced Threat Identification: Combine network traffic analysis with additional cybersecurity data sources, such as hardware- level monitoring and user behavior analytics, for a more comprehensive detection system.

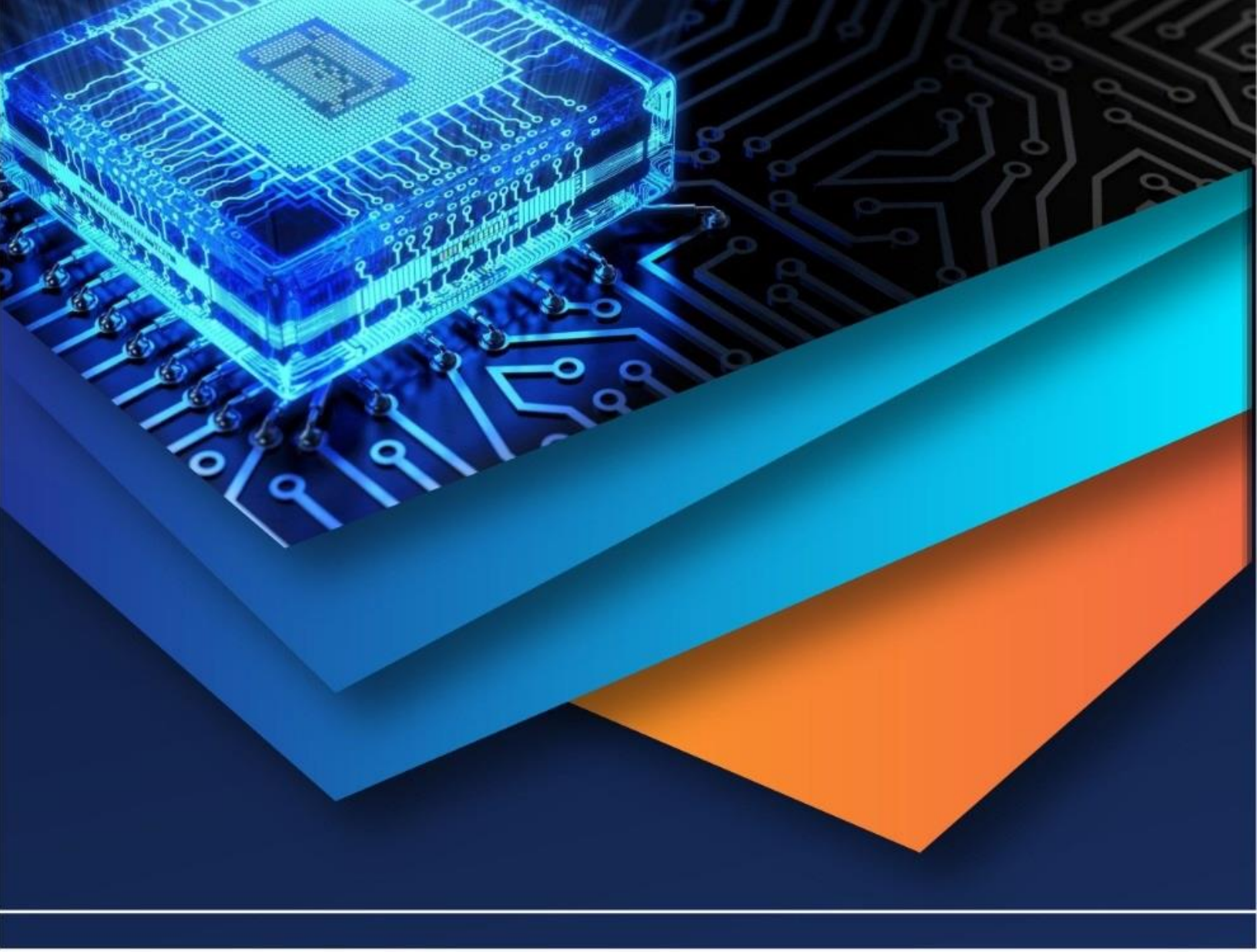
9) Explainable AI for Improved Cybersecurity Transparency: Develop AI models with explainability features to help network administrators understand attack patterns and enhance trust in automated security decisions.

10) Self-Healing Security Mechanisms: Incorporate self- healing capabilities where compromised nodes can autonomously recover and restore normal operation after mitigating cyber threats.

REFERENCES

[1] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," IEEE Trans. Autom. Control, vol. 58, no. 11, pp. 2715–2729, 2013.
[2] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in Proc. Amer. Control Conf., IEEE, 2013, pp. 3344–3349.
[3] M. Pajic et al., "Design and implementation of attack-resilient cyberphysical systems," IEEE Control Syst. Mag., vol. 37, no. 2, pp. 66–81, 2017.
[4] M. Ozay et al., "Machine learning methods for attack detection in the smart grid," IEEE Trans. Neural Netw. Learn. Syst., vol. 27, no. 8, pp. 1773–1786, 2015.
[5] Y. LeCun, Y. Bengio and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
[6] K. Crammer et al., "Online Passive-Aggressive Algorithms," Journal of Machine Learning Research, vol. 7, pp. 551-585, 2006.
[7] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5-32, 2001.
[8] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in Proc. 22nd ACM SIGKDD Intl. Conf. on Knowledge Discovery and Data Mining, 2016, pp. 785-794.
[9] A. Jindal et al., "Machine Learning-Based Cyber Threat Detection in WSNs," Neural Computing and Applications, Springer, 2023.
[10] Ozay, Mete, Inaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R. Kulkarni, and H. Vincent Poor. "Machine learning methods for attack detection in the smart grid." IEEE transactions on neural networks and learning systems 27, no. 8 (2015): 1773-1786.
[11] Tianfield, Huaglory. "Data mining based cyber-attack detection." System simulation technology 13, no. 2 (2017):
[12] 90-104.
[13] Pasqualetti, Fabio, Florian Dorfler, and Francesco Bullo. "Attack detection and ¨ identification in cyber- physical systems." IEEE Transactions on Automatic Control 58, no. 11 (2013): 2715-2729.
[14] Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks – Discusses real-time security strategies in WSNs, focusing on detection and mitigation mechanisms.
[15] Intrusion Detection System for Wireless Sensor Networks: A Machine Learning-Based Approach – Explores machine learning-based intrusion detection for WSN security.
[16] Gharavi, H. "Cyber-Physical Security for Distributed Smart Grid." Proceedings of the IEEE, 2019.
[17] Cui, J. et al. "Cyber-Attack Detection for Wireless Sensor Networks in Smart Grids." Sensors, 2020.
[18] Zarpelão, B. B., et al. "A survey of intrusion detection in WSNs." Journal of Network and Computer Applications, 2017.
[19] Yang, T., et al. "Anomaly Detection in WSNs using Deep Learning." IEEE Internet of Things Journal, 2022.
[20] Jindal, A. et al. "Machine Learning-Based Cyber Threat Detection in WSNs." Springer Neural Computing and Applications, 2023.
[21] Rao, R. et al. "Resilient Cybersecurity Framework for Wireless Sensor Networks in Smart Cities." ACM Transactions on Sensor Networks, 2021.
[22] Mahbub, K. et al. "Blockchain-Enabled Security Model for Wireless Sensor Networks." Journal of Cybersecurity and Privacy, 2023.
[23] Lin, C., et al. "AI-Based Intrusion Detection in Wireless Networks." IEEE Transactions on Information Forensics and Security, 2024.
[24] T. Yang et al., "Anomaly detection in WSNs using deep learning," IEEE Internet of Things Journal, vol. 9, no. 2, pp. 1504–1514, 2022.
[25] H. Tianfield, "Data mining-based cyber-attack detection," System Simulation Technology, vol. 13, no. 2, pp. 90–104, 2017.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)