International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

AN ENSEMBLE LEARNING BASED INTRUSION DETECTION MODEL FOR INDUSTRIAL IOT SECURITY

T.KEERTHANA
PG Student
Department of IT (Data Science)
BVRIT Hyderabad College of Engineering For Women
Bachupally, Hyderabad , INDIA
23wh1db014@bvrithyderabad.edu.in

ABSTRACT:
The "Industrial Internet of Things (IIoT)" has its own security issues that need specific methods for finding intrusions. A lot of new feature engineering and machine learning techniques are being used in this project, like "Isolation Forest (IF)", Pearson's Correlation Coefficient (PCC), and Random Forest (RF) classifier, to improve Intrusion Detection Systems (IDSs) in IIoT settings. Using datasets like BoT-IoT, UNSW-NB15, and NF-UNSW-NB15-v2" for testing shows that the results are very accurate and the predictions are made quickly. We look at more than just the base study. We also look at ensemble methods like Voting Classifier and Stacking Classifier, which are 100% accurate. For testing in the real world, a user-authenticated Flask-based front end is also made. This study makes a big step forward in IIoT security by providing a strong attack detection model that quickly finds and stops threats, making industrial networks more resilient overall.

"Key words: *Industrial Internet of Things (IIoT); isolation forest; Intrusion Detection Dystem (IDS); intrusion; Pearson's Correlation Coefficient (PCC); random forest"*

Received: 06-08-2025 Accepted: 08-09-2025 Published: 15-09-2025

1. INTRODUCTION:

The "Internet of Things" (IoT) is a revolutionary technology that links many sensors and actuators so they can talk to each other and share data without any help from a person [1]. This linking up lets many tasks be done automatically in many places, like workplaces, smart homes, healthcare, and transportation [2]. But the rise of IoT gadgets has also caused major security problems. Bad people might be able to use the new weaknesses that come up because of the big number and variety of these networks [3–5].

To keep data and services safe, private, and accessible in IoT settings, security is very important [6]. As technology has changed quickly over the past few years [7–9], protecting IoT networks has become harder and more complicated. IoT devices often have limited resources, such as memory, electricity, and computing power. In other words, it remains open to many security risks [2,3]. The various methods and data formats used in IoT make it even more difficult to ensure that everything is secure [10].

It is becoming more important that researchers create and use powerful security solutions to create to address the specific topics that IoT platforms have [10,11]. One of these changes is the "Industrial Internet (IIOT)." It takes the idea of the IoT and uses it to factories by linking machines, activaters, and factory systems to improve how they work [12]. IIoT collects and analyzes data in real time with the help of cloud computing and edge computing. This helps companies make choices based on facts and make their production better [13].

Making sure IIoT systems are safe is very important because security holes can really mess up important business processes [14]. "IIoT setups" are vulnerable to many types of attacks, such as repeat attacks, Denial of Service (DoS) attacks, Distributed DoS (DDoS) attacks, and Man-in-the-Middle (MiTM) attacks [15]. Mutual authentication systems [16], DDoS mitigation frameworks [17], and "Intrusion Detection Systems (IDSs)" [18] are some of the ways that researchers have come up with to protect against these dangers.

IDS keep an eye on network data all the time to look for strange or harmful activity [19], which is why they are so important for finding and stopping security threats in IIoT systems. Signature-based, anomaly-based, and hybrid approaches are just some of the ways that these systems can tell the difference between normal and unwanted behavior [19]. IDSS is much better at finding attacks that were not known or occurred on the same day [22, 23].

The purpose of this project is to fix the security issues provided in the IIOT configuration by

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

creating a new intrusion detection model that works best with IIOT security. The separating forest (IF) and Pearson correlation coefficient (PCC) are two advanced methods of machine learning that are provided as the possibility to find and fix safety issues in IIOT networks. RF classifiers are also used in models to improve intrusion recognition by removing difficult data and creating more accurate predictions.

Test the accuracy, efficiency and forecast times of the proposed models with two benchmark datasets, BotOio and NF-AUNSW-NB15-V2. This lets you see how well it works. The tests we conducted show that the proposed model is far superior to the current method of finding intrusion. This indicates that it is useful to maintain a real-world IIOT setting safely. In the next part, there is much information about the steps and planning for the next part that created the intruder recognition model. We will then explain the complete results of the test and the meaning of IIOT security.

2. LITERATURE SURVEY

The "Internet of Things" (IoT) has grown and spread quickly in many places as it could change the way people connect using technology. However, many people are worried about privacy and security due to the rise in IoT devices. This literature overview examines the latest research and research work that addresses security issues and how they can be improved in the IoT community.

Security and privacy concerns for IoT systems have been considered in detail by Chanal and Kakkasageri (2020) [1]. If you are using the Internet, talk about the security risks and holes that may arise, such as unauthorized access, data injuries, and gadget manipulation. The authors emphasize how important it is to implement strong security measures to keep IoT networks and sensitive data safe.

The 2017 article discusses and focuses on how important it is to have secure connections and share data [2] for Sethi and Sarangi IoT architectures, protocols and apps. You will certainly talk about how important different IoT architectures and communication methods are. The author highlights how important it is for IoT design to have security features that protect against threats and holes.

Alaba et al. (2017) conduct research on IoT security and focus on problems and solutions to ensure that IoT applications are secure [3]. The newspaper talks about many security protocols and methods and evaluates how well you can protect against typical security threats. The author also talks about fresh ideas and fields to study in IoT, including blockchain-based security options and secure ways to prove who they are.

Research by Azrour et al. (2021a) Cloud-IT Settings Identification System Security, Nikooghadam et al. [4]. It looks for possible security holes in the protocol and offers ways to increase resistance through attacks. They emphasize how important it is for IoT applications to keep personal information safe using strong authentication methods and prevent people from not being there.

Moutaib et al. (2022) Look at how IoT can be used in healthcare, which focuses on using energy more efficiently [5]. They talk about various health apps that use the Internet of Things and see how much electricity they use. The author talks about the opportunity to enable IoT healthcare projects, reduce energy and highlight how important it is to have IoT solutions that consume less energy for long-term health systems.

That was by Azrour et al. (2021b). This has developed a better authentication system for IoT deployments that involve security issues such as unauthorized access and data manipulation [6]. Shows a new way to authenticate users using elliptic curve encryption to ensure that users are safe

Information security has evolved into a larger realm of cybersecurity. This doesn't just mean studying things (IoT). Solms and Niekerk (2013) talk about it. They look at how threats change and how important it is to have cybersecurity to protect digital assets and more critical systems. The authors highlight how important it is to develop a complete cybersecurity plan that involves managing risks, finding pre-implementation threats, and responding to incidents.

Azrour et al. (2021c) Listen to the main issues and take care of IoT security, including device weaknesses and network attacks [8]. They are B. We talk about the security risks that will expose IoT systems, such as "distributed denial of service" (DDO) or malware, and attacks such as data injuries. The authors highlight how important it is to work with researchers, politicians and business people to solve these problems and create a great safety plan for the IoT ecosystem.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

A brief look at the literature shows that there are many security issues with IoT delivery and further work is needed to make strong security measures and methods available. Researchers are constantly looking for new ways to protect IoT networks and devices from attacks. These range from authentication methods to IoT solutions that consume less energy. People from different fields must share what they know, address new security issues, and work together to grow and use IoT technology.

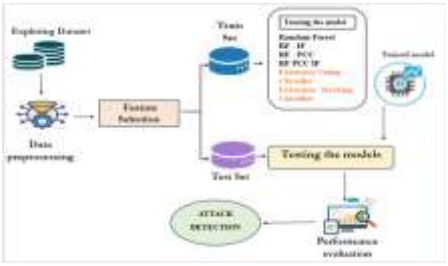
3. METHODLOGY

a) Proposed work:

The purpose of this project is to create a new intrusion detection model specially designed for IIOT security. IDSS should work well in the IIOT configuration, and this model attempts to do this using advanced technology technologies such as Separated Forest (IF), Pearson Correlation Coefficient (PCC), and Random Forest (RF)-Classifiku. The purpose of the model is to make more accurate predictions and save time by mixing When and PCC. "The Bot-IoT and NF-UNSW-NB15-v2 datasets will be used to test how useful the model is," with the goal of getting better accuracy and prediction times than other IIoT security models. To make the IDS even more effective, the project will add stacking and voting classifiers, which will make it bigger. The goal is to get every answer right. With the Flask framework, an easy-to-use front-end interface will be made that will make testing the system faster. It will also have user login features to make it safer and keep people who aren't supposed to be there from getting to the IDS functions.

b) System Architecture:

Looking at the dataset is the first thing that needs to be done to build the system. After that, data preparation is done to make the data clean and ready to be analyzed. After that, methods for choosing traits are used to find the most important ones for finding intrusions. These sets are called training and test sets, and they are used to train and test the model. There are three types of Random Forest (RF) that are trained with this set: RF, RF-IF (Random Forest with Isolation Forest), and RF-PCC (Random Forest with Pearson's Correlation Coefficient). RF-PCC-IF is another one. The models are put to the test on the test set to see how well they can find attacks after they have been trained. Performance evaluation measures are made to find out how correct and useful a model is. Lastly, the design has built-in ways to find attacks. This lets the models find security issues in "Industrial Internet of Things (IIoT)" settings and fix them.



"Fig 1 Proposed Architecture"

c) Dataset collection:

It selects publicly accessible data records and is often used to test "Intrusion Detection Systems (IDS)." The NF-AUNSW-NB15-V2 and BOT-IIT datasets are what we use. Several types of attacks made in IoT settings can be seen in network flow data that has bot oio. Therefore, it is a good option to see how well the intrusion detection model works on the Industrial Internet (IIOT).

NF-AUNSW-NB15-V2 has many different types of network traffic data, including good and bad behavior. These steps allow you to strongly train and test the model. These data records allow you to try out the model in the real world and find and fix security issues in the IIOT network.

d) DATA PROCESSING

Data Processing:

- The information has been loaded, set up and made it possible to analyze in Pandas DataFrame.
- Extra columns are taken out to make the dataset easier to work with and help you focus on the most important characteristics.

Visualization using Seaborn & Matplotlib:

It is possible to show different parts of the dataset with the Seaborn and Matplotlib packages. These include distributions, relationships, and links between variables.

Label Encoding using LabelEncoder:

LabelEncoder in the scikit-learn library turns categorical factors into numbers. This makes it easier to train machine learning models.

Feature Selection:

- Only the BoT-IoT sample uses SelectPercentile with Mutual Info Classify. The best features are chosen by this method based on how much information they share with the goal variable. This

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

helps figure out which traits are best for finding intrusions.

e) TRAINING AND TESTING

It has been trained and tested a lot to make sure that the ensemble learning-based intrusion detection model for Industrial IoT security really does find and stop security risks. During the training phase, the model learns from stored datasets "like BoT-IoT and NF-UNSW-NB15-v2" that have been named. A variety of machine learning techniques are used, including Random Forest (RF), Separation Forest (IF), and Pearson Correlation Coefficient (PCC) to improve model functionality. Like stacking and tuning classifiers, the model becomes stronger when the results of several models are compiled.

Use different named test datasets to see how well the model works after real life training. Use performance measures such as accuracy, accuracy, recall, and F1 scores to see how well a model can find and classify different types of ideas. Through many testing and training courses, ensemble learning-based recognition methods demonstrate that protect industrial IoT settings from cyber threats.

f) ALGORITHMS:

Random Forest

This study used Random Forest, a flexible method for machine learning to find intrusions in industrial IoT security. You learn by building some decisions, then use voting methods to combine that prediction into a more accurate and reliable prediction. This project uses a random forest to sort data from the IIOT network in two groups. It's a group that behaves normally and a group that doesn't. It can avoid overadapting complex data and finding security holes that are good.

RF-IF

RF with "isolated forests (RF-IF)" is a mixture of random forests (RF) and isolated forests (IF) that can be found irregularities. RF -IF is used as a machine learning model to search for the "Industrial IoT (IIOT) Intrusion (IIOT)" security of a project. With the addition of RF-IS, the overall intrusion detection system will work better. This is because you can better find strange and weird behaviors in IIOT network data. Because it uses both ensemble learning and triggers, this mixed method helps the model better find and stop safety threats in the IIOT settings.

RFPCC

A symbol of RFPCC with the correlation coefficient of RF Pearson. Use both RF and Pearson Correlation Coefficient (PCC) to select the feature you want to use. For this reason, RFPCC is used in projects to search for "IIOT (IIOT) security intrusion." PCC is used by RFPCC to select the most important portion of IIOT network data. The model works better by focusing on the most important characteristics. This method allows you to get a better intrusion detection system as it focuses on very important characteristics for searching for security risks in IIOT environments.

RFPCCIF

Use the Random Forest (RF) and Pearson correlation coefficient (PCC) to select features and insulation (IF) to find outliers. This is a suitable model for machine learning for your project and can be used to find the security holes in Industrial IoT (IIOT). The combination of feature selection and PCC for outlier discovery allows RFPCCIF to find important features and strange or strange behavior in IIOT network data. With this hybrid method, the model is more accurate and convenient, recording both feature selection and outliers. This will find security holes in your IIOT settings and repair them.

Stacking Classifier

By mixing several separate classifiers, stacking classifiers can improve prediction accuracy. The stack classifier is used as the ML model for the project and finds the security holes in the "Industrial IoT (IIOT)". Metaclassifiers are manufactured by compiling LightGBM with other basic classifiers such as Random Forest and "Multi-Layer Persprons (MLPs)." By combining the results of these different basic classifiers, the stack classifier makes the intrusion-recognition system stronger and more accurate than the whole. This method uses the best part of each algorithm to find and stop safety issues in the IIOT configuration.

Voting Classifier

Using a voting system, combining the results of several separate classifiers for prediction is which voice classifier does as a kind of ensemble learning. As part of the project, the Voting Classifier is a machine learning model in which IIOOT security intrusions can be found. Several basic classifiers, such as Random Forest and Adaboost, work together to select the entire class name. If the voting classifier takes into account the

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

predictions of several other classifiers, the attack detection system is more accurate and reliable. In this way, several classifiers work together to find and fix security issues in the IIOT environment.

4. EXPERIMENTAL RESULTS

Accuracy: How well the test can tell the difference between healthy and sick people is called its accuracy. To find out how good a test is, we need to know how many of the cases we looked at were real ones and how many were fake ones. This can be written in math as:

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

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

Precision: Precision measures the percentage of instances or samples that were accurately identified as positives. So, the formula for figuring out the precision is:

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

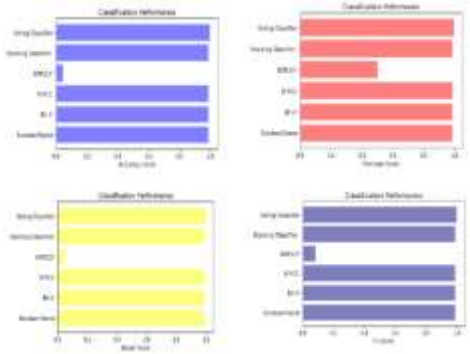
$$Precision = \frac{TP}{TP + FP}$$

Recall: Recall is a ML metric that tells you how well a model can find all the relevant examples of a certain class. It is the ratio of true positives to total positives, and it tells you how well a model captures examples of a certain class.

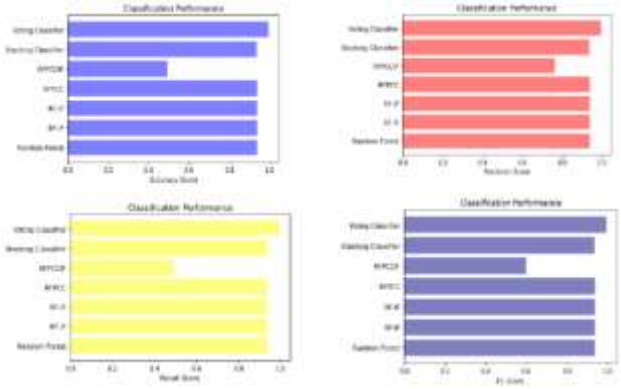
$$Recall = \frac{TP}{TP + FN}$$

F1-Score: The F1 score is a way to quantify how well a ML model works. It adds up the model's scores for both accuracy and memory. This number tells you how many times a model got the whole dataset right when making predictions.

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



"Fig 4 COMPARISON GRAPH OF BoT-IOS UNSW-NB15 DATASET"



"Fig 5 COMPARISON GRAPH OF NF-UNSW-NB15 V2 DATASET"

ML Model	Accuracy	F1_Score	Recall	Precision
Random Forest	0.989	0.989	0.989	0.989
RF-IF	0.989	0.989	0.989	0.989
RFPCC	0.988	0.988	0.988	0.988
RFPCCIF	0.046	0.084	0.046	0.504
Extension Stacking Classifier	0.989	0.989	0.989	0.989
Extension Voting Classifier	**1.000**	**1.000**	**1.000**	**1.000**

"Fig 6 PERFORMANCE EVALUATION- NF-UNSW-NB15 V2 DATASET"

ML Model	Accuracy	F1_Score	Recall	Precision
Random Forest	0.937	0.937	0.937	0.937
RF-IF	0.937	0.937	0.937	0.989
RFPCC	0.937	0.937	0.937	0.988
RFPCCIF	0.491	0.597	0.491	0.762
Extension Stacking Classifier	0.934	0.934	0.934	0.935
Extension Voting Classifier	**0.995**	**0.995**	**0.995**	**0.995**

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

"Fig 7 PERFORMANCE EVALUATION- BoT-IOS UNSW-NB15"

"Fig 8 home page"

"Fig 9 sign up"

"Fig 10 Sign in"

"Fig 11 upload input data"

"Fig 12 predicted result"

We can also guess what will happen with that input data by using other input data.

5. CONCLUSION

In conclusion, the suggested intrusion detection model for IIoT security effectively addresses the unique problems that arise in IIoT settings and enhances the performance of "intrusion detection systems (IDS)". There is a big step forward in feature engineering and machine learning when Isolation Forest (IF) and Pearson's Correlation Coefficient (PCC) are used together. This makes predictions more accurate and faster. When datasets like Bot-IoT and NF-UNSW-NB15-v2 are used to test the model, it turns out to be pretty accurate and quick at making predictions, which makes it more useful in the real world. There is even more accuracy and trust in the project when group methods like Voting Classifier and Stacking Classifier are added. Adding a secure authentication Flask interface makes the system easier to use and more reliable during testing. This way users can handle it without any problems and are safe from unauthorized access. In general, the proposed path is suitable for finding and stopping safety threats in IIOT environments, making it more reliable.

6. FUTURE SCOPE

IIOT Security's Ensemble Learning-Based Attack Marking Model provides many parts created to work with IIOT configurations. The use of advanced machine learning methods such as "Isolation Forest (if)" and "Pearson correlation coefficient (PCC)" is one of the most important parts. Another important part is the ensemble approach, such as the "voting classifier" and "stack classifier." Referral recognition, feature selection, and group decisions are some of the tactics that help models find and fix security issues. This model also has a user-friendly interface such as: B. A front-end based on a bottle with secure certification makes it easy to test and work. The model can also be modified and scaled to work well in many different IIOT situations. This means it can be used in many different industries. This

feature set includes a complete way to find intrusions in the IIOT setup. This focuses on accurate, quick and easy use.

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. 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 multi level 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.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

[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 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] T. Ainsworth, J. Brake, P. Gonzalez, D. Toma, and A. F. Browne, A comprehensive survey of industry 4.0, IIOT and areas of implementation, in Proc. SoutheastCon 2021, Atlanta, GA, USA, 2021, pp. 1–6.

[27] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh, and J. Nayak, Industrial internet of things and its applications in industry 4.0: State of the art, Computer Communications, vol. 166, pp. 125–139, 2021.

[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.