International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Deep Learning-Based Rule-Based Feature Selection for Intrusion Detection in Industrial Internet of Things Networks

[1]Archana V. Potnurwar, [2]Vrushali K. Bongirwar, [3]Samir Ajani, [4]Nilesh Shelke, [5]Mrunalee Dhone, [6]Namita Parati

Submitted: 17/05/2023 **Revised:** 03/07/2023 **Accepted:** 22/07/2023

Abstract-In the field of Industrial IoT area, It produces enormous volumes of data by utilising the power of sensors. The IIoT does, however, confront considerable obstacles, particularly in the form of cyber-attacks that can jeopardise organisations and interrupt operations. Sensitive information is stolen as a result of these attacks, in addition to causing losses in money and reputation.To address these risks, numerous Network Intrusion Prevention Systems (NIDSs) have been developed to protect IIoT systems. But creating a useful and intelligent NIDS is a challenging endeavour, largely because there aren't many large data sets that can be utilised to design and test such systems.In response to these difficulties, this research proposes a novel deep learning-based intrusion detection technique for IIoT systems. To help identify relevant data derived from TCP/IP packets, a hybrid rule-based feature selection mechanism is included in the proposed system. The solution attempts to increase the precision and effectiveness of intrusion detection in IIoT environments by utilising deep learning methods.In this study, deep learning techniques are employed to offer a novel method for industrial internet of things (IIoT) system intrusion detection. The proposed paradigm combines a Deep Feed Forward Neural Network model (DFFNN) with a hybrid rule-based feature selection strategy to quickly train and assess data obtained from TCP/IP packets. The effectiveness of the technique was evaluated on two well-known network datasets, NSL-KDD and UNSW-NB15. This study demonstrated the potential of the provided technique for classifying network attacks in scenarios of IIoT penetration. The trials used a number of evaluation measures to demonstrate the usefulness of the suggested method for precisely identifying and classifying intrusions within IIoT networks.

Keywords: *Intrusion detection, Deep Learning, Network Intrusion, Deep Feed Forward Neural Network, Industrial Internet of Things*

1Priyadarshini College of Engineering, Nagpur, Maharashtra, India
2Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India
3St. Vincent Pallotti College of Engineering and Technology, Nagpur, Maharashtra, India
4Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, Maharashtra, India
5G H Raisoni College of Engineering, Nagpur, Maharashtra, India
6Maturi Venkata Subba Rao (MVSR) Engineering College, Hyderabad, Telangana State, India.
1archanapotnurwar@gmail.com,
2bongirwarvk@rknec.edu, 3samir.ajani@gmail.com,
4nilesh.shelke@sitnagpur.siu.edu.in,
5mrunali.dhone@raisoni.net,
6namianand006in@gmail.com

I. Introduction

In IIoT "Automation of Everything" era has begun thanks to the fundamental changes and personal development that the modern industrial revolution has sparked. The power of computer networks is being used in this revolution to manage real-world applications, connect digital devices, and use data mining techniques [1]. People have access to an unprecedented amount of data and knowledge thanks to this disruptive wave, which creates new opportunities and development paths.This revolution promises enormous improvements in efficiency through the fusion of the physical and digital industries, resulting in a better standard of living and a more prosperous society. In this context, the Industrial Internet of Things (IIoT), which produces enormous volumes of data through numerous sensors, is essential. The IIoT has an impact on several industries, including healthcare, retail, the automobile industry, and transportation. The IIoT has enormous potential to improve productivity, efficiency, and operational effectiveness across many industries.Existing infrastructures and processes will be optimised by the IIoT. The ultimate goal is to develop completely original and cutting-edge goods and services. Innovative businesses understand how IIoT ideas and solutions may lead to organisational transformation, better offerings, and create wholly new business models. On the IIoT platform, dependability, production capacities, and customer happiness may all be considerably improved by utilising machine learning and deep learning algorithms. Innovative technology, sensors, software, and applications are combined to achieve this.

An extensive range of technologies must be connected and coordinated in order to provide the aforementioned advances. Improvements in cognitive automation, the workplace with smart area of Industry, intelligent data exploration, and other business intelligence fields are included in this. In this setting, a fundamental concept is the concept of a "digital twin," which refers to a virtual counterpart of real assets, processes, and more. The Internet of Things (IoT) and the abundance of data these systems and devices produce constantly change the digital twin, which is often connected to the IoT. By analysing this data, one may improve productivity, make better design decisions, simplify maintenance, and take care of a variety of other problems. The ability of any digital twin to continuously update and "learn" from changes in real-time is one of its distinguishing characteristics. Thanks to the Internet of Things (IoT) concept and its related solutions, organisations may now utilise vast amounts of data for better operational effectiveness and decision-making. With the growth of IIoT devices and implementations, companies now have severe concerns about protecting critical infrastructure and services [13]. One of the biggest threats to IIoT networks is malware that exploits zero-day flaws.

The gravity of these threats is demonstrated by a number of noteworthy events. The Stuxnet computer virus targeted Iran's nuclear programme in 2010. The Industrial Control Systems (ICS) of a dam in New York were compromised by Iranian hackers in 2013. Nearly 80,000 power outages occurred in Ukraine as a result of the BlackEnergy attack in 2015 [14, 15]. The network intrusion detection system (NIDS), a crucial tool for network security, enables the identification and containment of several internet-based attacks. The Industrial Internet of Things (IIoT) is crucial to the flow of data and information throughout modern infrastructure, making global network security of the biggest importance at the moment [16]. Network intrusion detection systems (NIDS) are widely used to identify and address network traffic to protect workstation systems from several grid breaches. [17] Defines intrusion as an intentional effort to defeat the security safeguards of an information system. Due to the risks that these intrusive frameworks present, researchers have been motivated to develop novel intrusion detection systems (IDSs).

This study's primary goal, according to [8], is to integrate the infrastructure that is being developed for Industrial Internet of Things (IIoT) applications. We evaluated the effectiveness of the technique using the NSL-KDD and UNSW-NB15 datasets. In this study, a hybrid feature selection method was developed, which included both a rule-based model and a genetic search tool. It was decided to include the element that best matched the class. Following a more thorough evaluation of the qualities based on their merits, the genetic search technique was used to identify the features with the highest value. The rule-based approach (rule assessment phase) was utilised to determine which feature subset contained the fewest features when two attribute segments had performance ratings that were equal.

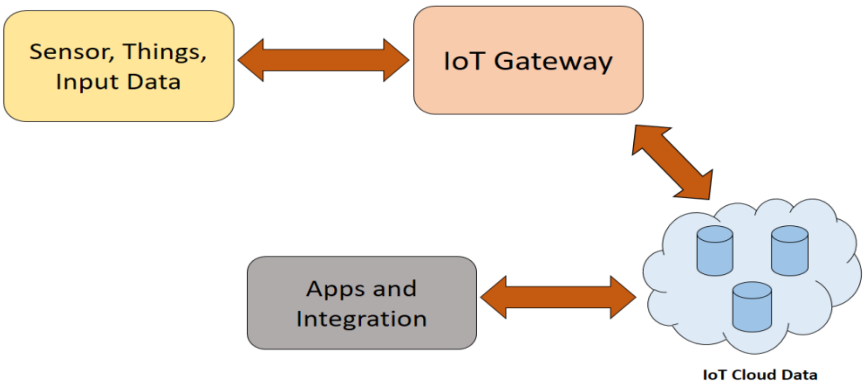


Fig. 1: Architecture of Industrial Internet of Things

An intelligent edge gateway is a piece of software that is tightly connected with sensor nodes and is made to collect, assemble, and clean up light data streams.

IoT Cloud: The IoT data cloud represents the core architecture that practisesfiles processing, neural networks, and artificially intelligent algorithms to manage and process massive volumes of data. Among its capabilities are devices control, stream analytics, managing events, rules engine, alerts, and updates. Additional features include end-to-end encryption, virtualization, which is big data analytics, authorization, software creation kits (SDKs), as well as application programming interfaces (APIs).

Application Integration and IoT Platform: This is the name for the supporting structure that connects different IT systems to ensure the efficient collection and processing of data throughout the whole operational loop. Planning, scheduling are just a few of the technologies it incorporates. Data analysis is divided into three categories using this strategy: descriptive, predictive, and prescriptive. Figure 1 depicts the four-layered IIoT architecture, which consists of the following components: objects (devices/sensors), intelligent gateways, IoT clouds, and business applications and connectors.

The presentation of the projected model to classify intrusions in IIoT networks is the primary objective of the research. Given the enormous number of features and parameters in the datasets employed, it was crucial to use effective feature selection algorithms in order to solve the high dimensionality challenge. As a result, the classifier works less and performs better. Using a feature extraction technique also enables the classifier to select the most crucial features while excluding those that can negatively affect its performance.

II. Review of Literature

By acting as a packet capture and decoding engine that is tasked with keeping track of network traffic and spotting suspicious activity, the Anomaly Detection System (ADS) contributes significantly to security management [23]. Security monitoring and abnormal behaviour detection are its two main duties. The ADS can successfully identify any variations from these patterns as potential intrusions, including both known and yet undiscovered threats [25], by creating patterns from the regular data [25].

During semi-supervised feature selection, Coelho et al. [36] suggested using a homogeneity metric to gauge the degree of similarity between label and data clusters. They discovered that incorporating cluster information can aid in feature relevance estimate and feature selection, particularly when there are few occurrences of labelled data. On the 42 features that make up the complete UNSW-NB15 dataset,Beluch et al. [37] explored classification methods using Apache Spark. The effectiveness of the algorithms Naive Bayes, Random Forest, the Decision Tree, and support vector machine (SVM) was evaluated. The outcomes showed that a random forest performed the best, with a precision of 97%.

Using a Random Forest classifier, Primartha and Tama [38] investigated the effectiveness of detection systems for intrusions (IDSs). Using a 10-fold cross-validation method, they evaluated the performance measures' accuracy and false alarm rate. The experiment made use of three datasets: NSL-KDD, UNSW-NB15, and GPRS. Comparisons were made between the performance of the proposed model and that of the multi-layered perception (MLP), Decision Tree, and NB-Tree classifier in the study. The outcomes showed that the proposed model, which applied a cross-validation technique and a classifier based on Random Forests with certain parameter values, was effective.

The [39] approach focused on selecting informational components that were particular to each category of assault rather than using generic features for all attacks. The suggested method's effectiveness in accurately detecting intrusions was demonstrated in research utilising the CICIDS2017 dataset.Dahiya et al. [40] recommended utilising Apache Spark to build an intrusion detection system in their work. They used the linear discriminant evaluation (LDA) and cyclic correlation analysis (CCA) feature reduction techniques. The Bayes naive, REP Tree, Random Tree, the Random Forest, the Random Committee, and The process of bagging methods are seven popular categorization algorithms.

A Convolutional Neural Network (CNN) was used in [41] to create a model for classifying malware. A dataset of 9,339 samples from 25 different malware groups were used in the investigation, which had a remarkable accuracy rate of 94.5%. Similar to this, in [42], the authors created a deep CNN that made use of colour image visualisation to identify online malware attacks. Their findings showed that categorization performance in assessing cybersecurity threats had improved.Researchers in [43] proposed the Random Coefficient Selecting and Mean Modification Method (RCSMMA)-based approach. When facing different contemporary cyber-attacks, our system performed well. The authors also highlighted some of the significant uses of such cities in [44], namely in the context of malware attacks, while also examining the significant privacy and security challenges that arise in the design of apps for smart cities.A robust steering and monitoring mechanism employing multivariate tuples was presented by [45] to reduce the impact of adversaries in global sensor networks. By defending the sensor network against potential malware threats, this protocol attempted to improve the security and integrity of it.

III. Publically Available Datasets

The dataset utilized for testing, analysis, and assessment has a significant impact on how well the detection system performs. The well-known NSL-KDD datasets, an enhanced version of the KDD CUP 99 database, have been used by numerous investigations. Through the elimination of duplicate entries and the selection of data based on relevance, the NSL-KDD dataset resolves the primary shortcomings of the KDD CUP 99 dataset. After pre-processing, it has 148,517 records (77,054 regular instances and 71,460 attacks). There are 41 attributes and a corresponding class label in every record. Probing, DoS, User to Root (U2R), Remote to Local (R2L), and Normal are the classes in this dataset. The NSL-KDD dataset is currently regarded as being out of date, despite its widespread use in IDSs.

A brand-new dataset named UNSW-NB15 is used to thoroughly assess our suggested work. The UNSW-NB15 dataset provides realistic, synthesised attack scenarios as well as current, everyday behaviours. There are 257,673 records in all, 93,000 of which indicate regular behaviour and 164,673 of which involve attacks. A classification label and 41 attributes make up each record. Fuzzers, Exploits, Backdoors, DoS, Reconnaissance, Shellcode, Worms, Generic, Analysis, and Normal are among the ten class labels in this dataset, with one representing normal behaviour and nine representing various sorts of assaults. The UNSW-NB15 dataset is used to ensure a thorough assessment of our planned study as shown in table 1.

Table 1: Description of Dataset

Dataset	**No of Records (After Pre-Processing)**	**Attributes**	**No of Attacks**	**Classes**	**Normal**	**Anomaly**
KDD CUP99	148,517	41	4	2	77054	71460
UNSW-NB15	257673	41	9	2	93,000	164,673

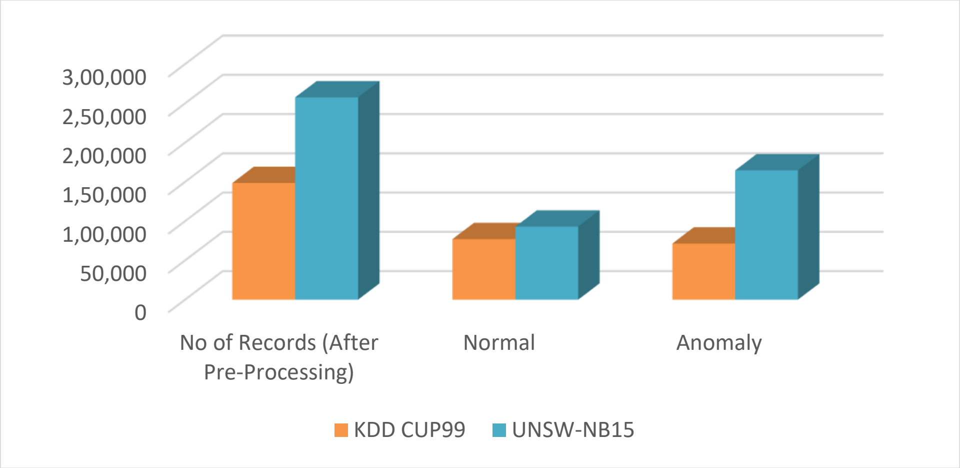


Fig. 2: Representation of Dataset description with Normal and Anomaly

IV. Proposed System

In this paper, a deep feed forward neural network (DFFNN) is used to construct an efficient anomaly detection technique (ADS) for IIoT scenarios. During the testing stage, a genetic search method and a rules-based algorithm are combined to create a dual extraction of features technique. The section evaluates the relationships between various traits and the target category. The process of selecting the feature having the strongest association to the category for inclusion is known as feature assessment. The genetic search engine then evaluates each feature's quality in light of this assessment, returning the traits with the highest suitability ratings. When two characteristic subsets possess the same performance score, the rule-based procedure (rule evaluation phase) selects the one with the fewest attributes.

The DFFNN is then fed with the chosen attributes to train models and categorise attacks. The DFFNN is designed with particular parameters to find instances of known and novel attacks. The DFFNN interprets the decreased hidden units to find harmful patterns during testing. The process ensures the thorough construction of a precise feature vector and captures the most pertinent features by utilising several hidden layers. The following subsections go into further detail about the suggested system technique.

a) (DFFNN) Deep Feed Forward Neural Network:

The deep feed forward neural network (DFFNN) method is a kind of artificial neural network with several layers of interconnected nodes, with information travelling entirely in one direction, from the input layer to the output layer. Jobs involving anomaly detection typically use it.The DFFN equation written as:

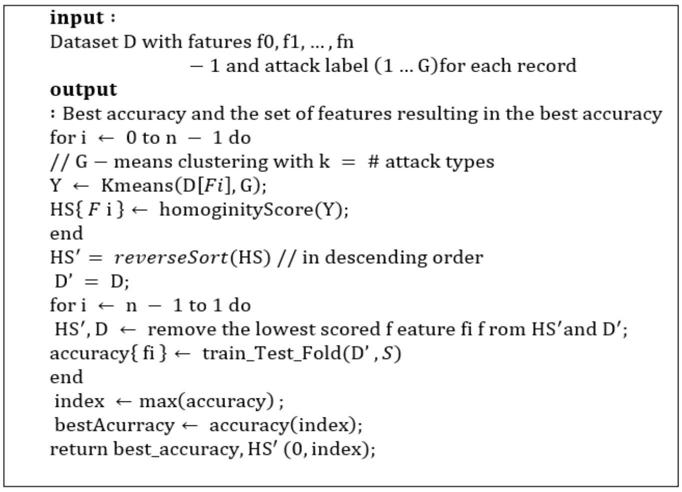
$$h = f(\sum i = 1nwi \cdot xi + b)$$

In this equation, h stands for the neuron's output, f for the activation function applied to the weighted sum of the inputs, w i for the weights assigned to each input x i, and b for the bias term.Each neuron's output from one layer acts as the following layer's neurons' input. The network's final output is produced when the output layer is reached, which is a continuous process. The network is given non-linearities via the activation function f, which enables it to recognise intricate patterns and connections in the data.Using a technique known as backpropagation, which entails calculating the gradient of a loss function with respect to the network parameters, the DFFNN modifies the weights and biases during the training phase. The weights and biases are then updated using this gradient to reduce loss and enhance network performance.

b) Feature selection and Deep Auto encoder (FSDAE):

For effective unsupervised learning, a feedforward neural network technique called a DAE is used [85]. The goal is to rebuild the input data so that the network's output equals the input. The input nodes and hidden units with nonlinear activation functions that make up the DAE together capture the fundamental structure of the data. By compressing the spatial dimensionality of the incoming data and identifying its most important properties, the DAE is able to effectively abstract it.

Algorithm for Feature selection:



```
input :
Dataset D with fatures f0, f1, … , fn
                  − 1 and attack label (1 … G)for each record
output
: Best accuracy and the set of features resulting in the best accuracy
for i ← 0 to n − 1 do
    // G − means clustering with k = # attack types
    Y ← Kmeans(D[$Fi$], G);
    HS{ $F$ i } ← homoginityScore(Y);
end
HS′ = $reverseSort$(HS) // in descending order
 D′ = D;
for i ← n − 1 to 1 do
     HS′, D ← remove the lowest scored f eature fi f rom HS′and D′;
    accuracy{ fi } ← train_Test_Fold(D′ , $S$)
end
 index ← max(accuracy) ;
 bestAcurracy ← accuracy(index);
return best_accuracy, HS′ (0, index);
```

Feature selection Phase:

Choosing a relevant subset of features from a larger, more accessible array of features is referred to as feature subset selection. It aims to make the input data less dimensional, which will improve the effectiveness and efficiency of machine learning models. When selecting a feature subset, each feature's significance or relevance is evaluated, and the subset that contains the most enlightening and discriminating features is selected. The objective of this subset is to retain the data's most crucial elements while eliminating any unnecessary or insignificant details.

$$P\ (C = c \mid Vi = vi)\ \neq p(C - c)$$

Where, P(C=c | Vi=vi) denotes the conditional probability of a class variable C being equal to c given that a feature variable Vi is equal to a certain value vi. The probability that the class variable C has a value other than c is represented by p(C-c).

Subset Evaluation:

We can estimate the relationship between a standardised test that combines these modules and the external parameter if we have a clear understanding of the relationship between each individual component and its corresponding external parameter as well as the inter-correlation among the various sets of parameters.

$$Rz = \frac{k_{r_z}}{\sqrt{k + k(k-1)rij}}$$

Where,

- Krz: This is the total of the cross-products between the variables r and z. It gauges how closely the two variables are related or covariate.
- k: This represents the number of observations or data points used to calculate the correlation coefficient. It reflects the sample size.
- rij: This represents the correlation coefficient between each pair of variables i and j. It is a measure of the strength and direction of the linear relationship between variables i and j.

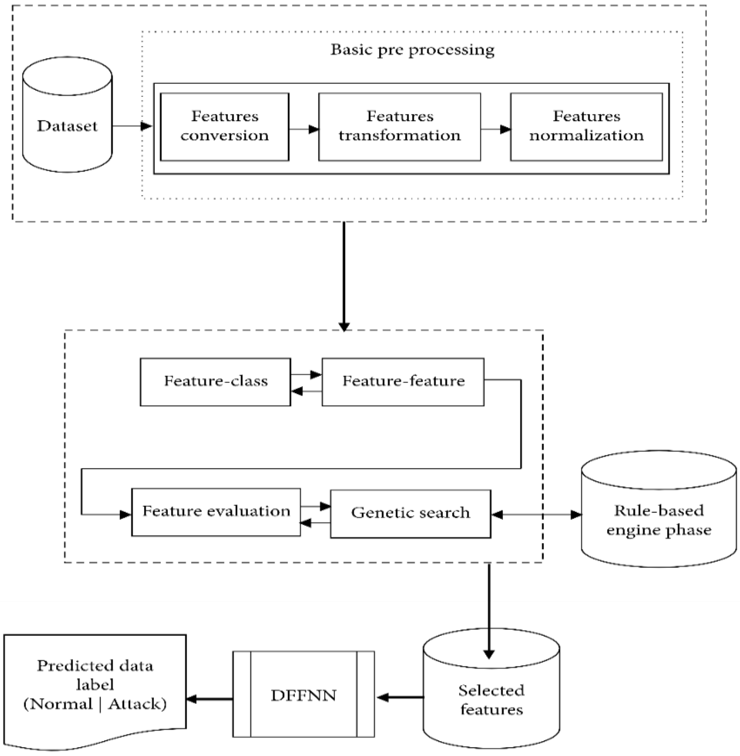


Fig.3: Proposed System Architecture for Intrusion Detection in IIoT

Genetic Search:

The phrase "genetic search" refers to an investigation technique that was motivated by natural evolution. An accuracy and simplicity combined metric known as a fitness function is defined in this search. A solution that maximises accuracy while minimising complexity is desired.

$$\text{Fitness} = \alpha * \text{Accuracy} - \beta * \text{Complexity}$$

A population of potential solutions is generated and evaluated iteratively using the genetic search method. Each of these solutions is represented as a member of a population, and each member represents a potential solution. To produce new generations of individuals, the existing individuals go through genetic processes like selection, crossover, and mutation. Higher fitness values are favoured by the selection process, while population variety is introduced by crossover and mutation.

Rule Engine:

When alternative feature subsets have the same fitness ratings, the rule-based approach selects the feature subgroup with the fewest features. In contrast, if there are no feature subsets with similar fitness values, the rule-based method selects the feature subgroup with the highest fitness value and sends it to the base classifier.

$$Re = \begin{cases} Vi, & if\ Vi \in F > \cap X_f \\ Vi, & if\ F_{hi\ \cap\emptyset} \end{cases}$$

The IIoT system is protected from hostile actions by the concept of intrusion detection proposed in this study. Figure 3 shows the training and testing steps as well as the suggested model's design. Figure 3 depicts the proposed intrusion detection framework designed specifically for the IIoT network. Within an IIoT environment, the scheme focuses on analysing and selecting crucial information from vast amounts of data. The initial phase of the proposed method involves data pre-processing, which encompasses feature transformation and normalization techniques.

C. Performance Analysis:

The suggested technique, which combines deeper learning with a rule-based model, was evaluated and compared to the performance of existing models using the performance measures listed below. Accurate and incorrect predictions from a classification task were totaled and contrasted with the reference outcomes. The F1-score, recall, specificity, recall, accuracy, and precision are some of the frequently used measurements.

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

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

$$F1\ \text{score} = \frac{2 \times \text{Recall} \times \text{Precision}}{(\text{Recall} + \text{Precision})}$$

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

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}}$$

Precision measures the fraction of accurate predictions that are positive, whereas accuracy represents the proportion of predictions that are correct. Specificity measures the accuracy with which negatives may be identified, while recall measures the proportion of actual positives that were properly anticipated. A single metric called the F1-score combines precision and recall. By dividing the total number of negative predictions by the number of valid negative predictions, specificity is determined. True-positive rate (TPR), also known as detection rate, is the percentage of attacks that have been correctly identified relative to all instances in the dataset. False alarm rate (FAR) is determined by dividing the number of records that have been incorrectly classified as negative by the total number of records that are actually normal. It offers the calculation for determining FAR.

V. Results and Discussion

The suggested methodology was put into practise utilising platforms for the R programming language, and its effectiveness was assessed using the performance indicators mentioned. The necessary DAE-DFFNN with a dual rule-based design was used, together with the NSL-KDD and UNSW-NB15 datasets, to smoothly incorporate all pertinent elements. The UNSW-NB15 dataset had 93,000 normal records and 92,000 attack records, compared to the 77,054 normal records and 71,460 assault records in the NSL-KDD dataset. 20% of the normal records were used for testing, which corresponds to 40%, 20%, and 60% of all testers for each dataset, respectively.The network architecture and parameters were chosen to produce the highest detection rate (DR) and the lowest false positive rate (FPR) based on experimental findings. The ideal network architectures for both datasets were selected for the proposed model. In the DAE feature selection model, the input layer had 41 nodes, the three hidden layers had 10, 3, and 10 nodes, and the output layer had 41 nodes. The output layer for the DFFNN model has two nodes. A learning rate of 0.0015 and an initial momentum of 0.2 were applied to the NSL-KDD dataset. L1 and L2 regularisations, an initial momentum of 0.2, a stable momentum of 0.4, a ramp momentum of 17, an annealing rate of 2–6, and for the UNSW-NB15 dataset.

Table 2: Performance Metric evaluation for Both Dataset

Dataset	**TP rate in %**	**FP rate in %**	**Precision in %**	**Recall in %**	**F1-score in %**	**ROC in %**	**Classification**
Using UNSW-NB15	98	11	97	98	98	98	Attack
	99	1	98	96	96	98	Normal
Using NSL-KDD	96	12	94	99	97	97	Attack
	99	13	98	93	96	98	Normal

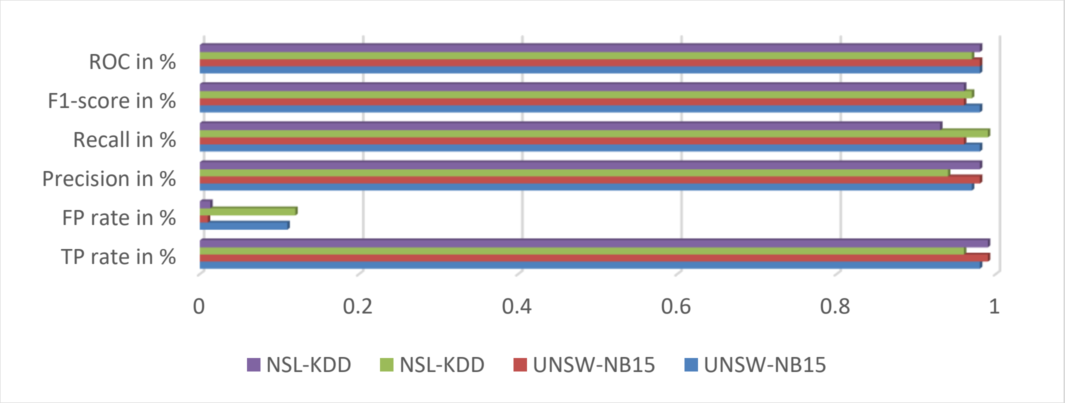


Fig. 4: Performance Metrics comparison for Both Dataset

The TP. As shown in table 2 and figure 4, rate for the "Attack" class and the "Normal" class, respectively, in the UNSW-NB15 dataset is 98% and 99%, respectively. The "Attack" class's FP rate is 11%, compared to the "Normal" class's FP rate of 1%. For the "Attack" class and the "Normal" class, respectively, the precision a measure of the proportion of genuine positives among anticipated positives is 97% and 98%. For the "Attack" class and 96% for the "Normal" class, respectively, the recall, also known as the true positive rate, is 98% and 96%. For both courses, the F1-score, which combines recall and precision, is 98%. The genuine positive rate versus false positive rate trade-off is represented by the ROC (Receiver Operating Characteristic) score, which for both classes is 98%.

The TP rate in the NSL-KDD dataset is 96% for the "Attack" class and 99% for the "Normal" class. The "Attack" class's FP rate is 12 percent, compared to 1.3% for the "Normal" class. The "Attack" class's precision is 94%, whereas the "Normal" class's precision is 98%. Recall for the "Attack" class is 99%, and for the "Normal" class it is 93%. The F1-score for both classes is 97%. For both classes, the ROC score is 97%.The effectiveness of the intrusion detection model for each dataset is revealed by these performance measures. A high ability to correctly recognise instances of attacks is indicated by the high TP rates and F1-scores. The low FP rates show that false alarms can be avoided effectively.

Table 3: Accuracy of model with different dataset

Dataset	Accuracy (%)	Detection Rate (%)	False Positive Rate (%)
NSL-KDD	98.12	98.0	0.9
UNSW-NB15	97.9	98.9	1.0

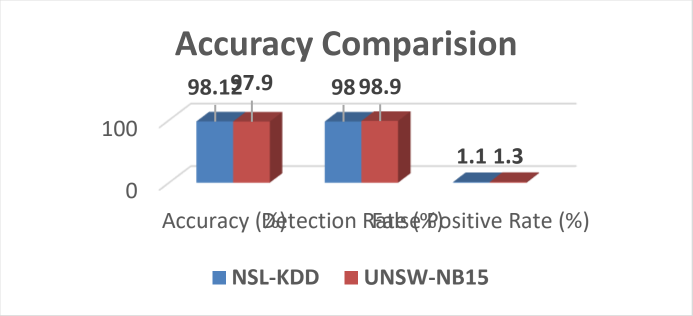


Fig. 5: Accuracy of Model using both Dataset

The model's accuracy in the NSL-KDD dataset is 98.12%, which is the percentage of occurrences that were properly classified. The detection rate, which gauges how well attacks can be identified, is 98.0%. The percentage of routine occurrences that are mistakenly labelled as assaults, or false positive rate, is 0.9%.

The model's accuracy on the UNSW-NB15 dataset is 97.9%. The detection rate, which measures how well attacks can be identified, is 98.9%. The rate of false positives is 1.0%.These performance metrics show how well the intrusion detection model classified instances correctly in both datasets. High detection rates demonstrate a potent capacity to recognise attacks, whereas high accuracy values show a good overall classification accuracy.

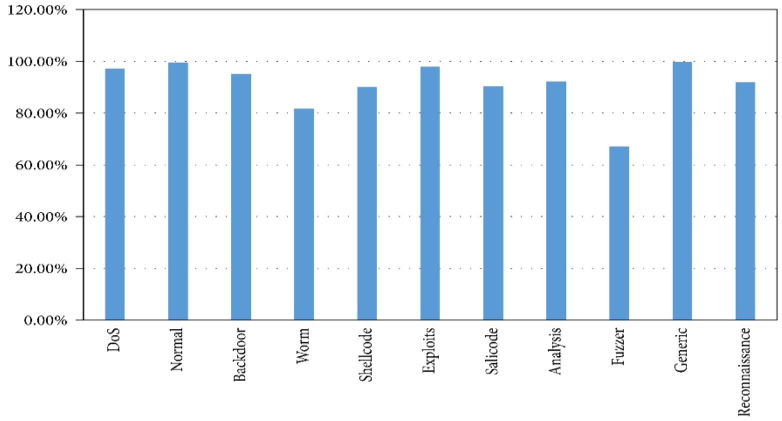


Fig. 6: Detection of Attack for UNSW-NB15 dataset

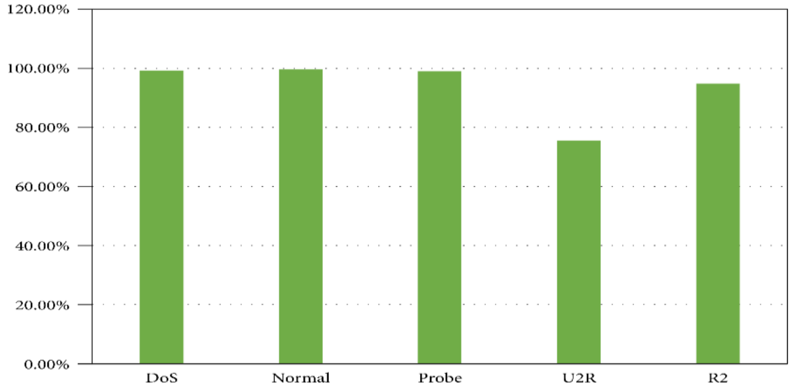


Fig 7: Detection of Attack for NSL-KDD dataset

The low false positive rates show a good capacity to reduce falsely classifying innocent occurrences as attacks. In general, the model performs well in identifying and differentiating between legitimate and harmful activity in the IIoT network.

VI. Conclusion

The Anomaly Detection System (ADS) model is introduced in this study as a tool for detecting malicious behaviour in Industrial Internet of Things (IIoT) networks using TCP/IP packet data. To efficiently capture the underlying network patterns for unsupervised learning, the model makes use of unsupervised deep learning techniques in conjunction with hybrid rule-based approaches and automated dimensionality reduction techniques. The suggested model successfully picks and discards key characteristics using a DAE-DFFNN architecture with a hybrid rule-based design, improving its overall performance.The suggested model, when tested on various samples from the NSL-KDD and NSW-NB15 datasets, achieves an exceptional detection rate of 98.0 percent and a low false alarm rate of 0.9 percent when compared to other current models in recent literature. These datasets were chosen because they are benchmark datasets and are often used by researchers for intrusion detection. By using only pertinent characteristics to categorise instances in the datasets, the incorporation of a hybrid rule-based feature selection mechanism improves the model's resilience.Future study may use data from actual IIoT systems that was collected in the real world to further validate the efficacy of the suggested methodology. This would reveal details on how it functions in actual environments. Additionally, the model might be expanded to support numerous protocols, enabling its use in a variety of IIoT scenarios. These developments would help to improve intrusion detection systems for IIoT networks as they are developed and improved over time.

References

[1] P. Ambika, “Machine learning and deep learning algorithms on the Industrial Internet of Things (IIoT),” Advances in Computers, vol. 117, no. 1, pp. 321–338, 2020.

[2] R. Ashima, A. Haleem, S. Bahl, M. Javaid, S. K. Mahla, and S. Singh, “Automation and manufacturing of smart materials in Additive Manufacturing technologies using the Internet of Things towards the adoption of Industry 4.0,” Materials Today: Proceedings, vol. 45, pp. 5081–5088, 2021.

[3] L. M. Gladence, V. M. Anu, R. Rathna, and E. Brumancia, “Recommender system for home automation using IoT and artificial intelligence,” Journal of Ambient Intelligence and Humanized Computing, pp. 1–9, 2020.

[4] T. Sherasiya, H. Upadhyay, and H. B. Patel, “A survey: intrusion detection system for internet of things,” International Journal of Computer Science and Engineering (IJCSE), vol. 5, no. 2, pp. 91–98, 2016.

[5] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, “Privacy and security concerns in IoT-based healthcare systems,” Internet of Things, pp. 105–134, 2021.

[6] E. A. Adeniyi, R. O. Ogundokun, and J. B. Awotunde, “IoMT-based wearable body sensors network healthcare monitoring system,” in IoT in Healthcare and Ambient Assisted Living, pp. 103–121, Springer, Singapore, 2021.

[7] K. Amit and C. Chinmay, “Artificial intelligence and Internet of Things based healthcare 4.0 monitoring system,” Wireless Personal Communications, pp. 1–14, 2021.

[8] F. E. Ayo, S. O. Folorunso, A. A. Abayomi-Alli, A. O. Adekunle, and J. B. Awotunde, “Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection,” Information Security Journal: A Global Perspective, vol. 29, no. 6, pp. 267–283, 2020.

[9] M. Abdulraheem, J. B. Awotunde, R. G. Jimoh, and I. D. Oladipo, “An efficient lightweight cryptographic algorithm for IoT security,” in Communications in Computer and Information Science, pp. 444–456, Springer, 2021.

[10] A. Bakhtawar, R. J. Abdul, C. Chinmay, N. Jamel, R. Saira, and R. Muhammad, “Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic,” Personal and Ubiquitous Computing, 2021.

[11] A. H. Muna, N. Moustafa, and E. Sitnikova, “Identification of malicious activities in industrial internet of things based on deep learning models,” Journal of information security and applications, vol. 41, pp. 1–11, 2018.

[12] E. Sitnikova, E. Foo, and R. B. Vaughn, “The power of hands-on exercises in SCADA cybersecurity education,” in Information Assurance and Security Education and Training, pp. 83–94, Springer, Berlin, Heidelberg, 2013.

[13] S. Dash, C. Chakraborty, S. K. Giri, S. K. Pani, and J. Frnda, “BIFM: big-data driven intelligent forecasting model for COVID-19,” IEEE Access, vol. 9, pp. 97505–97517, 2021.

[14] G. Tzokatziou, L. A. Maglaras, H. Janicke, and Y. He, “Exploiting SCADA vulnerabilities using a human interface device,” International Journal of Advanced Computer Science and Applications, vol. 6, no. 7, pp. 234–241, 2015.

[15] D. Kushner, “The real story of stuxnet,” IEEE Spectrum, vol. 50, no. 3, pp. 48–53, 2013.

[16] P. W. Khan and Y. Byun, “A blockchain-based secure image encryption scheme for the industrial Internet of Things,” Entropy, vol. 22, no. 2, p. 175, 2020.

[17] Q. Yan and F. R. Yu, “Distributed denial of service attacks in software-defined networking with cloud computing,” IEEE Communications Magazine, vol. 53, no. 4, pp. 52–59, 2015.

[18] A. C. Enache and V. Sgârciu, “Anomaly intrusions detection based on support vector machines with an improved bat algorithm,” in 2015 20th International Conference on Control Systems and Computer Science, pp. 317–321, Bucharest, Romania, May 2015.

[19] O. Folorunso, F. E. Ayo, and Y. E. Babalola, “Ca-NIDS: a network intrusion detection system using combinatorial algorithm approach,” Journal of Information Privacy and Security, vol. 12, no. 4, pp. 181–196, 2016.

[20] H. Zhang, D. D. Yao, N. Ramakrishnan, and Z. Zhang, “Causality reasoning about network events for detecting stealthy malware activities,” Computers & Security, vol. 58, pp. 180–198, 2016.

[21] M. R. Kabir, A. R. Onik, and T. Samad, “A network intrusion detection framework based on Bayesian network using a wrapper approach,” International Journal of Computer Applications, vol. 166, no. 4, pp. 13–17, 2017.

[22] Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, “A survey of intrusion detection on industrial control systems,” International Journal of Distributed Sensor Networks, vol. 14, no. 8, 2018.

[23] T. Cruz, L. Rosa, J. Proenca et al., “A cybersecurity detection framework for supervisory control and data acquisition systems,” IEEE Transactions on Industrial Informatics, vol. 12, no. 6, pp. 2236–2246, 2016.

[24] J. Camacho, A. Pérez-Villegas, P. García-Teodoro, and G. Maciá-Fernández, “PCA-based multivariate statistical network monitoring for anomaly detection,” Computers & Security, vol. 59, pp. 118–137, 2016.

[25] M. Grill, T. Pevný, and M. Rehak, “Reducing false positives of network anomaly detection by local adaptive multivariate smoothing,” Journal of Computer and System Sciences, vol. 83, no. 1, pp. 43–57, 2017.

[26] L. A. Maglaras, J. Jiang, and T. J. Cruz, “Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems,” Journal of Information Security and Applications, vol. 30, pp. 15–26, 2016.

[27] R. O. Ogundokun, J. B. Awotunde, E. A. Adeniyi, and F. E. Ayo, “Crypto-Stegno based model for securing medical information on IOMT platform,” Multimedia tools and applications, pp. 1–23, 2021.

[28] J. Soto and M. Nogueira, “A framework for resilient and secure spectrum sensing on cognitive radio networks,” Computer Networks, vol. 115, pp. 130–138, 2017.

[29] M. S. Abadeh, J. Habibi, and C. Lucas, “Intrusion detection using a fuzzy genetics-based learning algorithm,” Journal of Network and Computer Applications, vol. 30, no. 1, pp. 414–428, 2007.

[30] M. Aazam and E. N. Huh, “Fog computing microdata center-based dynamic resource estimation and pricing model for IoT,” in 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, pp. 687–694, Gwangju, Korea, March 2015.

[31] C. Cecchinel, M. Jimenez, S. Mosser, and M. Riveill, “An architecture to support the collection of big data in the internet of things,” in 2014 IEEE World Congress on Services, pp. 442–449, Anchorage, AK, USA, June 2014.

[32] N. Moustafa, J. Hu, and J. Slay, “A holistic review of network anomaly detection systems: a comprehensive survey,” Journal of Network and Computer Applications, vol. 128, pp. 33–55, 2019.

[33] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, “Machine learning models for secure data analytics: a taxonomy and threat model,” Computer Communications, vol. 153, pp. 406–440, 2020.

[34] N. Moustafa and J. Slay, “The evaluation of Network Anomaly Detection Systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,” Information Security Journal: A Global Perspective, vol. 25, no. 1-3, pp. 18–31, 2016.

[35] W. Shang, P. Zeng, M. Wan, L. Li, and P. An, “Intrusion detection algorithm based on OCSVM in industrial control system,” Security and Communication Networks, vol. 9, no. 10, p. 1049, 2016.

[36] F. Coelho, A. Braga, and M. Verleysen. 2012. "Cluster homogeneity as a semisupervised principle for feature selection using mutual information." ESANN. Bruges, Belgium 2012

[37] M. Belouch, S. El Hadaj, and M. Idhammad. 2018. "Performance evaluation of intrusion detection based on machine learning using Apache Spark." Procedia Computer Science 127 (2018): 1-6

[38] R. Primartha, and B. Tama. 2017. "Anomaly detection using random forest: A performance revisited." Data and Software Engineering (ICoDSE), 2017 International Conference on. IEEE, Palembang Sumatra Selatan, Indonesia 2017

[39] R. Vijayanand, D. Devaraj, and B. Kannapiran.2018. "Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with

genetic-algorithm-based feature selection." Computers & Security 77 (2018): 304-31.

[40] P. Dahiya, and D. Srivastava. 2018. "Network Intrusion Detection in Big Dataset Using Spark." Procedia Computer Science 132 (2018): 253-262.

[41] Z. Cui, F. Xue, X. Cai, Y. Cao, G. G. Wang, and J. Chen, "Detection of malicious code variants based on deep learning," IEEE Transactions on Industrial Informatics, vol. 14, no. 7, pp. 3187–3196, 2018.

[42] F. Ullah, H. Naeem, S. Jabbar et al., "Cyber security threats detection in internet of things using deep learning approach," IEEE Access, vol. 7, pp. 124379–124389, 2019.

[43] N. N. Hurrah, S. A. Parah, J. A. Sheikh, F. Al-Turjman, and K. Muhammad, "Secure data transmission framework for confidentiality in IoTs," Ad Hoc Networks, vol. 95, p. 101989, 2019.

[44] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," Transactions on Emerging Telecommunications Technologies, pp. 1–19, article e3677, 2019.

[45] B. D. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," Ad Hoc Networks, vol. 97, article 102022, 2020.

[46] Dr. Govind Shah. (2017). An Efficient Traffic Control System and License Plate Detection Using Image Processing. International Journal of New Practices in Management and Engineering, 6(01), 20 - 25. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/52

[47] Auma, G., Levi, S., Santos, M., Ji-hoon, P., & Tanaka, A. Predicting Stock Market Trends using Long Short-Term Memory Networks. Kuwait Journal of Machine Learning, 1(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/136

[48] Aoudni, Y., Donald, C., Farouk, A., Sahay, K. B., Babu, D. V., Tripathi, V., & Dhabliya, D. (2022). Cloud security based attack detection using transductive learning integrated with hidden markov model. Pattern Recognition Letters, 157, 16-26. doi:10.1016/j.patrec.2022.02.012 Dhabliya, D. (2021). Delay-tolerant sensor network (DTN) implementation in cloud computing.