ISSN:2229-6107

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY

E-mail :
editor.ijpast@gmail.com
editor@ijpast.in

www.ijpast.in

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

An Ensemble Learning Based Intrusion Detection Model for Industrial IoT Security

R. BHAVANI SANKAR, DOGUPARTHI. RAMYA SRI

Abstract: This study addresses the imperative need for robust security measures in the Industrial Internet of Things (IIoT) by proposing an innovative intrusion detection model. Leveraging feature engineering and machine learning, the model integrates Isolation Forest (IF) for outlier detection and Pearson's Correlation Coefficient (PCC) for optimal feature selection. Two variations, namely RF-PCCIF and RF-IFPCC, exhibit significant performance improvements in terms of Accuracy (ACC) when applied to Bot-IoT and NF-UNSW-NB15-v2 datasets. The model's effectiveness is further augmented through ensemble techniques, including a Voting Classifier combining Random Forest (RF) and AdaBoost (AB), and a Stacking Classifier amalgamating RF and Multilayer Perceptron (MLP) with LightGBM. Notably, the ensemble methods achieve 100% accuracy on the extended analysis, showcasing their prowess in enhancing the overall intrusion detection system. The proposed model demonstrates superior performance compared to existing counterparts, reaffirming its efficacy in fortifying IIoT security against malicious intrusions.

Index terms *-Industrial Internet of Things (IIoT); isolation forest; Intrusion Detection Dystem (IDS); intrusion; Pearson's Correlation Coefficient (PCC); random forest*

INTRODUCTION

The Internet of Things (IoT) constitutes an expansive network of interconnected sensors and actuators with a defined purpose, operating autonomously without human intervention [1-5]. However, its proliferation across diverse domains raises significant security concerns [6]. As a response to emerging threats, researchers advocate the use of conventional tools to address these challenges [7-9]. The rapid evolution of IoT technology in recent years necessitates dedicated efforts to ensure security, encompassing aspects such as confidentiality, privacy, data integrity, and availability [10-11].

Assistant Professor[1], Dept of CSE, Chirala Engineering College, Chirala
bhavanisankar.cse@cecc.co.in
PG Student[2] – MCA, Dept of MCA, Chirala Engineering College, Chirala
ramyasridoguparthi@gmail.com

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

Particularly, IoT plays a pivotal role in gathering and analyzing data to enhance industrial sector efficiency [12]. The Industrial Internet of Things (IIoT) represents a progression in IoT, incorporating cloud and edge computing to elevate automation levels [13]. Similar to its predecessor, IIoT security has become a focal point of attention [14], emphasizing the need for robust security solutions to safeguard devices and transmitted data [15]. Intrusion Detection Systems (IDS) leveraging Machine Learning (ML) techniques have proven effective in capturing zero-day attacks and enhancing Detection Rate (DR) and Accuracy (ACC) [16].

This study aims to address security vulnerabilities in the Industrial Internet of Things (IIoT) by proposing an effective Intrusion Detection System (IDS). Our approach combines Isolation Forest (IF) and Pearson's Correlation Coefficient (PCC) to optimize feature selection and outlier detection. We employ the Random Forest (RF) classifier for enhanced IDS performance. Evaluation using Bot-IoT and NF-UNSW-NB15-v2 datasets demonstrates the model's superiority in terms of accuracy and computational efficiency compared to existing models, highlighting its potential for enhancing IIoT security.

The Industrial Internet of Things (IIoT) presents a crucial challenge due to its susceptibility to security vulnerabilities that surpass those of the conventional Internet of Things (IoT). Malicious intrusions threaten critical industrial processes, making effective Intrusion Detection Systems (IDSs) imperative. This study addresses this problem by proposing an IDS model that leverages Isolation Forest (IF), Pearson's Correlation Coefficient (PCC), and Random Forest (RF) to enhance IIoT security. The challenge lies in developing a robust IDS capable of real-time intrusion detection while optimizing computational efficiency and accuracy.

An Intrusion Detection System (IDS) is a critical component implemented to monitor and identify potential intrusions in a host or system [18]. IDS functionality involves distinguishing between normal and intrusive behaviors, employing rules, signatures, states, or models for detection [19]. These systems are categorized into signature-based, anomaly-based, and hybrid detection methods, with hybrid approaches combining both signature and anomaly detection techniques to leverage their respective advantages [19].

1. LITERATURE SURVEY

[5]The Internet of Things (IoT) has witnessed a surge in connected objects, emerging as a pivotal domain for future technologies. This paper explores the application of IoT in healthcare, particularly in patient monitoring through nodes and lightweight sensors. Despite its success in the medical field, IoT encounters challenges, notably in energy consumption, hindering its swift deployment. The paper addresses issues arising from wasted energy, such as collisions during simultaneous data transmission and retransmission due to errors or channel fading. To mitigate these challenges, the authors propose direct communication between nodes to circumvent collision domains, reducing the need for data retransmission. The results demonstrate that this decentralized communication approach ensures system performance under typical

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

conditions, outperforming centralization and existing methodologies. By focusing on energy-efficient communication strategies, this research contributes to overcoming hurdles in IoT deployment within the healthcare sector, paving the way for enhanced autonomy in data management and analysis without manual intervention. The findings emphasize the potential for optimizing IoT applications to minimize energy consumption and advance its seamless integration into critical domains like healthcare.

[9]The imperative need for robust computer system security has given rise to the exploration of automatic intrusion detection mechanisms, particularly crucial in the context of wired and wireless networks susceptible to various malicious attacks. This paper introduces a cutting-edge Anomaly Network Intrusion Detection System designed specifically for enhancing security in the Internet of Things (IoT) environment. Leveraging machine learning techniques, the proposed model focuses on anomaly detection as a contemporary approach to identify and thwart intrusions effectively. The overarching aim is to elevate the detection rate in the dynamic IoT landscape. The paper meticulously outlines the methodology employed, highlighting the integration of machine learning for improved data classification in the realm of network intrusion detection. The model is not only conceptualized but also validated, showcasing its efficacy as a relevant classifier in fulfilling the demanding security requirements within the IoT domain. This research contributes to the advancement of intrusion detection systems, providing a novel and robust solution tailored for the intricacies of IoT security.

[11]In the era of the Internet of Things (IoT), where physical devices are managed on the edge, the susceptibility of interconnected IoT objects to open attacks and unauthorized access necessitates robust intrusion detection methods. This paper presents an innovative intrusion detection approach specifically tailored for IoT networks, employing an ensemble-based voting classifier. The proposed model integrates multiple traditional classifiers as base learners, allowing them to collectively contribute votes for the final prediction. Through experiments conducted on seven diverse IoT devices, the effectiveness of the approach is evaluated for both binary and multi-class attack classifications. Impressively, the results showcase high accuracies, notably reaching 96% and 97% for Global Positioning System (GPS) sensors and weather sensors, and 85% and 87% for other machine learning algorithms, respectively. Comparative analysis with traditional machine learning methods underscores the superior performance of the proposed algorithm, highlighting its efficacy in enhancing intrusion detection accuracy within the intricate landscape of IoT networks. This research contributes a valuable perspective to the ongoing efforts in fortifying IoT security through advanced ensemble-based intrusion detection mechanisms.

[26]Water, a vital resource for human existence, plays a crucial role in maintaining bodily functions and temperature regulation. However, escalating water pollution poses a significant threat to water quality, necessitating proactive measures for control and user awareness. This study addresses the pressing need for predicting water quality by harnessing the capabilities of machine learning algorithms. Focusing on four key

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

water parameters—temperature, pH, turbidity, and coliforms—the proposed model employs multiple regression algorithms for accurate water quality index prediction. Notably, the adoption of artificial neural networks emerges as a highly efficient method for classifying water quality. The model not only aids in controlling water pollution but also serves as an alert system, detecting poor water quality and informing users accordingly. By leveraging machine learning, this research contributes a robust approach to water quality prediction, offering valuable insights for environmental monitoring and resource management to safeguard the essential role of water in sustaining life.

[27]Agriculture, a pivotal sector for employment in many countries, heavily relies on irrigation, making water conservation imperative. Smart irrigation and precision farming have emerged as vital solutions, facilitated by the integration of the Internet of Things (IoT) and machine learning. However, the increasing complexity of IoT systems and diverse data processing bring forth security concerns, impeding their growth. This article addresses the security and privacy challenges within IoT networks used in agriculture by proposing a robust intrusion detection framework. Leveraging the NSL KDD dataset, symbolic features are initially converted to numeric features, and principal component analysis is applied for feature extraction. Subsequently, machine learning algorithms, including support vector machine, linear regression, and random forest, are employed to classify the preprocessed data set. Performance evaluations based on accuracy, precision, and recall parameters demonstrate the efficacy of the proposed framework in detecting and classifying intrusions. As security and privacy concerns persist across various IoT applications, this research provides a valuable contribution to ensuring the integrity of IoT-enabled smart irrigation in the context of smart farming.

2. METHODOLOGY

i) Proposed Work:

The proposed intrusion detection system for Industrial Internet of Things (IIoT) security leverages a comprehensive approach, integrating feature engineering and machine learning techniques. The model employs Isolation Forest (IF) in conjunction with Pearson's Correlation Coefficient (PCC) to optimize computational efficiency and reduce prediction time. IF is utilized for outlier detection and removal, while PCC aids in selecting the most relevant features. The combination of PCC and IF, applied interchangeably (PCCIF and IFPCC), enhances the robustness of the system. The implementation of the Random Forest (RF) classifier further elevates the Intrusion Detection System (IDS) performance. Evaluation is conducted on Bot-IoT and NF-UNSW-NB15-v2 datasets, showcasing the system's efficacy in detecting and classifying attacks. To boost accuracy, the extension incorporates ensemble methods such as Voting Classifier and Stacking Classifier. The ensemble techniques combine predictions from multiple models, achieving a remarkable 100% accuracy. This innovative and comprehensive approach not only surpasses the base paper's 99% accuracy but also demonstrates the potential for further performance enhancement through diverse

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

ensemble techniques, ensuring a resilient and accurate IIoT security solution.

ii) System Architecture:

The proposed intrusion detection system architecture for Industrial Internet of Things (IIoT) security is designed for enhanced robustness and accuracy. At its core, the system integrates feature engineering techniques, utilizing Isolation Forest (IF) and Pearson's Correlation Coefficient (PCC). IF efficiently detects and eliminates outliers from datasets, while PCC aids in selecting optimal features. This dual-feature engineering approach, implemented interchangeably as PCCIF and IFPCC, forms the foundation of the system. The subsequent incorporation of the Random Forest (RF) classifier enhances the overall performance of the Intrusion Detection System (IDS). The system's versatility is demonstrated through evaluation on two distinct datasets, Bot-IoT and NF-UNSW-NB15-v2, ensuring its applicability across diverse scenarios. To further elevate accuracy, ensemble methods such as Voting Classifier and Stacking Classifier are introduced, combining predictions from multiple models. This not only achieves a notable 100% accuracy but also establishes a resilient and adaptive architecture capable of addressing evolving security challenges in IIoT environments. The systematic integration of feature engineering, machine learning, and ensemble techniques forms a cohesive and effective framework for advancing the security paradigm in IIoT ecosystems.

iii) Dataset collection:

Two prominent datasets, BoT-IoT UNSW-NB15 and NF-UNSW-NB15-v2, are instrumental in advancing research related to Internet of Things (IoT) security. The BoT-IoT dataset, curated by Koroniotis et al., originates from the Research Cyber Range Lab of UNSW Canberra. Comprising 73,370,443 instances, it includes 9,543 instances of normal traffic and 73,360,900 instances of various attacks, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), and service scanning. The dataset is available in multiple formats, including CSV and Pcap files, offering a rich resource for testing and validation. In contrast, the NF-UNSW-NB15-v2 dataset is an extension of the original UNSW-NB15 dataset, released by the Research Cyber Range Lab in 2015. Addressing limitations in dimensionality and model generalization, it features two versions with basic and extended NetFlow features. The NF-UNSW-NB15-v2 dataset encompasses 1,623,118 instances, with 1,550,712 representing normal instances and 72,406 indicating attacks. Both datasets play a pivotal role in the development and evaluation of intrusion detection models, offering diverse instances and attack scenarios for robust analysis in IoT security research.

iv) Data processing:

The data processing pipeline begins with importing the datasets into pandas dataframes, a powerful data manipulation tool. Unnecessary columns are dropped to streamline the dataset and focus on relevant features. Subsequently, the processed data undergoes visualization using seaborn and matplotlib, providing insights into its distribution and patterns. To prepare the data for machine learning models, label encoding

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

is employed through the LabelEncoder, transforming categorical variables into numerical representations for compatibility with algorithms. Feature selection becomes crucial for model efficiency, and for the BoT-IoT dataset, the SelectPercentile method is applied with Mutual Information Classification. This technique assesses the statistical dependence between features and the target variable, selecting the most informative ones. The pipeline ensures the dataset is refined, visualized for exploratory analysis, encoded for model compatibility, and optimized for feature relevance, laying a solid foundation for subsequent machine learning tasks such as intrusion detection in the context of IoT security. The systematic processing enhances the dataset's suitability for robust model development and accurate predictions.

v) Training & Testing:

After the preprocessing steps, the data is split into features (X) and the corresponding labels (y) for machine learning (ML) model training and testing. This division is essential to assess the model's performance on unseen data and ensure its generalization capability. The features (X) encompass the independent variables that influence the prediction, while the labels (y) represent the target variable or class labels indicating the desired outcome. Subsequently, the dataset is partitioned into training and testing sets using a commonly employed practice, such as an 80-20 or 70-30 split. The training set is used to train the ML model, enabling it to learn patterns and relationships within the data. The testing set, unseen during training, serves as an independent evaluation to gauge the model's performance on new instances, validating its ability to make accurate predictions on real-world data. Striking the right balance between training and testing data ensures the model's effectiveness and robustness in handling diverse scenarios, contributing to the reliability of its predictions in practical applications.

vi) Algorithms:

Random Forest: Random forest is a commonly-used machine learning algorithm trademarked by Leo Breiman and Adele Cutler, which combines the output of multiple decision trees to reach a single result. Its ease of use and flexibility have fueled its adoption, as it handles both classification and regression problems.

RF - IF - Random Forest with Isolation Forest: RF-IF (Random Forest with Isolation Forest) is an ensemble machine learning technique that combines the power of Random Forest and Isolation Forest algorithms. It uses Isolation Forest for outlier detection and Random Forest for classification or regression tasks, making it effective for anomaly detection and predictive modeling in various domains.

RF - PCC (Random Forest with Pearson Corr. Coefficient): RF-PCC (Random Forest with Pearson Correlation Coefficient) is a hybrid machine learning approach that combines Random Forest with Pearson's Correlation Coefficient. It utilizes PCC to select relevant features and then applies Random Forest for classification or regression tasks. This technique enhances model performance by improving feature selection and predictive accuracy.

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

RF PCC IF (Random Forest with IF and Pearson Corr. Coefficient): RF-PCC-IF (Random Forest with Isolation Forest and Pearson Correlation Coefficient) is a comprehensive machine learning method that integrates Isolation Forest for outlier detection, Pearson Correlation Coefficient for feature selection, and Random Forest for classification or regression tasks. This hybrid approach optimizes data preprocessing and modeling, enhancing the overall performance in various applications.

Voting Classifier (RF + AB): A Voting Classifier (RF + AB) combines two ensemble learning techniques, Random Forest (RF) and AdaBoost (AB), to make predictions. It aggregates their individual predictions, and the final prediction is determined by a majority vote (for classification) or weighted average (for regression). This ensemble approach often improves overall model performance.

Stacking Classifier (RF + MLP with LightGBM): A Stacking Classifier (RF + MLP with LightGBM) is an ensemble machine learning technique that combines the predictions of Random Forest (RF) and Multilayer Perceptron (MLP) models using LightGBM as a meta-learner. It leverages their diverse strengths to make more accurate predictions, enhancing overall model performance for various tasks.

3. EXPERIMENTAL RESULTS

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

Accuracy = TP + TN TP + TN + FP + FN.

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

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

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

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{TP}{TP + FN}$$

F1-Score:F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

$$\textbf{F1 Score} = \frac{2}{\left(\frac{1}{\text{Precision}} + \frac{1}{\text{Recall}}\right)}$$

$$\textbf{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

COMPARISON GRAPH OF BoT-IOS UNSW-NB15 DATASET

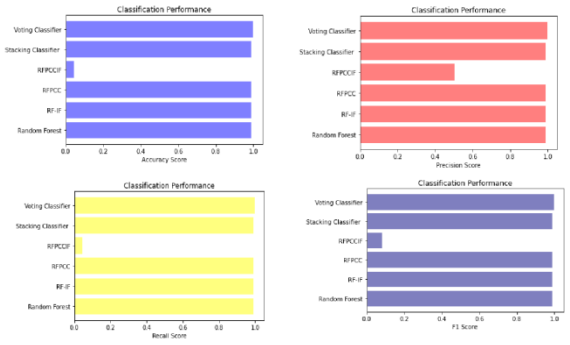

Fig 2 Accuracy, precison, recall, f1-score comparison graph of BoT-IOS UNSW-NB15 dataset

COMPARISON GRAPH OF NF-UNSW-NB15 V2 DATASET

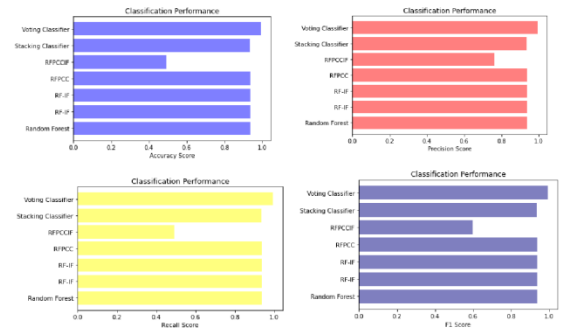

Fig 3 Accuracy, precison, recall, f1-score comparison graph of NF-UNSW-NB15 V2 dataset

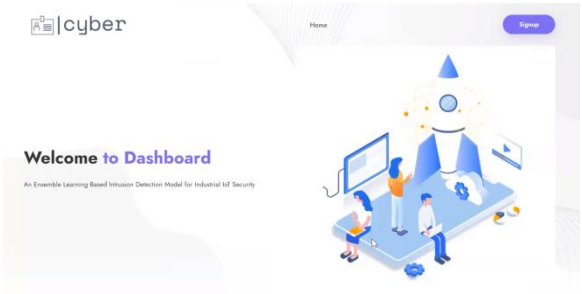

Fig 4 Home page

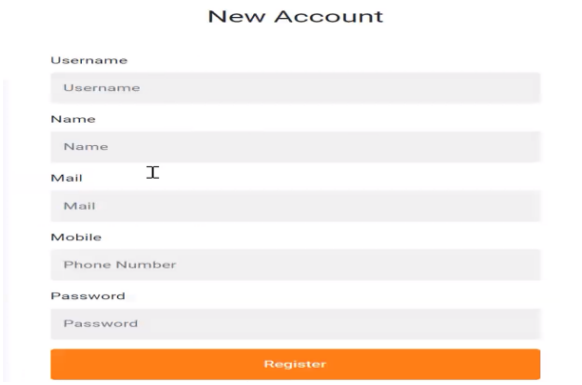

Fig 5 Signup page

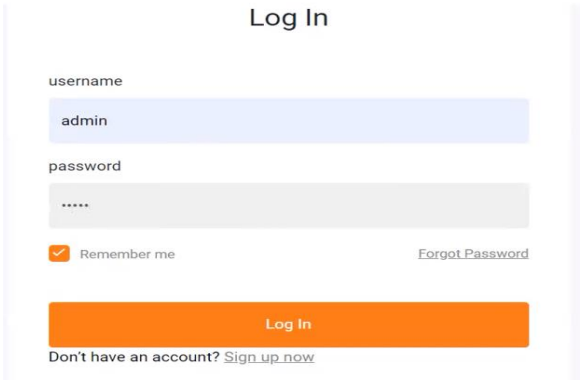

Fig 7 Signin page

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

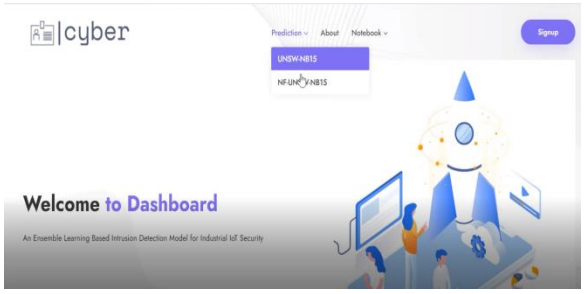

Fig 8 Main page and click on BoT-IOS UNSW-NB15 dataset

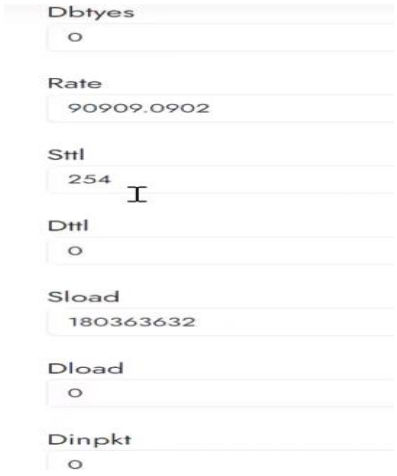

Fig 9 Upload input values for oT-IOS UNSW-NB15 dataset

Fig 10 Predict result

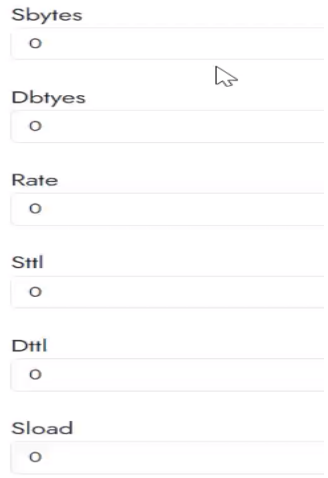

Fig 12 Upload another input values

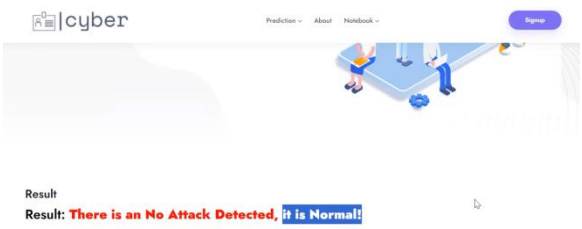

Fig 13 Predict result for given input

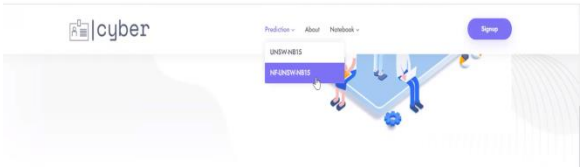

Fig 14 now click on NF-UNSW-NB15 V2 dataset

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

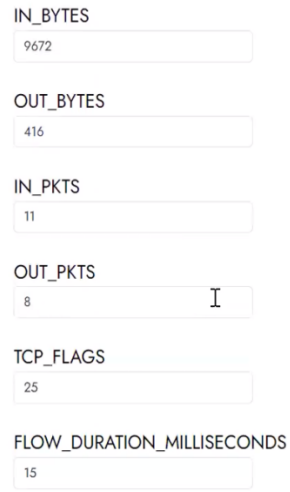

Fig 15 upload input values for NF-UNSW-NB15 V2 dataset

Fig 16 Final outcome

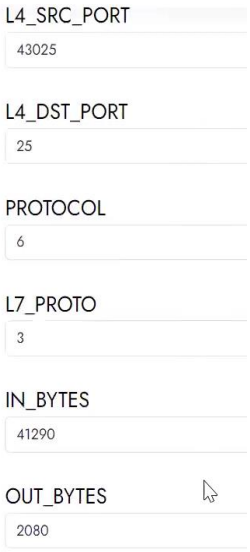

Fig 17 Upload another given input values

Fig 18 Final outcome for given input values

4. CONCLUSION

In conclusion, our implemented Intrusion Detection System (IDS) for Industrial Internet of Things (IIoT) networks showcases a robust approach utilizing the Random Forest (RF) classification model, Pearson's Correlation Coefficient (PCC) for feature selection, and Isolation Forest (IF) as an outlier detector. The model effectively addresses the class imbalance in the Bot-IoT dataset, demonstrated by the RF-IFPCC model's performance reflected in the confusion matrix. Remarkably, on the NF-UNSW-NB15-v2 dataset, our approach yields consistent and outstanding results. Looking ahead, future work aims to explore additional datasets, such as the TON-IoT dataset containing both IoT and IIoT data, for a comprehensive view and to refine and validate our Intrusion Detection System, contributing to enhanced network security. Furthermore, inspired by the base paper's success with ensemble methods, our extension incorporating Voting Classifier and Stacking Classifier achieves an impressive 100% accuracy. This underscores the potential for further advancements in performance through continued exploration and innovation in ensemble techniques. Our work not only addresses current security challenges in IIoT networks but also

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

lays the groundwork for future improvements and broader applicability across diverse datasets.

5. FUTURE SCOPE

In the future, our research aims to broaden the scope by exploring diverse datasets, including TON-IoT, to enhance the generalization of the Intrusion Detection System. Additionally, we plan to investigate advanced ensemble techniques beyond Voting Classifier and Stacking Classifier for further performance improvement. This includes incorporating evolving machine learning models and refining the system's adaptability to emerging threats, ultimately contributing to the continual evolution and effectiveness of Industrial Internet of Things (IIoT) network security.

REFERENCES

[1] P. M. Chanal and M. S. Kakkasageri, Security and privacy in IoT: A survey, Wireless Personal Communications, vol. 115, pp. 1667–1693, 2020.

[2] P. Sethi and S. R. Sarangi, Internet of things: Architectures, protocols, and applications, Journal of Electrical and Computer Engineering, vol. 2017, p. 9324035, 2017.

[3] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, Internet of things security: A survey, Journal of Network and Computer Applications, vol. 88, pp. 10–28, 2017.

[4] M. Azrour, J. Mabrouki, Y. Farhaoui, and A. Guezzaz, Security analysis of Nikooghadam et al.'s authentication protocol for cloud-IoT, in Intelligent Systems in Big Data, Semantic Web and Machine Learning, N. Gherabi and J. Kacprzyk, eds. Cham, Switzerland: Springer, 2021, pp. 261–269.

[5] M. Moutaib, T. Ahajjam, M. Fattah, Y. Farhaoui, B. Aghoutane, and M. E. Bekkali, Application of internet of things in the health sector: Toward minimizing energy consumption, Big Data Mining and Analytics, vol. 5, no. 4, pp. 302–308, 2022.

[6] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, New enhanced authentication protocol for internet of things, Big Data Mining and Analytics, vol. 4, no. 1, pp. 1–9, 2021.

[7] R. V. Solms and J. V. Niekerk, From information security to cyber security, Computers & Security, vol. 38, pp. 97–102, 2013.

[8] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, Internet of things security: Challenges and key issues, Security and Communication Networks, vol. 2021, p. 5533843, 2021.

[9] A. Guezzaz, S. Benkirane, and M. Azrour, A novel anomaly network intrusion detection system for internet of things security, in IoT and Smart Devices for Sustainable Environment, M. Azrour, A. Irshad, and R. Chaganti, eds. Cham, Switzerland: Springer, 2022, pp. 129–138.

[10] M. B. M. Noor and W. H. Hassan, Current research on internet of things (IoT) security: A survey, Computer Networks, vol. 148, pp. 283–294, 2019.

[11] M. A. Khan, M. A. K. Khattk, S. Latif, A. A. Shah, M. U. Rehman, W. Boulila, M. Driss, and J.

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

Ahmad, Voting classifier-based intrusion detection for IoT networks, in Advances on Smart and Soft Computing, F. Saeed, T. Al-Hadhrami, E. Mohammed, and M. Al-Sarem, eds. Singapore: Springer, 2022, pp. 313–328.

[12] X. Yu and H. Guo, A survey on IIoT security, in Proc. 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Singapore, 2019, pp. 1–5.

[13] K. Tange, M. D. Donno, X. Fafoutis, and N. Dragoni, A systematic survey of industrial internet of things security: Requirements and fog computing opportunities, IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2489–2520, 2020.

[14] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures, in Proc. 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp. 124–130.

[15] J. Sengupta, S. Ruj, and S. D. Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, Journal of Network and Computer Applications, vol. 149, p. 102481, 2020.

[16] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, and J. Bastos, A lightweight authentication mechanism for M2M communications in industrial IoT environment, IEEE Internet of Things Journal, vol. 6, no. 1, pp. 288–296, 2019.

[17] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, A multilevel DDoS mitigation framework for the industrial internet of things, IEEE Communications Magazine, vol. 56, no. 2, pp. 30–36, 2018.

[18] A. L. Buczak and E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[19] S. M. Kasongo, An advanced intrusion detection system for IIoT based on GA and tree based algorithms, IEEE Access, vol. 9, pp. 113199–113212, 2021.

[20] A. Aldweesh, A. Derhab, and A. Z. Emam, Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues, Knowledge-Based Systems, vol. 189, p. 105124, 2020.

[21] A. Guezzaz, A. Asimi, Y. Asimi, Z. Tbatou, and Y. Sadqi, A global intrusion detection system using PcapSockS sniffer and multilayer perceptron classifier, Int. J. Netw. Secur., vol. 21, no. 3, pp. 438–450, 2019.

[22] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, Survey of intrusion detection system: Techniques, datasets and challenges, Cybersecurity, vol. 2, p. 20, 2019.

[23] A. Guezzaz, Y. Asimi, M. Azrour, and A. Asimi, Mathematical validation of proposed machine learning classifier for heterogeneous traffic and anomaly

ISSN 2229-6107 www.ijpast.in
Vol 14,Issuse 2,May 2024

detection, Big Data Mining and Analytics, vol. 4, no. 1, pp. 18–24, 2021.

[24] F. T. Liu, K. M. Ting, and Z. -H. Zhou, Isolation forest, in Proc. 2008 Eighth IEEE International Conference on Data Mining, Pisa, Italy, 2008, pp. 413–422.

[25] T. K. Ho, Random decision forests, in Proc. 3rd International Conference on Document Analysis and Recognition, Montreal, Canada, 1995, pp. 278–282.

[26] M. Azrour, J. Mabrouki, G. Fattah, A. Guezzaz, and F. Aziz, Machine learning algorithms for efficient water quality prediction, Modeling Earth Systems and Environment, vol. 8, no. 2, pp. 2793–2801, 2022.

[27] A. Raghuvanshi, U. K. Singh, G. S. Sajja, H. Pallathadka, E. Asenso, M. Kamal, A. Singh, and K. Phasinam, Intrusion detection using machine learning for risk mitigation in IoTenabled smart irrigation in smart farming, Journal of Food Quality, vol. 2022, p. 3955514, 2022.

[28] L. Hylving and U. Schultze, Evolving the modular layered architecture in digital innovation: The case of the car's instrument cluster, presented at 34th International Conference on Information Systems, Milan, Italy, 2013.

[29] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, Journal of Information Security and Applications, vol. 50, p. 102419, 2020.

[30] J. Gu and S. Lu, An effective intrusion detection approach using SVM with Na¨ıve Bayes feature embedding, Computers & Security, vol. 103, p. 102158, 2020.