An Empirical Evaluation of Machine Learning Algorithms for Intrusion Detection in IIoT Networks

Mangesh Matke, Kumar Saurabh, Uphar Singh
Indian Institute of Information Technology, Allahabad, India
mangeshmatke9@gmail.com, pwc2017001@iiita.ac.in, pse2017003@iiita.ac.in

2023 IEEE 20th India Council International Conference (INDICON) | 979-8-3503-0559-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/INDICON59947.2023.10440779

***Abstract*—Industry's reliance on IoT has skyrocketed as the technology has developed and has transformed into the Industrial IoT (IIoT). The IIoT has brought significant benefits to the industry, including increased safety, efficiency, etc. These advancements are accompanied by security challenges such as large exposed attack areas in IIoT devices, therefore it has become increasingly important to use mechanisms to detect any attack or breach on the IIoT networks. An increasing corpus of research acknowledges the value of machine learning methods for anomaly detection. This paper highlights the importance of machine learning in anomaly detection in IIoT networks, provides a literature review of the implementations of ML algorithms in IIoT networks in the last decade, and finally a comparative study of ML algorithms for anomaly detection in IIoT network data. Support Vector Machine (SVM), Linear Regression (LR), K-nearest neighbor (KNN), and Random Forest (RF) are only a few of the ML techniques utilized in comparative analysis. Results of the comparative analysis show that RF algorithm works best for anomaly detection and the results of RF and KNN are comparable in multi-class classification.**

***Index Terms*—Industrial Internet of Things (IIoT), ToN-IoT, Machine Learning, Intrusion Detection System**

I. Introduction

The number of Internet-connected gadgets or "Things" (devices or sensors), also referred as the "Internet of Things(IoT)" is expanding quickly. IoT devices are becoming increasingly important in networks and industries. There is a rapid development of applications related to the IoT applications in a variety of industrial sectors, including the automobile and smart home systems, applications for spaceflight, healthcare, industry, and retail [4]. This poses numerous new security concerns and challenges [6]. IIoT exploits IoT in industrial frameworks to increase efficiency, log data, etc with the devices connected to the IIoT network. Owing to the usage of numerous protocols in IIoT, the number of trust boundaries is more, making the devices vulnerable to unauthorized access. Therefore, it becomes crucial to secure these networks from attackers Fig.1.

To secure the networks, intrusion detection methods have achieved great success. The different methods that can be used for detection are anomaly detection and signature-based methods. In signature-based methods, attackers are detected based on a signature i.e., an existing pattern in the data. In signature-based methods, it is quite difficult to detect newer attacks due to new signatures. In anomaly detection methods, a trust model is generated based on the given data and any data point not aligning with the trust model is regarded as an attack point.

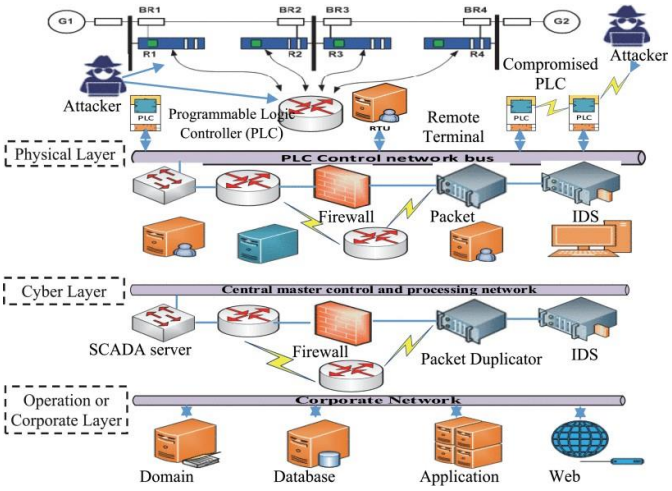

Fig. 1: A Cyber-attack Scenario on Industrial Control Network [21]

Verifying that these new detection models are accurate nevertheless, is still difficult, because of a lack of publicly accessible sets with proper feature sets. Also, the datasets used for model training are also too old with fewer attack vectors. This limitation doesn't always also. The key challenges in developing such data sets derive from:

1) IoT devices typically produce a lot less traffic than computers and servers in normal networks
2) The ongoing introduction of new "Things" on the Internet that constantly evolving traffic and attack kinds created.

The proposed work is to create new trust models using machine learning(ML) for anomaly detection in the network layer of IIoT. The manuscript addresses the following research problems.

1) **Importance of securing IIoT networks:** The paper highlights the need for securing Industrial Internet of Things (IIoT) networks from potential attackers. This raises the research problem of identifying effective security measures and intrusion detection techniques tailored to IIoT environments.
2) **Automatic Intrusion Detection methods for IIoT networks:** This manuscript discusses the significance

of using automatic intrusion detection methods for IIoT networks. This suggests a research problem of exploring and evaluating various automated approaches for detecting and mitigating intrusions in IIoT systems.

3) **Use of Realistic IIoT Dataset:** The TON-IoT dataset was developed to closely resemble real-world IIoT network traffic, making it ideal for testing IDS solutions in manufacturing environments. This guarantees that the IDS is put through its paces under testing conditions that are indicative of those found in real-world IIoT implementations.
4) **Use of ML frameworks for intrusion detection in IIoT systems:** The literature review covers the application of ML frameworks for intrusion detection in IIoT systems.
5) **Comparative analysis of implemented ML algorithms:** The paper presents a comparative analysis of different ML models implemented for intrusion detection in IIoT networks. This raises the research problem of evaluating and comparing the performance, accuracy, and efficiency of these algorithms to determine the most effective approach for IIoT intrusion detection.

The rest of the paper consists of a literature survey of the implementation of ML frameworks for intrusion detection in IIoT systems in section II, followed by the methodology section, which contains the description of the ML models used in section III. The results have been discussed in section IV and the conclusion of the work is summarized in section V.

II. Literature Review

As the IIoT is evolving rapidly, new surfaces for attacks are coming into existence, making the system more vulnerable to attackers. Due to the historic absence of security protocols in IIoT systems, the systems are blindsided and left exposed to attackers. This calls for the need for anomaly detection and prevention mechanisms to protect the systems from unauthorized access or attacks. ML (ML) and deep learning (DL) algorithms can be applied for anomaly detection. ML algorithms can detect patterns in the data and find any data point that does not align with the rest of the data, which can be used to classify attacks. Some research has already been conducted in the field of intrusion detection and prevention mechanisms in IIoT systems [17]–[20].

The tableI below presents a brief literature survey of the work similar to the proposed work with certain shortcomings which were proposed to address with this work. The authors in [1] have highlighted the importance and relevance of intrusion detection methods in IOT and IIOT platforms. The need for more availability of real-world datasets is cited as a major obstacle. They have simulated IIoT devices and trained ML algorithms for the devices separately. In paper [4], the authors use the same ML algorithm but on the simulated dataset of hardware breakdown to water SCADA device sabotage with 15 anomaly situations. The results are presented in the form of accuracy, precision, recall, and f1 score. In paper [2], authors have implemented the Naive Bayes algorithm and Support vector machine for intrusion detection in the NSL KDD dataset. Accuracy and misclassification rate, evaluation metrics are used for the comparative analysis of the models. The paper [3] investigates open-source ML frameworks, in an IIoT context in terms of usage, application, etc. The authors in [5] convert synthetic network data to time series data and apply three-time series-based algorithms i.e., matrix profiles, SARIMA(Seasonal Autoregressive Integrated Moving Average), and Long Short Term Memory(LSTM) based algorithms, in IIoT context as a use case. Three different time-synthetic time series datasets are used for the validation of algorithms. Matrix profiles work best with no parametrization required. The paper [6] presents the protocols used in SCADA systems, followed by the class of attacks on IIoT networks. It also gives a brief literature survey of the use of ML algorithms on IIoT datasets. Finally, a hybrid ML-based anomaly detection system is proposed with attacks like backdoor, SQL injection, and command injection. The hybrid model performs better than state-of-the-art models present in the literature. The paper [7] proposes a lightGBM architecture-based Intrusion detection system for edge-based Industrial IoT systems that are lightweight in terms of time complexity. It also presents a survey of literature based on other works related to edge-based intrusion detection mechanisms in Industrial IoT systems. The authors in [8] built an extremely Gradient Boosting (XGBoost) model to develop an intrusion detection system. The built model was validated using the datasets, TON-IoT and X-IIoTDS. One of the major challenges for the use of ML and deep learning methods is low accuracy models can not be deployed in real-world problems. The [9] discusses the pros and cons of the proposed solutions and provides a thorough evaluation of recent NIDS-based studies. The most recent developments in ML and Deep Learning (DL)-based Network Intrusion Detection Systems (NIDS) are then presented in terms of the proposed approach, selected dataset for validation and evaluation, and assessment metrics. The literature review highlights the importance of intrusion detection mechanisms. The rest of the paper presents the dataset description, a comparative study of different ML algorithms for the classification of attacks, and the identification of the class of attack.

III. Methodology

In this section, the dataset used in the proposed work of the study is discussed. The present study is based on the implementation of ML algorithms for intrusion detection in IIoT systems. Network data of the TON_IoT dataset is used for the validation of the implemented ML models.

A. Dataset Description:

The importance of using a heterogeneous dataset is stressed in the literature and a significant amount of literature is in favor of using heterogeneous datasets for anomaly detection. In this research, one such dataset i.e., the TON-IoT [1], [10]–[16] dataset is used. The table below showcases multiple datasets related to IoT and IIoT. The datasets listed are widely used by

Authors	Algorithms used	Dataset used	Contribution	Performance	Shortcomings
Abdullah AL-SAEDI et al. [1]	Logistic regression (LR), Linear Discriminant analysis(LDA), K-nearest neighbor(KNN), Classification and regression trees(RT), Random Forest (RF), Na¨ıve Bayes(NB), Support vector Machine(SVM), Long Short Term Memory (LSTM)	Telemetry dataset of TON_IoT dataset	Paper performs ML algorithms on individual devices and combined telemetry data	Accuracy: 0.88 Precision: 0.90	Only telemetry data is used. Low accuracy
Anish Halimaa A et al. [2]	Support Vector Machine, Na¨ıve Bayes	NSL KDD dataset	Applies ML algorithms	Accuracy: 97.29 Misclasification rate: 2.705	Only two algorithms are explored
Asharul Islam Khan et al. [3]	TensorFlow, Microsoft Cognitive Toolkit, Caffe, H2O, Torch and PyTorch	N/A	Investigates opensource libraries for intrusion in IIoT context	N/A	No implementation is provided
Gamal Eldin I. Selim et al. [4]	LR, LDA, KNN, NB, SVM, and Classification and Regression Tree (CART)	Simulated dataset	IDS for Water treatment plant	Accuracy: 83 Precision: 85	Attack classes are significantly less
Simon Duque Anton et al. [5]	Matrix profiles, Seasonal Autoregressive Integrated Moving Average, and Long Short Term Memory(LSTM) based algorithms	Simulated network data	Network data converted to time series data and applied ML algorithms	Accuracy: 99.5 F1 score: 40	The size of dataset used is quite small for analysis
Haipeng Yao et al. [7]	LightGBM	Not disclosed	A LightGBM architecture-based Intrusion detection system for edge-based Industrial IoT systems	Accuracy: 93.2 Precision: 99.9	The dataset used for validation are not discussed
Thi-Thu-Huong Le et al. [8]	eXtremely Gradient Boosting (XGBoost)	X-IIoTDS and TON_IoT	XGBoost based Network intrusion detection system	99.87 (X-IIoTDS) and 99.9 (TON IoT)	N/A
Abdallah R. Gad et al. [9]	LR, NB, DT, SVM, kNN, RF, AdaBoost, XGBoost	TON_IoT	IDS for Vehicular Adhoc Networks	For Random Forest: Accuracy: 97.9 Precision: 95.1 For XG-Boost: Accuracy: 99 Precision: 97.6	Performance Metrics for RF is low
Proposed Work	**LR, SVM, KNN, RF, DT**	**TON_IoT**	**IDS for Industrial IoT N/w**	**Accuracy: 99.1 Precision: 99.9**	**N/A**

TABLE I: Comparision of Literature Review Vs Proposed Work

researchers for applications like Network intrusion detection etc.

The concerned dataset contains three different data types making the dataset heterogeneous in nature. It includes ”Telemetry-data” of IoT and IIoT devices, Operating system data concerning operating systems like Windows and Ubuntu, and Network data in the form of network logs. The network data is used for testing the generated models for binary classification, to check whether a particular data accounts for an attack or a benign data point. Furthermore, multi-class classification is also implemented to find the particular class of attack for an attack if any.

B. Attack Classification

The classes of attacks in the ToN-IoT dataset comprise of:

1) Scanning attack: The attacker’s objective is to infiltrate the network by gathering information like open ports and IP addresses, serving as a precursor to subsequent attacks.
2) DoS attack: This aims to render the network inaccessible to legitimate users by flooding it with excessive information or requests, leading to a crash.
3) DDoS attack: Multiple computers collaborate to target a single machine or network, overloading its bandwidth with information or requests, ultimately causing a crash.
4) Ransomware attack: Ransomware encrypts system and service access, demanding a ransom for decryption.
5) Backdoor attack: Unauthorized access to a user’s machine is achieved, allowing the theft of sensitive information or financial data.
6) Injection attack: This involves injecting unnecessary code or fake data into a system, enabling the execution of commands to alter or extract information from the database.
7) Cross-site scripting attack: Trusted websites are compromised by injecting data that gets transmitted with user data on dynamic websites.
8) Password attack: Attackers attempt to breach password-protected systems, employing methods like guessing or brute force.
9) Man-in-the-middle attack: Attackers eavesdrop on and manipulate communications between users, creating deceptive interactions among them by altering messages.

Dataset	Year	Dataset size			Attacks	Attack classes	Features	IoT/ IIoT
		Total	Attack	Normal				
NSL-KDD	1998	4,898,431	3,925,650	972,781	4	”User to Root (U2R), Denial of Service (DoS),Probe, and Remote to Local (R2L)”	43	IoT
UNSW NB 15	2015	2,540,044	321,465	2,218,761	10	”Fuzzers, Analysis, Backdoors, DoS, Exploits, Shellcode, Generic, Reconnaissance, Worms”	49	IoT
TON-_IoT	2019	72,496,164	–	–	9	”Man in the middle, backdoor, Password, Ransomware, DoS, DDoS, Scanning, Injection, XSS”	115	IIoT
N-BaIoT	2018	7,062,606	3,394,204	3,668,402	11	Mirai, Bashlite	22	IoT
CICIDS 2017	2017	2,895,159	659,522	2,235,637	9	”DoS, DoS, Hulk, GoldenEye, DoS Slowhttptest, DoS Slowloris, Brute Force -Web, SQL, Brute Force -XSS, Injection, Infiltration, and Botnet”	80	IoT

TABLE II: Summary of IoT and IIoT Datasets

C. Proposed Methodology

The methodology of the proposed work is presented in Fig 3. The data is preprocessed by removing less correlated features, normalizing the data values, and so on. Then the enlisted ML models are implemented on the concerned data set to get the comparative analysis of the generated models. The dataset contains nominal as well as categorical values. The data was encoded as nominal values. Initially, the dataset raw log files are preprocessed for feature extraction. It involves the deletion of certain stop-words, the IP addresses of the source and destination are also mentioned. The features whose correlations with the target features were quite low were dropped from the dataset before further processing by using the Pearson correlation coefficient which is 0.3 in this case. To apply ML models on any given dataset it should have numerical values only. Some of the less co-related features and features with the most null values were dropped. Then the values with categorical values like the features containing the protocol type used in the network could be present as categorical values. All such values need to be encoded to numerical values using one-hot encoding and label encoding methods.

The TON_IoT dataset contains data from three different sources i.e.,

1) Telemetry data
2) Network data
3) Operating system data in the form of .pcap log files.

Feature extraction of such a dataset requires combining the data from various, heterogeneous sources to capture the underlying features of the data in the heterogeneous dataset. The produced model can later be validated by the realization of Intrusion Detection in IoT. The present study makes use of only network data of the concerned dataset. ML techniques are implemented on the discussed dataset to build an intrusion detection system for IIoT systems.

D. Models Used:

The ML models used are:

1) Linear Regression (LR): LR predicts one variable using another, with independent variables forecasting the dependent one. The loss function assesses model fit by comparing projected and actual results.
2) Support Vector Machine (SVM): SVM identifies the optimal multidimensional boundary for classifying new data points. It employs the outermost extremes as support vectors.
3) K-Nearest Neighbor (KNN): KNN is a straightforward supervised ML algorithm with minimal training required. It treats new data points as analogous to plotted ones, using a loss function that considers data point uncertainty. This function diminishes uncertainty by selecting the most representative data points.
4) Logistic Regression: Logistic regression predicts binary outcomes by modeling a binary dependent and one or more independent variables. It uses the sigmoid function to map input variables to probability values between 0 and 1. This approach is known for its simplicity, interpretability, and versatility.
5) Decision Tree(DT): Decision trees are widely used in supervised ML for classification and regression. They employ internal nodes for features, branches for decisions, and leaves for outcomes. The algorithm splits data based on significant attributes, using impurity reduction to rank feature relevance. Decision trees are adaptable to various data types but can overfit if too complex or with noisy data. Pruning, setting a maximum depth, and ensemble methods help mitigate this.
6) Random Forest(RF): RF is an ensemble learning system that employs numerous decision trees trained on random subsets of features. It mitigates decision tree overfitting and improves results by aggregating the votes of multiple trees. The MSE(mean squared error) serves as the common regression loss function, measuring the average squared difference between predicted and true labels across the dataset.

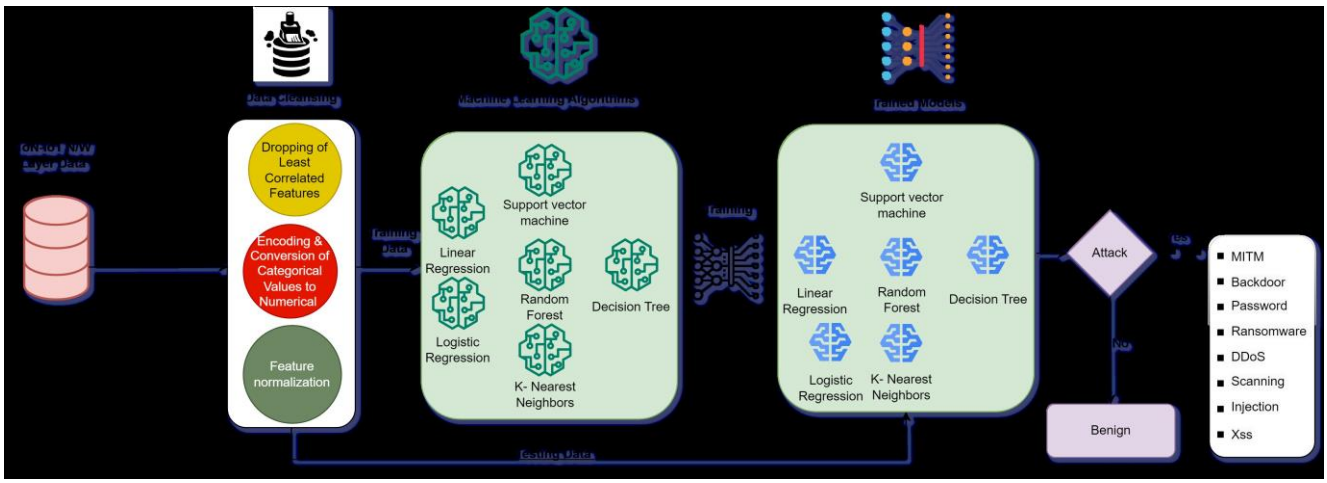

Fig. 2: Proposed methodology

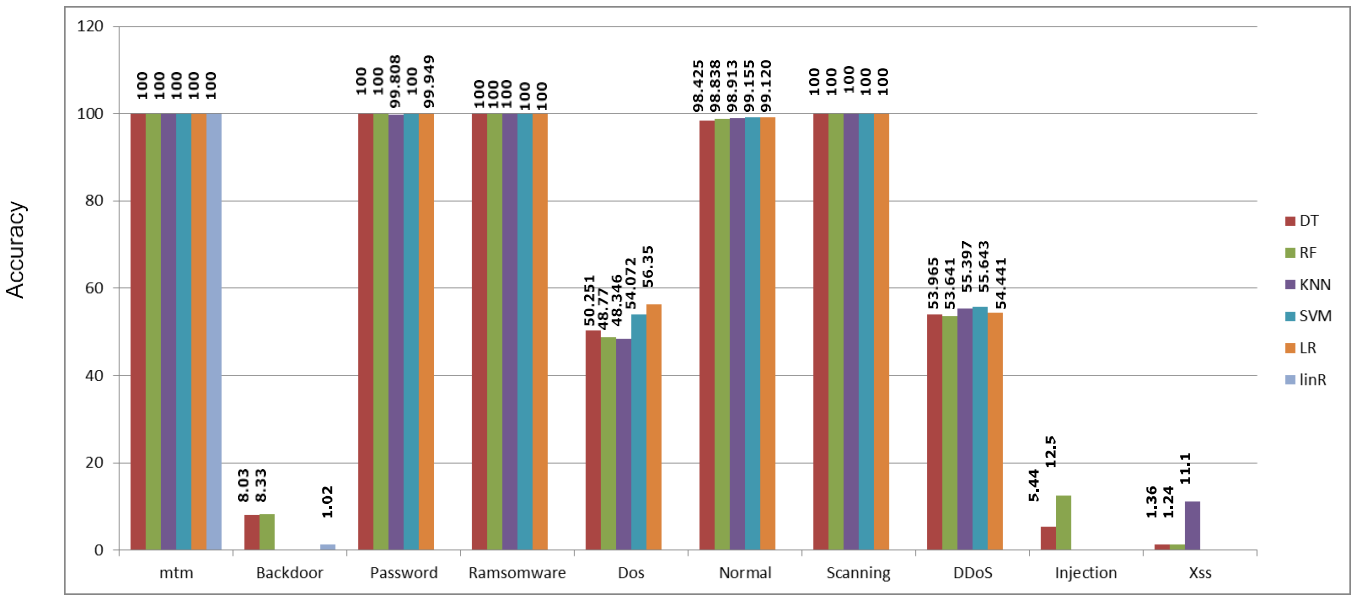

Fig. 3: Accuracy for Multi-class classification

IV. Results

The models are trained, and the ToN-IoT dataset is used to validate the models. The accuracy of the binary classification showing whether a particular tuple represents an attack or benign class data flow using multiple ML models namely LR, SVM, KNN, RF, DT is shown in Fig. 4.

The accuracy for the binary and multi-class classification is the highest for the random forest method as shown in Fig. 4and Fig. 3, its other performance metrics are also shown in Table III and Table IV.

The accuracy for the binary classification is comparable for the methods but for multi-class classification linear regression performs the worst and all other methods have comparable accuracy.

TABLE III: Binary Classification Results (Random Forest)

Class	Precision	Recall	F1-Score	Support
Normal	0.98	0.96	0.97	3,909
Attack	0.99	0.99	0.99	12,326
Accuracy			0.99	16,235
Macro Avg	0.98	0.98	0.98	16,235
Weighted Avg	0.99	0.99	0.99	16,235

V. Conclusion & Future Work

This study proposes a literature overview of the application of ML frameworks for intrusion detection in IIoT systems, highlighting the need to safeguard IIoT networks from attackers and discussing the value of autonomous intrusion detection approaches. In addition, a comparative analysis of

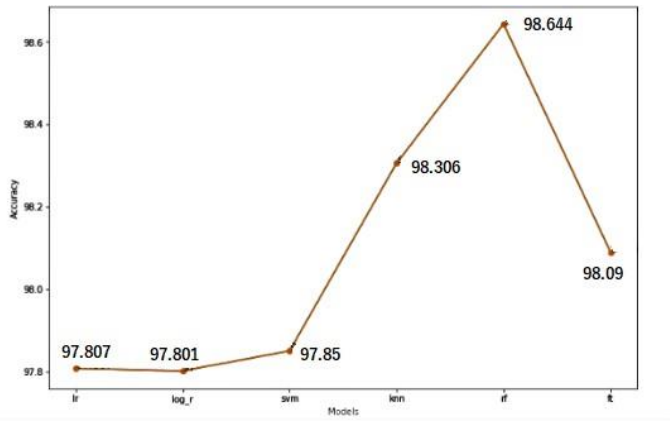

Fig. 4: Accuracy for binary classification

TABLE IV: Multi Classification Results (Random Forest)

Class	Precision	Recall	F1-Score	Support
Analysis	1.00	1.00	1.00	166
Exploits	1.00	1.00	1.00	4900
Reconnaissance	0.54	0.60	0.57	502
Backdoor	0.08	0.03	0.05	32
Generic	0.99	0.99	0.99	11839
DoS	1.00	1.00	1.00	521
Fuzzers	0.49	0.43	0.46	508
Normal	1.00	1.00	1.00	5855
Worms	0.12	0.07	0.09	29
Accuracy			0.97	24352
Macro Avg	0.69	0.68	0.68	24352
Weighted Avg	0.97	0.97	0.97	24352

the ML algorithms is presented. The accuracy for the binary classification and multi-class classification is the highest for the Random Forest model. The future work includes working on other heterogeneous datasets for validation of the models.

REFERENCES

[1] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, ”TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems,” in IEEE Access, vol. 8, pp. 165130-165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

[2] A. Halimaa A. and K. Sundarakantham, ”Machine Learning Based Intrusion Detection System,” 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 916-920, doi: 10.1109/ICOEI.2019.8862784.

[3] A. I. Khan and A. Al-Badi, “Open source machine learning frameworks for industrial internet of things,” Procedia Comput. Sci., vol. 170, pp. 571–577, 2020.

[4] G. E. I. Selim, E. E.-D. Hemdan, A. M. Shehata, and N. A. El-Fishawy, “Anomaly events classification and detection system in the critical industrial Internet of things infrastructure using machine learning algorithms - Multimedia Tools and Applications,” SpringerLink, Jan. 12, 2021. https://link.springer.com/article/10.1007/s11042-020-10354-1.

[5] S. Duque Anton, L. Ahrens, D. Fraunholz and H. D. Schotten, ”Time is of the Essence: Machine Learning-Based Intrusion Detection in Industrial Time Series Data,” 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 2018, pp. 1-6, doi: 10.1109/ICDMW.2018.00008.

[6] K. Khan, “Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things,” (PDF) Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things — Khaled Khan - Academia.edu. https://www.academia.edu/43115146/Machine _Learning Based Network Vulnerability Analysis of Industrial Internet - of_Things.

[7] H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang and L. Lu, ”Hybrid Intrusion Detection System for Edge-Based IIoT Relying on Machine-Learning-Aided Detection,” in IEEE Network, vol. 33, no. 5, pp. 75-81, Sept.-Oct. 2019, doi: 10.1109/MNET.001.1800479.

[8] T.-T.-H. Le, Y. E. Oktian, and H. Kim, “XGBoost for Imbalanced Multiclass Classification-Based Industrial Internet of Things Intrusion Detection Systems,” MDPI, Jul. 16, 2022. https://www.mdpi.com/2071-1050/14/14/8707.

[9] A. R. Gad, A. A. Nashat and T. M. Barkat, ”Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset,” in IEEE Access, vol. 9, pp. 142206-142217, 2021, doi: 10.1109/ACCESS.2021.3120626.

[10] N. Moustafa, “A new distributed architecture for evaluating AI-based security systems at the edge: Network TON _IoT datasets,” Sustainable Cities and Society, vol. 72, p. 102994, Sep. 2021, d10.1016/j.scs.2021.102994.

[11] N. Moustafa, “A new distributed architecture for evaluating AI-based security systems at the edge: Network TON _IoT datasets,” Sustainable Cities and Society, vol. 72, p. 102994, Sep. 2021, doi: 10.1016/j.scs.2021.102994.

[12] N. Moustafa, M. Keshky, E. Debiez and H. Janicke, ”Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications,” 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 848-855, doi: 10.1109/TrustCom50675.2020.00114.

[13] N. Moustafa, M. Ahmed and S. Ahmed, ”Data Analytics-Enabled Intrusion Detection: Evaluations of ToN_IoT Linux Datasets,” 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 727-735, doi: 10.1109/TrustCom50675.2020.00100.

[14] N. Moustafa, “New generations of Internet of Things datasets for cybersecurity applications based machine learning: TON_IoT datasets.” UNSW Sydney, 2019.

[15] N. Moustafa, “A Systemic IoT-Fog-Cloud Architecture for Big-Data Analytics and Cyber Security Systems: A Review of Fog Computing,” arXiv.org, May 04, 2019. https://arxiv.org/abs/1906.01055v1.

[16] J. Ashraf et al., “IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities,” Sustain. Cities Soc., vol. 72, no. 103041, p. 103041, 2021.

[17] K. Saurabh, T. Kumar, U. Singh, O. P. Vyas and R. Khondoker, ”NFDLM: A Lightweight Network Flow based Deep Learning Model for DDoS Attack Detection in IoT Domains,” 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2022, pp. 736-742, doi: 10.1109/AIIoT54504.2022.9817297.

[18] K. Saurabh et al., ”LBDMIDS: LSTM Based Deep Learning Model for Intrusion Detection Systems for IoT Networks,” 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2022, pp. 753-759, doi: 10.1109/AIIoT54504.2022.9817245.

[19] K. Saurabh, A. Singh, U. Singh, O. P. Vyas and R. Khondoker, ”GANI-BOT: A Network Flow Based Semi Supervised Generative Adversarial Networks Model for IoT Botnets Detection,” 2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Barcelona, Spain, 2022, pp. 1-5, doi: 10.1109/COINS54846.2022.9854947.

[20] K. Saurabh, S. Singh, R. Vyas, O. P. Vyas and R. Khondoker, ”MLAPS: A Machine Learning based Second Line of Defense for Attack Prevention in IoT Network,” 2022 IEEE 19th India Council International Conference (INDICON), Kochi, India, 2022, pp. 1-6, doi: 10.1109/INDICON56171.2022.10039777.

[21] M. M. Hassan, A. Gumaei, S. Huda and A. Almogren, ”Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model,” in IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6154-6162, Sept. 2020, doi: 10.1109/TII.2020.2970074.