A Super Learner Ensemble-based Intrusion Detection System to Mitigate Network Attacks

Ojo John Ajayi
Department of Cyber Security
National Open University Nigeria (ACETEL),
Abuja, Nigeria
aonejotech@gmail.com

Adesina Simon Sodiya
Department of Computer Science
Federal University of Agriculture,
Abeokuta, Nigeria
sinasodiya@gmail.com

Mustapha Aminu Bagiwa
Department of Computer Science
Ahmadu Bello University,
Zaria, Nigeria
mstphaminu@yahoo.com

Toluwase Ayobami Olowookere
Department of Computer Science
Redeemer's University,
Ede, Nigeria
olowookereta@run.edu.ng

2024 5th International Conference on Data Analytics for Business and Industry (ICDABI) | 979-8-3503-6871-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICDABI63787.2024.10800423

***Abstract*-Governments and corporate institutions are now mostly reliant on integrated digital infrastructures. These digital infrastructures are usually targets of cyber threats such as intrusion, for which intrusion detection systems (IDS) have emerged. One of the key needs for a robust IDS includes reducing the rate of false positives and thus improving accuracy. In this study, three traditional machine learning (ML) algorithms, including K-Nearest Neighbor (KNN), Naive Bayes (NB), and Decision Tree (DT), and three ensemble Machine Learning (ML) algorithms, including Random Forest (RF), Light Gradient Boosting Machine (LGBM), and Extreme Gradient Boosting (XGBOOST), were used on the UNSW-NB15 dataset from the Australian Centre for Cyber Security's Cyber Range Lab, to train intrusion detection models. A super-learner ensemble model was then built using the best two ensemble models (XGBOOST and RF) along with the best traditional model (KNN) as its base learners. The super-learner ensemble model was able to reduce false positives and improve detection accuracy with 98% accuracy. The model was then deployed in an IDS application to mitigate network attacks effectively and efficiently.**

Keywords- decision tree, ids, k-nearest neighbour, lgbm, machine learning, naïve bayes, random forest, super learning, and xgboost.

I. INTRODUCTION

Technology advancements have opened up previously unimaginable opportunities for people and businesses. Individuals and organizations mainly rely on fast-growing digital infrastructures that are intricately interconnected, because of the enormous quantities of information on computer systems and other information and communication technology (ICT) gadgets. Securing those quantities of information and ICT infrastructure for governments, individuals, and organizations is a major concern. Sensitive information, such as financial assets, personal information, and intellectual property, may have detrimental effects if there is unauthorized disclosure. Security rules and safeguards must be established to protect this data from unauthorized access or other breaches [1].

Cyberattacks and cybercrimes are becoming more frequent and intense, posing significant threats to a nation. To protect against these attacks, IDS monitors network security by detecting external intrusions and irregular server activity. IDS information is crucial for maintaining data integrity, privacy, and authenticity [2]. Monitoring activities within a network or computer system can help identify intrusions, which can undermine the security measures of a computer or network [3].

The agent module uses machine learning to identify potential attacks by analyzing large amounts of data. This data is then used to train ML algorithms, which can automatically identify and classify new attacks as they occur. This system can continuously learn and adapt to changing attack strategies, improving its ability to recognize new and previously unidentified threats. By identifying abnormalities in real time, this proactive defensive mechanism enables prompt reaction and mitigation of future security breaches, thereby enhancing the effectiveness of the IDS [4].

This paper is organized into six sections: section I is an introduction to the research, section II provides the related work of IDS, section III is the methodology of the study, section IV is the results and discussion discovered from the research, section V is the conclusion of the study.

II. RELATED WORK

In this section, a literature review of past research on machine learning in IDS is analyzed.

The increased threats of cyber incidents to organizations and the rise in the quantity of connected devices within enterprises are the two key causes driving the adoption of IDS/IPS from 2019 to 2025 [5]. As daily activities became more dependent on information sharing technologies, degrees of entry to these systems and unobstructed access to user activities became critical [6].

[7] explores the use of deep neural networks (DNNs) for identifying and classifying cyberattacks. DNNs are used to determine optimal network topologies and parameters using the KDDCup 99 dataset and hyperparameter selection methods. The model demonstrated good performance on KDDCup 99 and was used in various datasets, showing that DNNs outperform traditional ML models. The research suggests that using a distributed strategy to train complex DNN structures on advanced technology could improve performance.

[8] highlights the impact of the internet on social, political, and economic systems, removing geographical barriers and increasing the number of cybercriminals. They developed an

IDS lightweight based on a perceptron neural network with multiple layers and information gain to categorize attacks and traffic. The study tested an ANN-based IDS on the UNSW-NB15 dataset, using binarization discretization for continuous and ranking characteristics. The model achieved 76.96% accuracy and an MCC of 0.57, indicating a favorable correlation. The results suggest that the method is promising for real-time identification, and the UNSW-NB15 dataset is a useful network IDS dataset. However, the ensemble technique could have improved the detection rate in the study, which is shown in [9].

[10] emphasize the importance of Intelligent Distributed Systems (IDSs) in monitoring IoT network traffic flow. They argue that traditional IDS techniques, such as data mining and fuzzy methods, are inefficient due to their inability to select features correctly or utilize all dataset properties. To address this, a novel technique has been developed to determine the most advantageous feature selection for lightweight IDSs. The proposed method has a detection accuracy of over 90%, and when trained with Support Vector Machine (SVM) and neural networks, the dataset performed well in terms of accuracy and complexity.

[11] emphasize the importance of computer systems and interoperability for daily operations, but also warn of vulnerabilities exploiting them. They propose using deep learning methodologies to identify and categorize network intrusions for flexible and resilient intrusion detection systems. The UNSW-NB15 dataset demonstrated the effectiveness of the design, reflecting current network behavior through synthetic attack actions. However, the model's ability to handle zero-day attacks could be improved.

[12] states that in the Internet age, numerous attack categories are introduced daily, leading to a growing demand for efficient detection of diverse threats using Internet Detection Systems (IDSs). This study aimed to improve IDS detection rates using machine learning techniques. A unique classifier ensemble-based IDS was developed using a hybrid method that combined data and feature-level approaches. The ensemble models used expert knowledge to increase intrusion detection rates. The system's detection rates were found to be higher than the reference approach in the experiments.

[13] discuss the challenges of network security due to the growth of network size and data, highlighting the importance of intrusion detection systems (IDS) in preventing intrusion. The study analyzes current NIDS-based research, focusing on its advantages, disadvantages, recommended methodology, evaluation criteria, and dataset choice. The study highlights the need for modern datasets to effectively combat network threats, as the KDD Cup'99 and NSL-KDD datasets are limited in effectiveness due to their age.

[14] developed lightweight IoT devices using ML techniques for feature selection and classification. The filter-based method was used to select features, while the feature classification algorithm was compared using various ML techniques. The study's findings serve as a reference for selecting the best feature approach for ML, but other feature selection approaches and new ML algorithms should be investigated for real-time IoT device data. IDSs are the most important component of a secure network because of the enormous amount of data on the network [15]. By 2025, cybercrime is expected to damage the world's economy by $10.5 trillion. This demonstrates how crucial cybersecurity is to aid in defending against cyber threats or assaults [16].

III. METHODOLOGY

A. Framework

The proposed model for IDS is formulated by inducing predictive classifiers from the IDS dataset D as follows.

The dataset D...

$$D = \{a1, b1), (a2, b2) \dots \dots \dots . (aN, bN)\} \quad (1)$$

Where a ∈ A and is a vector of independent features of a dataset D. b ∈ B, b is a scalar-dependent feature also known as the label of the dataset D. n = 1, 2, N and N is the total number of feature instances in a dataset.

In the manner described in [17], a mapping function in equation 2 can be trained to show a relationship between input vectors (A) and their corresponding labels (B). A mapping function that can be used in the predictive classification of future instances of the dataset (D)

$$f(A) \rightarrow B \quad (2)$$

The prime objective in the IDS, b, is defined as 0 when there is no attack (normal); otherwise, it is 1. Therefore, for a new instance of the input vector (ai), the mapping function can predict a possible bi, as shown in equation 3.

$$f(ai) = bi \quad (3)$$

B. Description of the dataset

The study used the UNSW-NB15 dataset from the Australian Centre for Cyber Security's Cyber Range Lab, which contains over two million data samples from two simulation phases. The dataset has 2,540,044 records, divided into two sets for testing and training. The testing set had 82,332 records from various types of attacks, while the training set had 175,341 records. Both sets are named UNSW_NB15_set.csv shown in Table 1[18].

There are nine types of attacks in the dataset used for this research: fuzzers, exploits, shell code, worms, DoS, backdoors, analysis, reconnaissance, generic, and normal. The dataset categorized the attacks and the normal traffic by the number of events that occurred, as shown in Table 2 [19].

TABLE I. THE DISTRIBUTION OF CATEGORIZED ATTACKED TRAINED VALUES.

S/N	CLASS	CLASS LABEL	DISTRIBUTION
1	Normal	0	2218761
2	Attacks	1	321283
	Total		**2540044**

TABLE II. THE ATTACK CLASSIFICATION AND QUANTITY OF OCCURRENCES IN THE DATASET.

S/N	ATTACK CLASSIFICATION	NUMBER OF OCCURRENCES
1	Fuzzers	24246
2	Reconnaissance	13987
3	Shell code	1462
4	Analysis	2677
5	Backdoors	2329
6	Dos	16353
7	Exploits	44525
8	Generic	215481
9	Normal	2218761
10	Worms	174
	Total	**2540044**

C. *Architecture of the System*

The proposed IDS enables real-time analysis of traffic logs to identify potential attacks by analyzing differences from expected traffic [20]. The architecture includes a Data Capturing and Preprocessing Agent subsystem, Analyzer and Detection subsystem, and Attack Notifier subsystem shown in fig. 1.

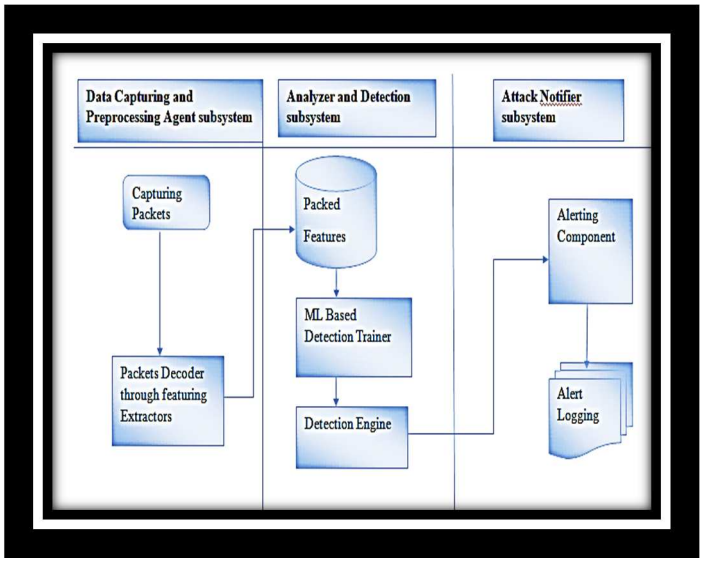


Fig. 1: Architecture of the Proposed IDS.

The Data Capturing and Preprocessing Agent subsystem, located at the entrance of our architecture, captures each packet of data flow through pcap.csv, divides it into segments, and sends it to the next module for processing. Packet decoders utilize recursive feature extraction for efficient data organization and analysis. This preprocessing step examines unprocessed packets based on predetermined behavior patterns, such as HTTP plug-ins. Observed packets are packed and sent to the ML-Based Detection Trainer.

The ML-Based Detection Trainer analyzes normal patterns and anomalies indicating potential attacks, transmitting this information to the alert system for notification to relevant parties, ensuring a comprehensive security response [21]. In this study, the analysis engine analyzes the data using ensemble ML methods. The development of ML techniques that can accurately identify and categorize various types of network threats is required to enhance the effectiveness of the IDS.

The Attack Notifier subsystem is responsible for sending alerts to security personnel or triggering automated responses to block access to affected systems. It may communicate with agents to adjust logging settings or gather additional information about attacks [22].

The study suggests using ensemble-based Super Learning techniques to improve the performance of IDSs in specific problem domains. It tests six basic ML algorithms, including KNN, RF, LGBM, XGBOOST, NB, and DT. The Superlearner method gauges the accuracy of multiple models based on ML models with multiple variables. The detection model process includes preprocessing, building, and evaluation modules, with the models combining to form an ensemble, predicting system efficiency, and forming intelligent IDS shown in Fig. 2.

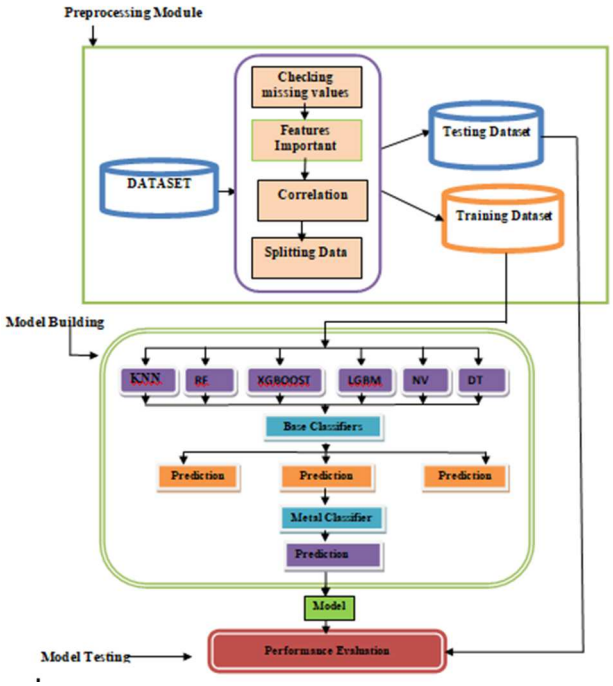


Fig. 2: Flow diagram of the performance evaluation of the Super Learning Ensemble.

IV. RESULTS AND DISCUSSION

A. *The trained classifiers exhibit receiver operating characteristic curves.*

The ROC-AUC performance of each classifier is unfolded and presented in this section. Each of the trained classifiers (NB, KNN, RF, XGBOOST, LGBM, and DT) was tested for cross-validation and ROC curves. Fig. 3 shows the results obtained from the fold. It can be observed that the AUC-ROC of XGBOOST, RF, and LGBM (0.98) surpasses those of NB (0.90), KNN (0.94), LR (0.89), and DT (0.90).

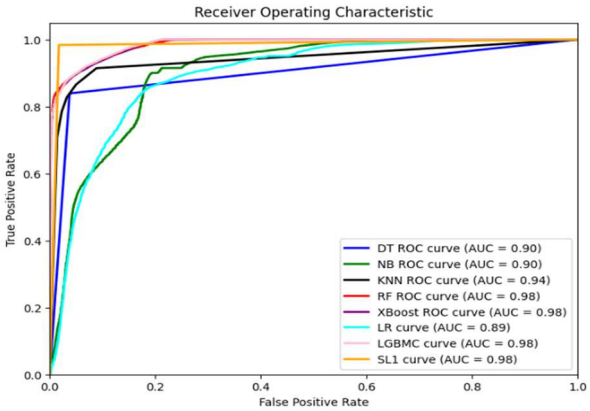
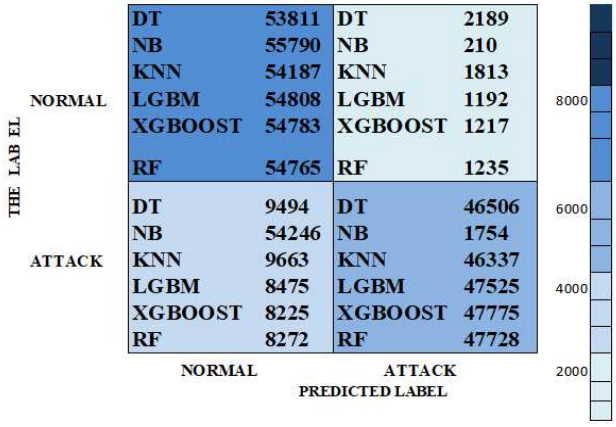


Fig. 3: The AUC-ROC of the base learner classifiers.

B. The confusion matrix obtained from trained classifiers.

The confusion matrix was obtained from the base learner classifier (NB, KNN, RF, XGBOOST, LGBM, and DT), which is shown in Table 3. The confusion matrix of the NB classifier obtained with total true positive is 55790, false positive 210, false negative 54246, total true negative 1754, KNN with total true positive 54187, false positive 1813, false negative 9663, total true negative 46337, DT classifier with total true positive 53811, false positive 2189, false negative 9494, total true negative 46506, RF classifier with total true positive 54765, false positive 1235, false negative 8272, total true negative 47728, XGBOOST with total true positive 54783, false positive 1217, false negative 8225, total true negative 47775, and LGBM with total true positive 54808, false positive 1192, false negative 8475, total true negative 47525 respectively.

TABLE III. THE CONFUSION MATRIX OF THE BASE LEARNER CLASSIFIERS.



C. Accuracy of the Six Classifiers

The accuracy measure performances of each of the six classifiers (NB, KNN, RF, XGBOOST, LGBM, and DT) were obtained as follows: The accuracy of NB is 0.5138, DT is 0.8957, KNN is 0.8975, RF is 0.9151, XGBOOST is 0.9157, and LGBM is 0.9134. It can be observed from Table 4 that the accuracy of XGBOOST (0.9157) surpasses that of NB (0.5138), KNN (0.8975), RF (0.9151), LGBM (0.9134), and DT (0.8957).

The study's performance assessment of six base models, using metrics like confusion matrix, ROC-AUC, and cross-validation metric, which reveals that the XGBOOST model outperformed other models.

TABLE IV. PERFORMANCE RESULTS ACROSS THE METRICS FOR BASE MODEL.

MODEL	ACCURACY	PRECISION	RECALL	F1-SCORE	ROC-AUC
NB	0.51	0.70	0.51	0.37	0.90
KNN	0.90	0.91	0.90	0.90	0.94
DT	0.90	0.90	0.90	0.90	0.90
RF	0.92	0.92	0.92	0.91	0.98
XGBOOST	0.92	0.92	0.92	0.92	0.98
LGBM	0.91	0.92	0.91	0.91	0.98

D. A superlearning ensemble model to detect intrusion

The superlearning ensemble detection model, trained using XGBOOST and RF best ensemble classifiers and KNN best traditional classifier, achieved impressive performance metrics like an f1-score of 0.98, recall of 0.98, and accuracy of 0.98. It accurately categorizes positive and negative occurrences, demonstrating resilience to adversarial attacks and striking a balance between recall and accuracy shown in Table 5.

TABLE V. CLASSIFICATION REPORT OF THE SUPERLEARNING ENSEMBLE MACHINE LEARNING.

Super Learner Accuracy: 0.98

Classification Report :

	precision	recall	f1-score	support
Normal	0.98	0.98	0.98	56000
Attack	0.98	0.98	0.98	56000
accuracy			0.98	112000
macro avg	0.98	0.98	0.98	112000
weighted avg	0.98	0.98	0.98	112000

Fig. 4 shows the AUC-ROC of the superlearning ensemble ML with a result of 0.98, which means that the curve is almost the same as the perfect classifier. This shows that the super-learning ensemble machine learning model performs efficiently and has outstanding predicted accuracy.

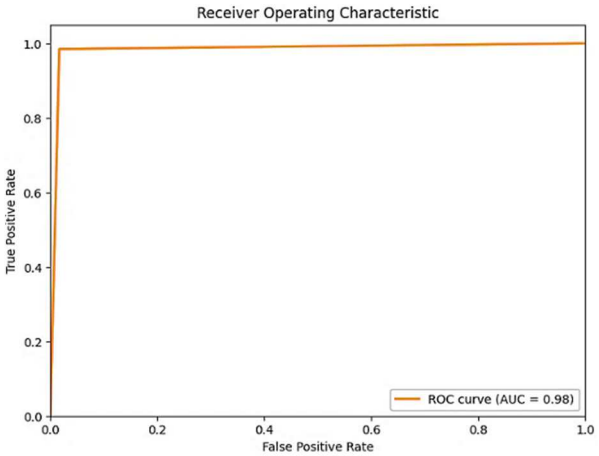
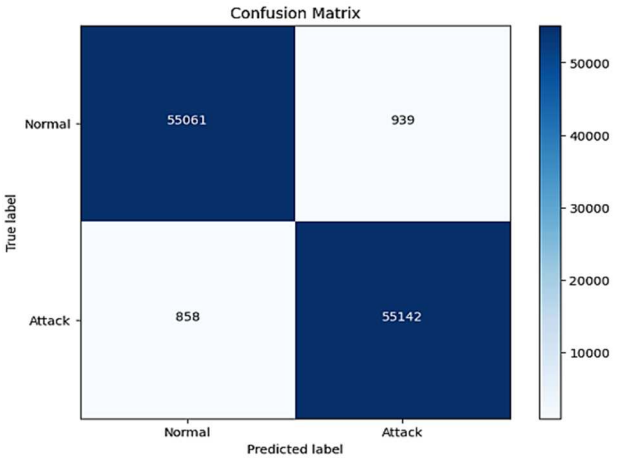


Fig. 4: Superlearning AUC-ROC Curve.

Table 6 shows the confusion matrix of the super learning classifier obtained with total true positives of 55042, false positives of 958, false negatives of 904, and total true negatives of 55096, respectively.

TABLE VI. CONFUSION MATRIX FOR SUPERLEARNING ENSEMBLE.



The accuracy of the super learning ensemble is 0.983. It can be observed that the accuracy of the super learning ensemble model surpasses that of the base model in this research.

The results obtained from each of the predictive classifiers in this research show the individual abilities of each base ML and super-learning ensemble ML to detect intrusion. The confusion matrix obtained from each of the trained classifiers is shown in Table 4. The results of the AUC-ROC curve are shown in Fig. 3: NB 0.90, KNN 0.94, RF 0.98, XGBOOST 0.98, LGBM 0.98, and DT 0.9. The results of the precision, recall, F1-score, and accuracy show that XGBOOST has the highest performance compared to other base classifiers (NB, DT, LGBM, RF, and KNN) across standard metrics measures.

Table 5 shows the results obtained from the super learning ensemble: precision (0.98), recall (0.98), accuracy (0.98), and F1-score (0.98), which outperformed the best of the base learners ML in Table 4. The accuracy of XGBOOST is 0.92, which is the best out-of-base classifier. When compared to the super learner (0.98), there is a clear difference: combining two or more ML models is better than one model alone, which prevents overfitting and results in more accurate predictions for detecting intrusion. The super learning IDS application contains both manual and data testing methods to predict normal packets or attacks, enabling more accurate predictions. In Fig. 5 users can access these methods through the provided website link. https://net-intrusion.streamlit.app.

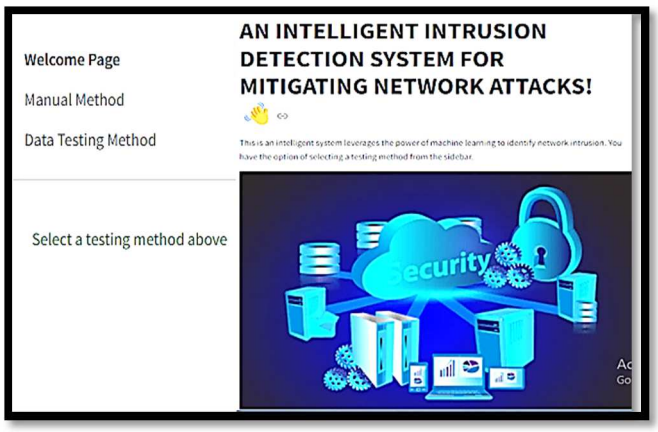


Fig. 5: A super learning app to predict intrusion or normal traffic.

E. Superlearning intrusion detection application for manual methods

The super-learning IDS application contains manual methods to predict normal packets or attacks. Fig. 6 shows the method of detecting intrusion through the manual method by entering the value of the packet attribute manually to predict either intrusion or normal traffic and the types of intrusion by clicking the predict button.

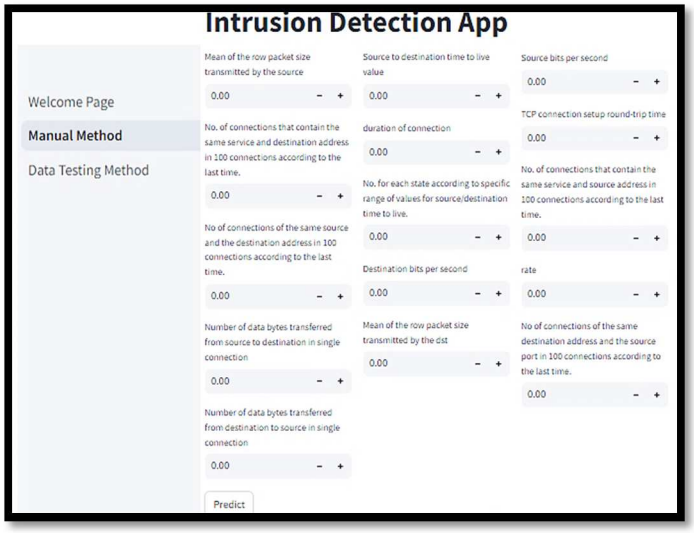


Fig. 6: Superlearning intrusion detection application for manual methods.

F. Superlearning intrusion detection application for data testing methods

Fig. 7 shows the method of detecting intrusion through the data testing method by selecting the pre-existing dataset row number to predict either intrusion or normal traffic and the types of intrusion by clicking the predict button.

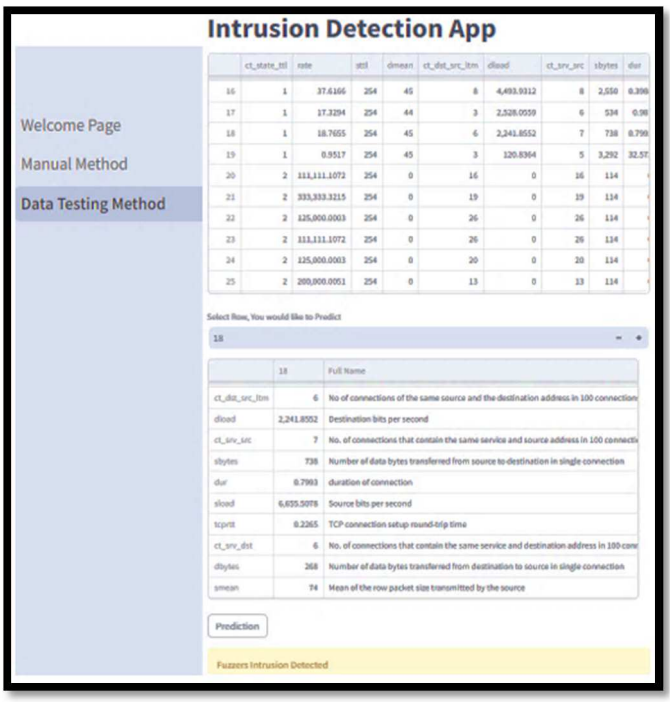


Fig. 7: Superlearning intrusion detection application for data testing methods.

V. CONCLUSION

This research explored intrusion detection using six induced classifiers (KNN, RF, LGBM, XGBOOST, NB, and DT) and their effectiveness on the UNSW-NB15 dataset. Results showed that each classifier has advantages and disadvantages, with some performing better in specific situations than others. Interestingly, the study found that the ensemble methods among them improve detection accuracy and robustness in IDS applications. The best two performing ensemble classifiers (XGBOOST and RF) and the best performing traditional classifier (KNN) were used as base classifiers in a Super-learning ensemble approach in the study. The resulting Super learning ensemble classifier achieved low false positives and enhanced accuracy, making it a proficient model for network attack detection. Further investigation into the use of this approach in various network contexts and an assessment of its efficacy against changing cyber threats could be considered in future studies, which would help improve precautions against cyber security threats.

REFERENCES

[1] A. Alfonso and C. Noelia, "The importance of ICT in society's needs: An empirical approach through Maslow's lens.," *BBVA Research DIGITAL ECONOMY,* vol. 5, no. 4, pp. 1-15, 2017.

[2] K. P. Al-Sakib, The State of the Art in Intrusion Prevention and Detection, New York: CRC Press Taylor and francis Group, 2010.

[3] F. Farahnakian and J. Heikkonen, "Anomaly-based Intrusion Detection Using Deep Neural Networks," International Journal of Digital Content Technology and its Applications , pp. 178-163, 2018.

[4] V. Pai, Devidas and N. D. Adesh, "Comparative analysis of Machine Learning algorithms for Intrusion Detection," IOP Conference Series: Materials Science and Engineering, pp. 1-8, 2021.

[5] R. Venkat, "Home: Information and Communications TechnologyIntrusion Detection System/intrusion Prevention System Market," Apr. 2021, [Online]. Available: https://www.wicz.com/story/43590708/intrusion-detection-system-market-expected-to-grow-at-a-cagr-of-12-during-the-forecast-period-20192025

[6] L. Zhiqiang, X. Bo, C. Bo, H. Xiaomei, and D. Mehdi, "Intrusion detection systems in the cloud computing: A comprehensive and deep literature review," *Wiley online*, vol. 34, no. 4, pp. 1–15, 2021.

[7] R. Vinayakumar, A. Mamou, K. P. Soman and V. Sitalakshmi, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. (1109/ACCESS.2019.2895334), pp. 1-26, 2019.

[8] O. Mebawondu, A. Olufunso and A. O. Adetunmbi, "Network intrusion detection system using supervised learning paradigm," Scientific African, pp. 1-11, 2020.

[9] O. Ajayi, A. Adetunmbi, T. Olowookere, and S. Sodiya, "Performance evaluation of ensemble learning algorithms and classical machine learning algorithms for phishing detection," in *Proceedings of the 2002 Smart, Secure and Sustainable Nation*, Nov. 2022.

[10] E. Özer, M. İskefiyel and J. Azimjonov, "Toward lightweight intrusion detection systems using the optimal and efficient feature pairs of the Bot-IoT 2018 dataset," International Journal of Distributed Sensor Networks, vol. 17, no. 10, pp. 1-15, 2021.

[11] L. Ashiku and D. Cihan, "Network Intrusion Detection System using Deep Leaming," *Elsevier Science Direct Procedia*, vol. 185, no. 2021, pp. 239–247, 2021.

[12] R. S. Uma and M. SureshN, "Security Enrichment in Intrusion Detection System Using Classifier Ensemble," *Hindawi Journal of Electrical and Computer Engineering*, vol. 10, no. 1155, pp. 1–7, 2020.

[13] Z. Ahmad, S. K. Adnan, and S. CheahWai, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Wiley Survey paper*, pp. 1–29, 2020, doi: 10.1002/ett.4150.

[14] F. Samir, F. Fouzi and B. Abderrahmane, "A Machine Learning-Based Lightweight Intrusion Detection System for the Internet of Things," International Information and Engineering Technology Association, vol. 33, no. 3, pp. 1-9, 2019.

[15] M. Mazinia, S. Babak, and M. Iraj, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and Adaboost algorithms," *King of saud University-Computer and Information ScienceS*, vol. 31, no. 2019, pp. 1–13, 2019.

[16] B. Ikusika, Jul. 2022, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4165204

[17] T. A. Olowookere and O. S. Adewale "A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach," Scientific African. 8. E00464. 10.1016/j.sciaf.2020.e00464, 2020.

[18] N. Koroniotis, N. Moustafa, E. Sitnikova, et al. "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics" Bot-IoT dataset. *Future Gener Comp Sy,* 100: 779–796 2019.

[19] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems," *Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet, WiCON 2020, Virtual Event, December 11, 2020, Proceedings*, p. 117, 2020.

[20] N. Gavrilovic, V. Ciric, and N. Lozo, "Snort ids system visualization interface for alert analysis," *Serbian Journal of Electrical Engineering*, vol. 19, no. 1, pp. 67–78, Jan. 2022, doi: 10.2298/sjee2201067g.

[21] N. M. Shanono, M. Zulkiflee, N. A. Abu3, W. Yassin, and M. A. Faizal, "Intrusion Detection System Architecture: Issues and Challenges," *Technology Reports of Kansai University*, vol. 62, no. 7, pp. 4121–4132, 2020.

[22] "Intrusion Detection System (IDS)," Jan. 2021, [Online]. Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids.