Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

Journal of Nonlinear Analysis and Optimization : Theory & Applications

Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng

Adaptive Machine Learning Models for Intrusion Detection in Wireless Sensor Networks

Mr.K. UDAY KIRAN[1] SHAIK THASLEEMA BEGUM[2]

#1 Assistant Professor Department of Master of Computer Applications
#2 Pursuing M.C.A   QIS COLLEGE OF ENGINEERING & TECHNOLOGY
Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

ABSTRACT

Wireless Sensor Networks (WSNs) have become integral to modern technology, supporting a range of monitoring applications but are highly susceptible to security threats such as unauthorized access, attacks, and other malicious activities. Such vulnerabilities can compromise WSNs' reliability, necessitating the implementation of Intrusion Detection Systems (IDS) for early detection and response. This study focuses on a machine learning-based IDS approach utilizing prominent datasets, including KDD Cup Data, NSL-KDD, UNSW-NB15, and AWID, to develop and evaluate robust detection models. The algorithms employed in this study include Logistic Regression, a tuned Logistic Regression (C=10), Convolutional Neural Network (CNN), Deep Neural Networks (DNN) with three and four layers, Long Short-Term Memory (LSTM), and hybrid methods like CNN + LSTM. Ensemble approaches, such as Majority Voting (LR + LR) and a Stacking Classifier (Bagging with Random Forest and Boosted Decision Tree with LightGBM), were also applied. Among these, the Stacking Classifier achieved 100% accuracy, highlighting its effectiveness in accurately detecting intrusions. This approach demonstrates a promising solution for securing WSNs by reducing false alarms and enhancing detection accuracy.

Index terms: Wireless Sensor Networks (WSNs), Intrusion Detection System (IDS), Adaptive Machine Learning, Anomaly Detection, Network Security

INTRODUCTION

The Wireless Sensor Network (WSN) serves as a primary source for communication inside the wireless base network domain. Wireless Sensor Networks (WSNs) use sensor nodes that connect via various topologies, including star, tree, or mesh. These nodes provide data flow and transmission inside the wireless network, with primary capabilities including sensing, processing, computing, and communication. Wireless Sensor Networks (WSNs) are used for monitoring, safeguarding, and tracking, offering a cost-efficient platform that utilises little energy resources for wireless network transmission. Wireless Sensor Networks (WSNs) are susceptible to unauthorised access by intruders, both internal and external; thus, robust procedures are implemented to safeguard sensor nodes and maintain network security. WiFi-based sensors are widely available on wireless networks and infrastructure, with their data accessible globally over TCP/IP via PCs or cellphones. Repeaters may be included as access points when the sensor is beyond the range of the Wi-Fi access point. Sensors may connect to a network by acquiring the SSID and password, and can thereafter transmit data to the server via a URL or IP address.

LITERATURE SURVEY

2.1 Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks:

https://link.springer.com/article/10.1007/s11276-023-03470-x

ABSTRACT: Underwater Wireless Sensor Networks (UWSNs) are the type of WSNs that transmit the data through water medium and monitor the oceanic conditions, water contents, under-sea habitations, underwater beings and military objects. Unlike air medium, water channel creates stronger communication barriers. In addition, the malicious data injection and other network attacks create security problems during data communication. Protecting the vulnerable UWSN channel is not an easy task under critical water conditions. Many research works proposed in the literature used cryptography principles and intelligent intrusion detection systems to secure the network activities from malicious nodes. However, the need for Machine Learning (ML) and Deep Learning (DL) associated Medium Access Control (MAC) principles is expected for handling the barriers in uncertain UWSN. In this regard, this article proposes a new Intrusion detection system with Integrated Secure MAC principles and Long Short-Term Memory (LSTM) architectures for organizing real-time neighbor monitoring tasks. The proposed system implements Generative Adversarial Network (GAN) driven UWSN channel assessment models and Secure LSTM-MAC principles to protect the data communication. In this regard, the proposed model creates the Intrusion Detection System (IDS) using trained distributed agents. These agents run in each legitimate sensor node contain novel LSTM-MAC engine, intrusion dataset, rule-based monitoring techniques, Secure Hashing Algorithm-3 (SHA-3), Two Fish algorithm and packet filtering tools. The proposed LSTM and agent-based model drives adaptive MAC channel operations to avoid malicious traffics in to legitimate nodes. In addition, this work implements neighbor-based packet monitoring, signal jamming and alert messaging procedures to build reliable security services against different types of attacks. The experiments and the observations reveal the performance of proposed techniques is proved to be 5% to 10% higher than existing techniques in various aspects measured with different metrics.

2.2 Hybrid Strategy Improved Sparrow Search Algorithm in the Field of Intrusion Detection:

https://ieeexplore.ieee.org/abstract/document/10077390

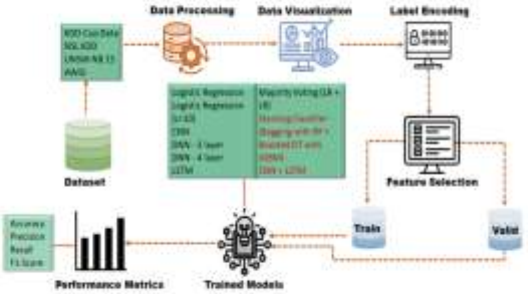
ABSTRACT: Aiming at the problem that Sparrow Search Algorithm(SSA) may fall into local optima and have slow convergence speed, a hybrid strategy improved sparrow search algorithm(HSISSA) is proposed in this paper, and it is applied to feature selection and model optimization of intrusion detection. First, a hybrid circle-piecewise map is proposed to initialize the population and improve the uniformity of the initial population distribution; second, merging the spiral search method in the vulture search algorithm and Levy's flight formula to update the positions of the discoverer and scouter, respectively, to expand the population search range and enhance the search capability; and finally, the simplex method and pinhole imaging method are used to optimize the position of sparrows with poor fitness and optimal fitness, to avoid stagnation in the population search and fall into local optima. The performance of the algorithm was optimized using the aforementioned methods. The algorithm was tested on 10 classical benchmark functions and combined with Wilcoxon rank-sum test analysis to verify its effectiveness, which showed improvements in convergence speed and accuracy. Finally, it was applied to the feature selection and model optimization of intrusion detection. On average, 7.6 features and 10.1 features were retained on the CIC-IDS2017 and UNSW-NB15 datasets, respectively, and 99.5% and 96.01% accuracies were achieved. The number and accuracy of the optimized features were better than those of the original algorithm. For the DenseNet and random forest models, HSISSA achieved 99.34% and 97.22% accuracy after optimization, respectively, which improved the performance of the models. Thus, the algorithm showed a better performance than the other algorithms.

2.3 A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks:

https://www.sciencedirect.com/science/article/abs/pii/S0957417422016451

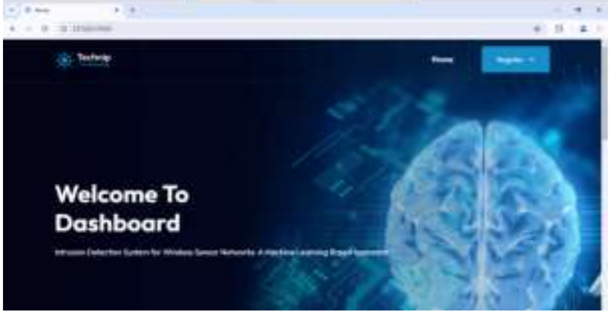
ABSTRACT: Wireless Sensor Networks (WSNs) is a promising technology with enormous applications in almost every walk of life. One of the crucial applications of WSNs is intrusion detection and surveillance at border areas and in the defence establishments. The border areas are stretched over hundreds to thousands of miles, hence, it is not possible to patrol the entire border region. As a result, an enemy may enter from any point absence of surveillance and cause the loss of lives or destroy the military establishments. WSNs can be a feasible solution for the problem of intrusion detection and surveillance at the border areas. Detection of an enemy at the border areas and nearby critical areas such as military cantonments is a time-sensitive task as a delay of a few seconds may have disastrous consequences. Therefore, it becomes imperative to design systems that can identify and detect the enemy as soon as it comes within the range of the deployed system. In this paper, we have proposed a deep learning architecture based on a fully connected feed-forward Artificial Neural Network (ANN) for the accurate prediction of the number of k-barriers for fast intrusion detection and prevention. We have trained and evaluated the feed-forward ANN model using four potential features, namely area of the circular region, sensing range of sensors, transmission range of sensors, and number of sensor for Gaussian and uniform sensor distribution. These features are extracted through Monte Carlo simulation. In doing so, we found that the model accurately predicts the number of k-barriers for both Gaussian and uniform sensor distribution with correlation coefficient (R = 0.78) and Root Mean Square Error (RMSE = 41.15) for the former and R = 0.79 and RMSE = 48.36 for the latter. Further, the proposed approach outperforms the other benchmark algorithms in terms of accuracy and computational time complexity.

System Architecture:

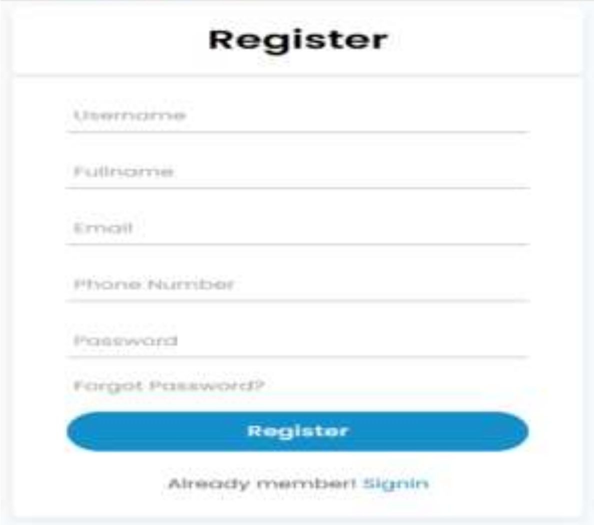


IMPLEMENTATION:

Dashboard - user Interface



Step 6


Register

Username

Fullname

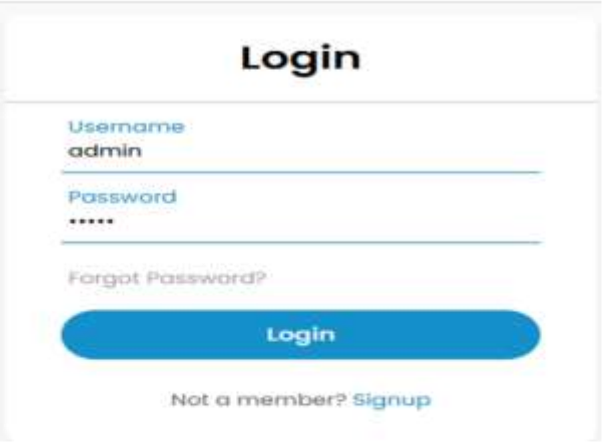
Email

Phone Number

Password

Forgot Password?

Step 7

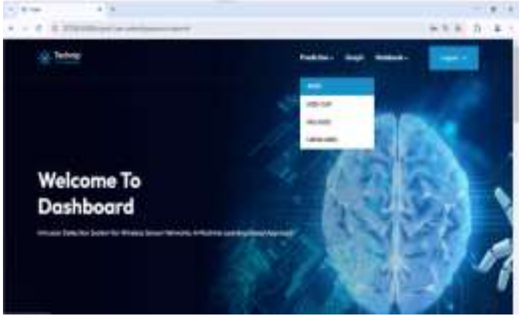

Login

Username
admin

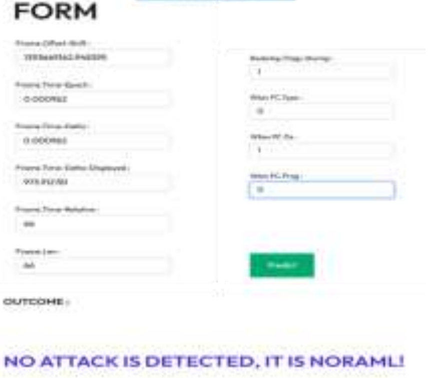
Password
•••••

Forgot Password?

Step 8



Step 9
Test case 1


FORM

Frame.Offset.Shift : [illegible]

Frame.Time.Epoch : [illegible]

Frame.Time.Delta : [illegible]

Frame.Time.Delta.Displayed : [illegible]

Frame.Time.Relative : [illegible]

Frame.Len : [illegible]

[illegible] : 1

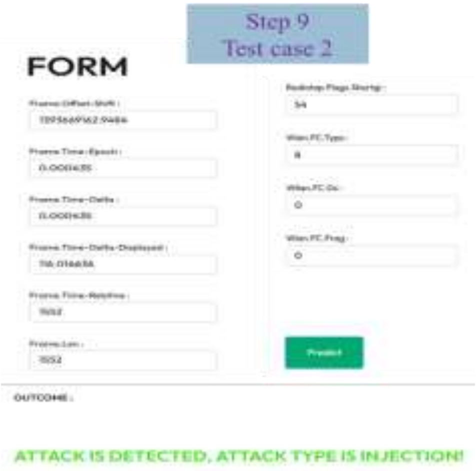
Wlan.FC.Type : 0

Wlan.FC.Ds : 1

Wlan.FC.Frag : 0

OUTCOME :

NO ATTACK IS DETECTED, IT IS NORAML!



Step 9
Test case 2

FORM

Frame-Offset-Shift :
1695669162.9484

Frame-Time-Epoch :
0.000435

Frame-Time-Delta :
0.000435

Frame-Time-Delta-Displayed :
116.016658

Frame-Time-Relative :
1552

Frame-Len :
1552

Radiotap-Flags-Shortgi :
54

Wlan-FC-Type :
8

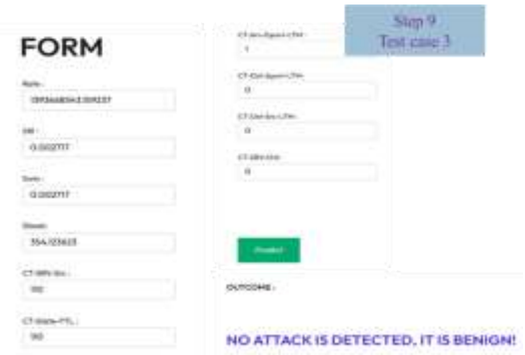
Wlan-FC-Ds :
0

Wlan-FC-Frag :
0

Predict

OUTCOME :

ATTACK IS DETECTED, ATTACK TYPE IS INJECTION!



Step 9
Test case 3

FORM

Rate :
1593668942.309237

Dur :
0.002717

Sinpkt :
0.002717

Sload :
354.123623

CT-SRV-Src :
90

CT-State-TTL :
90

CT-Src-Dport-LTM :
1

CT-Dst-Sport-LTM :
0

CT-Dst-Src-LTM :
0

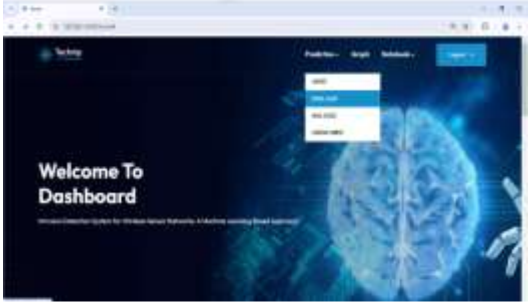
CT-SRV-Dst :
0

Predict

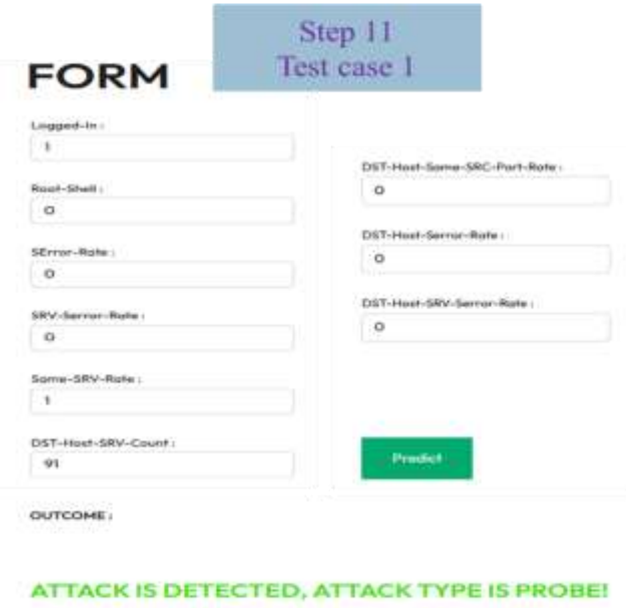
OUTCOME :

NO ATTACK IS DETECTED, IT IS BENIGN!

Step 10



Welcome To Dashboard



Step 11
Test case 1

FORM

Logged-In :
1

Root-Shell :
0

SError-Rate :
0

SRV-Serror-Rate :
0

Same-SRV-Rate :
1

DST-Host-SRV-Count :
91

DST-Host-Same-SRC-Port-Rate :
0

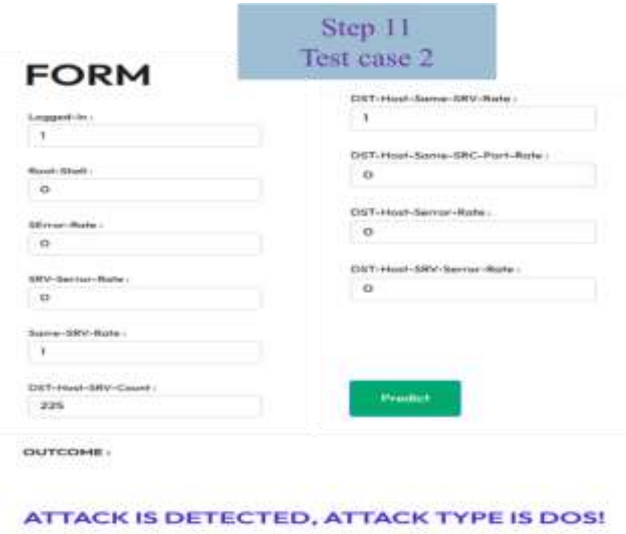
DST-Host-Serror-Rate :
0

DST-Host-SRV-Serror-Rate :
0

Predict

OUTCOME :

ATTACK IS DETECTED, ATTACK TYPE IS PROBE!



Step 11
Test case 2

FORM

Logged-In :
1

Root-Shell :
0

SError-Rate :
0

SRV-Serror-Rate :
0

Same-SRV-Rate :
1

DST-Host-SRV-Count :
225

DST-Host-Same-SRV-Rate :
1

DST-Host-Same-SRC-Port-Rate :
0

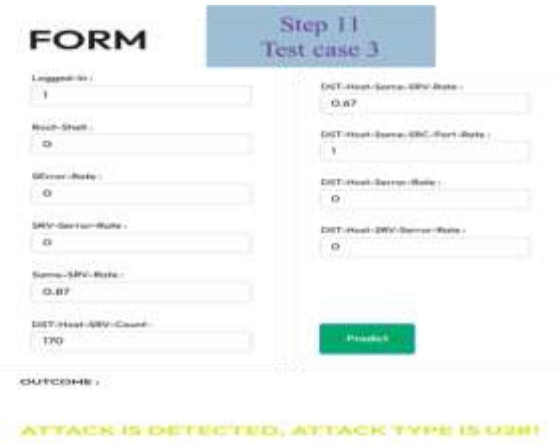
DST-Host-Serror-Rate :
0

DST-Host-SRV-Serror-Rate :
0

Predict

OUTCOME :

ATTACK IS DETECTED, ATTACK TYPE IS DOS!



Step 11
Test case 3

FORM

Logged-In :
1

Root-Shell :
0

SError-Rate :
0

SRV-Serror-Rate :
0

Same-SRV-Rate :
0.87

DST-Host-SRV-Count :
170

DST-Host-Same-SRV-Rate :
0.67

DST-Host-Same-SRC-Port-Rate :
1

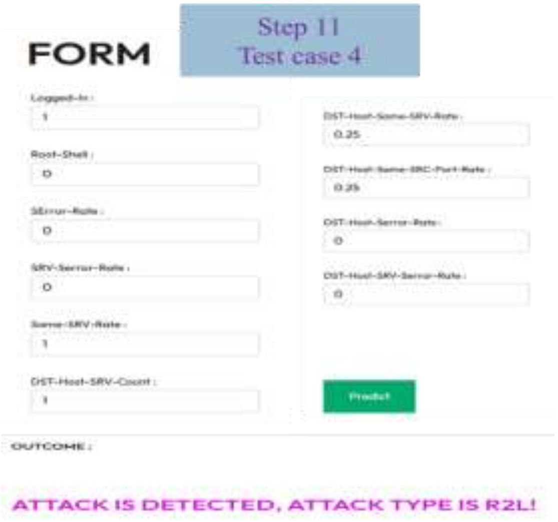
DST-Host-Serror-Rate :
0

DST-Host-SRV-Serror-Rate :
0

Predict

OUTCOME :

ATTACK IS DETECTED, ATTACK TYPE IS U2R!



Step 11
Test case 4

FORM

Logged-In : 1

Root-Shell : 0

SError-Rate : 0

SRV-Serror-Rate : 0

Same-SRV-Rate : 1

DST-Host-SRV-Count : 1

DST-Host-Same-SRV-Rate : 0.25

DST-Host-Same-SRC-Port-Rate : 0.25

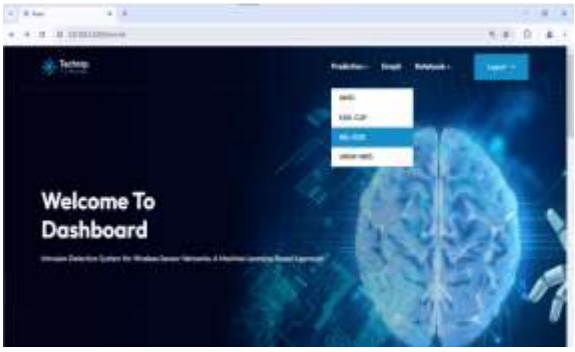
DST-Host-Serror-Rate : 0

DST-Host-SRV-Serror-Rate : 0

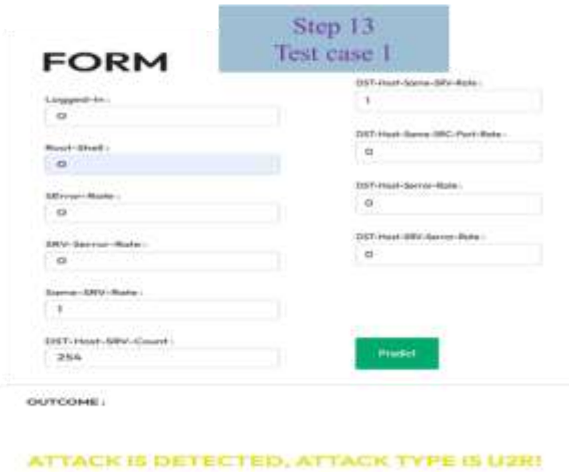
OUTCOME :

ATTACK IS DETECTED, ATTACK TYPE IS R2L!

Step 12



Welcome To Dashboard



Step 13
Test case 1

FORM

Logged-In : 0

Root-Shell : 0

SError-Rate : 0

SRV-Serror-Rate : 0

Same-SRV-Rate : 1

DST-Host-SRV-Count : 254

DST-Host-Same-SRV-Rate : 1

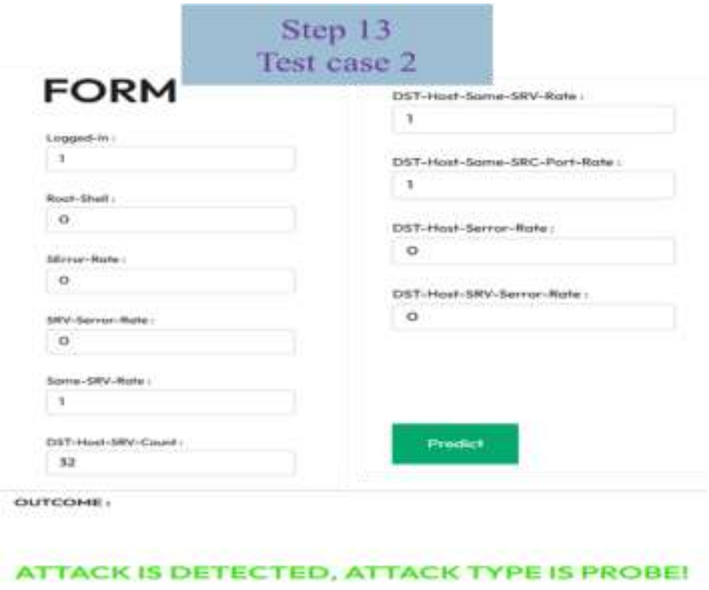
DST-Host-Same-SRC-Port-Rate : 0

DST-Host-Serror-Rate : 0

DST-Host-SRV-Serror-Rate : 0

OUTCOME :

ATTACK IS DETECTED, ATTACK TYPE IS U2R!



Step 13
Test case 2

FORM

Logged-In : 1

Root-Shell : 0

SError-Rate : 0

SRV-Serror-Rate : 0

Same-SRV-Rate : 1

DST-Host-SRV-Count : 32

DST-Host-Same-SRV-Rate : 1

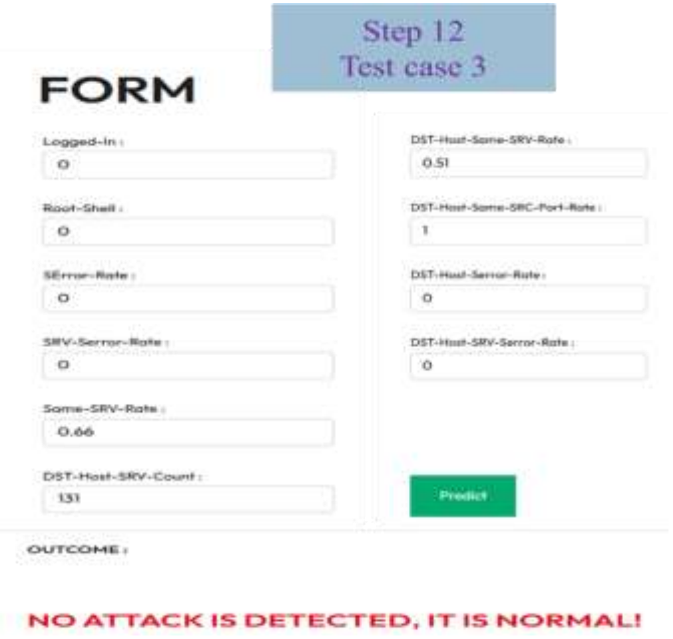
DST-Host-Same-SRC-Port-Rate : 1

DST-Host-Serror-Rate : 0

DST-Host-SRV-Serror-Rate : 0

OUTCOME :

ATTACK IS DETECTED, ATTACK TYPE IS PROBE!



Step 12
Test case 3

FORM

Logged-In : 0

Root-Shell : 0

SError-Rate : 0

SRV-Serror-Rate : 0

Same-SRV-Rate : 0.66

DST-Host-SRV-Count : 131

DST-Host-Same-SRV-Rate : 0.51

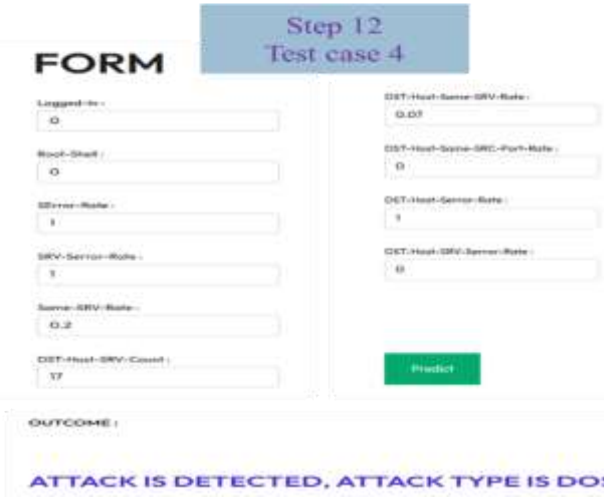
DST-Host-Same-SRC-Port-Rate : 1

DST-Host-Serror-Rate : 0

DST-Host-SRV-Serror-Rate : 0

OUTCOME :

NO ATTACK IS DETECTED, IT IS NORMAL!



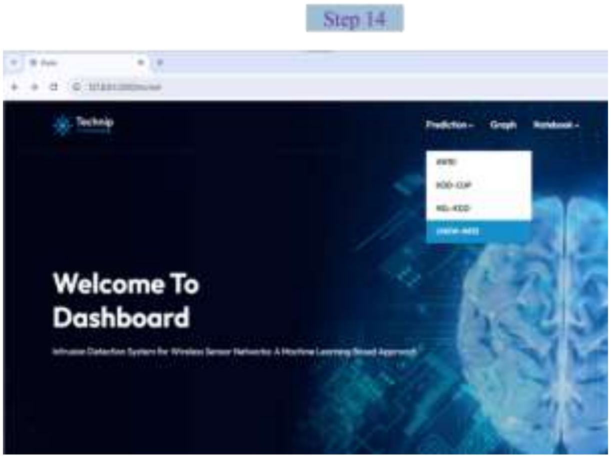
Step 12
Test case 4

FORM

Logged-In : 0
Root-Shell : 0
SError-Rate : 1
SRV-Serror-Rate : 1
Same-SRV-Rate : 0.2
DST-Host-SRV-Count : 17
DST-Host-Same-SRV-Rate : 0.07
DST-Host-Same-SRC-Port-Rate : 0
DST-Host-Serror-Rate : 1
DST-Host-SRV-Serror-Rate : 0

OUTCOME :

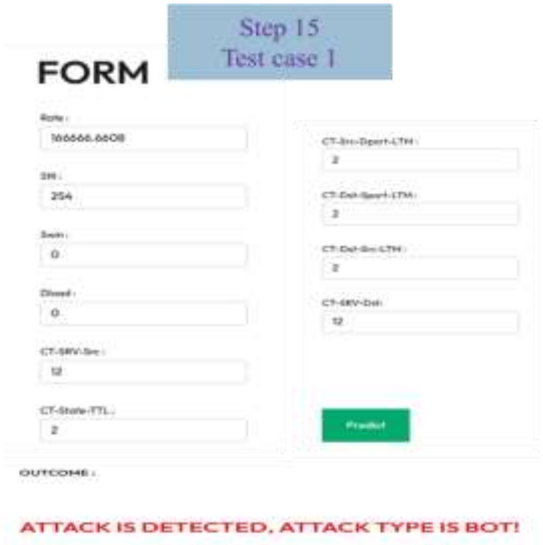
ATTACK IS DETECTED, ATTACK TYPE IS DO



Step 14

Welcome To Dashboard

Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach



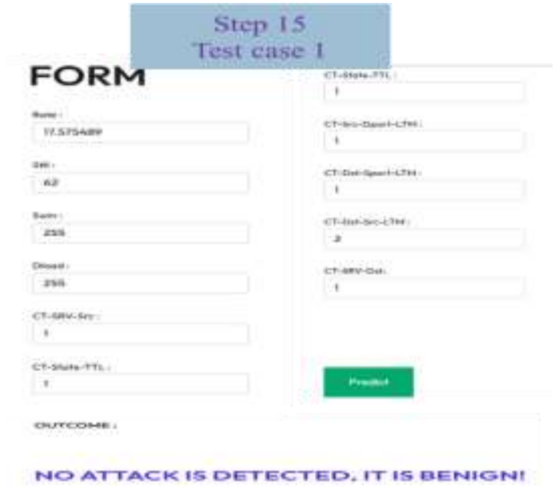
Step 15
Test case 1

FORM

Rate : 166666.6608
Sttl : 254
Swin : 0
Dload : 0
CT-SRV-Src : 12
CT-State-TTL : 2
CT-Src-Dport-LTM : 2
CT-Dst-Sport-LTM : 2
CT-Dst-Src-LTM : 2
CT-SRV-Dst : 12

OUTCOME :

ATTACK IS DETECTED, ATTACK TYPE IS BOT!



Step 15
Test case 1

FORM

Rate : 17.575489
Sttl : 62
Swin : 255
Dload : 255
CT-SRV-Src : 1
CT-State-TTL : 1
CT-State-TTL : 1
CT-Src-Dport-LTM : 1
CT-Dst-Sport-LTM : 1
CT-Dst-Src-LTM : 2
CT-SRV-Dst : 1

OUTCOME :

NO ATTACK IS DETECTED, IT IS BENIGN!

CONCLUSION

In conclusion, the machine learning-based Intrusion Detection System (IDS) for Wireless Sensor Networks (WSNs) successfully enhances security by identifying and mitigating potential threats with high accuracy. Given the vulnerabilities of WSNs to unauthorized access and various attacks, this IDS leverages multiple datasets—KDD Cup Data, NSL-KDD, UNSW-NB15, and AWID—to train robust models capable of detecting intrusions effectively. The system's use of diverse algorithms and ensemble techniques contributes to a comprehensive analysis of network traffic, identifying patterns that signal potential intrusions while reducing false alarm rates. Among the models tested, the Stacking Classifier, integrating Bagging with Random Forest and Boosted Decision Tree with LightGBM, achieved a standout performance, reaching 100% accuracy. This high level of precision underscores the IDS's potential for reliably securing WSNs in critical applications, from environmental monitoring to industrial control systems, where data integrity and network reliability are paramount. The IDS thus presents a strong solution to the evolving security challenges within WSNs.

Future work on this project can explore advanced techniques like federated learning to enhance privacy in distributed WSN environments, where data is processed locally on devices without centralized storage. Additionally, leveraging deep reinforcement learning could improve adaptive responses to new intrusion patterns, enabling more dynamic IDS configurations. Techniques like Explainable AI (XAI) could also be applied to make the IDS more interpretable, helping users understand detection results and refining model decisions for more efficient intrusion detection.

REFERENCES

[1] S. Rajasoundaran, S. V. N. S. Kumar, M. Selvi, K. Thangaramya, and K. Arputharaj, "Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks," Wireless Netw., vol. 30, no. 1, pp. 209–231, 2024.

[2] L. Tao and M. Xueqiang, "Hybrid strategy improved sparrow search algorithm in the field of intrusion detection," IEEE Access, vol. 11, pp. 32134–32151, 2023.

[3] A. Singh, J. Amutha, J. Nagar, and S. Sharma, "A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks," Expert Syst. Appl., vol. 211, 2023, Art. no. 118588

[4] S. B. Park, H. J. Jo, and D. H. Lee, "G-IDCS: Graph-based intrusion detection and classification system for CAN protocol," IEEE Access, vol. 11, pp. 39213–39227, 2023.

[5] R. Ramadan and K. Medhat, "Intrusion detection based learning in wireless sensor networks," PLOMS AI, vol. 2, no. 1, pp. 1–20, 2022.

[6] S. Mujeeb, T. A. Alghamdi, S. Ullah, A. Fatima, N. Javaid, and T. Saba, "Exploiting deep learning for wind power forecasting based on big data analytics," Appl. Sci., vol. 9, no. 20, p. 4417, Oct. 2019.

[7] S. M. Kasongo and Y. Sun, "A deep gated recurrent unit based model for wireless intrusion detection system," ICT Exp., vol. 7, no. 1, pp. 81–87, Mar. 2021.

[8] A. Wajahat, J. He, N. Zhu, T. Mahmood, A. Nazir, F. Ullah, S.

Qureshi, and S. Dev, "Securing Android IoT devices with GuardDroid transparent and lightweight malware detection," Ain Shams Eng. J., vol. 15, no. 5, May 2024, Art. no. 102642.

[9] E. K. Boahen, S. A. Frimpong, M. M. Ujakpa, R. N. A. Sosu, O. Larbi-Siaw, E. Owusu, J. K. Appati, and E. Acheampong, "A deep multi-architectural approach for online social network intrusion detection system," in Proc. IEEE World Conf. Appl. Intell. Comput. (AIC), Jul. 2022, pp. 919–924.

[10] T. Mahmood, J. Li, T. Saba, A. Rehman, and S. Ali, "Energy optimized data fusion approach for scalable wireless sensor network using deep learning-based scheme," J. Netw. Comput. Appl., vol. 224, Apr. 2024, Art. no. 103841.

[11] Z. Shaukat, A. A. Zulfiqar, C. Xiao, M. Azeem, and T. Mahmood, "Sentiment analysis on IMDB using lexicon and neural networks," Social Netw. Appl. Sci., vol. 2, no. 2, pp. 1–10, Feb. 2020.

[12] P. Satam and S. Hariri, "WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol," IEEE Trans. Netw. Service Manage., vol. 18, no. 1, pp. 1077–1091, Mar. 2021.

[13] T. Mahmood, J. Li, Y. Pei, F. Akhtar, S. A. Butt, A. Ditta, and S. Qureshi, "An intelligent fault detection approach based on reinforcement learning system in wireless sensor network," J. Supercomput., vol. 78, no. 3, pp. 3646–3675, Feb. 2022.

[14] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 184–208, 1st Quart., 2016.

AUTHORS

Mr. K. Uday Kiran is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Bapatla Engineering College, Bapatla. His research interests include Machine Learning Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.