Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

A CNN-Fuzzy Logic Approach for Real-Time Intrusion Detection and Prevention in Industrial IoT Systems

[1]*Aziboledia Frederick Boye, [2]Onate Egerton Taylor, [3]Vincent Ike Emeka, [4]Emmanuel Okoni, Bennett

[1]Rivers State University, Port Harcourt, Nigeria
[2,3,4]Rivers State University, Dept. of Computer Science, Port Harcourt-Nigeria
*Corresponding Author: Boye Aziboledia Frederick, E-mail: bayelsaforprogress2022@gmail.com

Abstract: With the growing integration of the Industrial Internet of Things, securing these systems from cyberattacks and cyber threats has become critical. This research proposes a novel real-time intrusion detection and prevention (IDPS) combining Convolutional Neural Networks (CNN) and Fuzzy Logic (FL) approach for the industrial IoT systems tested on the dataset. Implemented in Python programming language using the Jupyter environment, this hybrid model leverages CNN's spatial feature extraction capabilities with Fuzzy Logic's adaptability in handling data uncertainty, achieving an acceptable industrial accuracy of 92.5% for industrial IoT systems. The system also maintained an average low false positive rate (FPR) of 2.51%, underscoring its effectiveness in distinguishing benign from malicious activity within industrial IoT networks. Additionally, the model achieved an average detection rate (DR) of 92.9% during simulation, making the model viable and allowing a quick response to potential threats. The system's latency achieved low metric average results measured in 1.207 µsec, or 0.001207 milliseconds given a less percentage of 7.14% latency average acceptable and good and excellent for most industrial IoT applications. These findings demonstrate that a CNN-Fuzzy Logic approach offers both high accuracy and efficiency, proving to be a promising for industrial cybersecurity in industrial IoT environments.

Keywords: Intrusion Detection, Industrial IoT, Cybersecurity, CNN, Fuzzy Logic, Machine Learning, Dataset, Real-Time Threat Prediction time.

I. INTRODUCTION

The study entails an approach to improve detection and preventing threats in real-time using CNN-Fuzzy techniques in the industrial IoT ecosystem with a proposed approach to enhance the potential cyber threat in industry. The approach will improve performance metrics balancing accuracy, threat detection time, latency and the false positive rate in IDS. As technology continues to evolve, cybercrime is also growing at its own pace. Cyber actors are employing ever-more sophisticated tactics to target individuals, businesses and critical infrastructures. In today's complex industrial landscape, manufacturing organizations are confronted with an expanding spectrum of risks. This evolution exposes the sector to sophisticated cyber threats targeting critical infrastructure, operational technologies (OT), and supply chains, enhancing the cybersecurity landscape of the energy industry, offering several opportunities in the industry [53]. Effective owners and operators, the effective measurement and management of these risks are not just beneficial; they are essential for sustained operation and protection against potential threats [1]. The backbone of Industrial IoT is established by enabling a large plethora of technologies including IoT, cloud computing, big data analytics, artificial intelligence, cyber physical systems (CPS), etc. [47] This adoption of industrial IoT technology across industries has increased automation and productivity; however, it has also introduced new vulnerabilities, particularly from sophisticated cyberattacks. Traditional intrusion detection systems (IDS) struggle to keep up with the dynamic nature of industrial IoT networks, where diverse devices communicate and exchange data. So, conventional intrusion prevention methods such as access control firewalls and encryption cannot fully prevent systems from advanced attacks. Intrusion Detection System has become a crucial part of computer security, which is used in detecting the above-mentioned threat [57]. Hence the importance of intrusion detection and prevention systems, which play a crucial role in addressing these attacks and protecting against them [9]. Moreover, successful detection of new attacks requires a vast amount of data to create models of normal behavior and anomalies [5]. The need arises to utilize intrusion detection and prevention systems (IDSs) for training on a compelling dataset [29]. The study considers using platform datasets based on specific applications, anomaly detection, and the type of data available. This research specifically focuses on

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

evaluating the system's efficacy in identifying attacks using the Kaggle IIoTset dataset which encompasses varied industrial IoT attack patterns. The system was implemented using python programming language and Python Flask framework [24].

II. LITERATURE SURVEY

Current intrusion and detection and prevention (IDSPs) techniques for industrial IoT integrates using machine learning and anomaly detection but frequently suffer from high false positive rates and inadequate response times. CNN's ability to capture spatial features, combined with the flexibility of Fuzzy Logic for managing uncertainty, is a novel approach for IIoT security. Numerous studies have explored the application of ML-based IDSs in safeguarding industrial IoT ecosystems [3]. Listed several techniques in preventing cyberattacks, among thelist of best prevention practices was to Ensure the right Tools & Processes are in place, the author went to ahead to enlist intrusion detection and prevention systems (ID/PS) as a tool to mitigate or detect and prevent MitM attacks [47].An artificially full-automated intrusion detection system for Fog security against cyberattacks was proposed by [8]. They use multi-layered recurrent neural networks applied to the NSL-KDD dataset for detecting four types of attacks: DDoS, Probe, U2R and R2L. In addition, they do not implement blockchain in their solution as an integrated mechanism for monitoring and securing industrial IoT networks [47]. Another model integrates the CNN and the Bi-directional long short-term memory (BiLSTM), to learn the spatial and temporal features. The synthetic minority oversampling technique (SMOTE) algorithm is used to tackle the problem of minority classes in the unbalanced data. The CNN-BiLSTM model achieved an overall accuracy of 82.74% and 77.16% for NSL-KDD and UNSW-NB15, respectively [32]. In another research work presented by [27] where a dynamic malware detection framework using Deep Neural Network (DNN) and Convolutional Neural Network (CNN) was proposed for malware detection. Long Short-Term Memory (LSTM) is used to construct the machine learning model. Between CNNs and the LSTM network, a novel approach was used for determining suspicious samples of malware [27]. The evaluation report, a combination of DNN and LSTM provide effective in detecting new malware and achieved 91.63% accuracy. A real-time hybrid intrusion detection approach was proposed in which misuse approach was used to detect well known attacks while anomaly approach to detect novel attacks. In this work a high detection rate was achieved because patterns of intrusions that could escape the misuse detection could be identified as attack by the anomaly detection technique [14]. The model's accuracy increased incrementally each day up to a significant value of 92.65% on the last day of the experiment, also, as the model learns and trains the system each day, the rate of false negative decreases sharply. Also, a study in [19] focused on enhancing the detection rate of an intrusion detection system based on combining the fuzzy system and particle swarm optimization (PSO) method. The PSO method was implemented to generate a fuzzy rule base to detect DDOS attacks. Because of the fuzzy rules generated, the proposed fuzzy system was built, and the result reached 0.93% as an average detection rate [19]. Another research lists four (4) guards against Ransomware, including intrusion detection and prevention systems (ID/PS) and that organizations, like industrial IoT firms outsource to a managed detection and response (MDR) specialist. MDRServices include monitoring, detecting, alerting, and managing responses to potential attacks on your system[26]. proposed a hybrid model based on improved fuzzy and data mining techniques, which can detect both misuse and anomaly attacks [51]. Similarly, another proposed a scheme combining a genetic algorithm and fuzzy logic for network anomaly detection. The genetic algorithm is used to generate a digital signature of a network segment, and the fuzzy logic scheme decides whether an instance represents an anomaly. With real network traffic, the proposed approach achieves an accuracy of 96.53% and a false positive rate of 0.56% [28].

2.1 Machine Learning Algorithm

The study explores the features and integration of two algorithms, CNN and fuzzy logic, which are also machine learning (ML) classifiers. Authors describe machine learning classification techniques that have been utilized in numerous published papers to develop effective IDS using diverse datasets for diverse types of attacks. Machine learning is a subfield of artificial intelligence that involves constructing models using algorithms trained on specific data and then applying those models to other data to make predictions [39]. However, the rise of machine learning techniques has opened new possibilities for the detection of outlier data due to the availability of substantial amounts of information to be used by ML models. Scholars have made successful progress in integrating CNN and fuzzy logic, yet not many in industrial IoT systems. The conjunction the two techniques leverages the strength of both methodologies [44].The utilization of machine learning (leveraging Random Forest (RF) for feature extraction and Recurrent Neural Network (RNN) for classification) has significant importance in the identification and prevention of distributed denial of service (DDoS) attacks [23].

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

2.2 Industrial Internet of Things (IIoT)

As a subset of IoT, Industrial IoT covers the domains of machine-to-machine (M2M) and industrial communication technologies with automation applications, also enabling a large plethora of other technologies including IoT, cloud computing, big data analytics, artificial intelligence, cyber physical systems (CPS), humane-to-machine (H2M) etc. [36]. The manufacturing phase of the product lifecycle is where the IoT and Industry 4.0 meet, originating from the industrial IoT, which paves the way to better understanding of the manufacturing process, thereby enabling efficient and sustainable production [21]. By incorporating industrial IoT systems into large production and process plants, we can achieve the goal of becoming a Smart Industry [46]. Most especially, various techniques have been employed in the development of Network Intrusion Detection System to safeguard the network against the evolving nature of attack deployed by cyber-criminals. As a result, cybersecurity concerns have become more relevant across the field of manufacturing [17]. One of the main tracks of research in this field deals with developing effective cyber-security mechanisms and frameworks that can identify, classify, and detect malicious attacks in industrial IoT devices [38], and advise that there is no denying the importance of implementing an industrial IoT system with a lens toward the future. Any hardware used in industrial IoT should be secured using hardware security modules. Regular system security audits should be performed to ensure that system security is up to industry standards, especially in highly regulated industries [31]. The integrated IoT/IIoT systems need cybersecurity monitoring and control due to the present and unrelented cyberattacks on these systems [24].

2.3 Cybersecurity and Attacks

Machine learning as subset of artificial intelligence has become an indispensable tool in cybersecurity, addressing a range of challenges from threat detection, proactive and preemptive defense, is adept at pattern recognition and anomaly detection, that is why it excels in identifying potential threats, the ability of AI to learn from past incidents improves the accuracy of its response over time, making it adaptable to emerging tradecraft, enables organizations to leverage always-on vigilance, it helps protect your systems against known threats and potential future vulnerabilities [37]. The study entails the design of a machine learning model in real-time intrusion detection and prevention in industrial IoT ecosystem with the Kaggle dataset network profiles and pattern of ransomware, DDoS and MitM. Manufacturers are confronted said with a range of cybersecurity threats, including ransomware attacks that disrupt services to demand payment, distributed denial of service (DDoS) attacks that overwhelm systems, man-in-the-middle (MitM) that attacks that disrupt normal system operation may not be identified in time and could cause damage to equipment [5]., and advanced persistent threats (APTs) that target SCADA (supervisory control and data acquisition) and ICS systems, exposing operators to cyber incursions and events that could threaten physical safety [1]. SCADA, PLC and DCS systems, with their reliance on proprietary network protocols and equipment, have long been considered immune to the network attacks that have emerged recently in the networking paradigm. However, recent studies prove that this assumption is not correct. Recently, standards such as Ethernet, TCP/IP, and web technologies have been compromised to attack the ICSs [5]. Regarding the studies by industry, such as IBM, attacks targeting the ICSs are already up by 110 percent. Some recent notable ICS attacks include the cyber-attacks on the European Energy Company, New York dam attack, Russian cyber-attack on the Ukrainian power grid [40].

2.4 Cyberattacks by Industry and Revenue

Organizations hit by 99% cyberattack were able to identify the root cause of the attack, with exploited vulnerabilities, the most identified starting point for the second year running [53]. For instance, energy, oil/gas and utilities are the sector most likely to fall victim to the exploitation of unpatched vulnerabilities, this industry typically uses a higher proportion of older technologies more prone to security gaps than many other sectors. Government and organizations with abuse of compromised credentials have 49% (state/local) and 47% for central/federal of attacks began with the use of stolen login data, whereas IT, technology and telecoms and retail both reported that 7% of ransomware incidents began with a brute force attack [53].

2.5 Ransomware

The threat of ransomware attacks continues to grow both in terms of number of affected victims as well as the cost incurred by the people and organizations impacted in a successful attack [55]. A report reveals that ransomware has emerged as the predominant method for OT cyberattacks [1]. Ransomware takes over the victim's device, and blocks or encrypts the data, therefore, preventing the victim from using the device [20]. The victim can get back to using the device or its data only if ransom is paid [48]. With the rise of Ransomware-as-a-Service (RaaS) platforms, such as LockBit 3.0, available on the dark web, the threat landscape has intensified. For instance, IRGC-affiliated actors operating under the Cyber Av3ngers persona gained

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

access to the Israeli-made Unitronics Series ICS PLCs [11]. In response to the defacement, a few of the water-sector victims briefly shut down their systems and switched to manual operations. Research articles on cybersecurity and ransomware started getting published around the year 2016. There was research offering a defense plan to protect oil and gas automation and control systems [17].

2.6 Distributed Denial of Services (DDoS)

The digital threat landscape continues to evolve rapidly, with DDoS attacks reaching new levels of scale, complexity, and impact. These attack leverages multiple compromised systems to flood a target with overwhelming traffic, disrupting services and denying access to legitimate user's cybercriminals and state-sponsored actors increasingly exploit vulnerabilities in critical infrastructure such as utilities, aiming to disrupt operations, steal sensitive data or gain geopolitical leverage [31]. These attacks take various forms including DDoS published in [22]. A distributed denial of service (DDoS) is a malevolent attempt to make an online service unavailable to genuine customers by simply stopping or delaying the host server's service and is one of the most critical issues in network security[1]. DDoS has become more sophisticated in the last several years as the level of attack automation has increased [38]. During 2022, organizations around the globe mitigated an average of 29.3 attacks per day during Q4 2022, which was 3.5 times more compared to the 8.4 attacks per day the organizations saw at the end of 2021 [24].Several mitigation strategies have been introduced by various authors, not only detection techniques but also developed prevention systems to defend against DDoS attacks and minimize the destructive effects of these types of attacks on legitimate users of targeted systems by [1]. As for the power sector, these attacks can disrupt real-time monitoring systems, delay automated responses and hinder communication between grid operators. A prolonged DDoS attack on a smart grid can even lead to cascading failures that impact entire regions [16].

2.7 Man-in-the-Middle (MitM)

MitM attack is a type of attack carried out by a malicious internal user on two computers by pretending to one that he is the other [50]. MitM can be of two categories, Eavesdropping. Eavesdropping is passive as the adversary is only interested in the information passing through. In Manipulation MitM, the adversary changes data while masquerading it as the original sender[8]. In an MitM attack, an attacker sits in between two nodes (the sender and the receiver) and creates an independent connection by secretly relaying traffic between the nodes, making the attacked nodes believe that they are directly communicating with one another (by impersonating the sender for transmitting information to the receiver[4].

2.8 Cyberattacks Mitigation Strategies

Detecting and neutralizing an adversary inside your environment before they can compromise your backups or encrypting your data will considerably improve your outcomes [11]. The study will structure the cyberattack countermeasures or mitigations with the research objectives developing a model on real-time intrusion detection and prevention in industrial IoT systems (applications). Ransomware cyberattacks research for cybersecurity in CPS, appends that machine learning techniques were adopted as one of the most recommended tools for cyber security in energy and industrial sectors [49]. Also, with therefore, with the increasing sophistication and frequency of cyberattacks necessitate a robust and proactive cybersecurity posture [35], another paper suggests that IDSs/IPSs are a vital part of the Defense-in-Depth strategy, because so many inherent vulnerabilities are within the industrial IoT network, and an individual can only do so much to monitor potentially unwanted traffic [30], and has adopted several recent defense mechanisms against DDoS intrusions based on technical, operational defense/mitigation strategies including the trusted platforms of type of hybrid machine learning model [40]. It is necessary to have MitM detection systems in place that work together with other SIEM tools. It is necessary to have tools and processes that prevent these attacks in the first place . This is because analyzing traffic for anomalies and unauthorized devices enables timely responses, which is crucial to detecting and preventing MitM attacks in today's modern security landscape. Below is an example of a cyber actor trying to attack an industrial control system (ICS) [31]. However, one notable exception was a steep decline in tracking intrusions detected and remediated, from 52% in 2023 to only 28% in 2024. issues the following top recommendations as best practices for utilities, and other sectors. Change default passwords immediately, inventory ICS assets to find vulnerable devices and manage associated common vulnerabilities & exposures (CVEs), enforce user access controls and multifactor authentication for remote access, conduct a cybersecurity risk assessment focused on reducing exposure to the public-facing internet [13].

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

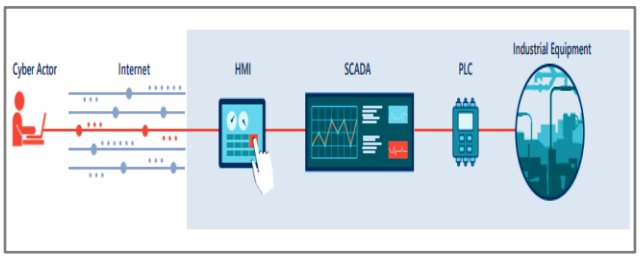

Figure 1: Cyber Actor Attacks ICS Infrastructure

In another research, implement threat detection and monitoring, develop and exercise cybersecurity incident response and recovery plans, etc. Fortunately, in the survey study 85% of organizations plan to improve their OT security capabilities in 2023. 70% of organizations also plan to increase their OT security budget allocation. This is a boost to securing critical infrastructure and smart manufacturing OT security which is part of industrial IoT system [7].

III. METHODOLOGY

This encompasses dataset collection, model selection, object-oriented approach, data flow diagrams, System design and analysis, model training and testing, and model performance evaluation, discussion and recommendations. The dataset obtained are the List of attack scenarios included in Normal traffic Kaggle Dataset and Edge-IIoTset dataset for Industrial Internet of a Thing attacks [24]. The Comma Separated Value (CSV) File secondary dataset obtained from Kaggle.com as extracted, the list of attacks scenarios included in the Edge IIoTset and the normal traffic dataset for industrial IoT attacks, also, description of extracted dataset features from all the attacks and the normal traffic that contains network traffics of DDoS, Ransomware and MitM profile attacks were used for the designing of the hybrid approach. Kaggle is a network activity dataset, which was extracted from the activities performed in an active network with attacks and anomalies. Such attacks/anomalies are the 229, 023 of DDoS attacks on an active HTTP flood attack, 1,230 of MitM attacks also done on an active network where the intruder mimics the real network protocols or activities. Then, 10, 926 Ransomware attacks on an active network using the loopholes in the system to gain access. 70% of the dataset network activity dataset collected were used for training, 30% for the testing process with the model [24].

3.1 System Architecture

The system architecture is made of the entry level, inference level, industrial level and action level. At the entry level of the system architecture, we have the quarantine database, network monitor and incoming network traffic. The Inference level is situated immediately below the entry level, and it comprise the two-machine learning (ML) features employed for the system design, it is made of the CNN inference engine and fuzzy logic inference engine. While CNN inference engine uses several types of classifiers, fuzzy logic inference engine uses membership functions. At the Industrial level, several industrial hardware or software's (industrial instrumentation on automation with different operational principles connected on network) been protected by the system. At this Action Level: This level is portioned for trained cybersecurity experts willing to deploy knowledge to mitigate against any intrusion and making corrections from the system during operational hours. The system architecture is shown below in figure 2.

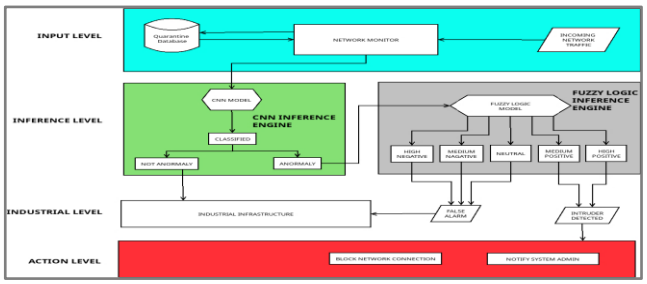

Figure 2: System Architecture

3.2 CNN Inference Engine Block

CNNas a pivotal approach in real-time detection and prevention systems including detection of anomalies. The Fig 5 below shows the CNN block and how it works during the hybrid ML model, where raw incoming network data is fed into the input layer (IL) of the CNN for processing. The Convolutional Layers (CL) then apply convolutional filters (kernels) to the input and incoming data, performs element-wise multiplication, capturing local patterns and features like edges and textures. The non-linear activation function like ReLU (Rectified Linear Unit) during the CNN extraction process is applied after each convolution to introduce non-linearity into the model allowing it to learn more complex patterns. Batch Normalization during the extraction process may be applied to stabilize and speed up training by normalizing the output of the CL. On the Pooling Layer (PL) which the feature extraction process occurred, the input from the CL is reduced to spatial dimensions of the feature maps, preserving essential information while decreasing computational load. The final layer of the feature process usually contains neurons corresponding to the output classes, using a SoftMax activation function for multi-class classification tasks indicating the presence of certain features or anomalies After

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

feature extraction, the processed data is passed through fully connected layers that classify the input into predefined categories (e.g., detecting objects, identifying actions).

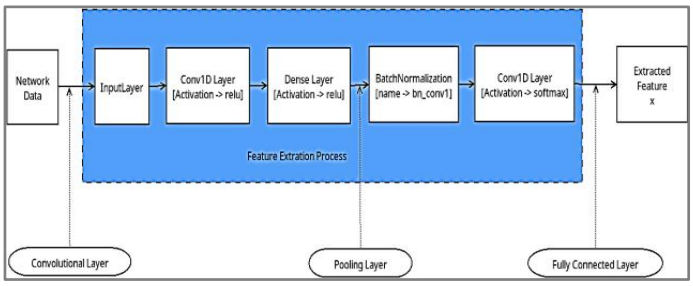

Figure 3: CNN Inference Engine Block

3.3 CNN Inference Engine Block

The model uses the fuzzy logic inference block to analyze data inputs and make decisions based on various parameters, also for the prevention and mitigating against anomalies, FL technique also helps in making proactive decisions to prevent incidents, which are mainly the anomalies from the CNN inference engine predicted (x) extracted features. So, the FL inference engine block does the prediction of the five states using a membership function to classify the suspected anomalies network into a High Negative anomaly, (x== 0), Medium Negative anomaly, (x>0 && x<=0.5) a Neutral anomaly, (x== 0.5), Medium Positive anomaly, (x>0.5) and a High Positive anomaly.(x=1). If the signature is found to be between a High Negative and Neutral anomaly, then it is a false alarm (x==0 and x==0.5), the network is then permitted to go through to the respective industrial infrastructure. Finally, if the ML is kept on auto, the anomaly is block or quarantined by the system, but if there is false alarm, the operator admin acts (the concern dept). Here it will involve the engineering team concern to acknowledge and reset the alarm on the industrial infrastructure concern. The FL inference engine block is shown in figure 6 below.

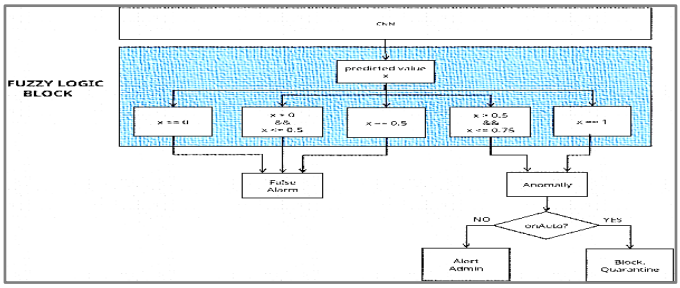

Figure 4: FL Inference Engine Block

IV. RESULT AND DISCUSSION

The training and testing procedures of machine learning are crucial for categorizing the Kaggle IIoTsets datasets and are essential aspects that influence the effectiveness of model design. The dataset used in the study was divided into two halves for training and testing. Seventy percent (70%) of the dataset network activity dataset collected was for training the model, while thirty percent (30%) for the model testing process during the study.

4.1 Model Evaluation Performance Results

The machine learning metrics, accuracy, precision, recall, F1-score and AUR-ROC of each machine learning classifier's performance were measured. The prediction time of attacks on the model and the metrics were performed and achieved using Python and Jupyter environment to execute these classifiers on the dataset. The study provides a comprehensive explanation of the terms being assessed and the evaluation results of the metrics and prediction or response time which depends on the model complexity, data size, hardware and the implementation of the model. The 2.51% average of the FPR achieved is a reasonable balance for detecting significant threats like DDoS, ransomware, and MitM attacks, especially when paired with a high true positive rate. It can be considered good for real-time intrusion detection and prevention, particularly for threats like DDoS ransomware, and MitM attacks in industrial IoT system. The results shown in table 4.9 below were obtained by simulating the industrial IoT system threat detection performance capabilities (TDPC) by users. The results capture various user's metric performance by the system starting from Boye to Saheed, and later Kelvin which accessed the system with their registered log details. The results from table 4.9 obtained during the system simulation were used to perform data visualization showing the graphical behaviour and performance of the system threat detection performance capabilities. This figure shows the attack types (DDoS, MitM, Normal and Ransomware) per user with chart during the system simulation. The figure graphically represents the trends of the false positive rate (FPR) and accuracy performance metric across different users during the system simulation. This figure represents the intrusion detection system analysis (IDS) showing the number of attacks and system performance metrics during the simulation process comparison of attack types.

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

Table 1: Model Evaluate Performance Metrics Results

Date	User(s)	Total Attacks	DDoS Attack	MitM Attack	Ransomware Attack	Normal Network	Blocked Attacked (%)	Quarantined Attacks (%)	Normal Network (%)	IPs	Latency (µsec)	FPR	Accuracy	ROC
010225	Boye	187	49	76	62	55	0.773	0.000	0.227	242	1.5624	2.50	92.5	8.30
080225	Taylor	146	61	47	67	60	0.745	0.008	0.255	196	1.5620	2.48	92.5	6.00
210225	Clement	158	55	58	52	58	0.731	0.000	0.269	216	0.8986	2.51	93.0	5.90
220225	Daniel	187	58	64	65	69	0.730	0.000	0270	256	0.3994	2.50	93.0	7.20
230225	Momotimi	198	57	62	79	57	0.788	0.000	0.212	269	1.5821	2.51	92.5	6.00
240225	Grace	191	56	67	66	58	0.767	0.000	0.233	249	1.5456	2.50	92.0	7.00
250225	Israel	181	60	65	56	54	0.770	0.000	0.230	235	1.2543	2.54	92.5	8.05
260225	Godswill	145	46	41	58	59	0.711	0.000	0.289	204	1.5804	2.50	92.5	7.81
270225	Rose	177	60	65	52	62	0.738	0.000	0.263	231	1.1465	2.50	92.5	6.50
280225	Miracle	149	52	50	47	52	0.741	0.000	0.259	201	0.4249	2.52	92.5	6.14
010325	Isaac	220	65	79	76	67	0.767	0.000	0.233	287	1.5802	2.50	92.5	5.60
070325	Patel	140	46	45	49	58	0.797	0.000	0.293	198	1.5626	2.49	92.5	7.33
110325	Saheed	253	78	94	81	75	0.771	0.000	0.229	328	0.8004	2.51	92.5	7.34
130325	Kelvin	189	70	56	63	50	0.791	0.000	0.209	239	1.4984	2.50	92.5	7.00
Average		179	57	63	62	59.57	0.760	0.000	0.248	240	1.2071	2.51	92.54	6.90

The entire dataset has been used in experiments. This experiment utilizes Python software and the Jupyter environment to execute these classifiers on the dataset. The model evaluation performance results are displayed on the main application window when a user (operator) engineers etc.) clicked on the model menu on the dashboard and the four (4) buttons, create model (CM), evaluate model (EM), view plot (VP) and clear results (CR) as design by the researcher The evaluation report, evaluation result and the graphical representation of performance metrics will be displayed on the industrial IoT system dashboard when a user clicked at the view plot (VP) button. Below is the figure showing the metric results of the model performance.

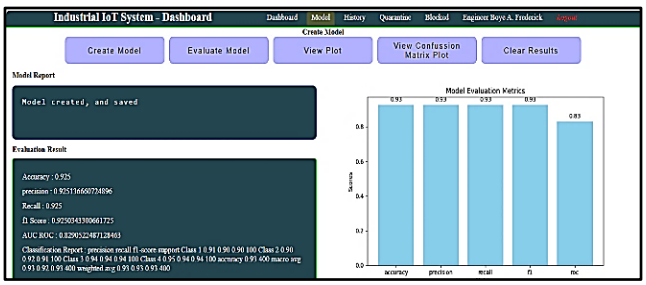

Figure 5: Model Evaluation Results

Figure 7 of the model evaluation scores all metrics the same after the model is created with balanced datasets before the evaluation. The detailed interpretation of the model evaluation performance metrics results in percentage (%) values. The model correctly classifies 92.5% of all instances. This indicates strong overall performance. Secondly, when the model predicts a positive class, it is correct 92.5% of the time. High precision indicates fewer false positives, making the model reliable when predicting positive instances. Thirdly, the model correctly identifies 92.5% of actual positive cases. A high recall means fewer false negatives, ensuring most of the actual positive cases are detected. A balance between precision and recall. The high F1-score confirms that the model maintains a good trade-off between false positives and false negatives. The Area Under the ROC Curve (AUC) measures how well the model distinguishes between positive and negative classes. A score of 82.9% indicates that the model performs well in differentiating classes, showing strong discriminatory power. The model result also achieved false positive rate (FPR) value of 2.50% of the 100 incoming alerts to the system. With these performance metrics, we can provide the overall performance of the model and recommend areas for improvement. Below is figure 8 showing the graphical representation of the performance evaluation metrics.

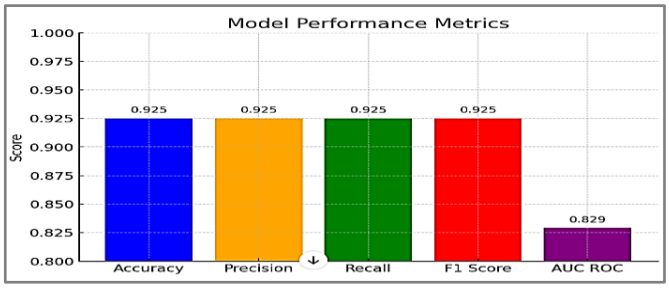

Figure 6: Graph of Performance Metrics

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

4.2 Analysis and Statistics of the Model

Analyzing the system and obtaining a statistical result are logs for viewing are shown in figure 9. A registered domain expert logs in with detail into the main industrial IoT system.

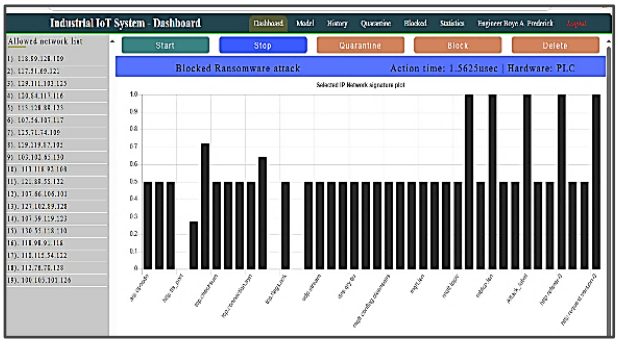

Figure 7: Industrial IoT System User Interface

The system was running with several different and incoming networks targeting the IP addresses of systems during the fourteen (14) system evaluation by a domain user, for instance, with a username as Emmanuel and password as Emmanuel, the simulation was performed. The figures 10show the system dashboard, the overall network statistics of 99 (0.762%) blocked attacks, 1 (0.008%) quarantined attack and normal free network of 30 (0.231%). This means the 99 (0.764%) attacks are made of DDoS, Ransomware and MitM as early intrusions experienced by industrial IoT systems. The results show Emmanuel industrial IoT system.

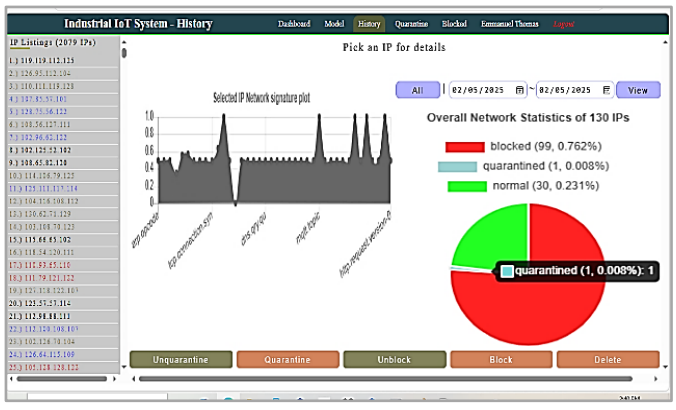

Figure 8: Graph of Emmanuel Metric Report

4.3 Intrusion Detection System Analysis

Figure 12 is the intrusion detection system analysis (performance metrics and number of attacks) achieved during the simulation at IFL lab. This result of attack types of numbers of DDoS, MitM and Ransomware with dates (over time) is the threat detection performance of the system.

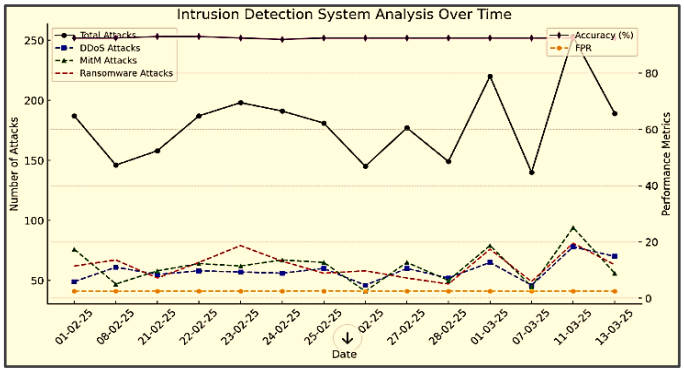

Figure 9: Intrusion Detection System Analysis

The performance comparative analysis of the three (3) with the proposed work as shown from figure 12, gives a result that the X-axis (Date) covers the timeline from 01-02-2025 to 13-03-2025. Left Y-axis (Number of Attacks), represents how many attacks were detected for each type. Whereas the Right Y-axis (Performance Metrics): Represents IDS performance (Accuracy and False Positive Rate). The data trends observed total attacks (black solid line), DDoS attacks (blue dashed square line), MitM attacks (green dashed triangle line) and Ransomware attacks (red dashed line).

Computing the latency values in percentage (%) and µseconds using the above table 4.9 on page 237, we have the following: To calculate the average of the latency in microseconds (µsec) and then express that average as a percentage, we need to define: We also compute the Latency (response time) Percentage (%) per Date using the formula:

= Latency % = (Latencyi/16.8978)×100, this will give us the following table 4 as shown below

Table 2: Latency in % per Date

Date	Latency (µseconds)	Latency (%)
010225	1.5624	9.24%
080225	1.5620	9.24%
210225	0.8986	5.32%
220225	0.3994	2.36%
230225	1.5821	9.36%
240225	1.5456	9.15%
250225	1.2543	7.42%
260225	1.5804	9.35%
270225	1.1465	6.78%
280225	0.4249	2.51%

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

010325	1.5802	9.35%
070325	1.5626	9.24%
110325	0.8004	4.74%
130325	1.4984	8.87%

4.4 Total Latency in µsec or (ms)

Latency (response time) is crucial in networking because it is the time it takes data packet to move from it source to destination. One of the objectives achieved in the study is the system latency which corresponds to the average in percentage of 7.14% computed as follows.

Total Latency=16.8978 µsec.

Average Latency (Response Time) = 16.8979/14 = 1.207µseconds.

Converting the total latency to percentage (%) we have Average Latency (%) = [1.207/16.8979] × 100. Average Latency (%) = 7.14%.

Average Latency = 7.14%. In industrial IoT systems, latency requirements are highly application-specific, but 7.14%of total latency (which corresponds to1.207 µsec average latency) is very good and acceptable for most industrial IoT applications.

4.5 Authors Comparative Metrics for Detection Rate, FPR and Latency

The system's behaviour or metric performance was achieved using parameters on table1 as the key system average (A) measured values indicators with an accuracy of 92.54, ROC average of 6.90, FPR average of 0.025 (2.51%), and latency of 1.207µsec (0.001207ms) average. Also, an average detection rate of 92.9%, which are the main objectives of this study. The chart below provides a clear visual summary of how the CNN & Fuzzy Logic approach industrial IoT system performs in terms of detection efficiency, reliability, and robustness. The chart system metric performance accuracy (A) achieved 92.54%, which indicates that the system correctly identifies both normal and malicious activities with over 92% certainty. This reflects a strong ability to generalize and adapt to the dataset's real-world traffic. The latency, which is measured in µsec has a corresponding average less percentage result of 7.14%.It demonstrates excellent sensitivity and minimal chances of missed threats crucial to real-time cybersecurity. Finally, the chart gives the FPR as 2.51% during the implementation analysis meaning the system rarely flags legitimate traffic as an attack and this improves trust, operational efficiency, and reduces alert fatigue in security.

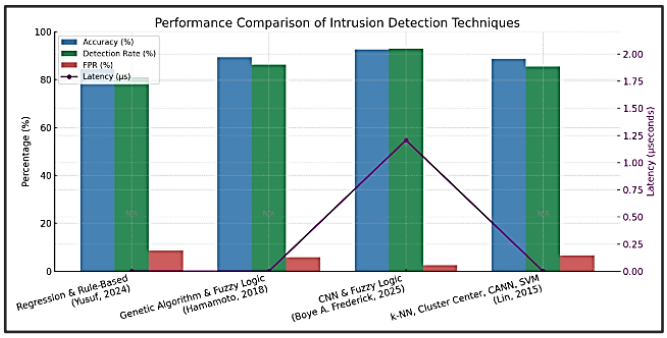

Figure 10: Metric for Accuracy, DR, FPR and Latency

The techniques, Regression, KNN, SVM offer relatively good accuracy and low latency but are slightly weaker in detection rate and FPR compared to hybrid AI approaches. The genetic algorithm + fuzzy logic has balanced performance but with high accuracy and low latency. The proposed approach of CNN + Fuzzy Logic achieves the highest accuracy and detection rate with the lowest false positives, but latency is higher due to the computational cost of deep learning models. Trade-off Identified: Increasing accuracy and detection rate often comes with higher latency. The chart highlights that CNN + Fuzzy Logic approach provides the most effective IDS performance, making it ideal for scenarios where detection accuracy and performance capability are more important than speed.

V. CONCLUSION

The model performs well with an accuracy of more than 90% compared to research in industrial IoT domain. The model also generates low false positive rate indicating that the model is effectively identifying intrusions while maintaining numbers of false positives and reasonably balance for detecting significant threats. For instance, a proposed hybrid model integrating CNN with Fuzzy logic approach in the same domain using other techniques achieved low results compared to the study. The system implementation analysis achieves a better threat detection performance capability ensuring near-instantaneous detection of malicious activity.

This simulation result of the system suggest that system improved the security by protecting critical infrastructure components like SCADA, PLC, DCS, and HMI etc. ensuring reliable operation of connected devices in industries such as manufacturing, energy, oil and gas and utilities. The model is technically suitable and shows promising potential for deployment in the industrial IoT domain, especially with high

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

accuracy and low false positive rate. The study recommended that The AUC ROC can be enhanced aiming for >85% instead of the average 6.70% AUC ROC as achieved or more using another hybrid AI techniques and incorporating real-world attack datasets for better model training. However, given the critical nature of DDoS, ransomware and MitM attacks, we recommend that further validation and continue improvement of the model is necessary to adapt to evolving attack vectors and ensure that it remains effective in a dynamic industrial IoT environment. Optimizing the system requires a combination of advanced detection models, multi-layered defense strategies, automated feedback loops, and adaptive learning. Finally, the study recommends that the model be tested in simulated or real-world IoT environments to ensure its practical effectiveness in detecting and preventing these threats.

ACKNOWLEDGEMENT

The author would like to express sincere gratitude to Engineers at Instrumentation Department Lab at IFL, Port Harcourt, for providing the facilities and support necessary for this research. Special thanks are also extended to my thesis lead supervisor, Associate Prof. Dr. E.O. Taylor, Associate Prof. Dr. E.O. Bennett and Professor. V.I.E Anireh reviewers for their valuable insights and constructive feedback, and colleagues which greatly contributed to the improvement of this work.

REFERENCES

[1] Jonathon G., Andrew M, E. Christian H. Dan Ricci, Tony T., Sarah F., Peter B, (2024), Industrial Cyber Manufacturing Handbook, *Industrial Cyber*, (Online).

[2] Ferrag, M.A., Friha, O., Hamouda, D., Maglaras, L., Member, S. & Janicke, H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning". *Institute of Electrical and Electronic Engineering TechRxiv conference.*

[3] Ramya, M. (2022).What Is a Man-in-the-Middle Attack? Definition, Detection, and Prevention Best Practices for 2022, www.spiceworks.com/it-security/data security/articles/man-in-the-middle-attack/.

[4] Panigrahi R. & S. Borah (2018), "A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems," *Int. J. Eng. Technol.*, vol. 7, no. 3.24, pp. 479–482.

[5] Abdallah E.E, W. Eleisah, & A. F. Otoom., (2022) "Intrusion detection systems using supervised machine learning techniques: A survey," *Procedia Comput. Sci.*, vol. 201, pp. 205–212, 2022. https://doi.org/10.1016/j.procs.2022.03.02.

[6] Sangeeta S., Ashish K., Navdeep S. R., & Shivanshu S., (2024), Intrusion detection and prevention systems in industrial IoT network, *Indian Academy of Sciences*, 49:244.

[7] Almiani, M., AbuGhazleh, B., Al-Rahayfeh, A., Atiewi, S. & Razaque, A. (2020). Deep Recurrent Neural Network for IoT Intrusion Detection System. *Science Direct Simulation Model for Practical Theory*, 101, 102031.

[8] Jiang, K., Wang, W., Wang, A. & Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access*, 8(32), 464 – 476.

[9] Dutt, I. (2018). Real Time Hybrid Intrusion Detection System. *International Conference on Communication, Devices and Networking*, 885-894.

[10] Einipour, A. (2018). Intelligent intrusion detection in computer networks using fuzzy systems. Global Journal of Computer Science and Technology, 2012.

[11] Guardian Nigeria (2022). Technology, Ransomware hits 71% of Nigerian organisations, guardian.ng/technology/ransomware-hits-71-of-nigerian-organisations/.

[12] Shanmugam, B. & Idris, N. B. (2019). Improved intrusion detection system using fuzzy logic for detecting anomaly and misuse type of attacks. *In Proceeding of 2009 International Conference of Soft Computing and Pattern Recognition*, 212-217.

[13] Hamamoto, A. H. Carvalho, L. F. L., Sampaio, D. H., Abrão, T. & Proença, M. L. (2018). Network anomaly detection system using genetic algorithm and fuzzy logic. *Expert Systems with Applications*, 92, 390-402.

[14] Ghanei H., Manavi F. & Hamzeh A. (2021). A novel method for malware detection based on hardware events using deep neural networks. *Journal of Computer Virology and Hacking Technology*, 17(4), 319–331.

[15] Jessica Lyons (2024), Schneider Electric ransomware crew demand $125k paid in Baguettes, *Cyber-Crime, theregister,com* (online).

[16] Brett Rowe (2024), Global Cybercrime Threats in 2024, and what to look out for, *Securus communication, (*Online).

[17] Nabil, M. A. M & Govardhan, A. (2012), Comparison study between Traditional and Object-Oriented Approaches to Develop all projects in Software Engineering. *International Journal of Computer Science*

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

and Information Technologies, 3(1), 3022 – 3028.

[18] Oliver E., Philipp K., & Paul T. (2019), Detection of Man-in-the-Middle Attacks on Industrial Control Networks, DOI: 10.1109/ICSSA.2016.19, *ResearchGate.*

[19] Omar S. A & Omar A. I. Al-Dabbagh (2021), Ransomware Detection System Based on Machine Learning, *Journal of Education and Science* (ISSN 1812-125X), Vol: 30, No: 5, 2021 (86-102).

[20] D. Maiorca, et al. "R-PackDroid (2017), API package-based characterization and detection of mobile ransomware," *Proceedings of the symposium on applied computing*.

[21] Ammarah C, Moeenuddin T, Adnan H, 1 Muhammad M. K, Fahad A, & Muhammad A. (2022), Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review, *Hindawi Security and Communication Networks Volume*, Article ID 8379532, 15 pages https://doi.org/10.1155/2022/8379532.

[22] Deval B., Maede Z., Aiman E., Raj J., Khaled K., Nader M. (2019), Cybersecurity for Industrial Control Systems: A Survey, *Computers and Security, Elseveir*. Pg18.

[23] McMillen D., (2019), "Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent," [Online]. Available: https://securityintelligence.com/attacks-targeting-industrialcontrol-systems-ics-up-110-percent.

[24] Abdalrahman G. A. & Varol H., (2019), "Defending against cyber-attacks on the internet of things*," in 2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, June 2019, pp. 1–6.

[25] Chris Hauk (2023), DDoS Attack Statistics, Facts, And Figures For 2023, pixelprivacy.com (Online).

[26] Atzori, L., Iera, A. & Morabito, G. (2010). The Internet of Things. *A Survey of Computer Network*, 54, 2787–2805.

[27] Sri R. D. & Mohan M. K. (2019), Cyber Security Affairs in Empowering Technologies, *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* 8(10S), 278-3075.

[28] Jonathan G., (2024), Targeting Critical Infrastructure: Recent Incidents Analyzed, industrialcyber.co/analysis/targeting-critical-infrastructure-recent-incidents-analyzed/

[29] H-ISAC, (2021), Distributed Denial of Service (DDoS), *Health-ISAC*, www. H-isac.org.

[30] Michael Ruppe, adesso Schweiz (2024), 19 Keys to Detecting and Preventing Man-In-The-Middle Attacks, *Forbes Technology* Councilwww.forbes.com/sites/forbestechcouncil/2024/03/07/19-keys-to-detecting-and-preventing-man-in-the-middle-attacks/

[31] Sophos (2024), The State of Ransomware 2024 Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity across 14 countries, conducted in January-February 2024.

[32] CISA, FBI & WaterISAC (2024) Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024, *Office of the Director of National Intelligence*.

[33] State of Operational Technology and Cybersecurity Report, 2024.

[34] Abu Rayhan & David Gross (2023). The Rise of Python: A Survey of Recent Research, *ResearchGate.* DOI: 10.13140/RG.2.2.27388.92809.

[35] Annual Report Insights Into ICS/OT Cybersecurity 2022, *TXOne Networks Inc*. (2022).

[36] Sanjay Fuloria (2022), Cybersecurity and Ransomware, *Academia Letters*, Article 4820. https://doi.org/10.20935/AL4820.

[37] Lucia S. (2024), The Role of AI in Cybersecurity, (www.crowdstrike.com/cybersecurity-101/artificial-intelligence/)(Online).

[38] Emiliano, S., Abusayeed, S., Song, H., Ulf, J. & Mikael, G. (2018). Industrial Internet of Things: Challenges, Opportunities, and Directions, *IEEE Transactions on Industrial Informatics*, X(X).

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

[40] Mohammad S, Chen F, Hamed B, Ali H & Rasoul R (2022), Classification and Detection of Malicious Attacks in Industrial IoT Devices via Machine Learning, *Conference paper, Open Access, link.springer.com*/chapter/10.1007/978-3-031-18326-3_10.

[41] HiveMQ (2024), Building Industrial IoT Systems in 2024, What's driving and delaying the business impact of IIoT. ivemq.com (Online).

[42] Khan, A., Sohail, A., Zahoora, U. & Qureshi, A. S. (2020). A survey of the recent architectures of deep convolutional neural networks. *Artificial Intelligence Review*, 53(8), 3455-5516.

[43] Mahmoud K. B., Issa A., Mohammad A., Hasan K., Nibras A., Ola A., Ahmed A. O. (2024), Web Attack Intrusion Detection System Using Machine Learning

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

Techniques, Vol. 20 No. 3.

[44] Yang, K., Ren, J., Zhu, Y., & Zhang, W. (2018). Active Learning for Wireless IoT Intrusion Detection. *IEEE Wirel. Communication*, 25, 19–25.

[45] Homeland Security, (2016), Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, *Industrial Control Systems Cyber Emergency Response Team* September 2016.

[46] Almiani, M., AbuGhazleh, B., Al-Rahayfeh, A., Atiewi, S. & Razaque, A. (2020). Deep Recurrent Neural Network for IoT Intrusion Detection System. *Science Direct Simulation Model for Practical Theory*, 101, 102031.

[47] Abu R.& David G. (2023). The Rise of Python: A Survey of Recent Research, *Researchgate*. DOI: 10.13140/RG.2.2.27388.92809.

[48] Sayeth S. A.L., Fareez, MMM & Vinothraj.T (2019), Python Current Trend Applications - An Overview Popular Web Development Frameworks in Python, *International Journal of Advance Engineering and Research Development*, 6(10).

[49] Desmedt Y, (2011) Man-in-the-middle attack, in: Encyclopedia of cryptography and security, *Springer*, 2011, pp. 759–759.

[50] Eurelectric, 2025, Cybersecurity in the Power Sector, *eurelectric.org*. (Online).

[51] Reliandoid 2025, DDoS Trends and Predictions for 2025, *relianiod.com* (Online).

[52] Boye, A.F., Taylor, E.O. and Bhagat, D., (2024). AI and Performance Capability of Cybersecurity in the Energy Industry. *ISAR Journal of Science and Technology*, 2(12), 29-36.

AUTHORS BIOGRAPHY

Mr. A. F Boye Studied Computer Science with B.Sc. degree at Rivers State University in 2011.M.Sc. & PhD (in View) at the same University in Nigeria 2022 and 2025 respectively. He is a researcher and a lecturer in the Department of Computer Science at Eastern Polytechnic Port, a member of the Computer Professionals of Nigeria (CPN), and a PhD scholar at RSU. A Reviewer with three journals, IOTCC, AJCST and ASTESJ. He has published eight (8) research papers in both local and international journals. His research works focus on Artificial Intelligence, Machine Learning, Expert System, Industrial IoT Systems.

Dr. O. E. Taylor Studied Computer Science with B.Sc. degree at Rivers State University, MSc at the University of Ibadan, & PhD at the University of Port Harcourt. He is currently an Associate Professor & a Lecturer in the Department of Computer Science, Rivers State University, Port-Harcourt. He is a member of the Computer Professionals of Nigeria (CPN). He has published over 50 research papers in reputed international journals. His research focuses on Machine Intelligence Systems, Cyber Security, & IoT.

Professor. V.I.E Anireh Studied Computer Science with BSc at UNN. MSc, & PhD at the University of University of Port Harcourt. He is currently a Professor of AI and a Lecturer in the Department of Computer Science, Rivers State University, Port Harcourt. He is a researcher and a member of IEEE. He has many scholarly publications in both local and international journals. His main research work focuses on Artificial Neural Networks, Machine Learning, Computer Networks, IoT, & Big Data.

Dr. E. O. Bennett graduated with a B.Sc. degree in Computer Science from Rivers State University, Rivers State, Port Harcourt, Nigeria in 1998, MSc and PhD at the University of Port Harcourt in 2008 and 2014 respectively. Currently he is an Associate Professor & a Lecturer in the Department of Computer Science, Rivers State University, Port-Harcourt. He is a member of the Computer Professionals of Nigeria (CPN). He has published over 50 research papers in reputed international journals. His research focuses on Algorithms, Parallel, Distributed & Intelligent Computing.

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 10, pp 1-13, October 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.210001
Available Online at https://www.jaiet.com

Citation of this Article:

Aziboledia Frederick Boye, Onate Egerton Taylor, Vincent Ike Emeka, & Emmanuel Okoni, Bennett. (2025). A CNN-Fuzzy Logic Approach for Real-Time Intrusion Detection and Prevention in Industrial IoT Systems. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 2(10), 1-13. Article DOI: https://doi.org/10.47001/JAIET/2025.210001

***** End of the Article *****