Journal of Animal Environment

(E-ISSN 2717-1396, ISSN 2717-1388)

Original Research Paper

Multi-Layer Intrusion Detection in Smart IoT Systems Using Voting Classifier and Explainable AI with Flask Integration

Guduru Jyothsna Devi [1],Radhika Rani Chintala[2]

[1]*M. Tech CSE, student, Dept. of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh 522302, India, Email: 2401050073cse@gmail.com*
[2]*Associate Professor, Dept. of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh 522302, India, Email: radhikarani_cse@kluniversity.in*

***Abstract*—The fast rise of IoT and IIoT settings has raised the need for lightweight, scalable and intelligent intrusion detection systems. In this work, we propose an exhaustive ML and DL-based Intrusion Detection System and evaluate it with respect to ToN_IoT, WUSTL-IIoT 2021 and Edge-IIoTset datasets. The data preprocessing techniques used are outlier removal, Chi square feature selection, imbalance handling using SMOTE and undersampling. Several algorithms were implemented including CNN , DNN, DT , RF , LightGBM , Bagging , stack ensemble using RF, LightGBM and DT , and voting ensemble of Boosted DT, Bagging RF and XGBoost . The results of the experiments show the good performance of CNN (93.8%), DNN (94.4%), RF (96.3%), DT (96.6%), and the best performance of LightGBM (98.4%, 98.9%, and 96.7%) for the voting ensemble on ToN_IoT, WUSTL-IIoT 2021, and Edge-IIoTset respectively. Explainable AI techniques, like SHAP and LIME, offer feature level explainability. The deployment with Flask and SQLite enables safe, real time intrusion detection, visualization and monitoring over distributed industrial networks worldwide.**

"Keywords—Internet of Things, Industrial Internet of Things, security, cyber-attacks, intrusion detection, machine learning, lightweight, data balancing, cross-dataset transfer learning".

I. INTRODUCTION

Automation, connectivity and data-driven insights are the driving force for the rapidly growing IoT and IioT revolution. This ecosystem is huge as more than 55.7 billion gadgets will be connected globally by 2025 [1]. But this increase comes with major cybersecurity dangers. It is found that in 2020, 33% of all infected devices were IoT devices, indicating that they are vulnerable [2]. As Industry 4.0 is becoming more prevalent, and IT and OT are increasingly being combined into CPS, critical infrastructure such as healthcare, energy, transportation and manufacturing are vulnerable to increasing cyber attacks. By 2025, the value of cybercrime is expected to be $10.5 trillion annually, and the attacks are likely to include those targeting the IoT/IIoT. [3] reported that the average cost of an industrial data breach is $4,240,000.

The IIoT architecture is layered, and it has Edge, Middleware, Application, IT/OT and Cloud Services layers each with its own set of vulnerabilities. The Edge Layer is vulnerable to physical manipulation, the Middleware to unauthorized API access and the Application to malware attacks. The IT/OT Layer faces insider threats and the Cloud Layer is exposed to continuous threats and significant breaches [4],[5]. It is not an unreasonable fear, as there have been real-world examples of this happening: the Mirai botnet, which attacked IoT devices to launch DDoS attacks, Stuxnet, which targeted SCADA systems, and Triton, which tried to disrupt industrial safety systems in 2017.

ML based IDS have come to the fore as a counter to such threats. As opposed to classic signature-based IDS which can only be effective against known attacks, ML methods can be effective in learning patterns and anomalies to detect emerging and unknown threats. This versatility makes ML very useful in the fast-changing and diverse IoT/IIoT environment [6]. Some benchmark datasets have been created to facilitate the development of IDSs, such as UNSW-NB15 [7], CICIDS [9], DS2OS [10] and LATAM-DDOS IOT [10] among others. The emulation of real life industrial settings is of special importance, such as TON_IoT, WUSTL-IIoT-2021 and Edge-IIoTset. Despite the effectiveness of these methods, there are still problems, including the case of extreme class imbalance, in which case there are far more regular traffic than abnormalities, and the resource constraints of IIoT devices which require light and efficient models [8].

For this purpose, this study summarizes existing studies on these datasets, carries out comparative studies between supervised and ensemble ML techniques, analyzes cross-dataset transfer learning and introduces real-time traffic monitoring for intrusion detection in IoT and IIoT environments.

II. RELATED WORK

Intrusion detection in IoT and IIoT systems has been extensively studied and researchers have used ML and DL techniques to fight sophisticated attacks. Mesadieu, Torre, and Chennamaneni [11] proposed a reinforcement learning based IDS for SCADA systems that is able to respond to dynamic threats with less need on labeled data. Similarly,

***Corresponding Author:**
Received: 13th July, 2026; Revised: 27th July, 2026; Accepted: 20th August, 2026; Available Online: 31th August, 2026
(DOI): 10.70102/AEJ.2026.18.4s.44

Eid et al. [12] concluded that preprocessing and balancing techniques can have an impact on the performance of classifiers on imbalanced data. In [13] the authors Eid et al. optimized CNN using multi-class SMOTE to increase the detection accuracy of minority classes and demonstrated the effectiveness of using synthetic oversampling and DL for improving the detection accuracy.

There are also suggestions of lightweight IDS for resource constrained IoT nodes. Farea and Küçük [14] developed a Machine Learning based IDS using Cooja simulator and focuses on the viability of the IDS in limited situations. In this context, Alshehri et al. [15] introduced a self-attention based deep CNN for IIoT, in which the attention mechanisms were introduced to model long-term dependence in traffic, and obtained superior results compared to the traditional CNNs.

Survey studies have a broader perspective. Bansal and Singhrova [16] compared the IDS techniques used in IoT/IIoT and highlighted issues like lightweight deployment, explainability and scalability. Nuaimi et al. [17] in a systematic study classified IDS based on ML and DL and highlighted a number of research gaps such as cross-dataset evaluation and explainability. The studies provide future study opportunities by identifying the deficits in development of IDS as it stands now.

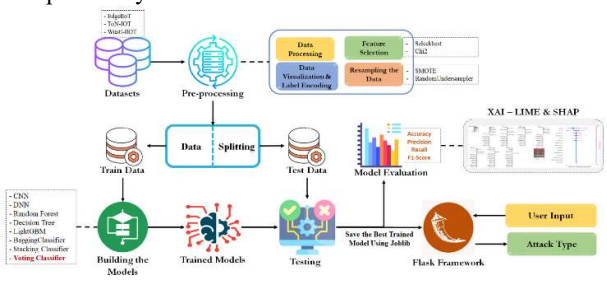
IDS research is still based on datasets. Guo et al. [18] tested models on the TON_IoT dataset and showed its suitability to benchmark real-world IIoT traffic. In order to increase the level of privacy provided by IDS, Belarbi et al. [19] presented a federated DL system which allows for distributed training without sharing the raw data. This method ensured the decentralized IoT network was scalable, secure and reliable.

The need for explainability and resilience for the use of IDS in safety-critical environments is growing. Oseni et al. [20] proposed an explainable DL intrusion detection system (IDS) for mobility in IoT. They adopted a methodology that combined interpretable AI with DL, addressing skepticism and accountability issues while providing transparency in prediction.

In general, the literature displays an evolution from traditional ML to advanced DL, reinforcement learning, federated learning and explainable AI. Researchers point to lack of data uniformity, low deployment complexity for IoT devices and transparency, privacy. The works illustrate the advances made and the challenges that lie ahead in developing full-fledged IDS for an IoT/IoE context.

III. Materials And Methods

The proposed system provides an efficient intrusion detection scheme with benchmark datasets, such as ToN-IoT, WUSTL-IIoT-2021 and Edge-IIoTset, for IoT and IIoT domains. It incorporates different ML and DL models such as [21] RF, DT, LightGBM, Bagging Classifier, Stacking Classifier, XGBoost, CNN, DNN and baseline models for comparison. This framework systematically trains and tests these algorithms to assess their capabilities of predicting anomalies and harmful behavior. We have designed a Flask based front end to allow us to provide real-time user interaction and intrusion prediction for usability. Additionally, the system uses [22] Voting Classifier ensemble, class balance techniques and explainable AI methods such as SHAP and LIME to enhance the interpretability and the level of features.



"Fig. 1. System Architecture"

The Fig.1 shows a ML pipeline for IoT security. The raw data sets are pre-processed, feature selected (Chi2) and re-sampled (SMOTE). Different models like CNN, Voting Classifiers are trained and evaluated after splitting the data. The best model is picked with evaluation metrics using joblib. The model is deployed using Flask to detect and interpret the real-time attack using XAI.

A) Dataset Collection

*i) EdgeIIoT:*EdgeIIoT dataset is a benchmark dataset for intrusion detection system in IoT and IIoT networks. [23]. It has 32,404 instances and 55 features which capture network traffic and protocol level characteristics like as TCP, UDP, DNS, MQTT and Modbus connections. The attacks included in the dataset are DDoS (UDP, ICMP, TCP), Port Scanning, Ransomware, Vulnerability Scanners and Password. It has a lot of negative traffic patterns present and can be employed as a comprehensive tool to test ML & DL-based real-time IDS models.

	frame.time	ip.src_host	ip.dst_host	arp.dst.proto_ipv4	arp.opcode	arp.hw.size	arp.src.proto_ipv4	icmp.checksum	icmp.seq_le
0	1.707159e+09	0	0	0	0	0	0	0	0
1	1.707159e+09	0	0	0	0	0	0	0	0
2	1.707159e+09	0	0	0	0	0	0	0	0
3	1.707159e+09	0	0	0	0	0	0	0	0
4	1.707159e+09	0	0	0	0	0	0	0	0

5 rows × 63 columns

Fig.2. EdgeIIoT Dataset

*ii) ToN-IoT:*The ToN-IoT dataset is a large-scale intrusion detection benchmark dataset for IoT environments. It has 190474 data points of 20 attributes. [24]. It contains various network information like ports, protocols, packet information, connection states, DNS information, and HTTP traffic. This Set contains 10 categories: normal, scanning, DDoS, injection, password, DoS, backdoor, XSS, ransomware and MITM attacks. ToN-IoT provides a well-balanced infrastructure for IEEE 802.11ae (Wi-Fi 6) heterogeneous traffic, as well as cyberattacks, and is an essential tool for training and evaluating intrusion detection algorithms.

	src_ip	src_port	dst_ip	dst_port	proto	service	duration	src_bytes	dst_bytes	conn_state	...	http_response_body_len	http_status_code
0	192.168.1.37	4444	192.168.1.193	49178	tcp	-	290.371539	101568	2592	OTH	...	0	0
1	192.168.1.193	49180	192.168.1.37	8080	tcp	-	0.000102	0	0	REJ	...	0	0
2	192.168.1.193	49180	192.168.1.37	8080	tcp	-	0.000148	0	0	REJ	...	0	0
3	192.168.1.193	49180	192.168.1.37	8080	tcp	-	0.000113	0	0	REJ	...	0	0
4	192.168.1.193	49180	192.168.1.37	8080	tcp	-	0.000130	0	0	REJ	...	0	0

5 rows × 44 columns

Fig.3. ToN-IoT Dataset

*iii) WUSTL-IIoT:*The WUSTL-IIoT 2021 dataset has been a comprehensive testbed of intrusion detection in the field of IIoT. There are 1,194,464 records and 45 characteristics. [25] It records extensive network flow features like packet and byte counts, jitter, loss rate, protocol behavior and application-level information. There are 5 types of traffic in the data set: regular, DoS, reconnaissance, command injection and backdoor attacks. WUSTL-IIoT 2021 is a

large scale industrial IoT network traffic dataset for supporting intrusion detection research and for facilitating an effective evaluation of ML and DL models.

	StartTime	LastTime	SrcAddr	DstAddr	Mean	Sport	Dport	SrcPkts	DstPkts	TotPkts	...	SAppBytes	DAppBytes	TotAppByte	SynAck	RunTime	sTos	SrcWinAct	DstWinAct	Traffic
0	2019-08-19 12:23:28	2019-08-19 12:23:28	192.168.0.20	192.168.0.2	0	59034	502	10	8	18	...	24	20	44	0.001176	0.053037	0	0.000000	0.0	normal
1	2019-08-19 15:13:24	2019-08-19 15:13:24	192.168.0.20	192.168.0.2	0	55841	502	10	8	18	...	24	20	44	0.001308	0.052681	0	0.000000	0.0	normal
2	2019-08-19 13:41:31	2019-08-19 13:41:31	192.168.0.20	192.168.0.2	0	63774	502	10	8	18	...	24	20	44	0.000690	0.051760	0	0.000000	0.0	normal
3	2019-08-19 12:43:19	2019-08-19 12:43:20	209.240.235.92	192.168.0.2	0	61771	80	4	0	4	...	0	0	0	0.000000	0.089555	0	419.338613	0.0	DoS
4	2019-08-19 14:49:44	2019-08-19 14:49:48	192.168.0.20	192.168.0.1	3	0	0	14	0	14	...	476	0	476	0.000000	3.500055	0	525.146562	0.0	normal

5 rows × 49 columns

Fig.4. Wustl-IIOT Dataset

B) Pre-Processing:

*i) Data preprocessing:*Data preprocessing involves converting data into a form that can be used and removing any Null Values, Duplicates, Outliers etc. to prevent bias, remove duplicates and prevent unrealistic traffic patterns due to the presence of outliers. This eliminates features like IP address or timestamp, which are redundant, thus reducing noise, dimensionality, and computational complexity, allowing models to focus on the most important features for accurate and effective intrusion detection.

*ii) Data Visualization:*In IoT/IIoT, data visualization can be used to analyze feature relationships and traffic pattern. The correlations between variables are highlighted, multi-collinearity and redundancy are pointed out and the outcome visualizations show the distribution of type of attacks and the imbalances in traffic. These insights are useful for feature engineering/selection and preprocessing, and help learners to detect the relevant and representative data patterns for achieving robust intrusion detection capabilities.

*iii) Label Encoding:*The main purpose of label encoding is to numerically represent categorical information for machine learning models. Features such as protocol type, service or attack type are assigned unique numbers, and although meaning is preserved, algorithms can efficiently process them. This transformation enables the fast processing of categorical information, which leads to accurate learning and predictions in IoT and IIoT Intrusion Detection Systems.

*iv) Feature Selection:*Feature Selection reduces the number of dimensions by using only informative features and discards the redundant ones. It employs techniques like SelectKBest using chi-squared tests to identify good feature-label relationships. The technique improves interpretability and reduces the training time required to get good performance, while keeping intrusion detection models accurate, efficient and successful at recognizing advanced attack patterns.

*v) Data Resampling:*Class imbalance problem is addressed in intrusion detection data sets by data resampling. There are methods such as SMOTE (over-sampling minority classes) and RandomUnderSampler (under-sampling majority classes) to balance the classes. It does not introduce any bias to the classifier, makes the classifier more sensitive to rare threats and enhances the precision, recall and F1-scores. Balanced data is beneficial for fair learning and is useful for improving model performance for several attack classes.

C) Training and Testing:

The model performance may be properly evaluated if the dataset is divided into training and testing subsets. In most cases, it goes into training, where algorithms learn about patterns and relationships in the IoT and IIoT data. The testing set is held out from training, thus giving an unbiased evaluation of the prediction power. This is applied to verify the generalization of intrusion detection models in real world scenarios through the evaluation of important metrics like accuracy, recall, precision and F1 score.

D) Algorithms

*Convolutional Neural Network (CNN):*CNNs learn spatial hierarchies of information from network data to detect complicated patterns and anomalies. It enables high precision intrusion detection, near real-time response and resilience to attacks, which can be identified through their subtle fingerprints in huge datasets, and offers rapid processing of huge data sets.

$$\square(\square,\square) = \sum_{\square}\sum_{\square} \square(\square+\square,\square+\square)\cdot\square(\square,\square) \quad (1)$$

*Deep Neural Network (DNN):*The complex nonlinear interaction of the features of IoT and IIoT is represented by DNN, which has several hidden layers. It is able to capture complex feature interactions, classifies normal as well as harmful activity, adapts to various data sets, and offers reliable anomaly detection with improved accuracy and real-time performance.

*Random Forest (RF):*RF fuses predictions from a multitude of decision trees built on randomly selected features, resulting in greater stability, reduced overfitting, high dimensional data support, support for class imbalance, and interpretable feature importance for accurate and resilient intrusion detection.

$$\square\square\square\square = 1 - \sum_{\square=1}^{\square} (\square\square)^2 \quad (2)$$

*Decision Tree (DT):*DT hierarchically partitions data into rules that are easy to interpret and can be used to rapidly and accurately identify regular and malicious traffic. [26] It can easily handle category and numerical features and is used as a base for ensemble models.

$$\square\,(\square) = 1 - \sum_{\square=1}^{\square} \square_{\square}^2 \quad (3)$$

*LightGBM:*LightGBM constructs sequential gradient boosted trees to correct the mistakes of the previous trees, and it is efficient to deal with huge dimensional and imbalanced network data. It enhances the accuracy of detection, provides feature importance evaluation and enables fast, scalable and resilient intrusion monitoring.

*Bagging Classifier:*Bagging creates numerous base classifiers using random samples of the data, which decreases variance and overfitting. It enhances generalization, deals with imbalanced classes, reinforces detection of different assaults and guarantees scalable, interpretable and reliable categorization of network traffic.

*Stacking Classifier:*The stacking method uses multiple base models and a meta-learner, and takes advantage of the strengths of the various classifiers. It reduces bias, variance, and boosts generalization, provides better identification of complex incursions, and ensures robust high accuracy classification in different IoT and IIoT datasets.

$$\hat{\square} = \square(\square_{\square\square\square\square}) = \square\big(\square_1(\square),\square_2(\square),\ldots,\square_{\square}(\square)\big) \quad (4)$$

*Voting Classifier:*Multiple classifiers are used in voting, which is applied to combine multiple classifiers, so that it is more resilient and accurate. It takes advantage of the free functionalities of the models, addresses the issue of class imbalance, and provides trustworthy, understandable and scalable real-time detection of normal and malicious network traffic.

$$\hat{□} = □□□□□□_{□}\left(\sum_{□=1}^{□} □□\,(\hat{□}_{□} = □)\right) \quad (5)$$

E) Integration of XAI and Flask Framework:

The system incorporates the explainable AI (XAI) techniques and also has an easy to use user interface developed by utilizing the Flask framework. It has registration and login process in the front-end with a SQLite database to ensure secure interaction with the system. Network feature values provided by the users are the input to the system. The input is preprocessed and fed to the trained ML models. These models then analyse the data and predict intrusion detection. The result is presented in a simple way on the front end which allows the possibility to use and access at real time.

The system is complemented with the Voting Classifier ensemble to boost the predicted accuracy and resilience. Additionally, feature dependency and importance can be explained using XAI methods such as LIME and SHAP, which offer model interpretable explanations of the decision-making process. The combination of cutting-edge ensemble learning and feature explainability offers a sensitive detection capability that is also explainable and justifiable, thus elevating the trust and insight levels of users in IoT and IIoT network security contexts.

IV. Experimental Results

*Accuracy:*The accuracy of the test is its ability to correctly identify the patient and healthy cases. We should find out how many true positives and true negatives there are in all the cases we looked at to find out how accurate a test is. In Maths, this can be expressed as:

$$Accuracy = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} (6)$$

*Precision:*Precision considers the percentage of correctly classified occurrences or samples, compared to the total number of occurrences or samples that were labeled as positive. So, the formula of determining the precision is:

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} (7)$$

*Recall:*Recall in ML is a measure of the ability to identify all of the instances of a particular class that are important. It's the proportion of the positive observations correctly predicted to all the positive observations, meaning the percentage of "all" values in one class that were correctly predicted.

$$Recall = \frac{\text{TP}}{\text{TP} + \text{FN}} (8)$$

*F1-Score:*The F1 score is a way to quantify how accurate a ML model is. Composes the accuracy and recall values of the model. Accuracy is the proportion of times that a model made a correct prediction in the entire data set.

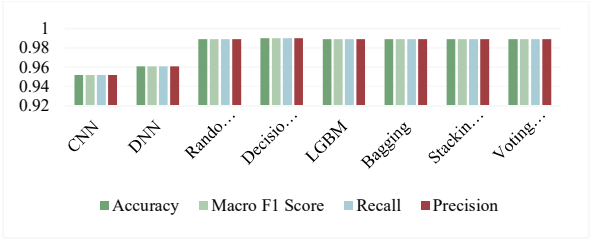
$$F1\ Score = 2 * \frac{Recall\ \text{X}\ Precision}{Recall + Precision} * 100 (9)$$

"Table.1 Performance Evaluation – Wustl-IIoT 2021 Dataset"

ML Model	Accuracy	Macro F1 Score	Recall	Precision
CNN	0.952	0.952	0.952	0.952
DNN	0.961	0.961	0.961	0.961
Random Forest	0.989	0.989	0.989	0.989
Decision Tree	0.990	0.990	0.990	0.990
LGBM	0.989	0.989	0.989	0.989
Bagging	0.989	0.989	0.989	0.989
Stacking Classifier	0.989	0.989	0.989	0.989
Voting Classifier	**0.989**	**0.989**	**0.989**	**0.989**

As presented in Table.1, the overall performance in IoT/IIoT intrusion detection is best at DT, having the highest prediction accuracy.

Fig.5. Comparison Graph – Wustl-IIoT 2021 Dataset



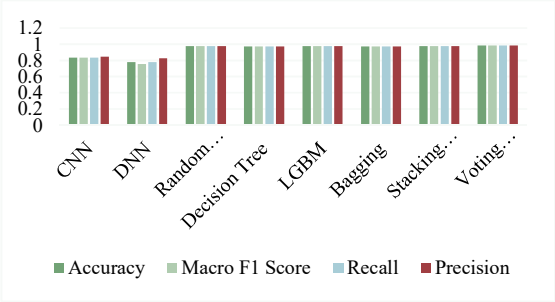
The highest metrics obtained by DT with 0.990 is shown in fig.5. Green means Accuracy, light green means Precision, blue means Recall and red means Macro F1 Score.

"Table.2 Performance Evaluation – ToN-IoT dataset"

ML Model	Accuracy	Macro F1 Score	Recall	Precision
CNN	0.837	0.836	0.837	0.845
DNN	0.779	0.755	0.779	0.825
Random Forest	0.976	0.976	0.976	0.976
Decision Tree	0.972	0.972	0.972	0.973
LGBM	0.977	0.977	0.977	0.977
Bagging	0.973	0.973	0.973	0.973
Stacking Classifier	0.978	0.978	0.978	0.978
Voting Classifier	**0.984**	**0.984**	**0.984**	**0.985**

Table.2 indicates that Voting Classifier has the best performance in the categorization of network intrusions for IoT and IIoT setting, demonstrating the robustness and accuracy of the system.

Fig.6. Comparison Graph – ToN-IoT Dataset



The best performance is obtained for the Voting Classifier as seen in fig.6. Green denotes Accuracy, red for Precision, blue for Recall and light green for Macro F1 Score. This helps to highlight the differences between models.

Table.3 Performance Evaluation – Edge-IIoT dataset

ML Model	Accuracy	Macro F1 Score	Recall	Precision
CNN	0.938	0.938	0.938	0.938
DNN	0.944	0.941	0.944	0.954
Random Forest	0.963	0.963	0.963	0.969
Decision Tree	0.966	0.965	0.966	0.972
LGBM	0.966	0.966	0.966	0.973
Bagging	0.966	0.965	0.966	0.973
Stacking Classifier	0.966	0.965	0.966	0.973
Voting Classifier	**0.967**	**0.967**	**0.967**	**0.972**

The Voting Classifier in Table.3 has the best overall performance, which means that it outperforms the other models studied.

Fig.7. Comparison Graph – Edge-IIoT Dataset

Voting Classifier is the best performing model with the accuracy in green, Macro F1 Score in light green, Recall in blue and Precision in red as seen in the models analyzed in fig.7.

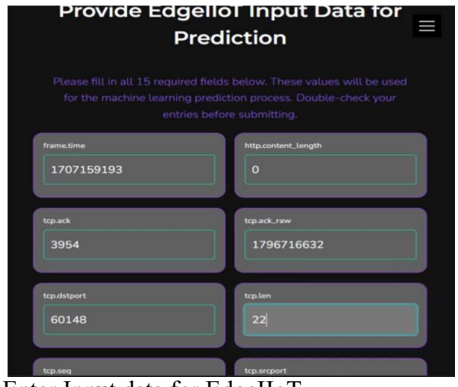


Fig.8. Enter Input data for EdgeIIoT

In Fig.8, users input the values of EdgeIIoT dataset to detect and classify certain network attack types by the system.

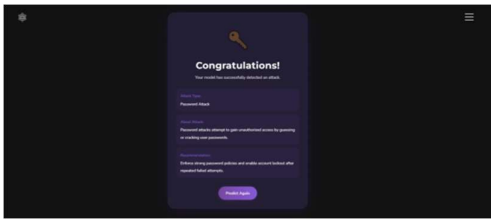


Fig.9. Predicted Results for EdgeIIoT

The system processes the EdgeIIoT input and correctly identifies that it is a " Password Attack" in Fig.9.

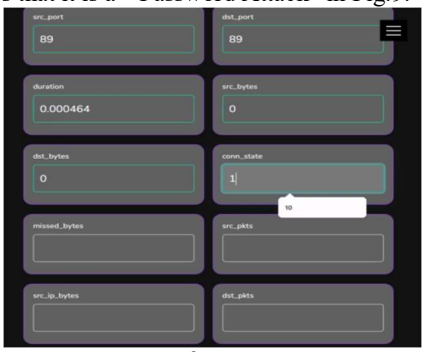


Fig.10. Enter Input Data for ToN-IOT

The users enter the values of the ToN-IoT datasets in Fig.10. The system is able to analyze the network traffic and to detect particular sorts of attacks.

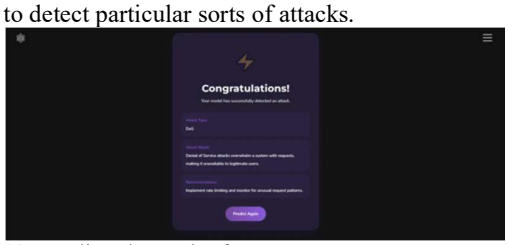


Fig.11. Predicted Results for ToN-IOT

The system analyzes the ToN-IoT input and accurately classifies network intrusion as a DOS attack as shown in Fig.11.

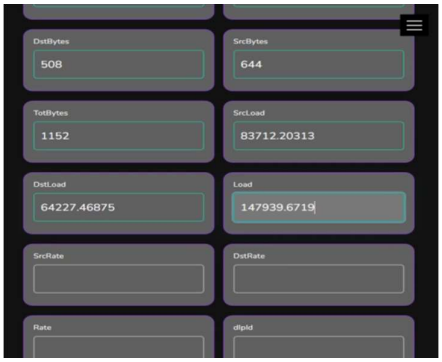


Fig.12. Enter Input Data for Wustl-IIOT

In Fig.12, the user provides the data from the WUSTL-IIoT dataset and the system is able to analyze the network traffic and identify some type of attack.

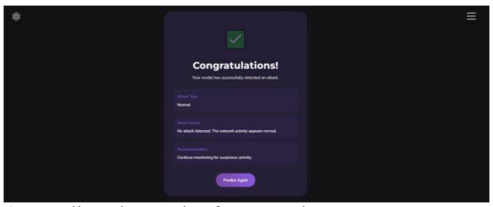


Fig.13. Predicted Results for Wustl-IIOT

With WUSTL-IIoT input to the system as shown in Fig.13, the system is able to classify the network activity as normal and hence it is not detected as an attack.

V. CONCLUSION

This research demonstrates the effectiveness of hybridization of lightweight machine learning algorithms with ensemble methods in resilient intrusion detection in IoT and IIoT. High dimensional and imbalanced network traffic could be dealt with by extensive preprocessing steps, chi-square feature selection and undersampling or SMOTE class balancing on various datasets. Ensemble methods, when combined with individual classifiers, evinced a huge improvement in both detection and generalization reliability. The Voting Classifier proved to be resistant to heterogeneous attacks and achieved a voting accuracy of 98.4%, 98.9%, and 96.7% on ToN_IoT, WUSTL-IIoT 2021, and Edge-IIoTset, respectively. explainable AI tools SHAP and LIME enhanced transparency, while the Flask implementation on SQLite facilitated real-time, interpretable and secure intrusion detection for practical IoT and IIoT cybersecurity monitoring.

For future work, we would like to implement this ML based intrusion detection system on microcontroller platforms for IoT and IIoT and test it in real-world scenarios. Emphasis will be on energy efficiency, latency, adaptability and computational optimization. The integration with lightweight security protocols and edge intelligence will enhance the scalability, resilience and practicality, delivering strong, accurate and efficient intrusion detection in industrial and large scale IoT deployments.

REFERENCES

[1] Alam, K., Monir, M. F., Hassan, Z., & Habib, M. T. (2024, October). Optimizing IoT Network Intrusion Detection: A Deep Learning Approach. In 2024 7th Conference on Cloud and Internet of Things (CIoT) (pp. 1-5). IEEE.

[2] Lazzarini, R., Tianfield, H., & Charissis, V. (2023). A stacking ensemble of deep learning models for IoT intrusion detection. Knowledge-Based Systems, 279, 110941.

[3] Kim, Y. G., Ahmed, K. J., Lee, M. J., & Tsukamoto, K. (2022, August). A Comprehensive Analysis of Machine Learning-Based Intrusion Detection System for IoT-23 Dataset. In International Conference on Intelligent Networking and Collaborative Systems (pp. 475-486). Cham: Springer International Publishing.

[4] Morshedi, R., Matinkhah, S. M., & Sadeghi, M. T. (2024). Intrusion detection for IoT network security with deep learning. Journal of AI and Data Mining, 12(1), 37-55.

[5] Eren, K. K., Küçük, K., Özyurt, F., & Alhazmi, O. H. (2025). Simple Yet Powerful: Machine Learning-Based IoT Intrusion System With Smart Preprocessing and Feature Generation Rivals Deep Learning. IEEE Access.

[6] J. A. Beauty Angelin and C. Priyadharsini, ‘‘Deep learning based network based intrusion detection system in industrial Internet of Things,’’ in Proc. 2nd Int. Conf. Intell. Data Commun. Technol. Internet Things (IDCIoT), Jan. 2024, pp. 426–432.

[7] M. Ramaiah and M. Y. Rahamathulla, ‘‘Securing the industrial IoT: A novel network intrusion detection models,’’ in Proc. 3rd Int. Conf. Artif. Intell. For Internet Things (AIIoT), May 2024, pp. 1–6.

[8] S. I. Popoola, A. L. Imoize, M. Hammoudeh, B. Adebisi, O. Jogunola, and A. M. Aibinu, ‘‘Federated deep learning for intrusion detection in consumer-centric Internet of Things,’’ IEEE Trans. Consum. Electron., vol. 70, no. 1, pp. 1610–1622, Feb. 2024.

[9] Z. Ahmed and S. S. Askar, ‘‘EdgeGuard: Machine learning for proactive intrusion detection on edge networks,’’ Artif. Intell. Cybersecurity, vol. 1, pp. 37–43, Jun. 2024.

[10] R. S. Tiwari, D. Lakshmi, T. K. Das, A. K. Tripathy, and K.-C. Li, ‘‘A lightweight optimized intrusion detection system using machine learning for edge-based IIoT security,’’ Telecommun. Syst., vol. 87, no. 3, pp. 605–624, Nov. 2024.

[11] ***F. Mesadieu, D. Torre, and A. Chennamaneni, ‘‘Leveraging deep reinforcement learning technique for intrusion detection in SCADA infrastructure,’’ IEEE Access, vol. 12, pp. 63381–63399, 2024.***

[12] ***A. M. Eid, B. Soudan, A. B. Nassif, and M. Injadat, ‘‘Comparative study of ML models for IIoT intrusion detection: Impact of data preprocessing and balancing,’’ Neural Comput. Appl., vol. 36, no. 13, pp. 6955–6972, May 2024.***

[13] ***A. M. Eid, B. Soudan, A. B. Nassif, and M. Injadat, ‘‘Enhancing intrusion detection in IIoT: Optimized CNN model with multi-class SMOTE balancing,’’ Neural Comput. Appl., vol. 36, no. 24, pp. 14643–14659, Aug. 2024.***

[14] ***A. H. Farea and K. Küçük, ‘‘Machine learning-based intrusion detection technique for IoT: Simulation with cooja,’’ Int. J. Comput. Netw. Inf. Secur., vol. 16, no. 1, pp. 1–23, Feb. 2024.***

[15] M. S. Alshehri, O. Saidani, F. S. Alrayes, S. F. Abbasi, and J. Ahmad, ‘‘A self-attention-based deep convolutional neural networks for IIoT networks intrusion detection,’’ IEEE Access, vol. 12, pp. 45762–45772, 2024.

[16] K. Bansal and A. Singhrova, ‘‘Review on intrusion detection system for IoT/IIoT-brief study,’’ Multimedia Tools Appl., vol. 83, no. 8, pp. 23083–23108, Aug. 2023.

[17] M. Nuaimi, L. C. Fourati, and B. B. Hamed, ‘‘Intelligent approaches toward intrusion detection systems for industrial Internet of Things: A systematic comprehensive review,’’ J. Netw. Comput. Appl., vol. 215, Jun. 2023, Art. no. 103637.

[18] ***G. Guo, X. Pan, H. Liu, F. Li, L. Pei, and K. Hu, ‘‘An IoT intrusion detection system based on TON IoT network dataset,’’ in Proc. IEEE 13th Annu. Comput. Commun. Workshop Conf. (CCWC), Mar. 2023, pp. 0333–0338.***

[19] O. Belarbi, T. Spyridopoulos, E. Anthi, I. Mavromatis, P. Carnelli, and A. Khan, ‘‘Federated deep learning for intrusion detection in IoT networks,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), vol. 3125, Dec. 2023, pp. 85–99.

[20] ***A. Oseni, N. Moustafa, G. Creech, N. Sohrabi, A. Strelzoff, Z. Tari, and I. Linkov, ‘‘An explainable deep learning framework for resilient intrusion detection in IoT-***

enabled transportation networks,'' IEEE Trans. Intell. Transp. Syst., vol. 24, no. 1, pp. 1000–1014, Jan. 2023.

[21] ***D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, ''Intrusion detection system using feature extraction with machine learning algorithms in IoT,'' J. Sensor Actuator Netw., vol. 12, no. 2, p. 29, Mar. 2023.***

[22] M. M. Shtayat, M. K. Hasan, R. Sulaiman, S. Islam, and A. U. R. Khan, ''An explainable ensemble deep learning approach for intrusion detection in industrial Internet of Things,'' IEEE Access, vol. 11, pp. 115047–115061, 2023.

[23] M. Wang, N. Yang, and N. Weng, ''Securing a smart home with a transformer-based IoT intrusion detection system,'' Electronics, vol. 12, no. 9, p. 2100, May 2023.

[24] S. Li, G. Chai, Y. Wang, G. Zhou, Z. Li, D. Yu, and R. Gao, ''CRSF: An intrusion detection framework for industrial Internet of Things based on pretrained CNN2D-RNN and SVM,'' IEEE Access, vol. 11, pp. 92041–92054, 2023.

[25] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, and M. Elsharief, ''A federated learning-based approach for improving intrusion detection in industrial Internet of Things networks,'' Network, vol. 3, no. 1, pp. 158–179, Jan. 2023.

[26] ***A. M. Eid, A. B. Nassif, B. Soudan, and M. N. Injadat, ''IIoT network intrusion detection using machine learning,'' in Proc. 6th Int. Conf. Intell. Robot. Control Eng. (IRCE), Aug. 2023, pp. 196–201.***

[27] T. Gaber, J. B. Awotunde, S. O. Folorunso, S. A. Ajagbe, and E. Eldesouky, ''Industrial Internet of Things intrusion detection method using machine learning and optimization techniques,'' Wireless Commun. Mobile Comput., vol. 2023, pp. 1–15, Apr. 2023.

[28] ***B. Xu, L. Sun, X. Mao, R. Ding, and C. Liu, ''IoT intrusion detection system based on machine learning,'' Electronics, vol. 12, no. 20, p. 4289, Oct. 2023.***

[29] Z. Benamor, Z. A. Seghir, M. Djezzar, and M. Hemam, ''A comparative study of machine learning algorithms for intrusion detection in IoT networks,'' Revue d'Intell. Artificielle, vol. 37, no. 3, pp. 567–576, Jun. 2023.

[30] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, ''X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things,'' IEEE Internet Things J., vol. 9, no. 5, pp. 3962–3977, Mar. 2022.