IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Intelligent Security Framework For Industrial Iot Using Nature Inspired Optimization With Ensemble Machine Learning

T.Suneetha[a],P.Pradeep Kumar[b],Y.Jagadeesh Kumar[c],K.Mohini Devi[d]

T.SUNEETHA *PGSTUDENT*

a. Sri*SriSivaniCollegeofEngineering,Srikakulam,AndhraPradesh,Indi*

P.PRADEEP KUMAR *ASSOCIATEPROFESSOR*

b.SriSriSivaniCollegeofEngineering,Srikakulam,AndhraPradesh,India

c. Y.JAGADEESH KUMAR *ASISSTANTPROFESSOR*

d. SriSivaniCollegeofEngineering, Srikakulam,AndhraPradesh,India

*e.*K.MOHINI DEVI *ASISSTANTPROFESSOR*

f. *SriSivaniCollegeofEngineering, Srikakulam,AndhraPradesh,India*

.**ABSTRACT**

The worldwide expansion of the Internet of Things (IoT) has been characterized by significant growth, as seen by the widespread use of diverse devices in domains such as housing environments, transportation systems, healthcare facilities and industrial sectors. The introduction and integration of the IoT concept in industrial environments has resulted in significant modifications to the architecture of Industrial Automation and Control Systems (IACS), as well as the widespread interconnectivity of various industrial systems. The outcome of this development is often known as the Industrial IoT(IIoT), which eliminates the obstacle of linking IACS with separate traditional Information and Communication Technology (ICT) platforms. In contemporary times, the IoT has begun to affect upon our individual lives and extend its influence beyond our immediate surroundings, therefore establishing a foundation for imminent cyber-attacks targeting the IoT. The extensive utilization of the IoT has produced a productive ground for potential assaults against IoT systems. Machine learning (ML) algorithms have been used as effective tools for enhancing the security of wireless communication in IIoT-based systems, as well as addressing a range of cyber security issues. Hence, this study presents an improved ensemble model for intrusion detection that utilizes Firefly Algorithm (FA) to classify hostile behaviors in network data within the context of IIoT. The performance of the proposed model was evaluated usingprecision, recall, F1 score,accuracy, F2 score and ROC-AUC

metrics on the X-IIoTIDDataset, which is an IIoT-based cyber security dataset. The obtained findings were compared to those of other recent state-of-the-art ML models, and it was observed that our model exhibited superior performance.

Keywords:ML, IoT, IIoT, Attack, Security, Optimization, IDS

1.Introduction

The IoTis a system of interconnected devices which help support the interaction between "things" and it allow to the development the distributed applications using more complex structures like computing.The IoT is constantly advancing, with a growing number of connected devices. This expansion leads to the accumulation of more data, which is then evaluated and used to develop intricate algorithms. These algorithms enable the automation of various operations, resulting in increased efficiency.Under the IoT supper class, the IIoT subclass is one of the categories, which refers to IoT technologies utilized in industrial contexts, specifically in manufacturing plants. The IIoT refers to the use of IoT technology specifically in the industrial sector, particularly for advanced manufacturing purposes.[1].The IIoT was a network of sensors and self-contained devices that communicate with industrial applications via the internet/network. This network allows for data collection, analysis and production optimization, increasing efficiency and lowering manufacturing and service costs.IIoT technology could assist industrial companies increase productivity by improving predictive maintenance plans i.e. the state and functionality of equipment to predict when it may occur. The industrial internet reference architecturemay serve as a reference for developing sophisticated systems in the IIoTdomain [2].

Based on statistics from Oxford Economics, the IIoT has the potential to affect sectors that contribute to 62% of the Gross Domestic Product (GDP) in the G20 nations. Therefore, the implementation of IIoT in various industries is expected to be the primary catalyst for productivity and innovation in the next decade [3].The IIoT has numerous uses in industries such as Self-driving vehicles, Healthcare, Optimizing the efficiency of machines, Minimizing human mistakes, Improvement in distribution and logistics, as well as a reduction in the overall amount of accidents. With the rise of IIoT applications, there is a corresponding increase in security concerns and cyber-attacks. [4]. The most common threats in IIoT systems are man-in-the-middle attacks, denial-of-service attacks, device exploitation, data interception and tampering, firmware and vulnerabilities in software and so on. To improve the security of IIoT systems, we should examine the following specific traditional aspects: frequently updating and patching firmware and software,secure network communications,installing intrusion detection and prevention systems, train employees on cyber-security best practices, establish incident reaction and recovery plans, conduct frequent security evaluations and penetration tests. Over the last decade, several cyber-attacks have targeted the IIoT, impacting both software and hardware components. These assaults have impacted various system elements, including the status of pumps and sensors.[5, 6].Many businesses use Intrusion Detection Systems (IDS) to defend against malicious attacks and safeguard the security of IIoT nodes and networks.[7].Hybrid IDSs aim to improve upon the shortcomings of signature and anomaly-based IDSs. Traditional IDS suffer from high false-positive rates and limited detection accuracy, leading to inaccurate results.

By harnessing the capabilities of artificial intelligence (AI), machine learning (ML) has facilitated the development of cutting-edge solutions that simplify procedures, improve decision-making, and optimize operations.[8].ML is crucial for contextual analysis in the IIoT, since it improves the system's ability to analyze and resolve network difficulties and problems with IoT devices over time [9]. ML approaches are the most often used techniques for conducting intrusion detection [5]. ML may enhance the process of experimental learning and decision-making in different systems by boosting their abilities and capacity without the need for explicit programming [10]. Recent studies have shown that ML algorithms may effectively mitigate many security vulnerabilities and enhance the efficiency of anomaly-based detection approaches [11-13]. The application of the ML-based model for the IIoT-based network still faces various challengessuch asLow Processing Ability and Data Analytics[14]. Algorithms for ML are used to classify anomaly events such as attacks and IIoT hardware failures. Malicious activity is classified using various methods such as Support Vector Machine (SVM), Linear

Discriminant Analysis (LDA), Logistic Regression (LR),Naïve Bayes (NB),k-nearest neighbours (KNN) and CART. The results reveal that CART and NB perform the best in terms of accuracy, precision, recall and F1score [15].

Traditional ML techniques, such as Bayesian Belief Networks (BBN) and SVM, have been employed in cyber-security. The huge amounts of data generated by IIoT require the use of a ML-based system that has been designed to its specific requirements. TheML model is adaptable and the scalability increases with very low performance fluctuations, so this demands the need of developing more advanced ML approaches and optimization strategies for efficiently processing massive amounts of data in the manufacturing industry. Industrial IoT combines operational technology (OT) and information technology (IT) for addressing safety and security concerns [16].

To handle the IIoT dataset using ML could be a huge challenge. Ensuring the security and privacy of the information, it is the complicated task to train the model accordingly. IIoT dataset are high dimensional data, so it is a challenging task for ML algorithm to handle the complex dataset and finding the learning patterns for accurate predictions. Due to diversity nature of IIoT dataset, it is quite challenging for ML model to handle it. Sample collection of IIoT data is not always same because it most probably depends on network behaviour. Data imbalance can lead to make a biased model which can't maintain equilibrium state between the IIoT dataset of majority and minority classes. Normally ML models are running in one setup parameter, which is by default. Every time one parameter setup not giving us a better performance due to diversity nature of data in IIoT. So to avoid these limitation hyper-parameter of models are essential factors in ML. Hyper-parameters in ML are defined by the user to control the learning process and to improve the learning rate of the model. Hyper-parameter tuning is iterativeand it also can try out in different combinations of parameters and values, so it will impact the model complexity and performance to detect the IIoTnetwork.ML model hyper-parameter optimization is a method used to improve performance by identifying the optimal combination of hyper-parameter values within a certain time frames. Automatic hyper-parameter selection approach for determining the optimal network configuration is the most important aspect in IIoT. Various optimization approaches are used to find the optimal hyper-parameters with Grid Search, Genetic Algorithm, Bayesian Optimization, Random Search, Particle Swarm Optimization (PSO), Firefly Algorithm (FA)[17], Simulated Annealing, Ensemble Method etc. Among all optimization FA is a most popular.Several studies stated that FA is employed for hyper-parameter tuning for ML model and it gives a significant result in anomaly detection of IIoT network. FA can be utilized in IIoT to optimizing communication protocols, scheduling tasks in industrial processes, or improving the overall efficiency and reliability of IIoTsystems. Using ML approaches and realistic FA, we can improve cyber-attack detection models by training them with route data sets [18].The standardFA technique is used to find the optimal values of hyper-parameters in order to achieve a greater level of accuracy in detecting attacks. [19].This research mainly offers the following main contributions:

- The IIoT ecosystem comprises a diverse range of devices and sensors that generate a substantial amount of data. The use of a ML technique is a significant analytical tool for promptly analysing vast amounts of data and producing quick and effective conclusions in real-time.
- An IDSemploying a method called FA_XGBoost has been proposed to detect and minimize cyber-attacks in an IIoT environment.
- This study assessed many performance measures, including as recall,precision, F2 score, ROC-AUC, F1-score and accuracy, to compare the effectiveness of advanced ML ensemble methods versus classic ML models. The suggested model demonstrated a remarkable accuracy of 99.91%, outperforming existing advanced ensemble and conventional ML methods.

The following sections of the research are organized in the succeeding way. Section 2 describes a thorough examination of the relevant literature. Section 3 illustrates an elaborate description of the proposed work. Section 4 discusses over the experimental setup and describes an overview of the dataset. Section 5 offers a comprehensive examination of the simulation findings. Section 6 describes a definitive overview of the research.

2 Literature Studies

To effectively respond to harmful attacks, the IIoT must continually develop its security protection technologies to ensure its own security. IIoT security poses a significant problem for industrial actors and academic research, integrating security measures like intrusion detection improves IIoT environment security. Relevant research keeps on expanding and improvesdefenses against dangerous attacks, which will give vital support for the growth of industrial internet security.This section discusses the previous related work done on IIoT IDS framework.

Qaddoori et al. (2023) [20]utilized the ML models to develop a lightweight IDS for edge devices to detect MQTT-based threats by taking MQTT dataset. Multiple security mechanisms ensure reliable and secure data sharing between fog nodes and edge devices during updates and security assessment of the suggested security model get up to99.69% accuracy. Agarwal et al. (2023) [21],the SDT (Splinted Decision Tree) method classifies the obtained features into different incursion groups and this approach splits the feature space, allowing for faster decision-making while maintaining accuracy. The NSL-KDD dataset is utilized to train and evaluate the model and proposed hybrid methodology outperformed standard intrusion detection approaches in terms of accuracy. Finally the model is resilient to network traffic variations and accurately detects both known and unknown intrusions. Todetecting intrusions in the IIoT, the Hybrid Deep Convolutional Auto encoder and Splinted Decision Tree (HDCA-SDT) technique is applied on NSL-KDD dataset and the accuracy of their detection is made up 98.9%.

Kota et al. (2021) [22],The IoT-HML system uses the induced wheel optimization (IWO) algorithm to construct clusters. Information is sent from the source node to the destination through the cluster head (CH), preventing data loss and improving security by ensuring a trusted path. This research demonstrates how a coach and player learning neural network (CP-LNN) can be utilized to monitor industrial processes and prevent accidents through basic control tactics.A hybrid ML technique is proposed for IIoT, which enableto overcome problems in both information security issues with accurate monitoring and control system by taking Synthetic dataset and the accuracy results are compared betweenexisting classifier like SVM 90.15%, KNN 93.1%, Deep Neural Network (DNN) 94.23% and purposed classifier CP-LNN 98.5%. Mrabetet al. (2022) [23],Their methodology might be used to enhance the security of IIoT designs for smart manufacturing. This involves using blockchain technology with ML algorithms. The TON_IoT dataset was used to evaluate the performance metrics of ML classifiers in an industrial setting, specifically against typical assaults and the accuracy results based on model classifiers are Decision Tree (DT) 99.96%, SVM 99.95 %, Random Forest (RF) 99.76%, Naive Bayes 78.1% , ANN 99.97% .

Zolanvari et al. (2019) [24] found that ML may address the existing gap in identifying new forms of attacks, such as backdoor, command injection and SQL injection. They demonstrated the effectiveness of an ML-based anomaly detection system in accurately detecting these assaults. To conduct a vulnerability assessment of IIoT systems, it is necessary to identify common malicious attacks, analyze the related risks, and investigate the use of ML techniques to minimize these threats. Toevaluated the performance of model by using Synthetic dataset, the accuracy results based on ML classifiers are RF 99.99%, LR 99.90%, DT 99.98%, KNN 99.98%, NB 97.48%, SVM 99.64%, ANN 99.64%. Kumar et al. (2022) [25], An IIoT IDS has been created utilizing the Inception network and Convolutional Neural Network (CNN). Experimental results show that this method provides information with high accuracy, an accurate detection rate and a low false alarm rate. Performance comparison of Traditional CNN is (98.25%) and Inception CNN is (75.03%) based on mobile network dataset. So the suggested model (Inception CNN) achieves a higher detection rate with a lower false positive rate and greater data accuracy.

Khan et al.(2021) [26]evaluated the trustworthiness of IIoT devices by analysing their location knowledge, temporal experience and behaviouralpatterns. The model suggests applying KNN clustering and SVM to classify the extracted attributes based on the neutrosophic weighted product method (WPM). The simulated sensor dataset gives 100% accuracy. The suggested neutrosophicSVM approach accurately identifies trust boundaries and calculates the final trust score. Chen et al. (2021) [27]presented a classification approach for detecting anomalies in ICS (Industrial control systems) environments. The suggested Long Short-Term Memory (LSTM) detection model was

evaluated utilizing ICS datasets from diverse sources and shown effective performance accuracy 86.58%.The suggested detection approach categorizes traffic flow protocols and discovers anomalies within each. There technique minimizes training time and enhances detection efficiency in diverse network contexts.

Supervised ML was used to automate IIoT role engineering and fine-grained access control by Usman et al. (2023) [28]. Their mapping methodology secures user confidentiality and resource access in SCADA-enabled IIoT environments using a fine-tuned multilayer feed forward artificial neural network (ANN) and an extreme learning machine (ELM) for role engineering. For the SCADA dataset, ELM was 89% accurate and ANN 96%. Naik et al. (2022) [29] compared anomaly detection ML classification methods. RF, LR, Light GBM, DT, and KNN are compared in this article. Four IIoT datasets were examined using PyCaret. On Demand versus Response and E-filtration painting maintenance datasets, RF achieved 99% and 98% accuracy, KNN 94% accuracy in semiconductor production, and RF 93.98% in HRSS. RF introduced the greatest anomaly detection accuracy (98.15%). The RF method surpasses with multivariate IIoT datasets.

Table 1: Summary of Existing Studies

Methods Used	Proposed Method	Performance Measures	Dataset	Benefit of the Study	Limitation of the Study	Year
DT RF GB	DT	Accuracy=99.68 % Precision=99.67% Recall=99.68% F1 score=99.66%	MQTTset dataset	It is effective against a wide range of internal and external attacks and strikes a balance between strong performance and high security.	The security issue might be arises in case of multi-tier IIoT structure.	2023
DL-IDPS PRI-IDS CNN-LSTM HDCA-SDT	HDCA-SDT	Accuracy=98.90 % Precision=98.70% Recall=98.20% F-Measure=98.50%	NSL-KDD dataset	The HDCA-SDT framework efficiently detects and classifies abnormalities in complicated datasets by introducing feature extraction capabilities.	The IIoT new dataset which could be acquired from the actual world quit be challenging for this model.	2023
ANN ELM	ANN	Accuracy=96.00% precision=93.00%, Recall=88.00%	SCADA Dataset	The highest level of flexibility may be quickly and	Not applicable for implementing attribute-	2023

		F1score=91.00%		efficiently achieved with fine-grained access control.	based access control for IIoT use cases.	
ANN DT SVM RF NB	ANN	Accuracy=99.97% Precision=100.00 % Sensitivity=100.00 %	TON_IoT dataset	Designing, structuring and implementing data structure and smart contracts in manufacturing.	Incorporate future technologies like 5G/6G communication systems in the network/ protocol layer is a challenging task.	2022
Traditional CNN Inception CNN	Inception CNN	Accuracy=75.03% Precision=73.67% Recall=75.01% F1 score=73.66%	mobile network data	To develop security and anti-intrusion technologies for IIoT.	The model has not been validated in a complex multi-interaction network, nor has it been applied in large-scale industrial processes.	2022
RF LR Light GBM DT KNN	RF	Accuracy=98.15% AUC=99.48% Recall=94.22% Precision=97.92% F1 score=96.03% Kappa=94.82% MCC=94.85%	HRSS dataset	Provides remarkable findings for multidimensional IIoT information.	In IIoT, complex and diverse data from various sensors can be combined to create an ensemble model for more accurate findings on large datasets.	2022
SVM KNN DNN CP-LNN	CP-LNN	Accuracy= 98.50% Sensitivity=97.30 % Specificity=98.20 % Precision=98.35% Recall=98.32% F-Measure=97.49%	Synthetic Dataset	CP-LNN utilized for the optimal best path computationfor monitoring the industry and preventing accidents by basic control strategies	It will not applicable for the diverse network.	2021
Neutrosophic K-NN						

clustering Neutrosophic support vector machine (SVM) classification	Neutrosophic support vector machine (SVM)	Accuracy= 100.00% Specificity=99.90 % Precision=98.30% Recall=100.00% F1 score=99.10%	Synthetic Dataset	To improve IIoT device experiences, extract features and provide a trust score for better decision-making.	Unable to address scalability issues in the industrial trust computation	2021
LSTM classification model	LSTM	Accuracy= 86.58% Precision=95.81% Recall=64.84% F1 score=77.33%	ICS datasets	This technique minimises training time and enhances detection efficiency in diverse network contexts.	The problem may come from cross-correlating security warnings across different levels of ICS settings.	2021
RF DT KNN LR SVM ANN NB	RF	Accuracy=99.99% MCC=96.81% Sensitivity=97.44 % UR=52.56%	Synthetic Dataset	A feature priority ranking was conducted to identify the key elements that distinguish attack traffic from normal traffic.		2019

3 Materials and Methodologies

Hyper-parameter tuning has always been a crucial part of prediction models. In this part, we introduce the existing research on these approaches.

3.1 XGBoost

XGBoost[30] is a potent approach for both regression and classification tasks. It is employed as a collection of successful programs derived from Kaggle tournaments. XGBoost is anensemble ML algorithm, utilizes the gradient boosting framework to iteratively construct decision trees in order to fit a value with residual and enhance the efficiency and performance of learners. XGBoost differs from gradient boosting by use a Taylor expansion to estimate the loss function. This approach results in a model that achieves a more favourable balance between bias and variance. Additionally, XGBoost often requires fewer decision trees to achieve greater accuracy. XGBoost is described below.
Let's consider a sample set with $'n'$ samples and $'m'$ features, denoted as$D = (xi, yi)$ $(|D| = n, xi \in Rm, yi \in R)$, where $'x'$ represents the eigenvalue and $'y'$ represents the actual value.The method aggregates the outcomes of $'N'$ trees to get the ultimate anticipatedvalue shown in Eq. (1).

$$\hat{y}_i = \sum_{n=1}^{N} f_n(xi), f_n \in F, Where\ F\ is\ the\ set\ of\ decision\ stumps\ or\ trees \quad \text{Eq. (1)}$$

3.2 Firefly Algorithm (FA)

The FA is an instance of swarm intelligence algorithm that was designed by Yang. Fireflies, often known as lightning bugs are typically seen emitting flashes of light in the sky during summer

evenings. The flashing activity of fireflies serves either to attract a potential mate or to protect themselves from predators. Another significant attribute of fireflies is that both the brightness of their light and the air's impact on the light intensity diminish as the firefly moves away from a brighter source. This decreased intensity occurs because the air absorbs the light as the distance between the firefly and the source grows. Consequently, the intensity of light is directly proportional to the degree of fitness. Despite this, the complicated nature of the natural habits of fireflies serves as a driving force to establish three assumptions in order to formulate a functional algorithmic approach. The following are the presumptions.

Fireflies were thought to be unisex and attracted to each other regardless of their gender.

The brightness of fireflies has a direct correlation to their attractiveness, which decreases with increasing distance.

The light intensity or brightness is determined by the practical implementation of the objective function.

In this context, the symbol $LI(d)$ denotes the intensity of light at a certain distance $'d'$, whereas $'LI_0'$ represents the intensity of light at the source. In addition, when simulating actual natural systems in which the surrounding environment partly absorbs light, the FA utilizes the $'\gamma'$ parameter to represent the light absorption coefficient. The majority of FA versions often use the Gaussian form in order to mimic the combined effect of the $'\gamma'$ coefficient and the inverse square rule for distance. The Eq. (2) represents the light intensity.

$$LI(d) = LI_0 * e^{-\gamma d^2} \quad \text{Eq. (2)}$$

Additionally, as seen in Eq. (3), the attraction $'\beta'$ of a particular firefly is precisely proportional to its light intensity and also relies on distance. The parameter $'\beta_0'$ represents the level of attract when the distance is zero $(d = 0)$. Eq. (3) is often substituted by Eq. (4) in practical applications.

$$\beta(d) = \beta_0 * e^{-\gamma d^2} \quad \text{Eq. (3)}$$

$$\beta(d) = \frac{\beta_0}{1 + \gamma d^2} \quad \text{Eq. (4)}$$

The Eq. (4) and (5) is the fundamental FA search equation for an individual $'k'$. In each iteration $i + 1$, individual $'k'$ travels to a new position $'x_k'$ towards individual $'l'$ with higher fitness. The Eq. (5) is expressed as follows.

$$x_k^{i+1} = x_k^i + \beta_0 * e^{-\gamma d_{k,l}^2}\left(x_l^i - x_k^i\right) + \alpha^i(u - 0.5) \quad \text{Eq. (5)}$$

The randomization parameter is represented by α. The random integer produced from either a Gaussian or uniform distribution is denoted as $'u'$. The spatial separation between two observed fireflies $'k' and 'l'$ is represented by $'d_{k,l}'$. The typical values that provide satisfactory solutions for most issues are 1 for $'\beta_0'$ and a range of values between 0 and 1 for $'\alpha'$.

3.3 Proposed Work

This section aims to analyse the effectiveness of optimization technique by comparing them on the X-IIoTID dataset. We employed an IIoT dataset, partitioned into a ratio of 80:20 for training and testing, respectively. We employed the conventional ML model in conjunction with an ensemble method. Subsequently, we evaluated its computational expense after hyper-tuning by optimization strategy like FA. In order to identify the most efficient methods for adjusting the hyper-parameters of the XGBoost algorithm, FA optimization technique has been evaluated based on their computational complexity. Figure 1 depicts the sequential process of the proposed approach.

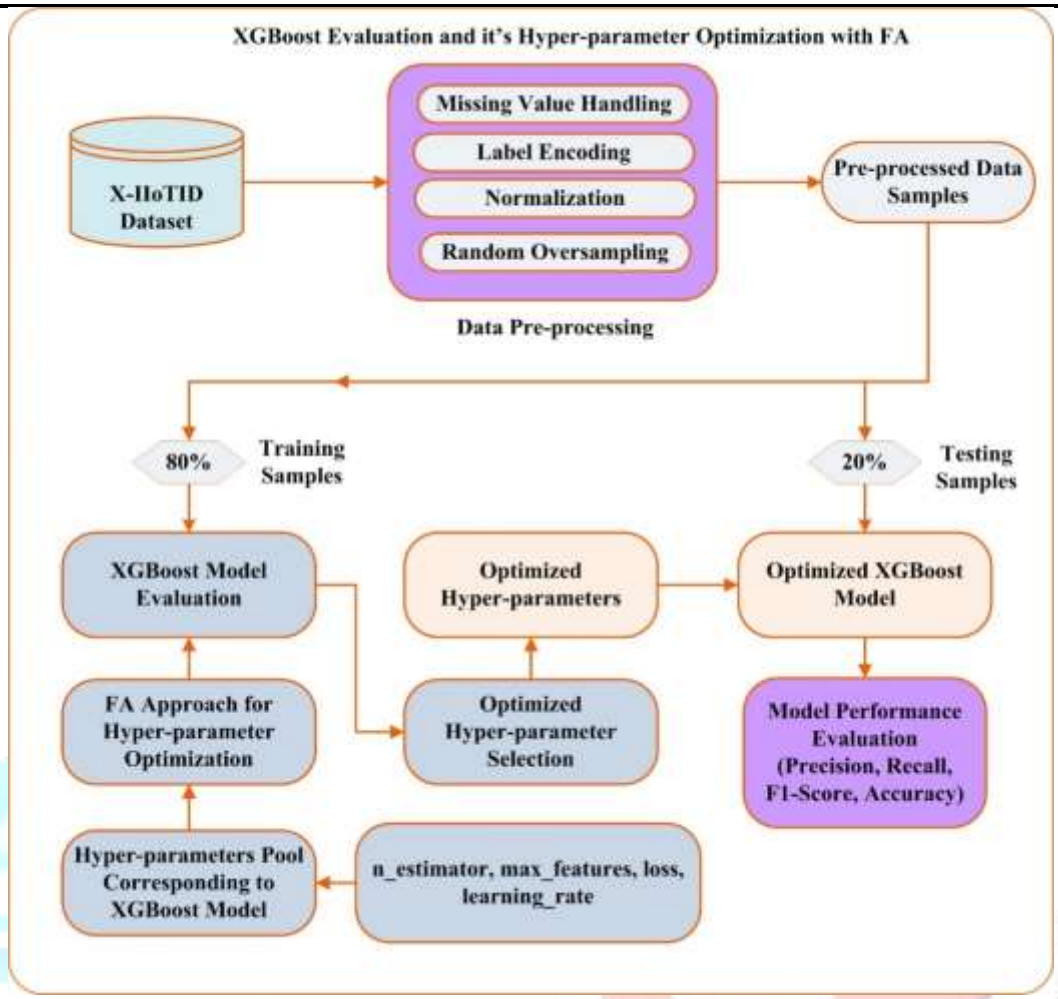


Figure 1: Proposed FA_XGBoost Architecture

4 Dataset Overview and Simulation Environment

The following section offers a comprehensive summary of several crucial information including specifics on the dataset, the simulation environment and a comparative evaluation of the outcomes derived from the proposed methodologies in contrast to previous research.

4.1 Simulation Setup

A HP Pavilion System with the following configurations has been employed for implementing the suggested approach, in addition to many ML methods and ensemble learning techniques for comparison: Required hardware for the experiment includes a 12th Gen Intel(R) Core (TM) i5-1240P 1.70 GHz processor, 32 GB of RAM, Windows 11 Home and an Intel iRISXe graphics processing unit. It also uses the Python programming language, ML methods and Google Colab Notebook for experiments. The research also makes use of the open-source ML framework Scikit-learn, data analysis tools NumPy and pandas, and visualization tools seaborn and matplotlib.

4.2 Dataset Overview

The X-IIoTID dataset for intrusion detection was obtained from IEEE-Data Port [31]. The final version of the X-IIoTID dataset contains 820,834 instances (421,417 observations/instances for normal and 399,417 for attacks), as well as 68 characteristics.

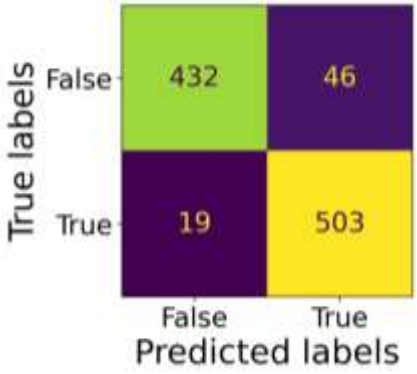
5 Result Analysis and Discussion

For evaluating the efficacy of the proposed method, the experimental process incorporates a range of ML and ensemble learning techniques. This section describes comprehensive information on the analysis of the findings. This research investigated a range of ML approaches, including LR, DT, SVM, KNN, as well as ensemble methods such as RF, AdaBoost, XGBoost and FA_XGBoost. Furthermore, all the approaches being studied, including the one suggested, were evaluated for their performance using measures such as precision, recall, F1 score, F2 score, ROC-AUC score and accuracy. The FA_XGBoost ensemble classification model stands out over all other models, obtaining an exceptional accuracy of 99.91%, precision of 0.9994, recall of 0.9991, F1 Score of 0.9992, F2 Score of 0.9990 and ROC-AUC score of 0.9994. The results indicate that, when evaluating measures such as precision, recall, F1 score, F2 score, ROC-AUC Score and accuracy, the proposed methodology shows more effectiveness compared to conventional ML methods and ensemble approaches. Table 2 presents a comprehensive analysis of the assessment measures used for evaluating the efficacy of different ML and ensemble methodologies, along with a suggested approach.

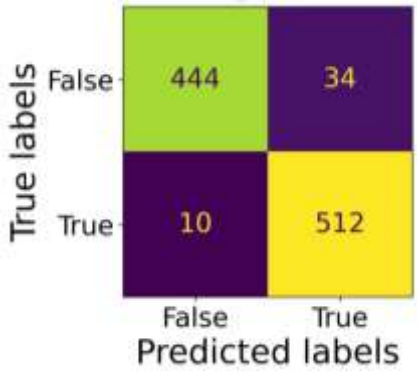
Table 2: Performance Comparison of All Classification Model

Classification Model	Accuracy (In %)	Precision	Recall	F1 Score	F2 Score	ROC-AUC Score
LR	93.67	0.9570	0.9030	0.9300	0.9140	0.9750
SVM	95.60	0.9770	0.9280	0.9520	0.9380	0.9930
KNN	97.20	0.9870	0.9530	0.9700	0.9600	0.9910
Adaboost	99.40	0.9941	0.9942	0.9941	0.9939	0.9981
XGBoost	99.60	0.9930	0.9970	0.9950	0.9970	0.9960
DT	99.64	0.9965	0.9963	0.9964	0.9960	0.9984
RF	99.70	0.9971	0.9970	0.9970	0.9970	0.9990
Proposed FA_XGBoost	**99.91**	**0.9994**	**0.9991**	**0.9992**	**0.9990**	**0.9994**

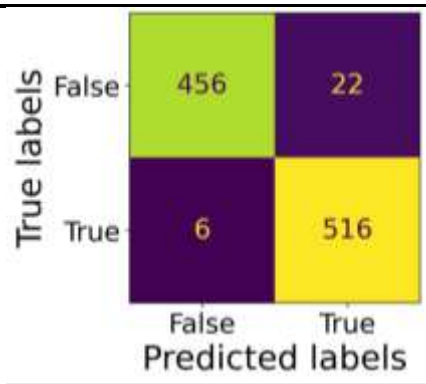
Figure 2(a) to (h) displays the confusion matrix of the proposed approach and other methods in relation to the testing data. Figures 3(a) to 3(h) show the Receiver Operating Characteristic (ROC) curves and the related Area under the ROC Curve (AUC) values for labels 1 to 6.This result demonstrates the efficacy of the proposed methodology in figure 2 (h) and 3 (h).



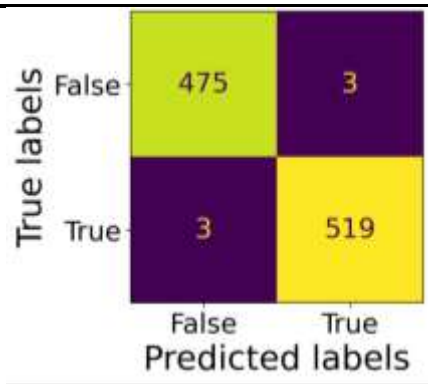
(a) LR



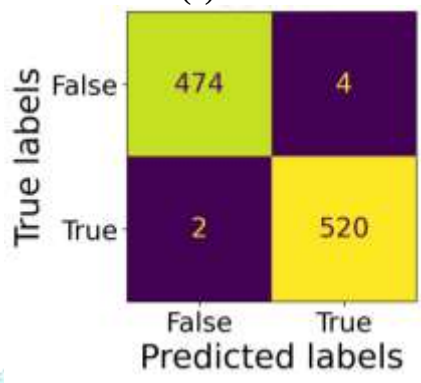
(b) SVM



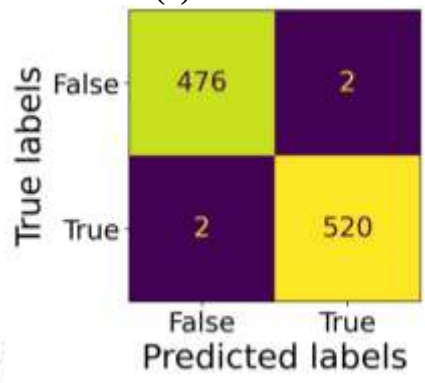
(c) KNN



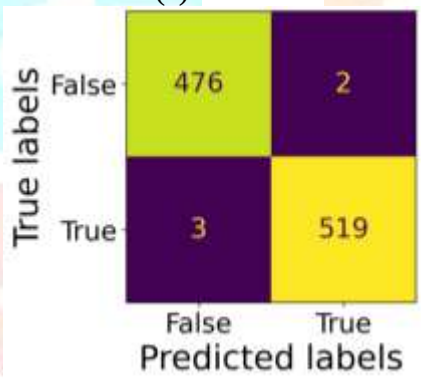
(d) AdaBoost



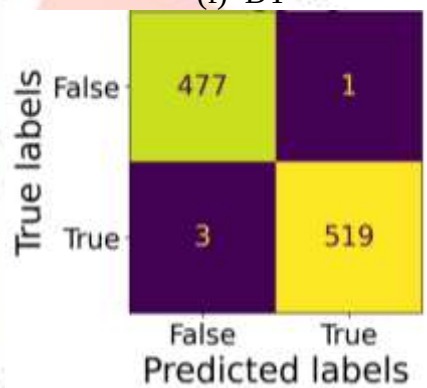
(e) XGBoost



(f) DT

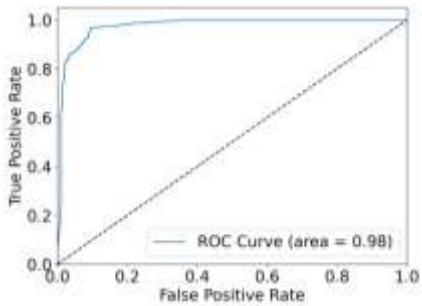


(g) RF

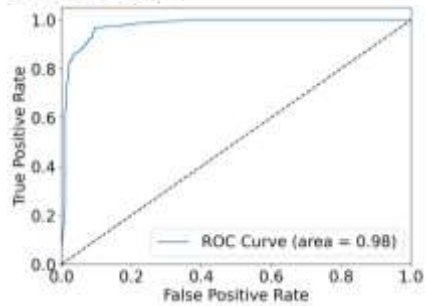


(h) Proposed FA_XGBoost

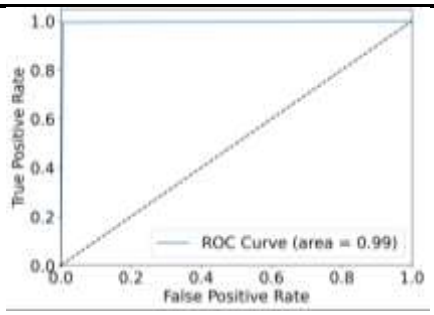
Figure2: Confusion Matrix Analysis for all Investigated Models



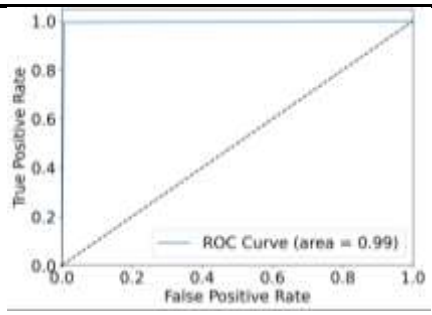
(a) LR



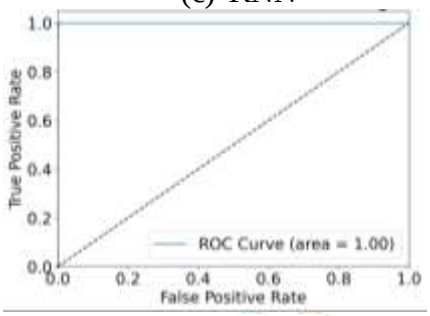
(b) SVM



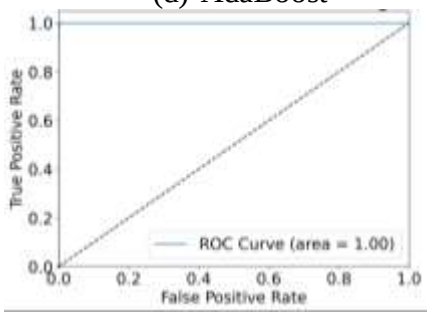
(c) KNN



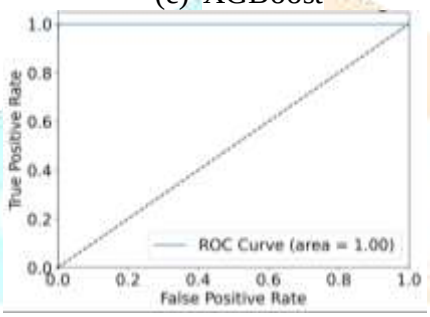
(d) AdaBoost



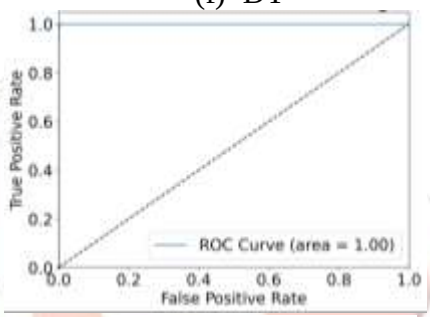
(e) XGBoost



(f) DT



(g) RF



(h) Proposed FA_XGBoost

Figure 3: ROC-AUC Analysis for all Investigated Models

Figure 4 displays the graphical depiction of the accuracy results for all the ML and Ensemble approaches that were examined in this research. The figure demonstrates that the proposed FA_XGBoost model has attained a higher level of accuracy in comparison to the accuracy of the analysedML algorithms and other ensemble techniques. According to the visual observations, the recommended solution consistently demonstrates superiority in each area of IIoT communication features. The system's resilience and effectiveness is addressing cyber-attacks in real-world IIoT environments.

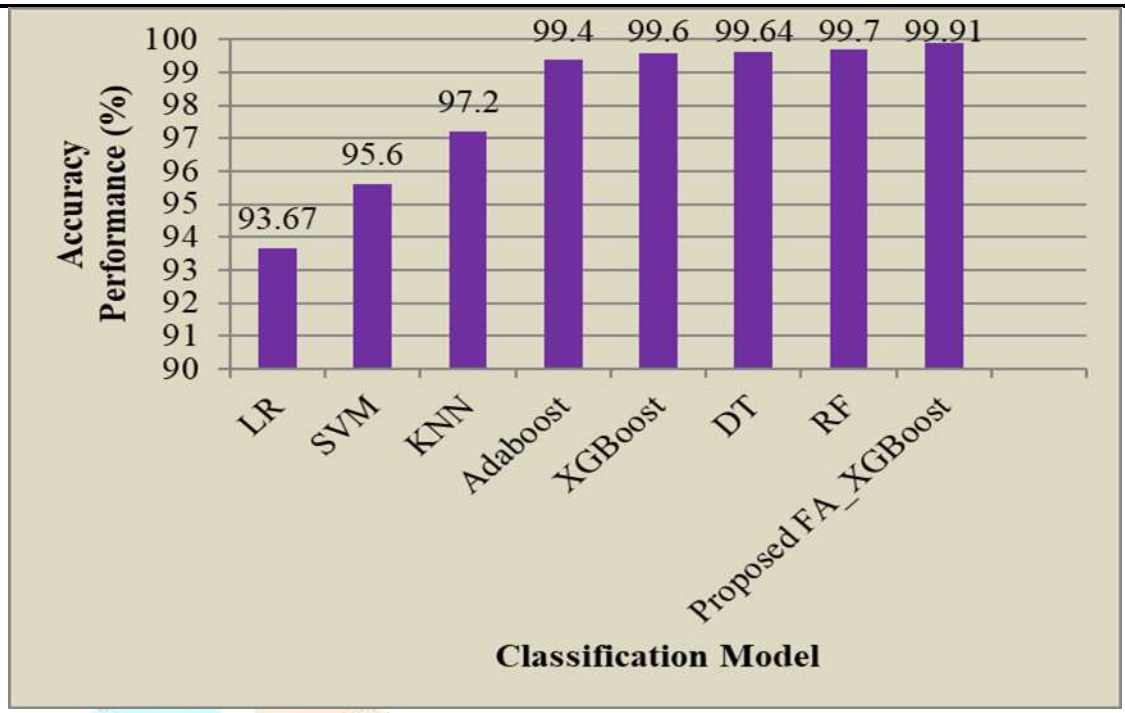


Figure 4:Accuracy Analysis All Considered Model

6 Conclusion and Future Scope

In recent years, the increasing use of advanced technology and the simultaneous growth of the worldwide population have led to a continuous rise in expenditures for IIoT and related services. Furthermore, the rapid progress in IoT technology has greatly contributed to the substantial growth of the IIoT, with the main aim of improving the overall prosperity of businesses. Hence, it is essential to include the IIoT in the sector to ensure the delivery of cost-efficient services of exceptional calibre. A major challenge faced while implementing the IIoT ecosystem is the increasing vulnerability to cyber-attacks. To strengthen the security of the IIoT ecosystem against cyber-threats, several researchers are actively involved in developing various techniques to strengthen its defenses against hostile cyber incursions. This research presents an improved method that utilizes FA_XGBoost ensemble learning to enhance the accuracy of IDS and protect the security of IIoT systems concurrently. Moreover, the results and assessments continuously indicate that the proposed model has attained a precision rate of 99.91% when compared to other models. The model's potential enhancement may be attained via the combination of ML techniques, DL methodologies and complex algorithms.

References

1. Xiong Luo, Ji Liu, Dandan Zhang, Xiaohui Chang, A Large-scale web QoS prediction scheme for the Industrial Internet of Things based on kernel machine learning algorithm, Computer Network, 101 (2016) 81-89.
2. https://www.spiceworks.com/tech/iot/articles/what-is-iiot/.
3. https://www.iberdrola.com/innovation/what-is-iiot.
4. Abbas Yazdinejad, Mostafa Kazemi, Reza M. Parizi, Ali Dehghantanha, Hadis Karimipour, “An ensemble deep learning model for cyber threat hunting in industrial internet of things”, Digital Communications and Networks 9 (2023) 101–110.
5. A. Al-Abassi, H. Karimipour, A. Dehghantanha, R.M. Parizi, An ensemble deep learning-based cyber-attack detection in industrial control system, IEEE Access 8 (2020) 83965–83973.
6. A. Yazdinejad, R.M. Parizi, A. Bohlooli, A. Dehghantanha, K.-K.R. Choo, A highperformance framework for a network programmable packet processor using p4 and fpga, J. Netw. Comput. Appl. 156 (2020), 102564.

7. Hakan Can Altunay, ZaferAlbayrak, " A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks", Engineering Science and Technology, an International Journal 38 (2023) 101322.
8. https://onix-systems.medium.com/what-are-the-advantages-and-disadvantages-of-machine-learning-d2a4eb025929.
9. P. Ambika, "Chapter Thirteen - Machine learning and deep learning algorithms on the Industrial Internet of Things (IIoT)", Volume 117, Issue 1, 2020, Pages 321-338.
10. K. Suthar, Q.P. He, Multiclass moisture classification in woodchips using iiotwi-fi and machine learning techniques, Comput. Chem. Eng. 154 (2021), https://doi.org/10.1016/j.compchemeng.2021.107445 107445.
11. H. Alaiz-Moreton, J. Aveleira-Mata, J. Ondicol-Garcia, A. L. Muñoz-Castañeda, I. García, and C. Benavides, "Multiclass classification procedure for detecting attacks on MQTT-IoT protocol," Complexity, vol. 2019, pp. 1-11, 2019.
12. E. Jove, J. Aveleira-Mata, H. Alaiz-Moretón, J.-L. Casteleiro-Roca, D. Y. Marcos del Blanco, F. Zayas-Gato, et al., "Intelligent One-Class Classifiers for the Development of an Intrusion Detection System: The MQTT Case Study," Electronics, vol. 11, pp. 422- 433, 2022.
13. M. A. Ferrag, L. Shu, H. Djallel, and K.-K. R. Choo, "Deep learning-based intrusion detection for distributed denial of service attack in Agriculture 4.0," Electronics, vol. 10, pp. 1257-1282, 2021.
14. https://www.hindawi.com/journals/wcmc/2023/3939895.
15. Gamal Eldin I. Selim, EZZ El-Din Hemdan, Ahmed M. Shehata &Nawal A. El-Fishawy, " Anomaly event classification and detection system in critical industrial internet of things infrastructure using machine learning algorithm", volume 80, pages 12619-12640, 2021.
16. Attila Frankó ,GergelyHollósi , DánielFiczere and Pal Varga, " Applied Machine Learning for IIoT and Smart Production—Methods to Improve Production Quality, Safety and Sustainability",Sensors 2022, 22, 9148. https://doi.org/10.3390/ s22239148.
17. Yang, Xin-She. "Firefly algorithms for multimodal optimization." International symposium on stochastic algorithms. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. Doi: 10.1007/978-3-642-04944-6_14.
18. Jawad Ahmad Syed Aziz Shah,Shahid Latif, Fawad Ahmed, Zhuo Zou, Nikolaos Pitropakis, "DRaNN_PSO: A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things",Journal of King Saud University – Computer and Information Sciences 34 (2022) 8112–8121.
19. Qian You and Bing Tang, "Efficient task offloading using particle swarm optimization algorithm in edge computing for industrial internet of things",Journal of Cloud Computing: Advances, Systems and Applications (2021) 10:41 https://doi.org/10.1186/s13677-021-00256-4.
20. Qaddoori, Sahar L., and Qutaiba Ibrahim Ali. "An efficient security model for industrial internet of things (IIoT) system based on machine learning principles." *Al-Rafidain Engineering Journal (AREJ)* 28.1 (2023): 329-340.
21. Agarwal, Neha, Rajendra Pandey, and SmithaRajagopal. "RESEARCH ON IIOT SECURITY: NOVEL MACHINE LEARNING-BASED INTRUSION DETECTION USING TCP/IP PACKETS." *Proceedings on Engineering* 5.S1 (2023): 63-68.
22. Kota, Prabhakar N., Ashok S. Chandak, and B. P. Patil. "IOT-HML: A hybrid machine learning technique for IoT enabled industrial monitoring and control system." Concurrency and Computation: Practice and Experience 35.3 (2023): e7458.
23. Mrabet, Hichem, et al. "A secured industrial Internet-of-things architecture based on blockchain technology and machine learning for sensor access control systems in smart manufacturing." Applied Sciences 12.9 (2022): 4641.
24. Zolanvari, Maede, et al. "Machine learning-based network vulnerability analysis of industrial Internet of Things." IEEE Internet of Things Journal 6.4 (2019): 6822-6834.
25. Kumar, A. Arun, and Radha Krishna Karne. "IIoT-IDS Network using Inception CNN Model." Journal of Trends in Computer Science and Smart Technology 4.3 (2022): 126-138.

26. Khan, Mohammad Ayoub, and Norah Saleh Alghamdi. "A neutrosophic WPM-based machine learning model for device trust in industrial internet of things." Journal of Ambient Intelligence and Humanized Computing 14.4 (2023): 3003-3017.
27. Chen, Chia-Mei, Zheng-XunCai, and Gu-Hsin Lai. "A study of identifying attacks on industry internet of things using machine learning." Computer Science & Information Technology (CS & IT) (2021): 77-82.
28. Usman, Muhammad, et al. "Automatic Hybrid Access Control in SCADA-Enabled IIoT Networks Using Machine Learning." *Sensors* 23.8 (2023): 3931.
29. DS, BhupalNaik, VenkatesuluDondeti, and SivadiBalakrishna. "Comparative analysis of machine learning-based algorithms for detection of anomalies in IIoT." International Journal of Information Retrieval Research (IJIRR) 12.1 (2022): 1-55.
30. Ramraj, Santhanam, et al. "Experimenting XGBoost algorithm for prediction and classification of different datasets." International Journal of Control Theory and Applications 9.40 (2016): 651-662.
31. https://ieee-dataport.org/documents/x-iiotid-connectivity-and-device-agnostic-intrusion-dataset-industrial-internet-things.

lighten the workload of human operators performing manual surveillance and facilitate making proactive decisions which would reduce the impact of incidents and recurring congestion on roadways. This article presents a novel approach to automatically monitor real time traffic footage using deep convolutional neural networks and a stand-alone graphical user interface. The authors describe the results of research received in the process of developing models that serve as an integrated framework for an artificial intelligence enabled traffic monitoring system. The proposed system deploys several state-of-the-art deep learning algorithms to automate different traffic monitoring needs. Taking advantage of a large database of annotated video surveillance data, deep learning-based models are trained to detect queues, track stationary vehicles, and tabulate vehicle counts. A pixel-level segmentation approach is applied to detect traffic queues and predict severity. Real-time object detection algorithms coupled with different tracking systems are deployed to automatically detect stranded vehicles as well as perform vehicular counts. At each stages of development, interesting experimental results are presented to demonstrate the effectiveness of the proposed system. Overall, the results demonstrate that the proposed framework performs satisfactorily under varied conditions without being immensely impacted byenvironmental hazards such as blurry camera views, low illumination, rain, or snow.

Background or Context:
Manual traffic surveillance is time-consuming and prone to human error.

Objective or Aim:
To design and implement an AI-powered traffic monitoring system using deep learning for vehicle detection, counting, congestion monitoring, and stationary vehicle identification.

Methods / Methodology Summary:
This system employs YOLOv3, Faster R-CNN, Mask R-CNN, and CenterNet, integrated into a GUI, trained on annotated video data for real-time detection and tracking.

Key Results / Findings:
The system achieved high accuracy in detecting congestion (92.8%) and vehicle types (up to 99%), demonstrating robustness under varying environmental conditions.

Conclusion or Implications:
The model provides a scalable, cost-effective, and automated solution for intelligent traffic surveillance and management.