ISSN 2277-2685
IJESR/Jan-Mar. 2025/ Vol-15/Issue-1/304-316
Kappala Manjunath*et. al.*, / International Journal of Engineering & Science Research

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

[1] M. Dharani Kumar, [2] Kappala Manjunath

[1]Assistant Professor, M. Tech (Ph.D), Department of Computer Science and Engineering, PVKK institute of technology, Anantapur, Andhra Pradesh, India.

[2]M. Tech Student, Department of Computer Science and Engineering, PVKK institute of technology, Anantapur, Andhra Pradesh, India.

ABSTRACT

wireless Sensor Networks (WSNs) are critical for a variety of monitoring applications, but they are prone to security concerns such as unauthorized access, attacks, and other malicious behavior, which can jeopardize their reliability. To mitigate these concerns, using Intrusion Detection systems (IDS) is critical for early detection and response. several datasets, such as KDD Cup data, NSL KDD, u.s.a.-NB 15, and AWID, are often used to train and assess IDS models. feature selection is an vital step in improving the performance of these fashions, and strategies like SelectKBest paired with the ANOVA F-take a look at offer effective feature reduction and increased accuracy. the use of these datasets and feature selection methods, the paper analyzes the use of a Stacking Classifier strategy that mixes Bagging with Random forest and Boosting with decision Tree algorithms. This approach achieves high accuracy throughout all datasets tested, presenting a complete strategy to the troubles faced by safety risks in WSNs. The findings highlight the price of ensemble processes in optimizing IDS performance for stepped forward security in WSNs.

"Index Terms *- WSN, Wi-Fi, NIDS, WIDS attacks, security issues, network threats, feature engineering, multiclass classification, inclusive innovations.".*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are becoming increasingly more important in present day communication systems, providing a versatile and efficient means of records switch in a variety of applications together with environmental monitoring, healthcare, and industrial automation. those networks are made from a huge quantity of sensor nodes that display and transmit data in a diffusion of topologies, such as star, tree, and mesh. these sensor nodes' key functionalities consist of sensing, processing, computation, and communication, allowing them to effectively monitor and perform multiple systems in real time [1][2]. WSNs are an green and value-effective opportunity for wi-fi network traffic communique, especially in regions with constrained electricity assets, because they're designed to consume minimal power [3]. This makes WSNs best for tracking and shielding far flung or hard-to-attain areas.

however, despite their severa advantages, WSNs are vulnerable to a variety of safety issues, which includes unauthorized get admission to, attacks, and different malicious moves that would jeopardize the network's reliability and capability. WSNs are often deployed in touchy regions, therefore guaranteeing their security is critical to their efficacy. Unauthorized get admission to can come from both internal and external sources, posing severe threats to the network's integrity and the facts it carries [4][five. Given the growing reliance on wireless

networks for vital infrastructure, comprehensive security features are required to defend sensor nodes and the records they collect.

sensors, which are typically used in WSNs, are widely available because they can connect to wi-fi networks and switch data over high-quality distances via TCP/IP. those sensors may join to the network using the SSID and passphrase, letting them communicate information to servers thru URL or IP cope with [6]. while sensors aren't inside range of a get admission to point, repeaters may be used to boom insurance and assure non-stop records transmission. at the same time as sensors are convenient and very powerful, they also enhance the network's exposure to prospective attacks.

To alleviate these risks, it is necessary to implement a Intrusion detection system (IDS). A Intrusion detection system (IDS) is a mechanism that identifies and prevents unauthorized access to the network by monitoring users for indicators of potential threats [7]. The IDs are categorized in two types: based on host elements and network based. The host-based ID is integrated into a device and is directly monitored by various methods and users, whereas the network-based ID is disseminated throughout the network to identify potential infiltration attempts.The most prevalent type of IDS in WSNs is network-based, which provides distributed monitoring throughout the complete network to detect capability threats [8].

2. RELATED WORK

the security of wireless Sensor Networks (WSNs) has been a key topic in current years as they are increasingly used in sensitive applications. The vulnerability of WSNs to unauthorized get entry to and various forms of attacks has resulted in the development of improved Intrusion Detection systems (IDS) to mitigate those risks. severa studies have contributed to the boom of IDS for WSNs, each focusing on a exceptional location, such as detection methodologies, power efficiency, and attack classification.

Boahen et al. [9] proposed a deep, multi-architectural technique to intrusion detection in online social networks. The studies focused on integrating several architectures to improve detection accuracy by combining deep learning strategies with network behavior analysis. This method underlines the want of hybrid fashions in addressing the complexity of figuring out malicious pastime in dynamic contexts, while also imparting beneficial insights into the possibilities of multi-architectural fashions for improving IDS performance.

Mahmud et al. [10] The scalable wireless sensor proposed an energy-efficient data transmission solution for the network utilizing a deep learning framework. His findings underscored the necessity for energy economy in wireless sensor networks, particularly in the context of large-scale networks. The authors demonstrate that intensive learning approaches can effectively integrate data from several sensor sources, hence enhancing accuracy in intrusion detection while minimizing vulnerabilities. This observe emphasizes the trade-off among electricity intake and detection performance in wi-fi sensor networks, that is important in real-global programs with limited assets.

Granato et al. [11] investigated intrusion detection in networks, employing a modular and optimized ensemble of classiwi-fiers. Her research provided a hybrid ensemble approach that integrates the distinctive classics to improve recognition binding, exploring current intrusion detection-fashion. The system has improved the possibility of recognizing different storm patterns by combining the strengths of numerous classification techniques. This

examines how the capabilities of ensemble strategies to improve identity robustness and adaptability are highlighted in wireless networks.

Mahmood et al. [12] passed smart error-recognition in wireless sensor networks that rely on algorithms in reinforcement learning models. The authors highlighted the benefits of learning learning to improve the cognitive process by constantly adapting to new and emerging threats. This approach allows IDs to learn from their surroundings and improve over the years, resulting in more accuracy and response to new protection issues. The advantages of learning learning are an important step in developing a larger autonomous and intelligent IDS system for WSN.

Tao and Xueqiang [13] proposed a hybrid technique to improve the Sparrow search algorithm for intrusion recognition. Her approach included numerous strategies to improve WSN's identity detection talent. Hybrid methods use optimization strategies to improve identification methods, allowing the system to efficiently select and classify attacks. This study provides to the developing body of studies on IDS optimization techniques, Highlighting its importance for executing the incursion and its role in enhancing infiltration accuracy.

Singh et al. [14] They examined the application of deep learning to predict the amount of OK-Barriers needed to detect disturbance in a circular radius using Wi-Fi sensor networks. Their research targeted on the use of deep studying models to expect the location of community boundaries on the way to successfully become aware of intrusions. This answer makes use of deep learning to expect community behavior and optimize barrier placement, hence growing WSN security. the object describes a singular way to combining deep learning with community topology optimization to improve intrusion detection.

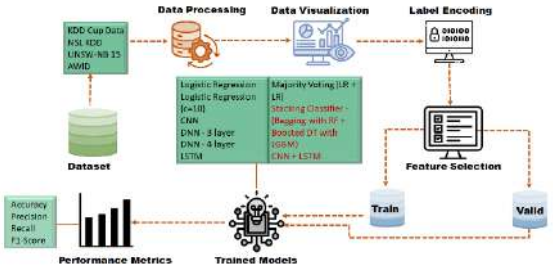
Rajasoundaran et al. [15] counseled a comfy and green intrusion detection system for underwater wireless sensor networks primarily based on LSTM-MAC concepts. To cozy underwater wireless sensor networks, the authors created a version that combines long short-term memory (LSTM) networks with Medium access control (MAC) standards. This aggregate enables the system to pick out intrusions even as improving community speed. Their findings provide vital insights closer to protecting specialty WSNs, such as the ones applied in underwater environments, wherein traditional IDS fashions may not be directly relevant.

Park et al. [16] introduced G-IDCS, a graph-based system for intrusion detection and classification within the Controller Area Network (CAN) protocol. The authors employed graph-based methods to represent community interactions. which advanced intrusion detection and assault category. This paintings is especially applicable for WSNs that use specialised conversation protocols, as it gives a singular way to attack detection in protocol-based networks.

Kandhro et al. [17] They examined the detection of harmful disruptions and real -time attacks in systems of completely cyber security based on IoT.They supplied an IDS system that might integrate IoT devices with actual-time intrusion detection talents. The authors hoped to enhance the safety of complex systems by detecting malicious activity because it occurred using IoT and machine learning. Their findings are vital in the context of IoT-enabled WSNs, due to the fact the dynamic environment necessitates actual-time detection and reaction to security dangers.

3. MATERIALS AND METHODS

The proposed system intends to improve the security of wireless sensor networks (WSN) by creating a forward detection system (IDS) that can identify a number of security threats. The system trains and evaluates the IDS models using a selection of relatively famend datasets, along with KDD Cup data [20], NSL KDD, u.s.-NB 15, and AWID [21]. SelectKBest is used with the ANOVA F-take a look at to decide the maximum relevant functions for class, ensuing in progressed version overall performance. Logistic Regression [18], Logistic Regression with a regularization parameter (c=10), Convolutional Neural Networks [19], Deep Neural Networks (DNN) with three and 4 layers, and lengthy quick-time period memory (LSTM) networks will all be investigated. moreover, hybrid fashions consisting of CNN + LSTM and Majority voting (which mixes Logistic Regression models) could be examined. The Stacking Classifier, which combines Bagging with Random woodland and Boosting with decision Tree, will also be used to improve detection overall performance in the device.



"Fig.1 Proposed Architecture"

Design (Figure 1) The Wi-Fi sensor use machine learning to identify network penetration. The procedure commences with data processing and visualization, subsequently advancing to delineate code and functional selections. The data is divided into education and validation sets. more than one machine learning models [18], such as logistic regression, CNN, DNN, and LSTM, are advanced and tested. further, ensemble approaches such as majority balloting and stacking classifiers are The model is utilized to enhance performance. The final model mostly relies on performance metrics such as accuracy, precision, recall, and F1 score.

i) Dataset Collection:

This study uses datasets, "KDD, NSL KDD, usa-NB15, and AWID", to evaluate the efficacy of intrusion detection structures for wi-fi sensor networks.

The AWID dataset [21] includes 313,248 entries and 84 attributes, with a primary focus on wireless intrusion detection. The dataset includes the following essential properties after feature selection: "body.offset_shift', 'frame.time_epoch', 'frame.time_delta', 'body.time_delta_displayed', 'frame.time_relative', 'frame.len', 'radiotap.flags.shortgi', 'wlan.fc.type', 'wlan.fc.ds', and 'wlan.fc.frag'." those features seize crucial aspects of wireless frames, such as timing, frame length, and sure flags, which provide beneficial information for identifying network irregularities and in all likelihood intrusions in wi-fi networks.

	frame.interface_id	frame.dlt	frame.offset_shift	frame.time_epoch
0	?	0.0	1.393668e+09	0.000000
0	?	0.0	1.393668e+09	0.001056
0	?	0.0	1.393668e+09	0.000141
0	?	0.0	1.393668e+09	0.000156
0	?	0.0	1.393668e+09	0.001842

5 rows × 154 columns

"Fig.2 Dataset Collection Table – AWID-CLS-R-Tst"

The KDD dataset [20], which focuses on community infiltration, contains 125,973 entries and 42 characteristics. The dataset includes the following features after feature choice: "logged_in', 'root_shell','serror_rate','srv_serror_rate','same_srv_rate', 'dst_host_srv_count', 'dst_host_same_srv_rate', 'dst_host_same_src_port_rate', 'dst_host_serror_rate', and 'dst_host_srv_serror_rate'." those features are vital for identifying network attacks and intrusions, as they offer a targeted set of attributes for improving the efficacy of intrusion detection systems.

	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment
0	0	tcp	ftp_data	SF	491	0	0	0
1	0	udp	other	SF	146	0	0	0
2	0	tcp	private	S0	0	0	0	0
3	0	tcp	http	SF	232	8153	0	0
4	0	tcp	http	SF	199	420	0	0

5 rows × 42 columns

"Fig.3 Dataset Collection Table – KDDCUP"

The NSL KDD dataset, which focuses on intrusion detection, consists of 125,972 devices and forty three characteristics. The dataset consists of the subsequent capabilities after characteristic selection: "logged_in`, 'root_shell','serror_rate','srv_serror_rate','same_srv_rate', 'dst_host_srv_count', 'dst_host_same_srv_rate', 'dst_host_same_src_port_rate', 'dst_host_serror_rate', and 'dst_host_srv_serror_rate'." those abilities are vital for detecting community intrusions and assaults, as they offer a polished set of trends that enhance the accuracy of intrusion detection models.

	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot
0	0	udp	other	SF	146	0	0	0	0	0
1	0	tcp	private	S0	0	0	0	0	0	0
2	0	tcp	http	SF	232	8153	0	0	0	0
3	0	tcp	http	SF	199	420	0	0	0	0
4	0	tcp	private	REJ	0	0	0	0	0	0

5 rows × 43 columns

"Fig.4 Dataset Collection Table – NSL-KDD"

The united states-NB15 dataset carries 82,332 facts and forty five capabilities centered on community intrusion detection. The dataset consists of the subsequent critical attributes after function selection: "rate`,'sttl','swin', 'dwin', 'ct_srv_src', 'ct_state_ttl', 'ct_src_dport_ltm', 'ct_dst_sport_ltm', 'ct_dst_src_ltm', and 'ct_srv_dst'." the ones

attributes are crucial for figuring out community assaults, shooting numerous site visitors patterns, and supplying insights into community glide conduct for you to growth the accuracy of intrusion detection algorithms.

	id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	...	ct_dst_sport_ltm
0	1	0.000011	udp	-	INT	2	0	496	0	90909.0902	...	1
1	2	0.000008	udp	-	INT	2	0	1762	0	125000.0003	...	1
2	3	0.000005	udp	-	INT	2	0	1068	0	200000.0051	...	1
3	4	0.000006	udp	-	INT	2	0	900	0	166666.6608	...	1
4	5	0.000010	udp	-	INT	2	0	2126	0	100000.0025	...	1

5 rows × 45 columns

"Fig.5 Dataset Collection Table – UNSW-NB15"

ii) Pre-Processing:

a) Data Processing: The data record is cleaned by removing zero values and double entries to ensure that the data is satisfactory and reliable. This approach eliminates anomalies along with lack of information and unnecessary data records before the index of the data record is reset, allowing for seamless analysis. The modified data records are organized for modeling by receiving the simplest applicable entries and reward classes distributions that follow the robust and independent data of machine learning applications.

b) Data Visualization: Data visualization involves the use of bar diagrams for class distribution analysis. This provides insight into class equalization of data records. Heatmap is used to show correlations between numeric variables and practical links and dependencies. These visible devices help you close the shape of your data record, find patterns, and find a choice of feed features in ModelAB Advent.

c) Label Encoding: Category facts such as class names are converted into numerical formats using label coding to ensure interoperability with machine learning algorithms. Each class is assigned with a unique, full-numbered price so that the model can effectively interpret and bypass the data. This phase ensures that category features are seamlessly integrated throughout the training.

d) Feature Selection: Statistical approaches are used to select the most relevant features. The SelectKBest approach uses analysis of variance (ANOVA) to evaluate traits via relevance and pick the pinnacle ten individuals to the target variable. This minimizes dimensionality, will increase computational performance, and improves model correctness by concentrating on vital features.

iii) Training & Validation:

The data file is divided into training and test kits for evaluating the efficiency of machine learning models. Data subgroup is used for training, permitting the model to find out patterns and correlations between the functions. The remaining facts is about apart for testing, which allows us to assess the version's accuracy, precision, and generalization. This divide ensures a radical assessment of the version's predicting ability on formerly unreported data.

iv) Algorithms:

DNN-3Layer: A 3-layer deep neural network discovers complicated patterns in data by combining multiple layers of neurons. It successfully captures non-linear interactions, making it best for comprehending complicated feature dependencies and predictive modeling with excessive accuracy.

DNN-4Layer: A four-layer deep neural network adds another layer of complexity to sample popularity, allowing for more certain characteristic extraction. it is suitable for jobs demanding advanced representation learning and overcoming problems in high-dimensional data environments.

CNN: Convolutional Neural Networks excel in feature extraction, particularly from structured or grid-like statistics. Their folding layers [19] recognize spatial hierarchies, and bundling layers are particularly clever when recording localized data, as they are aware of spatial hierarchies and bundling layers minimize dimensions.

LSTM: A long-term short-term memory network is ready with continuous facts, but long-term dependencies are retained. Gating algorithms eliminate gradient problems and allow for accurate learning from time series or time-based datasets.

CNN+LSTM: The spatial properties of CNNs and temporal connections recorded by the hybrid-LSTM model improve the extraction function. This design is characterized by jobs that require both spatial and sequential data to improve prediction accuracy and functional integration.

Logistic Regression: A linear version assesses the hyperlinks among traits and binary outcomes. Its [18] simplicity and interpretability make it best for figuring out the relevance of capabilities and acquiring baseline predicting performance.

Logistic Regression (C=10): increasing the regularization strength to C=10 prevents overfitting by regulating feature weights. It moves a compromise among complexity and model generalization, ensuing in sturdy predictions.

Majority Voting (LR + LR (C=10)): The ensemble technique combines predictions from two logistic regression models with varying regularization parameters. It improves decision stability and accuracy by combining the complimentary capabilities of every model.

Stacking Classifier: This ensemble approach combines Random woodland's bagging capabilities with choice Tree boosting. It captures many feature associations, which improves prediction performance via complimentary learning.

4. RESULTS & DISCUSSION

Accuracy: The accuracy of a check is its potential to as it should be distinguish between patient and healthy instances. In order to assess the accuracy of the inspection, in all evaluated cases, it must be calculated in the ratio of real positives and real negatives. This can be mathematically articulated:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (1)$$

Precision: The correctness reflects the ratio of precisely labeled instances among recognized individuals. Consequently, it is articulated as a formula for determining precision:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (2)$$

Recall: Recall in Machine Learning involves a computation that assesses a model's capacity to recognize all pertinent instances of a chosen category. This constitutes the anticipated affirmative remarks for comprehensive genuine positivity and offers insight into the model's efficacy in identifying events within a particular category.

$$Recall = \frac{\text{TP}}{\text{TP} + \text{FN}} (3)$$

F1-Score: The F1 score is a metric used to assess the precision of a machine learning model. It incorporates precision while neglecting the framework of a model. The accuracy meter assesses the rate of accurate predictions produced by a version within the data set.

$$F1\ Score = 2 * \frac{Recall\ \text{X}\ Precision}{Recall + Precision} * 100 (1)$$

Table (1 to 4) Generate a matrix for the accuracy, precision, recall, and F1 score of each algorithm. Stacking systematically classifies all other algorithms across all matrices. Tables facilitate a comparative analysis of the Matrix for strategic opportunities.

"Table.1 Performance Evaluation Metrics for AWID-CLS-R-Tst"

ML Model	**Accuracy**	**Precision**	**Recall**	**F1_score**
DNN-3Layer	0.977	0.767	0.998	0.861
DNN-4Layer	0.959	0.759	0.999	0.856
CNN	0.973	0.974	0.968	0.970
LSTM	0.971	0.765	0.975	0.845
CNN+LSTM	0.976	0.976	0.974	0.974
Logistic Regression	0.344	1.000	0.344	0.511
Logistic Regression(C=10)	0.976	0.978	0.976	0.976
Ensemble Model	0.976	0.978	0.976	0.976
Stacking Classifier	**0.989**	**0.989**	**0.989**	**0.989**

"Table.2 Performance Evaluation Metrics for KDDCUP"

ML Model	**Accuracy**	**Precision**	**Recall**	**F1_score**
DNN-3 Layer	0.864	0.483	0.955	0.637
DNN-4 Layer	0.860	0.562	0.973	0.704
CNN	0.844	0.790	0.668	0.701
LSTM	0.826	0.788	0.885	0.816

CNN+LSTM	0.888	0.794	0.594	0.660
Logistic Regression	0.830	0.849	0.830	0.831
Logistic Regression(C=10)	0.832	0.851	0.832	0.833
Ensemble Model	0.831	0.850	0.831	0.832
Stacking Classifier	**0.938**	**0.943**	**0.938**	**0.940**

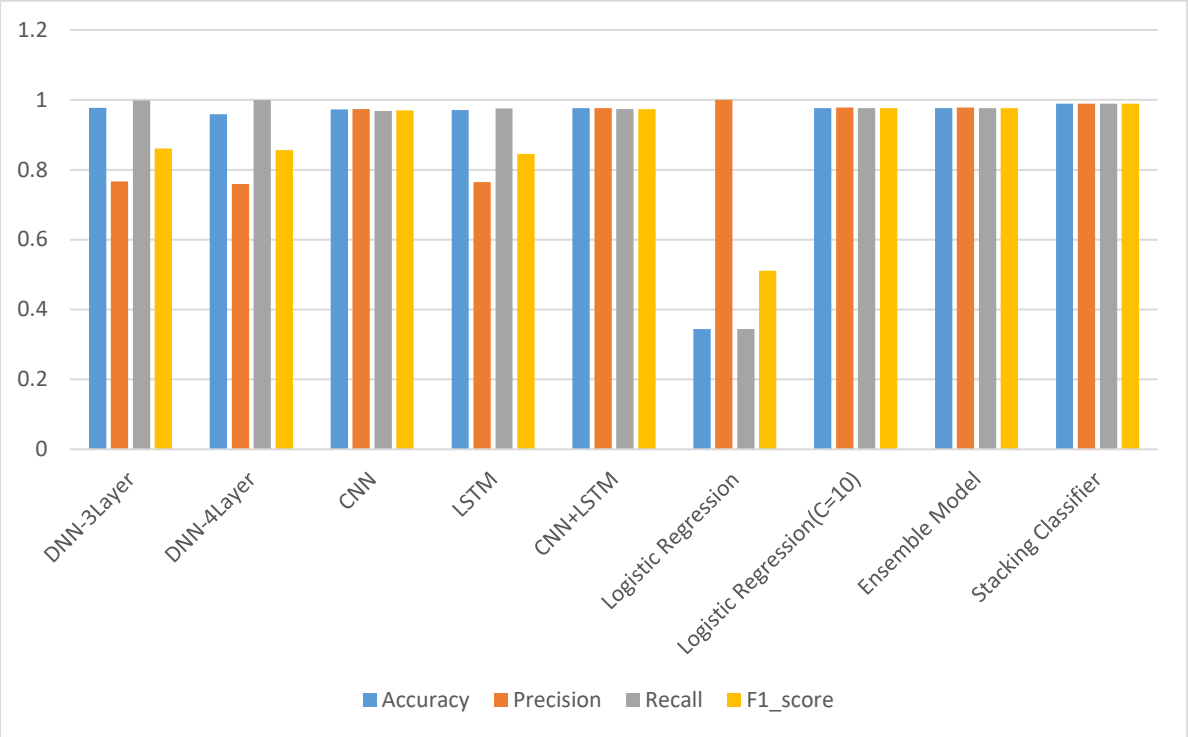
"Table.3 Performance Evaluation Metrics for NSL KDD"

ML Model	**Accuracy**	**Precision**	**Recall**	**F1_score**
DNN-3 Layer	0.858	0.512	0.982	0.666
DNN-4 Layer	0.819	0.495	0.959	0.645
CNN	0.833	0.769	0.574	0.639
LSTM	0.812	0.685	0.914	0.769
CNN+LSTM	0.859	0.772	0.557	0.628
Logistic Regression	0.817	0.835	0.817	0.818
Logistic Regression(C=10)	0.826	0.843	0.826	0.828
Ensemble Model	0.820	0.839	0.820	0.821
Stacking Classifier	**0.932**	**0.935**	**0.932**	**0.933**

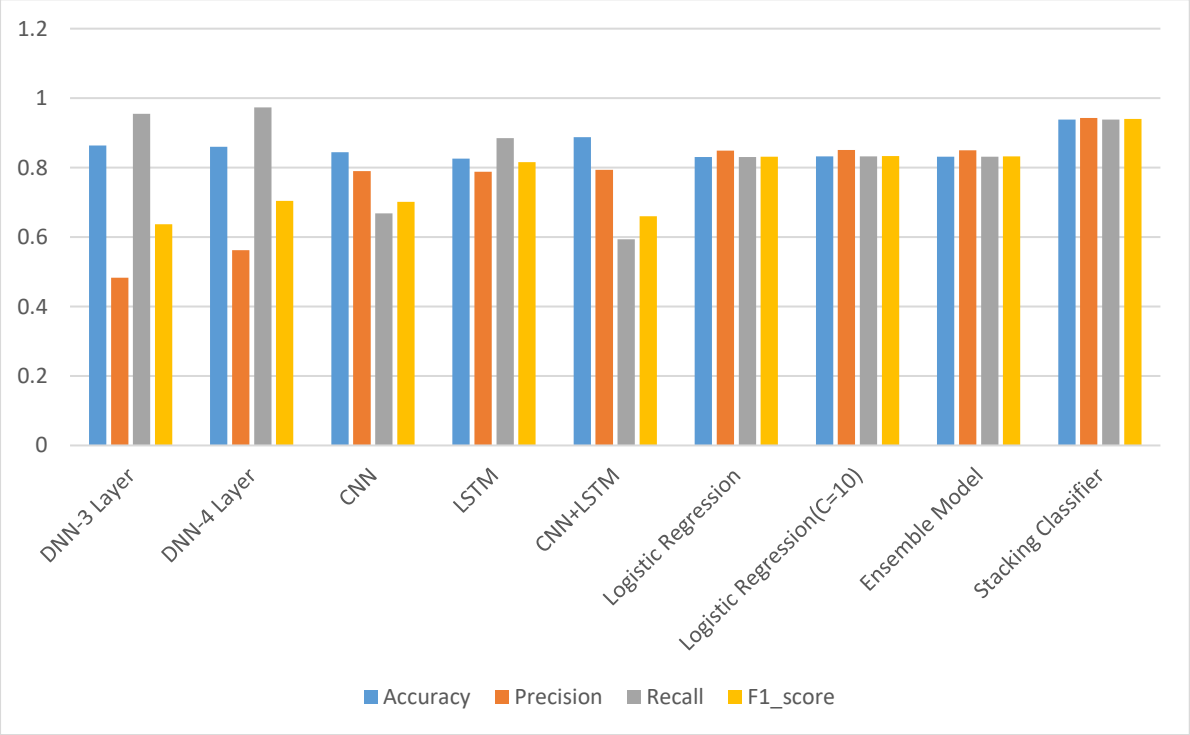
"Table.4 Performance Evaluation Metrics for UNSW-NB15"

ML Model	**Accuracy**	**Precision**	**Recall**	**F1_score**
DNN-3 Layer	0.833	0.712	0.581	0.608
DNN-4 Layer	0.834	0.624	0.644	0.606
CNN	0.860	0.867	0.886	0.874
LSTM	0.825	0.846	0.779	0.801
CNN+LSTM	0.869	0.869	0.871	0.870
Logistic Regression	0.720	0.722	0.720	0.720
Logistic Regression(C=10)	0.823	0.823	0.823	0.823
Ensemble Model	0.818	0.819	0.818	0.818
Stacking Classifier	**0.938**	**0.938**	**0.938**	**0.938**

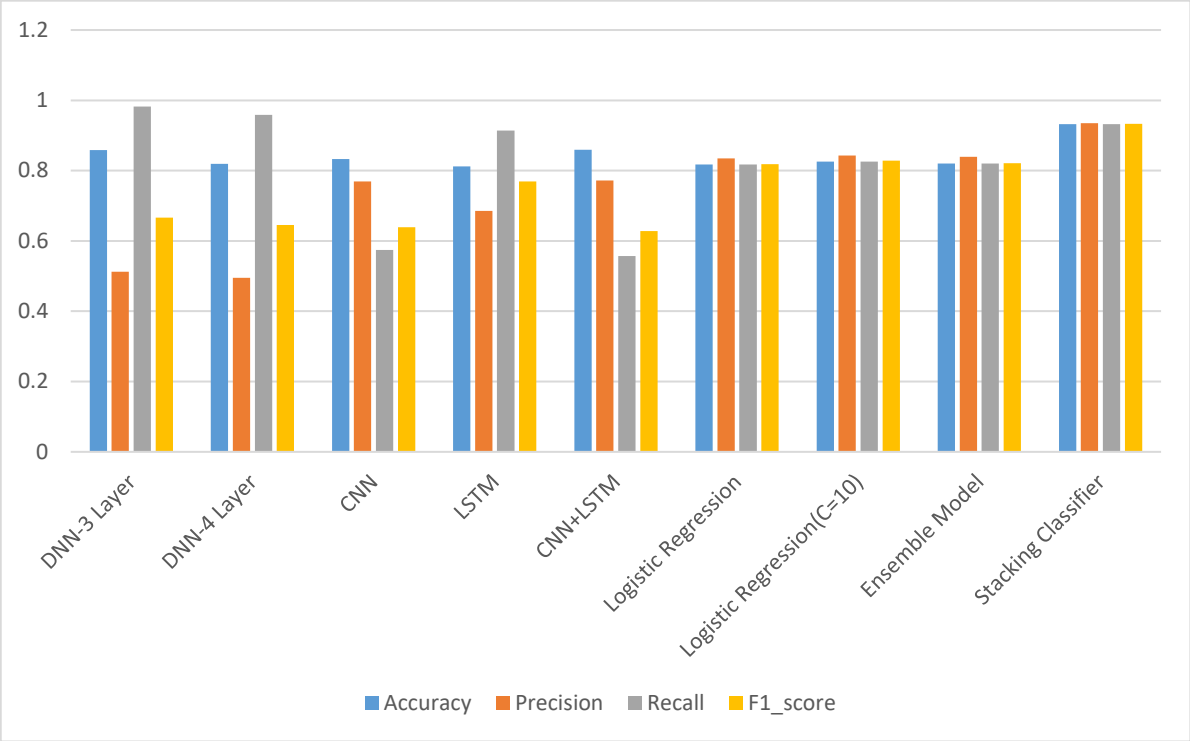
"Graph.1 Comparison Graphs for AWID-CLS-R"



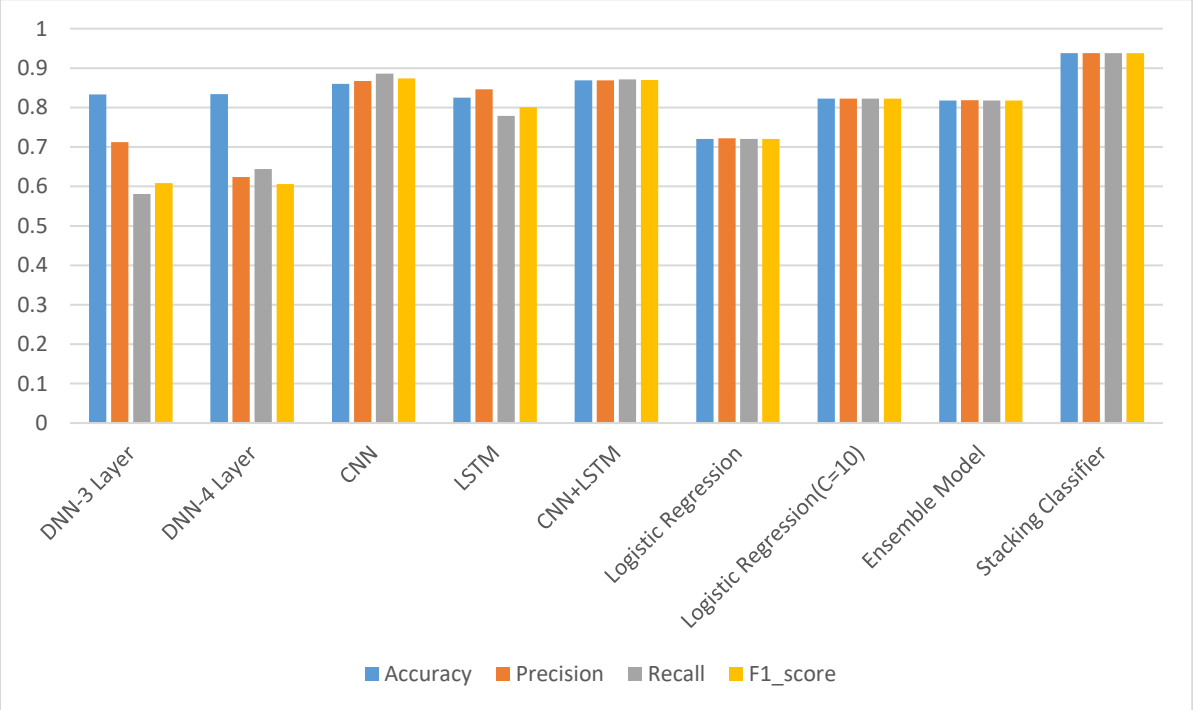
"Graph.2 Comparison Graphs for KDDCUP"



"Graph.3 Comparison Graphs for NSL KDD"



"Graph.4 Comparison Graphs for UNSW-NB15"



In one or four graphs, accuracy shows blue, orange accuracy, gray memory, F1 score in yellow and AUC in blue. Compared to other models, the stacking method shows exceptional performance across all metrics and reaches the highest values. The above marks mean these conclusions.

5. CONCLUSION

The knowledge-based Intrusion Detection System (IDS) for Wireless Sensor Networks (WSNs) significantly enhances security by precisely identifying and mitigating attacks. The Intrusion Detection System (IDS) utilizes multiple datasets to exploit the vulnerabilities of Wi-Fi Sensor Networks (WSNs) to assaults and unauthorized access.KDD Cup information, NSL-KDD, u.s.a.-NB15, and AWID—to construct resilient fashions for detecting intrusions. a major element of this application is feature choice, accomplished by methodologies such as SelectKBest and ANOVA F-test, which optimize data for greater version efficacy. The studies emphasizes the utilization of a Stacking Classifier technique, integrating Bagging with Random forest and Boosting with decision Tree algorithms, to decorate detection efficacy. This ensemble technique attains a first rate accuracy of 93% across three datasets and demonstrates awesome performance with 98.9% accuracy in the AWID dataset, highlighting its reliability and efficacy. The IDS employs powerful machine learning algorithms alongside tailored datasets to deliver a comprehensive answer for addressing protection concerns in WSNs, facilitating early detection, speedy response, and improved reliability for essential applications. The effects illustrate the transformative capability of ensemble learning in protecting WSN environments from harmful actions.

In the ***future***, the performance of the IDS for Wireless Sensor Networks (WSNs) can be further enhanced by incorporating additional advanced machine learning algorithms such as deep learning methods for enhanced precision and instantaneous detection. furthermore, investigating hybrid models that integrate anomaly-based and signature-based detection techniques may yield extra effective threat identification. enhancing the system's capacity to control larger, more numerous datasets and integrating adaptive learning mechanisms for evolving attack styles will maintain its relevance and efficacy in safeguarding WSNs over time.

REFERENCES

[1] M. Mittal, R. P. de Prado, Y. Kawai, S. Nakajima, and J. E. Muñoz-Expósito, ‘‘Machine learning techniques for energy efficiency and anomaly detection in hybrid wireless sensor networks,’’ Energies, vol. 14, no. 11, p. 3125, May 2021.

[2] K. Haseeb, N. Islam, T. Saba, A. Rehman, and Z. Mehmood, ‘‘LSDAR: A light-weight structure based data aggregation routing protocol with secure Internet of Things integrated next-generation sensor networks,’’ Sustain. Cities Soc., vol. 54, Mar. 2020, Art. no. 101995.

[3] R. Guetari, H. Ayari, and H. Sakly, ‘‘Computer-aided diagnosis systems: A comparative study of classical machine learning versus deep learning based approaches,’’ Knowl. Inf. Syst., vol. 65, no. 10, pp. 3881–3921, Oct. 2023.

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

[5] W.Wang, S.Jian, Y. Tan, Q. Wu, and C.Huang, ‘‘Representation learning based network intrusion detection system by capturing explicit and implicit feature interactions,’’ Comput. Secur., vol. 112, Jan. 2022, Art. no. 102537.

[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] G. Granato, A. Martino, L. Baldini, and A. Rizzi, ‘‘Intrusion detection in Wi-Fi networks by modular and optimized ensemble of classifiers: An extended analysis,’’ Social Netw. Comput. Sci., vol. 3, no. 4, p. 310, Jul. 2022.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] I. A. Kandhro, S. M. Alanazi, F. Ali, A. Kehar, K. Fatima, M. Uddin, and S. Karuppayah, "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures,’’ IEEE Access, vol. 11, pp. 9136–9148, 2023.

[18] M. A. Rahman, A. T. Asyhari, O. W. Wen, H. Ajra, Y. Ahmed, and F. Anwar, ‘‘Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection,’’ Multimedia Tools Appl., vol. 80, no. 20, pp. 31381–31399, Aug. 2021, doi: 10.1007/s11042 021-10567-y.

[19] B. Alenazi and H. E. Idris, ‘‘Wireless intrusion and attack detection for 5G networks using deep learning techniques,’’ Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 7, pp. 1–6, 2021.

[20] KDD Dataset, Intrusion detection dataset, Available at: https://www.kaggle.com/datasets/toobajamal/kdd99-dataset

[21] Zhiqing Cui, AWID-CLS-R, Available at: https://www.kaggle.com/datasets/zhiqingcui/awidclsr