

# WIRELESS NETWORK SECURITY ENHANCEMENT WITH ZITA

Ms. HARSHINI A<sup>1</sup>, Mr. SANKARA NARAYANAN S T<sup>2</sup>,

<sup>1</sup> Ms. HARSHINI.A, M.sc CFIS, Department of Computer Science Engineering,

[harshiniaruljustin@gmail.com](mailto:harshiniaruljustin@gmail.com) 9361471854, Dr. DR. M.G.R Educational and Research Institute, Chennai, India

<sup>2</sup> Mr. SANKARA NARAYANAN S.T, Assistant Professor, Center of Excellence in Digital Forensics, Chennai, India.

\*\*\*

**Abstract** - With the growing cybersecurity threats, predictive maintenance has turned out to be a critical approach for ensuring reliability and efficiency in wireless networks. In this paper, we demonstrate the use of supervised machine learning methods in predictive maintenance for the detection and mitigation of attacks on wireless networks. Using past network data containing different network metrics and security attacks, our developed model predicts possible network attacks. To pass this intercept, users use the supervised learning; this means that the model is trained on labelled datasets, where instances of network attacks were explicitly identified. Save relevant network features using feature engineering and selection to improve model prediction ability. The trained model is then deployed to monitor network traffic continually in real-time to detect anomalous patterns that can indicate potential attacks. By detecting such threats at an early stage, proactive measures such as network reconfiguration, traffic filtering, and incident response can be initiated, minimizing the impact of a cyberattack and maintaining operational continuity. By integrating prediction into maintenance strategy, the book segment combines predictive analytics with traditional maintenance practices, thus facilitating a proactive maintenance framework capable of adjusting to the evolving threat landscape, thereby directly contributing to the literature on future-proofing wireless networks.

**Key Words:** Predictive maintenance, supervised machine learning, Wireless networks, Cybersecurity, Predictive modelling, Anomaly detection, Real-time monitoring, Network security management

## I. INTRODUCTION

We propose ZITA, a framework for strengthening the security of wireless networks based on intelligent threat detection, adaptive response methods, and optimized encryption algorithms. ZITA [1] is a security enhancement framework that utilizes real-time network analytics and machine learning techniques to proactively identify vulnerabilities and mitigate emerging threats with minimal latency and overhead. *Wireless Network Security* [2] refers to the set of protocols, tools, and practices designed to protect wireless networks from unauthorized access, data theft, and other cyber threats by ensuring the confidentiality, integrity, and availability of data transmitted over wireless channels. *Adaptive Security Response* [3] is a dynamic defence mechanism that adjusts its actions based on the severity and type of detected threat. ZITA's response strategy includes

automated reconfiguration, selective encryption, and isolation of affected nodes to minimize impact. *Machine Learning* [4] in *Network Security* involves the application of algorithms that enable systems to learn from network traffic patterns and historical attack data, improving their ability to detect anomalies and predict future threats without explicit programming. *Encryption Methodology* [5] refers to the approach and algorithms used to encode data so that it remains confidential and inaccessible to unauthorized users. ZITA employs lightweight, context-aware encryption methods that balance security with processing efficiency in wireless environments.

## II. LITERATURE REVIEW

Qinghai Zhou, Liangyue Li and et al. [6] had proposed Adversarial Attacks on Multi-Network Mining: Problem Definition and Fast Solutions, address the problem of attacking multinet network mining through the way of deliberately perturbing the networks to alter the mining results. The key idea of the proposed method is effective and efficient influence functions on the Sylvester equation defined over the input networks, which plays a central and unifying role in various multi-network mining tasks. The proposed algorithms bear three main advantages, including (1) effectiveness, being able to accurately quantify the rate of change of the mining results in response to attacks; (2) efficiency, scaling linearly with more than 100 speed-ups over the straightforward implementation without any quality loss; and (3) generality, being applicable to a variety of multi-network mining tasks with different attacking strategies.

Jakub Breier, Xiaolu Hou and et al. [7] had proposed FooBaR: Fault Fooling Backdoor Attack on Neural Network Training Neural network implementations are known to be vulnerable to physical attack vectors such as fault injection attacks. In this work, explore a novel attack paradigm by injecting faults during the training phase of a neural network in a way that the resulting network can be attacked during deployment without the necessity of further faulting. Such malicious inputs are obtained by mathematically solving a system of linear equations that would cause a particular behaviour on the attacked activation functions, similar to the one induced in training through faulting.

Zakaria Abou El Houda, Abdelhakim Senhaji Hafid, and et al.,[8] had proposed MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning Using SDN and Blockchain. Distributed denial-of-service (DDoS) attacks

continue to grow at a rapid rate plaguing Internet Service Providers (ISPs) and individuals in a stealthy way. In particular, MiTFed consists of: (1) a novel distributed architecture that allows multiple SDN based domains to securely collaborate in order to cope with sophisticated security threats while preserving the privacy of each SDN domain; (2) a novel Secure Multiparty Computation (SMPC) scheme to securely aggregate local model updates; and (3) a blockchain based scheme that uses Ethereum smart contracts to maintain the collaboration in a fully decentralized, trustworthy, flexible, and efficient manner.

**Dr. G. Umarani Srikanth [9]** had proposed Prediction of Network Attacks Using Machine Learning Techniques. The networked systems become more and more pervasive and businesses still acquire a lot of sensitive data online, so that the quantity and class of cyber-attacks and network security breaches has risen dramatically. There are also instances that so many volumes of data are hacked even without the knowledge of the people concerned. So far setting an Intrusion Detection System (IDS), it is obvious to set the true working environment to model the possibilities of attacks the objective of this work is to investigate machine learning based algorithms for enhancing packet connection transfers forecasting using ensemble learning voting classifier techniques. It is proposed to deploy AI-based technique to precisely anticipate the DOS, R2L, U2R, Probe and large assaults. Results showed that the viability of the proposed AI calculation strategy can be contrasted and the best exactness with accuracy, Recall and F1 Score.

**Jin yin Chen, Jian Zhang, and et al., [10]** had proposed Time-Aware Gradient Attack on Dynamic Network Link Prediction. In network link prediction, it is possible to hide a target link from being predicted with a small perturbation on network structure. There have been many recent studies to generate adversarial examples to mislead deep learning models on graph data. However, none of the previous work has considered the dynamic nature of real-world systems. In this work, we present the first study of adversarial attack on dynamic network link prediction (DNLP). The proposed attack method, namely time-aware gradient attack (TGA), utilizes the gradient information generated by deep dynamic network embedding (DDNE) across different snapshots to rewire a few links, so as to make DDNE fail to predict target links.

### III. PROPOSED METHODOLOGY

**Data Collection:** When collecting data to make predictions, we split it into two parts: the Training set & the Test set. Usually, we use a 7:3 ratio. This means that 70% is for Training & 30% is for Testing. We build the Data Model using methods like Random Forest, logistic regression, Decision Trees, and Support Vector Classifier (SVC). After training on the Training set, we check the accuracy of our model with the Test set.

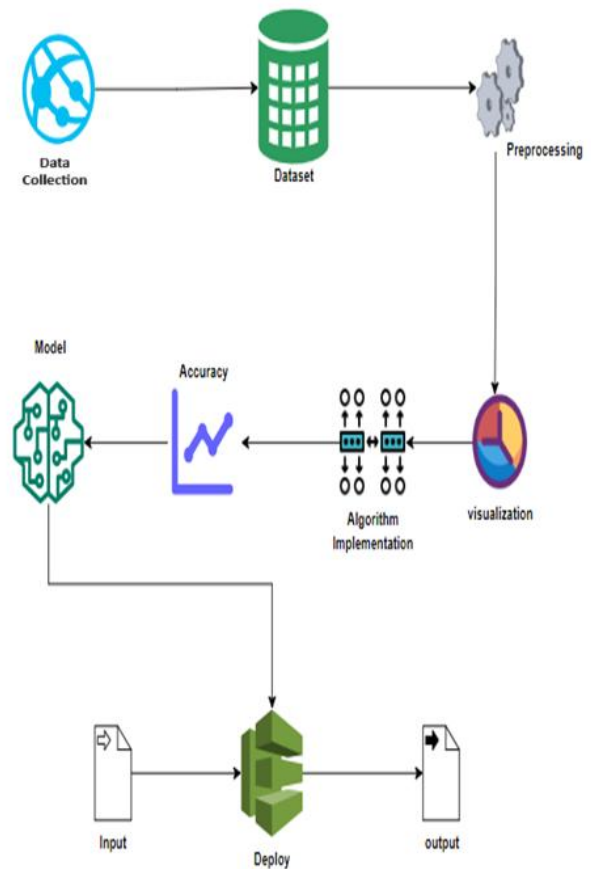
**Data Pre-processing:** Data preprocessing is a crucial step in the data analysis and machine learning process. It involves transforming raw data into a clean and organized format to ensure better performance of models and accurate results. Real-world data is often incomplete, inconsistent, or contains

errors and noise. Preprocessing helps correct these issues so that data becomes suitable for further analysis.

**Complement Naïve Bayes:** This is a type of Naïve Bayes algorithm made for when you have unbalanced datasets. It helps improve accuracy in classifying by changing how we calculate probabilities. This is really helpful for text classification & spotting rare events.

**Adaboost Classifier:** Adaboost is a boosting method that brings together several weak classifiers to make one strong classifier. It pays more attention to hard cases by adjusting weights, which helps make the model more accurate.

**Extra Tree Classifier:** This algorithm works like Random Forest but brings in more randomness when choosing features and splits. This can make it quicker and sometimes gives better accuracy with big datasets.



### SYSTEM ARCHITECTURE

*Fig -1: Flowchart*

This image represents a flowchart outlining the process of implementing AI for enhancing cyber network threat security. Below is a detailed explanation of each component in the diagram:

#### 1. Data Processing:

- **Data-Preprocessing using Numpy and Pandas:**
  - **Numpy:** Used for numerical computations, handling arrays, and mathematical operations.

- **Pandas:** Used for data manipulation, cleaning, and structuring the dataset.

## 2. Data Visualization:

- **Matplotlib & Seaborn:** These Python libraries are used for creating graphs and visualizations to analyze network attack patterns.

## 3. Model Building:

- The model is trained using three different machine learning algorithms:
  - **Complement Naïve Bayes**
  - **Adaboost Classifier**
  - **Extra Tree Classifier**
- The models are trained and compared to determine which one provides the best accuracy.
- The final model is saved in. **pkl format** (Pickle format) for deployment.

## 4. Integration of Model with Web App:

- The trained AI model is connected to the web application.
- Users interact with the web app through various pages:
  - **Landing Page**
  - **Register Page**
  - **Login Page**
  - **Home Page**
  - **Input Page (for attack data)**
  - **Wireless Networks Attack Prediction Page (shows model predictions)**

## IV. FINDINGS

In the study of wireless network attacks using machine learning, we began with thorough data preprocessing to ensure data quality and relevance, which included handling missing values, normalizing features, and encoding categorical variables. Data visualization techniques were employed to uncover patterns and insights, revealing the distinct characteristics of various attack types. We then compared the performance of three different algorithms assessing their accuracy, precision, and recall metrics. The Random Forest algorithm consistently outperformed the others, demonstrating superior robustness and reliability in attack classification. Finally, **ETC (Extra Trees Classifier)** achieved the **highest accuracy at 99.90%**. This model is likely leveraging ensemble learning with a forest of randomized decision trees, which often results in high performance, especially with well-pre-processed data.

Enhancing threat detection by integrating advanced machine learning algorithms to improve accuracy and reduce false positives in wireless network security systems. Developing adaptive models that can learn from evolving attack patterns and dynamically update defences to mitigate emerging wireless network threats.

## 1.Naive Bayes Classifier

### • Description:

This model is a variant of the Naive Bayes classifier, designed to handle imbalanced datasets better. CNB is particularly effective for text classification tasks and works by calculating the probability of each class using the complement of the actual class data, improving accuracy over standard Multinomial Naive Bayes in many cases.

### • Output:

**Accuracy:** 71.81815443922419

The Classification Report of ComplementNB				
	Precision	recall	F1-score	support
<b>0</b>	0.56	0.53	0.55	66408
<b>1</b>	0.85	0.90	0.87	66408
<b>2</b>	0.55	0.47	0.51	66408
<b>3</b>	0.93	0.86	0.90	66408
<b>4</b>	0.67	0.83	0.74	66408
<b>Accuracy</b>			0.72	332040
<b>Macro average</b>	0.72	0.72	0.71	332040
<b>Weighted average</b>	0.72	0.72	0.71	332040

*Table:4.1*

## 2. AdaBoost Classifier

### • Description:

This module uses an adaptive classification approach, where weak learners (like decision stumps) are combined and adjusted based on performance on misclassified data. Adaptive classifiers improve learning by focusing more on difficult examples over iterations.

### • Output:

**Accuracy:** 91.31098662811709

The Classification Report of AdaBoost Classifier				
	Precision	recall	F1-score	support

0	0.75	1.00	0.86	66408
1	1.00	0.99	1.00	66408
2	0.96	0.67	0.79	66408
3	0.93	0.97	0.95	66408
4	1.00	0.93	0.96	66408
Accuracy			0.91	324086
Macro average	0.93	0.91	0.91	324086
Weighted average	0.93	0.91	0.91	324086

Table:4.2

average				
---------	--	--	--	--

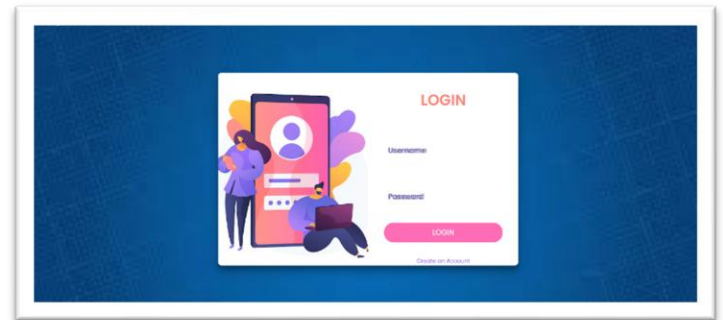


Table:4.3

### 3. Extra Trees Classifier

- Description:**

This is an ensemble learning method that builds multiple unpruned decision trees and aggregates their results. Unlike Random Forests, Extra Trees introduces more randomness by splitting nodes using randomly selected cut-points, which often results in faster training and robust generalization.

- Output:**

**Accuracy:** 99.8978666156514

#### Highest Accuracy Module:

- Extra Trees Classifier with **99.90%**.

The Classification Report of Extratree Classifier				
	Precision	recall	F1-score	support
0	1.00	1.00	1.00	64817
1	1.00	1.00	1.00	64817
2	1.00	1.00	1.00	64817
3	1.00	1.00	1.00	64817
4	1.00	1.00	1.00	64817
Accuracy			1.00	324086
Macro average	1.00	1.00	1.00	324086
Weighted	1.00	1.00	1.00	324086

#### LOGIN PAGE

Fig 4.1 - Login Page

#### REGISTER PAGE

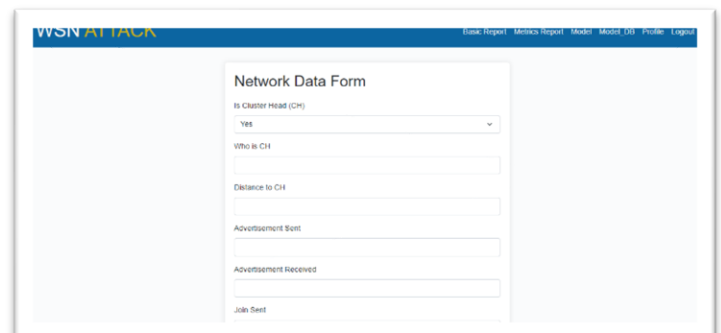



Fig 4.2 - Register Page

#### MODEL PAGE:



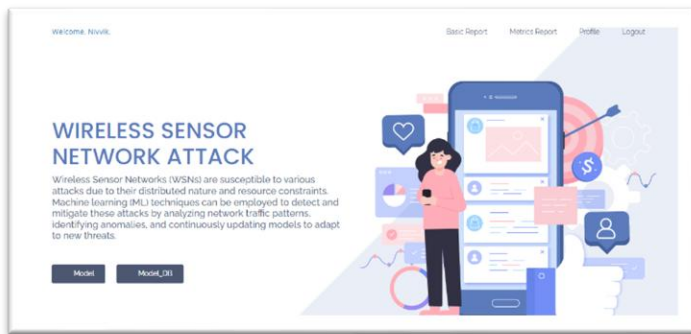


Fig 4.3 – Data input Page

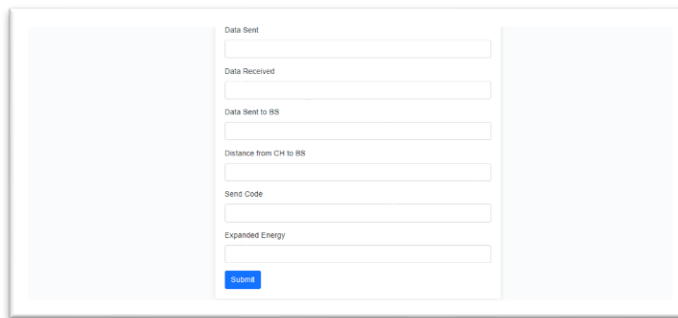


Fig 4.4 – Data input Page

## HOME PAGE

Fig 4.5 -Result page

## V. ACKNOWLEDGEMENTS

I want to sincerely thank everyone who helped us finish this study project. We would first and foremost like to express our sincere gratitude to Dr. M.G.R. Educational and Research Institute in Chennai for giving us the academic setting and facilities we needed to complete this project.

I am incredibly grateful to Mr. Sankara Narayanan S T, Assistant Professor at the Centre of Excellence in Digital Forensics, for her excellent advice, unwavering support, and perceptive criticism during the study. Her knowledge and guidance were very helpful in determining the focus and Caliber of this job. I would also like to express our gratitude to our peers and colleagues who have offered helpful advice and encouragement along our trip. We are very grateful to the Department of Computer Science Engineering faculty for their support and academic guidance.

## VI. CONCLUSION

In the study of wireless network attacks using machine learning, we began with thorough data preprocessing to ensure data quality and relevance, which included handling missing values, normalizing features, and encoding categorical variables. Data visualization techniques were employed to uncover patterns and insights, revealing the distinct characteristics of various attack types. We then compared the performance of three different algorithms assessing their accuracy, precision, and recall metrics. The Random Forest

algorithm consistently outperformed the others, demonstrating superior robustness and reliability in attack classification. Finally, we integrated our machine learning model with the Django framework, allowing for seamless deployment and monitoring of network security, thus providing an effective solution for detecting and mitigating wireless network attacks.

## II. REFERENCE

1. N. Ghose, "ZITA: Zero-Interaction Two-Factor Authentication using Contact," *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 1-14, Apr. 2023. [Online]. Available: [https://cse.unl.edu/~nghose/pubs/journal/GHOSE\\_TMC\\_2023-main.pdf](https://cse.unl.edu/~nghose/pubs/journal/GHOSE_TMC_2023-main.pdf)School of Computing+1ACM Digital Library+1
2. N. Ghose, "ZITA: Zero-Interaction Two-Factor Authentication Using Contact," *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 1-14, Apr. 2023. [Online]. Available: <https://dl.acm.org/doi/abs/10.1109/TMC.2023.3321514>ACM Digital Library+1School of Computing+1
3. A. Baig, "12 Best Practices for Wireless Network Security," *GlobalSign Blog*, Jun. 2022. [Online]. Available: <https://www.globalsign.com/en/blog/12-best-practices-wireless-network-security>GlobalSign
4. Kaspersky, "How to Improve your Wireless Network Security," *Kaspersky Resource Center*, 2017. [Online]. Available: <https://www.kaspersky.com/resource-center/preemptive-safety/wireless-network-security-simple-tips>Kaspersky
5. eSecurity Planet, "Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained," *eSecurity Planet*, May 2023. [Online]. Available: <https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks/eSecurityPlanet+1Informa TechTarget+1>
6. Cloudi-Fi, "Zero Trust Wi-Fi: The Ultimate Guide to Securing Your Wireless Network," *Cloudi-Fi Blog*, Sep. 2023. [Online]. Available: <https://www.cloudifi.com/blog/zero-trust-wifi-security-guide>Cloudi-Fi - Unleash your connectivity+1Cloudi-Fi - Unleash your connectivity+1
7. NetAlly, "Best Practices in Wireless Access Point Security," *NetAlly CyberScope Blog*, Jul. 2023. [Online]. Available: <https://cyberscope.netally.com/blog/best-practices-in-wireless-access-point-security>NetAlly CyberScope
8. CISA, "Securing Wireless Networks," *Cybersecurity and Infrastructure Security Agency*, Dec. 2020. [Online]. Available: <https://www.cisa.gov/news-events/news/securing-wireless-networks>CISA
9. ITSecurityWire, "Emerging Trends and Technologies in Wi-Fi Security," *ITSecurityWire*, Jan. 2023. [Online]. Available: <https://itsecuritywire.com/featured/emerging-trends-and-technologies-in-wi-fi-security/>ITSecurityWire
10. Wi-Fi Alliance, "Protected Management Frames Enhance Wi-Fi® Network Security," *Wi-Fi Alliance*,

- [Online]. Available: <https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security>  
[Wi-Fi Alliance](#)
11. TechTarget, "Wireless Security: WEP, WPA, WPA2 and WPA3 Differences," *TechTarget*, Jan. 2023. [Online]. Available: <https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2Lifewire+2Informa>  
[TechTarget+2eSecurity Planet+2](#)
  12. Portnox, "10 Strategies for Boosting Your Wireless Network Security," *Portnox Blog*, Jan. 2023. [Online]. Available: <https://www.portnox.com/blog/security-trends/10-strategies-for-boosting-your-wireless-network-security/Portnox>
  13. Keepnet Labs, "Privacy in Wireless Networks," *Keepnet Labs Blog*, Jan. 2023. [Online]. Available: <https://keepnetlabs.com/blog/privacy-in-wireless-networksKeepnet Labs>
  14. New York State, "802.11 Wireless Network Security Standard," *New York State Information Technology Standard*, Mar. 2025. [Online]. Available: <https://its.ny.gov/80211-wireless-network-securityIT Services>
  15. Ruckus Networks, "Wi-Fi 7 and Security: What You Need to Know," *Ruckus Networks Blog*, Oct. 2023. [Online]. Available: <https://www.ruckusnetworks.com/blog/2023/wi-fi-7-and-security-what-you-need-to-know/Ruckus Networks>
  16. L. G. Pedroza Renteria, "Enhancing Wireless Network Security," *LinkedIn*, Feb. 2023. [Online]. Available: <https://www.linkedin.com/pulse/enhancing-wireless-network-security-leonel-giovanny-pedroza-renteria-egxhcLinkedIn>
  17. Zenarmor, "What are the Ways to Improve Network Security?" *Zenarmor Documentation*, Oct. 2023. [Online]. Available: <https://www.zenarmor.com/docs/network-security-tutorials/what-are-ways-to-improve-network-securityZenarmor>
  18. S. A. Hoseini et al., "Cooperative Jamming for Physical Layer Security Enhancement Using Deep Reinforcement Learning," *arXiv preprint arXiv:2403.10342*, Mar. 2024. [Online]. Available: <https://arxiv.org/abs/2403.10342arxiv.org>
  19. Y. E. Sagduyu et al., "When Wireless Security Meets Machine Learning: Motivation, Challenges, and Research Directions," *arXiv preprint arXiv:2001.08883*, Jan. 2020. [Online]. Available: <https://arxiv.org/abs/2001.08883arxiv.org>
  20. R. Fotuhi et al., "Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol," *arXiv preprint arXiv:2001.06077*, Jan. 2020. [Online]. Available: <https://arxiv.org/abs/2001.06077arxiv.org>