International Journal of Scientific Research and Modern Technology (IJSRMT) *ijsrmt.com*
Volume 4, Issue 5, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i5.542

Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment

Surendra Narang[1]; Anila Gogineni[2]

[1,2]Independent Researcher

Publication Date: 2025/06/11

Abstract

Cloud computing serves as a critical technology in modern digital systems because it provides organizations with benefits that equally come with corresponding problems. AI-powered cloud security now functions as a vital strategical tool which tackles rising complex and advanced cyber threats in the existing cloud computing era. This study investigates how to achieve zero trust security in intrusion detection networks using AI and how successful it is at resolving security issues in cloud networks. For the protection of IoT/IIoT networks, the zero-trust approach may function better. Access to network resources requires authorization and verification before any connection can be made because all users and devices are considered untrustworthy by default. This paper presents a zero-trust machine learning intrusion detection system (IDS) for protecting IIoT and IoT networks. The research proposes a Zero-Trust security model based on XGBoost for detecting attacks within the Edge-IIoTset dataset. Model performance enhancement required two steps: Min-Max scaling for normalization and SMOTE to balance classes during the data preprocessing process. XGBoost classifier operates on split training and testing data to detect threats that include Normal, DDoS, Enumeration, and Malware. To evaluate the performance of proposed XGBoost model according to accuracy, precision, recall, f1score, ROC, and confusion matrix. The proposed model surpasses traditional models by attaining 94.55% accuracy while K-Nearest Neighbors achieves 79.18% and AdaBoost reaches 86.29%, and Recurrent Neural Networks achieves 91% accuracy. The model shows reliable performance according to precision evaluation results of 95.46% combined with recall outcome of 98.38% and F1-score of 94.22%. The outcomes of comparative study and evaluation demonstrate the accuracy of risk detection abilities for Zero-Trust implementations which enhances security measures in contemporary digital systems.

Keywords: *Cybersecurity, Zero Trust (ZT), Internet of Things (IoT), edge-IIoTset dataset, Machine Learning, XGBoost, SMOTE.*

I. INTRODUCTION

In the last ten years remote work frameworks together with mobile technology along with cloud computing have made cyber networks more complex than ever before. Future organizational systems have become more flexible and adaptable because of innovations, but it remains at continuous risk. Security methods that are based on the perimeter are very vulnerable to perimeter breaches since they depend on reliable people and equipment inside the network[1][2]. These models struggle to handle cyberattacks that include internal threats in combination with network movement between systems[3][4]. This is because the current image has been enhanced, therefore calling for enhanced security measures due to various emerging attacks that include phishing, ransomware, and supply chain attacks that aim at business networks. It is important to note that companies that were complacent and only relied on perimeters such as the Zero Trust (ZT) engaged a 40% increase in successful intrusions in 2024 based on the Cisco Cybersecurity Readiness Index[5][6]. A solution to these problems is provided by ZT security, which follows the idea of "never trust, always verify[7]," meaning that trust is always being reevaluated and that access is allowed according to the least privilege principle[8][9]. A major step forward in the development of contemporary network security was the introduction and distinguishing characteristics of the zero-trust security paradigm[10][11].

With the use of an intrusion detection system (IDS), zero-trust networks may quickly identify suspicious activity or possible cyberattacks, which helps to reduce the risk of

Narang, S., & Gogineni, A. (2025). Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment. *International Journal of Scientific Research and Modern Technology*, *4*(5), 60–70. https://doi.org/10.38124/ijsrmt.v4i5.542

cyberattacks[12]. IDS enable the efficient response of network systems to ever-changing threats while preserving their security and integrity[13]. As the number of users and devices grows, automated real-time monitoring and dynamic security assessments, essential aspects of ZA, require solutions and methods capable of handling large volumes of data[14][15]. Artificial intelligence (AI) algorithms can play a pivotal role in overcoming these challenges through intelligent monitoring, evaluation, and decision-making processes[16][17]. Prior studies have explored the potential of AI frameworks to enhance maritime NIDSs, which would lead to more rapid and accurate detection of cyberattacks like DDoS, ransomware, phishing, and backdoor attacks, thereby fortifying marine cyber defense systems[18][19]. Marine NIDS has relied on deep neural networks and other strong learning algorithms to make very accurate predictions because of these algorithms' capacity to understand the spatial linkages in data from IoT networks and identify harmful risks[20].

Marine NIDS may use AI to solve the problems of transparency and dependability that have been mentioned above. To solve the problems of trustworthiness and openness in cybersecurity, it incorporates measures such as robust authentication, constant review of the confidence levels of AI-based NIDS models, and real-time monitoring of network traffic. ZT's implementation of the "trust no one, verify everything" approach allows NIDS professionals to get a deeper comprehension, trustworthiness, and authentication of network users while simultaneously enabling just-in-time threat mitigation[21]. This approach uses layered explainable NIDS to detect and thwart the covert attempts of cybercriminals who want to compromise the security, privacy, and accessibility of maritime cyberspace[22].

➢ *This Study Introduces the Edge-IIoTset Dataset and a Zero-Trust-Based IDS that Employs ML to Safeguard IoT/IIoT Networks from Cyberattacks. The Following Research Contribution of this Work as:*

- The study implements a zero-trust security framework for intrusion detection, ensuring in IIoT networks.
- The methodology includes handling missing values, removing duplicates, label encoding, and Min-Max normalization to enhance data quality and improve model performance.
- The study addresses the issue of imbalanced attack distributions using the SMOTE, ensuring a well-balanced dataset for training.
- XGBoost, an ensemble learning technique, is leveraged to improve classification accuracy by integrating multiple DT for robust attack detection.
- Reliability is guaranteed by conducting thorough evaluations of the model using important performance measures, including accuracy, precision, recall, F1score, ROC curve, and confusion matrix.
- The proposed architecture is beneficial for cloud and edge computing environment because it is a scalable and elastic security solution which makes it suitable for real time IIoT applications.

➢ *Significance and Motivation of the paper*

This paper is relevant because the concept of IIoT networks is still in its formative stages, giving rise to vulnerabilities, with possibilities of cyber threats like DoS attacks, malware, and enumeration assaults. Conventional security measures do not fit as the best solution for IIoT because of the heterogeneity and flexibility of such a system. This research is justified by the need to adopt Zero-Trust architectural model, which perpetually authenticates users, denies them unnecessary access, and monitors for behavior anomalous to the organization. Therefore, the study contributes to the development of high-performance, adaptable, and efficient cybersecurity solutions that improve threat detection and response based on the usage of the XGBoost-based intrusion detection system and the principles of Zero Trust. An escalating use of IIoT in critical infrastructures, manufacturing, healthcare, and smart cities all the more emphasise the need to find comprehensive, close-knit AI solutions oriented towards effective protection of the contemporary industrial networks.

➢ *Novelty and Justification*

This research is unique because it improves cybersecurity in IIoT contexts by combining a Zero-Trust security framework with an XGBoost-based IDS. The proposed security method delivers continuous authentication alongside verification for all network entities, which effectively decreases attack vulnerability levels. The paper uses data preprocessing that involves Min-Max normalization and SMOTE to handle the data imbalance problem. Besides, employing XGBoost classifier for the purpose of the multiple-class attack detection contributes toward this approach's differentiation from traditional machine learning models, thereby suggesting a higher detection rate. The justification for this work stems from the increasing sophistication of cyber threats targeting IIoT networks, which require robust, scalable, and adaptive security mechanisms. By leveraging a highly optimized threat detection model, this research provides a practical, real-time security solution for Edge-IIoT environments, contributing to the advancement of AI-driven Zero-Trust architectures in modern cybersecurity.

➢ *Organization of the Paper*

- *The Rest of the Paper's Outline is Below:*

Literature reviews are covered in Section II, while research methods are detailed in Section III. Section IV presents the experimental results, whereas Section V presents the findings.

II. LITERATURE REVIEW

Table I presents a brief summary of the literature study on zero-trust with advanced cybersecurity solutions employing ML, which is followed by a thorough evaluation of the materials.

Al-Sharafi *et al.* (2025) create a CIoT-ready EGTO-FLADC, an improved artificial gorilla troop optimizer that uses FL for assault detection and categorization. Through FL and the attack detection procedure, the EGTO-FLADC

strategy seeks to enhance CIoT environment security. The Marine Predator Algorithm (MPA) model is combined with the traditional GTO model in the EGTO method. Using the Edge IIoT set dataset, they assess how well the EGTO-FLADC method performs. In comparison to preexisting models, the EGTO-FLADC method demonstrated a considerable improvement in accuracy during experimental validation, with a value of 93.11%[23].

Barach (2025), zero-trust security framework, ZSDN-Guard developed specifically for software-defined networking (SDN) settings. To ensure the security of all network assets and connections, the suggested system makes use of deep learning methods and ZTA principles. CALSeq2Seq1 is a traffic anomaly detection module that is integrated into ZSDN-Guard. The experimental results show that even when the network is under assault, ZSDN-Guard manages to keep the throughput at about 80.5%[24].

Elsayed and Bay's (2024) work introduces a novel architecture that addresses security vulnerabilities in healthcare IoT devices via the use of ML. According to the results of the tests, when applied to the CICIoT2023 dataset, the model has the potential to drastically reduce expenses while simultaneously achieving zero-day detection accuracy. The accuracy for predicting different attacks is up to 93.6%[25].

Nawshin *et al.* (2024) look to improve the security of IoT networks by detecting malware on Android with the use of AI. A novel method for detecting Android malware, DP-RFECV-FNN, is based on the zero-trust concept of the IoT and uses an FNN with Differential Privacy (DP). DP-RFECV-FNN is able to distinguish between malicious and benign Android apps based on their dynamic properties with an accuracy of up to 93.49 percent[26].

Kim and Song (2024), a Zero-Trusted Perspective ABDM that examines packets for different external access reasons and identifies suspicious behavior. Consequently, an accuracy of about 93% for aberrant behaviour was recorded. The advancement of ICT technology has made it feasible to work from home more often and in a wider range of locales[27].

Teymourlouei (2023), the zero trust (ZT) concept is the foundation of this approach; it holds that no implicit confidence should be bestowed onto assets or user accounts only because of their physical or network location or ownership of them. advise using a random forest ML strategy to assess ZT compliance. Using these parameters, the model achieved a classification accuracy of over 95% for all six businesses' compliance[28].

Table 1 Summary of the Related Work for Zero Trust Security using Machine Learning Techniques in Threat Detection

Ref no.	Methodology	Dataset	Key Findings	Limitations	Future Work
Al-Sharafi et.al. (2025)	Federated Learning (FL), TCN-GRU, Enhanced Gorilla Troop Optimizer (EGTO)	Edge IIo Tset	Achieved 93.11% accuracy for attack detection in CIoT	Needs real-world validation	Extend to other IoT environments
Barach et.al. (2025)	Zero Trust, Deep Learning, CALSeq2Seq1	SDN dataset	80.5% network throughput under attack	Limited to SDN environments	Deploy in large-scale SDN settings
ElSayed et.al. , (2024)	Convolutional ML Architecture	CICIoT 2023	93.6% accuracy, zero-day attack detection, 10x cost reduction	Limited real-world applicability	Enhance adaptability to various healthcare devices
Nawshin et.al. (2024),	Differential Privacy, Feedforward Neural Network	Android static & dynamic features	accuracy (static), 93.49%-94.36% (dynamic)	Focuses on Android malware only	Generalize to other platforms
Kimet.al. (2024)	Abnormal behavior detection using time series analysis	Not specified	93% accuracy for detecting abnormal behavior	Lacks dataset details	Extend to broader network security applications
Teymourloueie t et.al. (2023)	Random Forest for ZT compliance verification	Not specified	95% accuracy for compliance classification	Limited to compliance evaluation	Expand to real-time monitoring

III. METHODOLOGY

The proposed methodology for detecting network attacks in the Edge-IIoTset dataset follows a best approach, including data preprocessing, normalization, class balancing, model training, and performance evaluation. Initially, the dataset undergoes cleaning by handling missing and duplicate values using Pandas, followed by label encoding for categorical features. Normalization is applied using the Min-Max scaling method to ensure uniform feature scaling, which improves model performance. A balanced dataset is created for training using the SMOTE, which addresses the class imbalance problem. Training and testing then use an 80:20 split of the data. This classification

procedure employs the XGBoost model, a decision-tree-based ensemble learning approach; it enhances prediction accuracy by integrating the capabilities of many decision trees. Accuracy, precision, recall, F1score, ROC curve, and confusion matrix are some of the assessment metrics used to quantify the model's performance in successfully identifying all attack types in the dataset.

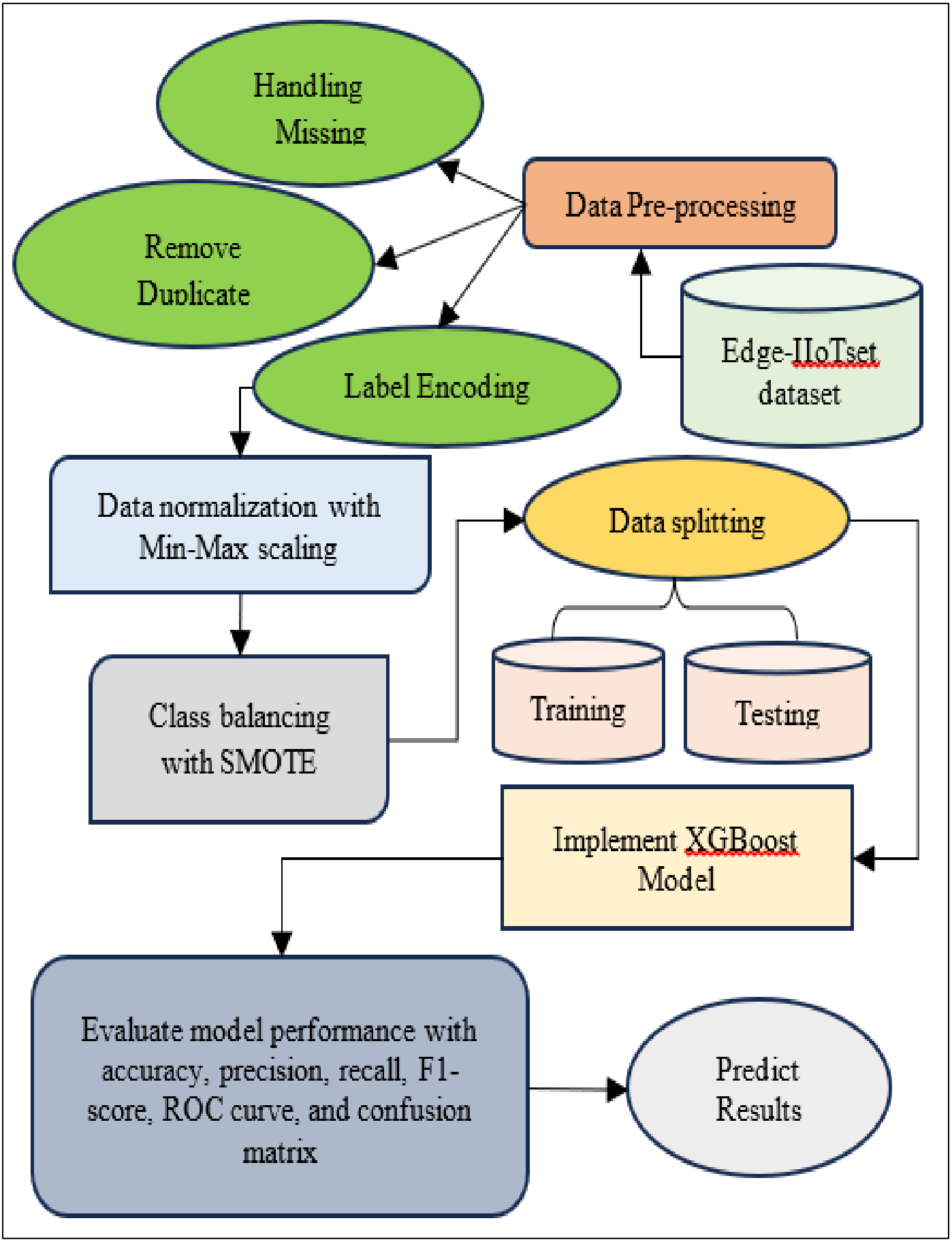

Fig 1 Flow Chart Advanced Cybersecurity for Zero Attacks Using ML Models

According to the methodology and proposed flowchart (Figure 1), each and every step discussed below:

➢ *Data Collection*

The Edge-IIoT set dataset contains sixty-one characteristics derived from a test bed that comprises the following layers: Cloud Computing, software-defined networking, Fog Computing, IoT and IIoT perception, blockchain network, and network services virtualisation. The essential needs of IoT communications are satisfied by these qualities. The dataset contains 20,939,646 records, with 11,209,923 representing regular traffic and 9,729,723 corresponding to 14 attack classes, as shown in Figure 1.

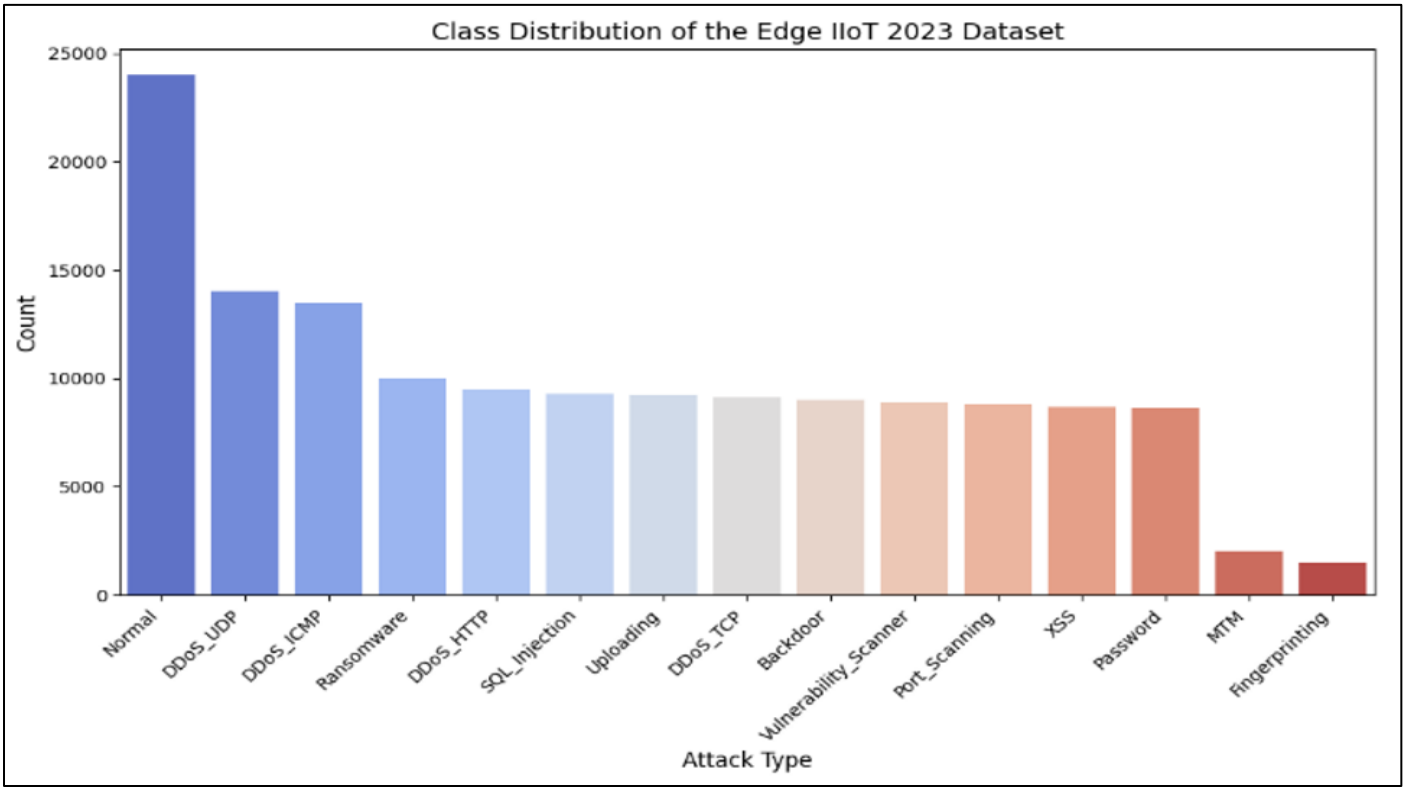

Fig 2 Bar Plot of Class Distribution of Edgeiiot Dataset

Figure 2 illustrates the class distribution of the Edge-IIoT dataset using a bar plot, highlighting the imbalance among different attack types and normal traffic. The "Normal" class exhibits the highest count, significantly exceeding all other categories, indicating a skewed dataset. Among the attack types, "DDoS_UDP," "DDoS_ICMP," and "Ransomware" show relatively high frequencies, while "MTM" and "Fingerprinting" have the lowest counts. This visualization emphasizes the need for careful consideration of class imbalance when training machine learning models on this dataset to ensure effective detection of all attack types.

➢ *Data Pre-Processing*

The initial stage of machine learning is called data preprocessing, during which the input is changed or encoded so that the computer can process or read it more rapidly. Stated differently, it might also mean that the model method is able to quickly analyse a data's characteristics. The first step in training a model is to ensure that the dataset is free of empty or undefined instances. For this test, we validated the dataset using the Pandas module that is integrated into Python. Certain variables in the used EdgeIIoT dataset are missing. Got rid of all the cases when a value was missing from the dataset. The following data preprocessing used on input dataset.

- *Handling Missing Values:*

Handling missing values is the process of replacing or estimating missing values in a dataset. It's an important step in data science because missing values can lead to inaccurate or biased results.

- *Removing Duplicate Values:*

The process of finding and eliminating duplicate records from a dataset is called removing duplicate values or deduplication. It's important to remove duplicate values to ensure data accuracy and integrity.

- *Label Encoding:*

One popular method of encoding that works well with categorical data is label encoding. Each category is assigned a unique number value. Some categorical characteristics are present in the dataset that was used. Since there are several classes for every given category characteristic, one-hot encoding necessitates additional storage space and processing time[28]. To quantify the categorical characteristics, this research used the label encoder method.

➢ *Data Normalization*

Data preparation for ML/DL algorithms often makes use of normalisation. The goal of normalization is to provide a consistent scale for numerical column values in a dataset while preserving the range of possible values. The

EdgeIIoT dataset contains characteristics with unique values. The model's performance is negatively affected by features with negative values, and there are features with thousands of values. The values are normalised between 0 and 1, employing the min-max approach, as displayed in Equation (1), in order to address this issue. The NumPy package in Python is used to turn data into an array and reshape it.

$$X_{new} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Where x represents the original value, X_{min} and X_{max} are the minimum and maximum values of x, and $X_{new}$is the normalized value.

➢ *Class balancing with SMOTE Technique*

The solution of real-world classification problems, particularly multiclass classification, often leads to a class-imbalanced situation. It is risky to balance network traffic data before training since it could lead to inferior model generalisation and simplify the complexity of actual network dynamics. It is equally important to look at an oversampling method using the EdgeIIoT dataset to see how well it works with or without oversampling for more realistic and generalised model performance. Both the theoretical and practical implications of this method support its use in our proposed ZTA framework. Figure 3 shows how this work uses the SMOTE[29] to create a balanced dataset for future training by oversampling a minority class in the training set. This rectifies the issue of uneven distribution in the EdgeIIoT dataset.

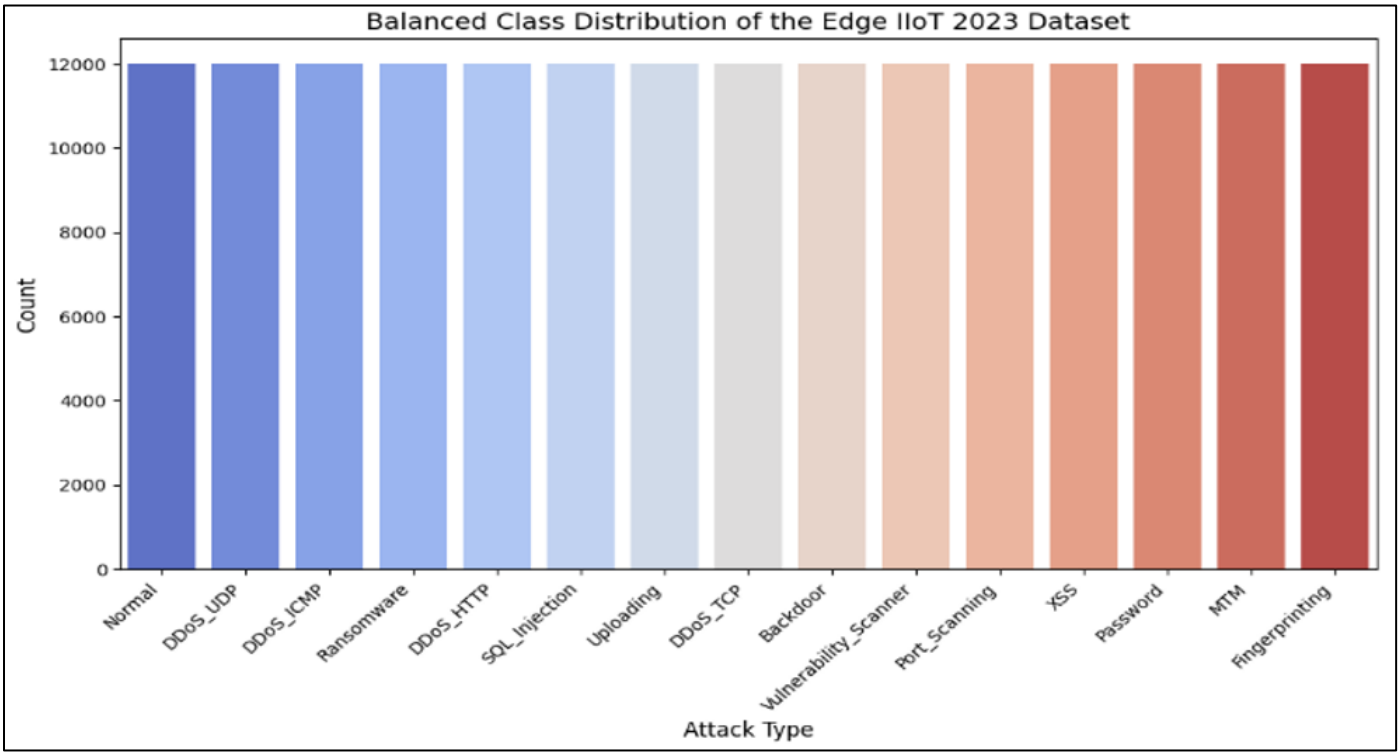

Fig 3 Bar Plot of Balanced Class Distribution of Edgeiiot

Figure 3 displays the balanced class distribution of the Edge-IIoT dataset, showcasing a uniform representation of each attack type and normal traffic. Unlike the original dataset, which was heavily skewed towards the 'Normal' class, this plot demonstrates an equal count for all categories, ensuring that no single class dominates the dataset. This balanced distribution is crucial for training ML models that can effectively detect all attack types without bias towards the majority class. A more accurate and fair assessment of the model's performance may be achieved since the bar heights are consistently the same across all categories. This means that the training process is affected by each assault type to the same extent.

➢ *Data Splitting*

The data set splits into two parts through data splitting: one part trains the model, and the other part tests it. To train a model and validate its performance with real-world data, an 80:20 ratio splits the dataset into 80% training and 20% testing parts. By splitting data sets this way, the model can train on patterns in source data before being tested on fresh data for accurate validation.

➢ *Classification of XGBoost (XG) Model*

One method for ensemble learning is XGBoost, which use decision trees to provide forecasts[30][31]. Reduce the disparity between the expected and actual values by using it to minimise a loss function; this may be used to regression situations. Equation (2) represents the mathematical paradigm for XGBoost regression:

$$y = f(x) \quad (2)$$

In where f(x) is the XGBoost model that uses x to forecast y, y is the expected property price, and x is a vector of input characteristics like square footage and bedroom count. The XGBoost loss function is used to compute f(x) from a set of decision trees that have been trained to minimize the MSE. To arrive at the final prediction, the model takes an average of the outcomes from each decision

tree. The XGBoost regression model may be presented in its generic form as Equation (3):

$$y = \sum(k = 1\ to\ K)\ fk(x) \quad (3)$$

Where K is the sum of all the ensemble DT' predictions and fk(x) is the predict of the k-th tree. Every tree's forecast is based on the weighted average of the values learnt for its leaves during training[32][33]. The XGBoost model's prediction for a given input x is determined by summing the predictions of all the ensemble DT.

➢ *Performance Metrics*

There is a sufficient evaluation of the ML models' performance according to accuracy and model cost reductions. Factors like accuracy, precision, recall, F1Score, ROC, and confusion matrix are used for assessment throughout the experiment. These metrics assess the model's performance based on many criteria. The available notations are TP for the amount of correctly categorised attacks, TN for the amount of correctly classified non-attacks, FP for the amount of incorrectly classified attacks, and FN for the amount of records that were incorrectly classified as non-attacks. Below, we will go over the following performance metrics:

- *Accuracy (ACC)*

Its capacity to identify malicious packets and classify them accordingly. Any percentage estimate may be used for every sample. Here is the mathematical expression for accuracy:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (4)$$

- *Precision (Pre)*

The following is an algebraic expression of the proportion of packets determined to be attacks as a fraction of all packets:

$$Precision = \frac{TP}{TP+FP} \quad (5)$$

- *Recall (Rec)*

A mathematical measure of the system's ability to detect security breaches and properly identify threats, sometimes known as the true positive rate:

$$Recall = \frac{TP}{TP+FN} \quad (6)$$

- *F1-Score (F1)*

This is theoretically defined as the harmonic average of recall and precision.

$$F1 - score = 2 \times \frac{precision \times recall}{precision+recall} \quad (7)$$

- *Roc-Auc*

Performance metrics like as ROC-AUC are often used to assess a model's capacity for classification, especially in situations involving binary classification. How well the model can differentiate among positive and negative categories is assessed by this metric.

IV. RESULT AND DISCUSSION

In this section provide the experimental outcomes of proposed XGBoost classifier results on EDGE-IIOT Dataset for Zero attacks classification in terms of performance measures. The experiment performs on Python simulation tool with Google Collab also included Sk-learn, NumPy, pandas, and seaborn libraries on HP laptop Intel i7Core processer 8Th Generation. The below tables and figures provide the results of implemented model also comparison between existing and proposed models.

➢ *Results of XGBoost model*

In this section provide the results of proposed XGBoost model on the Edge-IIOT dataset for Zero-Trust security, achieving 94.55% accuracy, 95.46% precision, 98.38% recall, and a 94.22% F1-score, shows in table II. These results highlight its effectiveness in accurate and reliable threat detection.

Table 2 Xgboost Classifier Performance on Edge-IIOT Dataset

METRICS (%)	XGBOOST
ACCURACY	94.55
PRECISION	95.46
RECALL	98.38
F1-SCORE	94.22

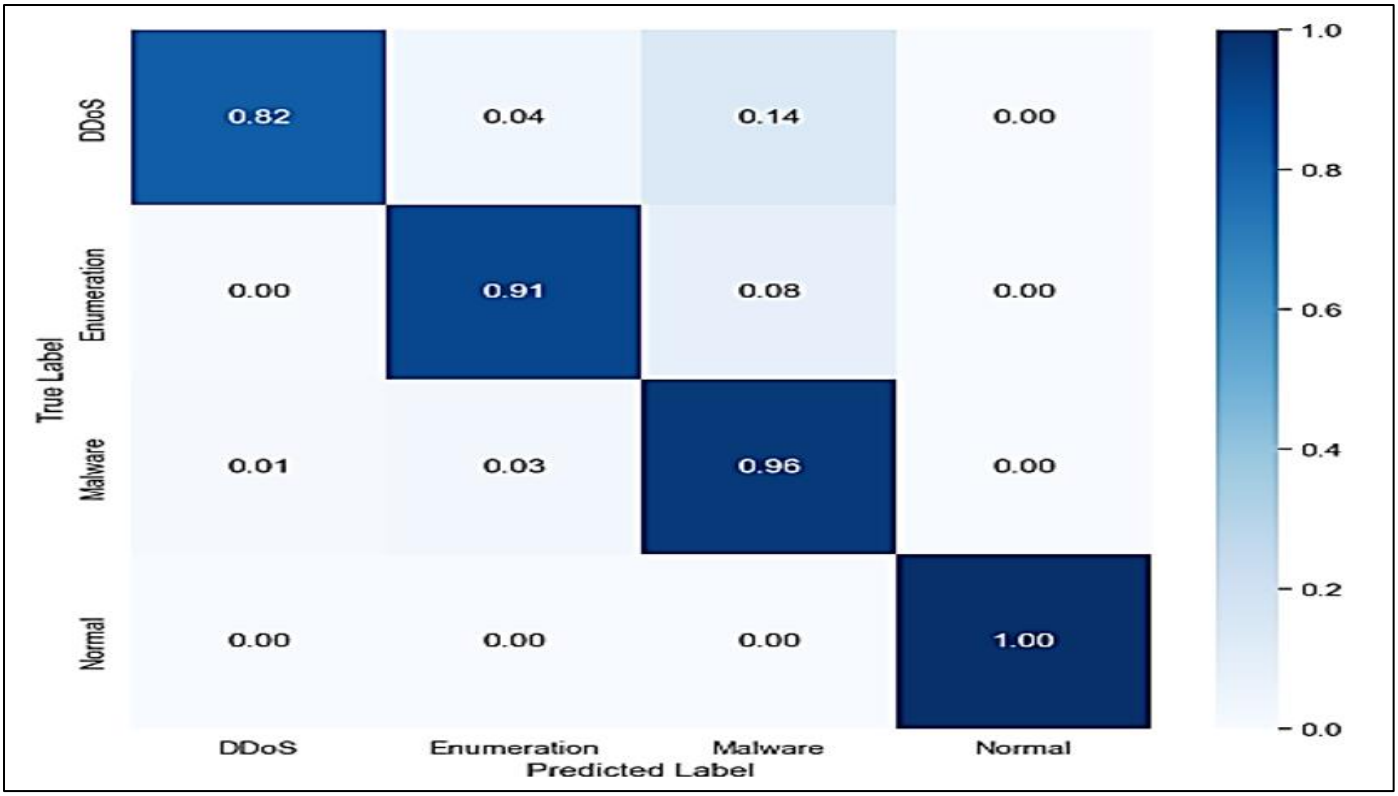

Fig 4 Confusion Matrix of XGBoost Model on Edge-IIOT Dataset

Figure 4 shows the XGBoost model's confusion matrix for the Edge-IIOT dataset, which shows how well the model performed in four categories: DDoS, Enumeration, Malware, and Normal. The matrix reveals high accuracy for the Normal class, achieving a perfect 1.00 score, indicating flawless classification. Similarly, the Malware class exhibits strong performance with a 0.96 accuracy, suggesting effective identification. The Enumeration class also demonstrates good accuracy at 0.91. The DDoS class demonstrates a slightly reduced accuracy rate of 0.82 because the model incorrectly assigned some attacks to the Enumeration and Malware classes according to the 0.04 and 0.14 values. The visual presentation delivers precise understanding of how the model recognizes Edge-IIOT attacks together with regular system activity.

	precision	recall	f1-score	support
DDoS	0.94	0.82	0.88	120
Enumeration	0.94	0.91	0.93	150
Malware	0.92	0.96	0.94	180
Normal	0.94	1.00	0.97	200
accuracy			0.94	650
macro avg	0.94	0.92	0.93	650
weighted avg	0.94	0.94	0.93	650

Fig 5 Classification Report of XGBoost Model on Edge-IIOT Dataset

Figure 5 shows the classification report of XGBoost applied to Edge-IIOT data that contains performance metrics about DDoS, Enumeration, Malware, and Normal classes. All tested metrics display robust performance results in the report, which shows precision scores between 0.92 to 0.94 besides recall scores between 0.82 to 1.00, and F1-scores between 0.88 to 0.97. Notably, the Normal class achieved perfect recall and the highest F1-score, while the DDoS class showed slightly lower recall. The model achieves 0.94 overall accuracy, and its precision metrics and recall metrics, and F1-score metrics produce high scores through macro averaging and weighted averaging approaches. Evaluation metrics gain meaning through the support column which displays the number of samples grouped by class category.

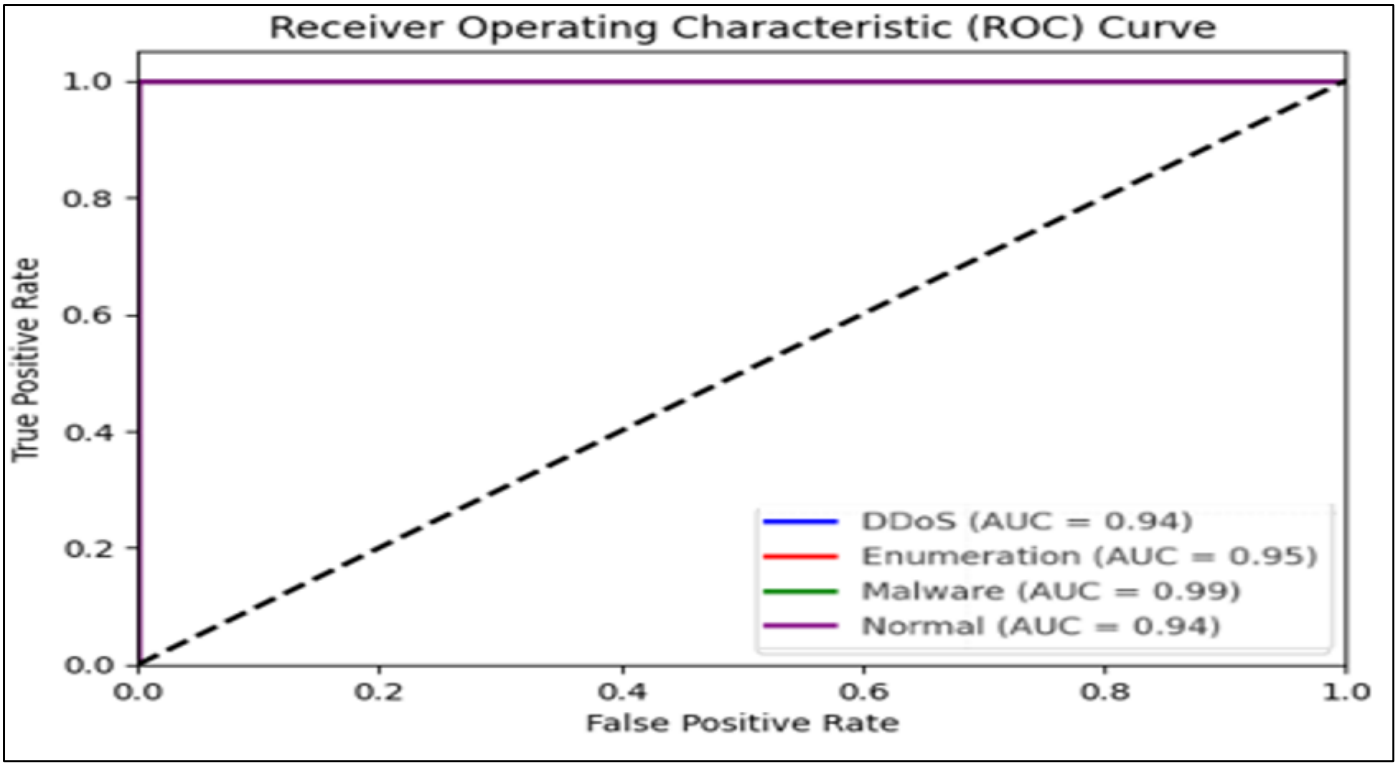

Fig 6 ROC Curve of XGBoost Model on Edge-IIOT Dataset

Figure 6 displays the ROC curve for the XGBoost model when trained with the Edge-IIOT dataset that shows its performance in classifying the categories between DDoS, Enumeration, Malware, and Normal. This model proves effective through its high prediction accuracy since the Malware class obtains an AUC value of 0.99. The Enumeration class follows with an AUC of 0.95, while both the DDoS and Normal classes exhibit an AUC of 0.94. The classification values show how the model distinguishes attack types from normal traffic but demonstrate minor differences between attack categories. The XGBoost model demonstrates outstanding robustness for safeguarding Edge-IIOT environments because of its accurate threat detection abilities according to the ROC curve.

➢ *Comparative Analysis*

In this section provide the comparison among existing (AdaBoost (AB), KNN and RNN) and proposed (XGBoost) models for zero attacks security on Edge-IIOT dataset.

Table 3 Comparison of AI Models for Edge-IIOT

METRICS	ACCURACY	PRECISION	RECALL	F1 SCORE
XGBOOST	94.55	95.46	98.38	94.22
ADABOOST[34]	86.29	86.32	86.46	86.30
KNN[35]	79.18	79.18	79.18	79.18
RNN [36]	91	91	91	91

Table III shows an evaluation of AI models for Edge-IIOT through four performance measurement factors, including Accuracy, precision, recall and F1Score. The XGBOOST model proves superior to all other models by reaching 94.55% accuracy along with 95.46% precision and 98.38% recall, and 94.22% F1 score, which indicates strong classification potential. The performance metrics from AdaBoost demonstrate reliability because this model achieves 86.29% accuracy yet falls behind XGBoost for effectiveness. The predictive abilities of KNN remain limited due to constant metrics, which results in an accuracy level of 79.18%, indicating a restricted capacity to accommodate diverse data distributions. The RNN demonstrates balanced performance through its 91% score across all metrics, although it provides less efficiency than XGBoost. The evaluation demonstrates XGBoost surpasses all models in Edge-IIOT because of its predictive strength although RNN shows stable performance as an alternative solution.

➢ *Discussion*

XGBoost demonstrates better performance than all existing models which include AdaBoost, KNN and RNN for securing Edge-IIOT environments through Zero-Trust methodologies.

- *XGBoost Outperforms Other Models*

Achieves the highest accuracy (94.55%), precision (95.46%), recall (98.38%), and F1-score (94.22%), proving its superiority in Zero-Trust security for Edge-IIOT.

- *Comparative Model Performance*

RNN (91%) performs better than AdaBoost (86.29%) and KNN (79.18%), but all lag behind XGBoost in detecting cyber threats.

- *XGBoost's Strengths*

Advanced boosting and feature selection enhance classification accuracy, making it the most reliable model for securing Edge-IIOT environments.

The proposed XGBoost model delivers several key benefits for Zero-Trust security at Edge-IIOT by achieving high detection accuracy and superior precision alongside strong threat detection agility that proves better than traditional models AdaBoost, KNN, and RNN. Multiple attack type classification capability of this model provides greater security which reduces both security risks and speeds up responses in real-world deployment scenarios. The study emphasizes that advanced AI security protocols need implementation in Edge-IIOT networks because this enhance threat resilience while decreasing cyber risks in these systems. Therefore, the outcome of the present study provides evidence in support of developing scalable and real-time security solutions for industrial and smart grid applications using XGBoost. As for future improvements, hyperparameter and ensemble deep learning model tuning on the models in the system can be extended to improve the detection precision. Moreover, introducing the concept of federated learning strategies could enhance the level of security, but at the same time, protect data from unauthorized access and breaches derived from continuous technological advancement.

V. CONCLUSION

With the advances in both the frequency and sophistication of attacks, and their continuous development, there is a greater need for sound and effective means of identification and protection. The present paper discusses a novel AI-based architecture of ZT in cloud systems with an increased focus on real-time threat identification. This research presents a way of implementing the Zero-Trust architectural framework alongside the XGBoost model, to Checkpoint IDS for IoT/IIoT networks security against cyber threats. The Zero-Trust principle is used in the proposed system where the trust is not inherent and is constantly validated and threats are detected. Despite this, the model presents high accuracy (94.55%) and demonstrates a high level of effectiveness in evaluating all key points compared to typical ML algorithms like AdaBoost and KNN or RNN. The comparative analysis demonstrates the superiority of XGBoost in accurately identifying threats such as DDoS, Enumeration, and Malware, reinforcing its potential for real-world cybersecurity applications. In summary, this study highlights the need to combine ML-based IDS with Zero-Trust principles in order to strengthen the resistance of contemporary digital environments to changing cyberthreats.

REFERENCES

[1]. Microsoft, “Zero Trust Maturity Model,” Microsoft Secur., 2020.

[2]. V. Kolluri, “OF, AEIIG THE DIGITAL REALM: AI-DRIVEN ANTIVIRUS AND CYBER THREAT INTELLIGENCE‖(Vol. 2, No. 11).”

[3]. H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, “Theory and Application of Zero Trust Security: A Brief Survey,” 2023. doi: 10.3390/e25121595.

[4]. M. I. Khan, A. Arif, and A. R. A. Khan, “AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity,” BIN Bull. Informatics, vol. 2, no. 2, pp. 248–261, 2024.

[5]. S. Ashfaq, S. A. Patil, S. Borde, P. Chandre, P. M. Shafi, and A. Jadhav, “Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis,” J. Electr. Syst., 2023, doi: 10.52783/jes.688.

[6]. V. Prajapati, “Role of Identity and Access Management in Zero Trust Architecture for Cloud Security : Challenges and Solutions,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 3, pp. 6–18, 2025, doi: 10.48175/IJARSCT-23902.

[7]. S. S. S. Neeli, “Critical Cybersecurity Strategies for Database Protection against Cyber Attacks,” J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, p. 5, 2023.

[8]. M. Hasan, “Enhancing Enterprise Security with Zero Trust Architecture : Mitigating Vulnerabilities and Insider Threats through Continuous Verification and Least Privilege Access,” ECPI Univ. NV Newport News, VA, USA, 2024.

[9]. N. Patel, “AI-Enhanced Zero Trust Security Architecture for Hybrid and Multi-Cloud Data Centers: Automating Trust Validation, Threat Detection, and Mitigation,” Int. J. Nov. Trends Innov., vol. 3, no. 1, pp. a13–a18, 2025.

[10]. S. Nie, J. Ren, R. Wu, P. Han, Z. Han, and W. Wan, “Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment,” Sensors, vol. 25, no. 2, p. 550, Jan. 2025, doi: 10.3390/s25020550.

[11]. S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. Paul Aderemi, “Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches,” in 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICIPTM59628.2024.10563348.

[12]. S. Sh, “Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure,” J. Glob. Res. Electron. Commun., vol. 2, no. 2, pp. 01–07, 2025, doi: 10.5281/zenodo.14955016.

[13]. N. Patel, “AI-Powered Intrusion Detection And Prevention Systems in 5G Networks,” Int. Conf. Commun. Electron. Syst. - ICCES-2024, 2024.

[14]. M. I. Khan, A. Arif, and A. R. A. Khan, “The Most Recent Advances and Uses of AI in Cybersecurity,” BULLET J. Multidisiplin Ilmu, vol. 3, no. 4, pp. 566–578, 2024.

[15]. J. L. Deepak Dasaratha Rao, Sairam Madasu, Srinivasa Rao Gunturu, Ceres D’britto, “Cybersecurity Threat Detection Using Machine Learning in Cloud-Based Environments: A Comprehensive Study,” Int. J. Recent Innov. Trends Comput. Commun., vol. 12, no. 1, 2024.

[16]. S. O. Valentyn Sobchuk , Roman Pykhnivskyi , Oleg Barabash , Serhii Korotin, “SEQUENTIAL INTRUSION DETECTION SYSTEM FOR ZERO-TRUST CYBER DEFENSE OF IOT/IIOT NETWORKS,” Adv. Inf. Syst., vol. 8, no. 3, 2024.

[17]. B. Boddu, “Essential Cybersecurity Measures for Databases to Mitigate Cyber Attacks,” https://www.ijirmps.org/research-paper.php?id=231460, vol. 11, no. 6, p. 8, 2023.

[18]. W. Liu et al., “Intrusion Detection for Maritime Transportation Systems with Batch Federated Aggregation,” IEEE Trans. Intell. Transp. Syst., 2023, doi: 10.1109/TITS.2022.3181436.

[19]. R. Tarafdar, “AI-POWERED CYBERSECURITY THREAT DETECTION IN CLOUD ENVIRONMENTS,” Int. J. Comput. Eng. Technol., vol. 16, no. 1, pp. 3858–3869, Feb. 2025, doi: 10.34218/IJCET_16_01_266.

[20]. Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, “A Deep Learning Model for Network Intrusion Detection with Imbalanced Data,” Electron., 2022, doi: 10.3390/electronics11060898.

[21]. M. Shore, S. Zeadally, and A. Keshariya, “Zero Trust: The What, How, Why, and When,” 2021. doi: 10.1109/MC.2021.3090018.

[22]. E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, “Zero-Trust Marine Cyberdefense for IoT-Based Communications: An Explainable Approach,” Electronics, vol. 13, no. 2, p. 276, Jan. 2024, doi: 10.3390/electronics13020276.

[23]. A. M. Al-Sharafi et al., “Ensuring Zero Trust Security in Consumer Internet of Things Using Federated Learningbased Attack Detection Model,” IEEE Access, vol. 13, no. April, pp. 54423–54438, 2025, doi: 10.1109/ACCESS.2025.3551212.

[24]. J. Barach, “Towards Zero Trust Security in SDN: A Multi-Layered Defense Strategy,” ICDCN 2025 - Proc. 26th Int. Conf. Distrib. Comput. Netw., pp. 331–339, 2025, doi: 10.1145/3700838.3703671.

[25]. Z. ElSayed, N. Elsayed, and S. Bay, “A Novel Zero-Trust Machine Learning Green Architecture for Healthcare IoT Cybersecurity: Review, Analysis, and Implementation,” in SoutheastCon 2024, 2024, pp. 686–692. doi: 10.1109/SoutheastCon52093.2024.10500139.

[26]. F. Nawshin, D. Unal, M. Hammoudeh, and P. N. Suganthan, “AI-powered malware detection with Differential Privacy for zero trust security in Internet of Things networks,” Ad Hoc Networks, vol. 161, p. 103523, 2024, doi: https://doi.org/10.1016/j.adhoc.2024.103523.

[27]. H.-W. Kim and E.-H. Song, “Abnormal behavior detection mechanism using deep learning for zero-trust security infrastructure,” Int. J. Inf. Technol., vol. 16, no. 8, pp. 5091–5097, 2024, doi: 10.1007/s41870-024-02110-7.

[28]. H. Teymourlouei, “A Machine Learning Approach to the Evaluation of Zero Trust Compliance in Network Infrastructure,” in International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME 2023, 2023. doi: 10.1109/ICECCME57830.2023.10253205.

[29]. X. Xu, W. Chen, and Y. Sun, “Over-sampling algorithm for imbalanced data classification,” J. Syst. Eng. Electron., 2019, doi: 10.21629/JSEE.2019.06.12.

[30]. W. Zhang et al., “Human-Centric Machine Learning : Addressing Bias and Fairness in AI Systems Human-Centric Machine Learning : Addressing Bias and Fairness in AI Systems,” no. June, 2024.

[31]. Y. H. Rajarshi Tarafdar, “Finding majority for integer elements,” J. Comput. Sci. Coll., vol. 33, no. 5, pp. 187–191, 2018.

[32]. Wankar H, Dimble K, Dasgaonkar P, Chavan V, and Sayyad A, “Property Price Prediction Engine Using XGBoost Regression,” Int. J. Creat. Res. Thoughts, vol. 11, no. 4, pp. 190–194, 2023.

[33]. J. Thomas, “Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics,” J. Emerg. Technol. Innov. Res., vol. 8, no. 9, 2021.

[34]. T. Al Nuaimi et al., “A comparative evaluation of intrusion detection systems on the edge-IIoT-2022 dataset,” Intell. Syst. with Appl., 2023, doi: 10.1016/j.iswa.2023.200298.

[35]. M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, “Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning,” IEEE Access, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[36]. E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J. M. Lee, and D. S. Kim, “Zero-Trust Marine Cyberdefense for IoT-Based Communications: An Explainable Approach,” Electron., 2024, doi: 10.3390/electronics13020276.