IRJAEH

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 110- 117
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0015

A Comparative Study of Machine Learning and Deep Learning Approaches for Enhancing Intrusion Detection in IOT Environments

Shwethashree G C[1], *Manjula S*[2]

[1,2] *Department of Computer Science and Engineering, Sri Jayachamarajendra College of Engineering, JSS Science and Technology University, Mysore, Karnataka, India.*

Emails: *shwethashree@jssstuniv.in*[1]

Abstract

With the increasing deployment of IOT and Edge Cloud environments, ensuring the security of these systems against cyber-attacks bas become a critical challenge. Traditional intrusion detection systems (IDS) often fall short in addressing the complexity and scale of attacks in such heterogeneous environments. This paper aims to explore machine learning (ML) and deep learning (DL) techniques for efficient attack detection in IOT environments, with a focus on evaluating the performance of various models. The objective was to analyses the effectiveness of model, i.e., XGBoost (XGB) in identifying attacks using the TON-IoT dataset. The findings showed that XGB achieved an accuracy of 95.04%. The paper concludes that advanced ML and DL models, especially ensemble methods, offer significant improvements in intrusion detection. The novelty of this work lies in comparing various state-of-the-art approaches on a insights for enhancing security in Edge Cloud environments.

Keywords: *IoT security, Edge Cloud, intrusion detection, XGBoost, DenseNet, machine learning, deep learning, ensemble classifiers, TON-IoT dataset.*

1. Introduction

The Internet of Things (IoT) Edge Cloud environment, which combines the capabilities of cloud computing, edge computing, and the IoT, marks a paradigm shift in contemporary computing. Figure 1 shows the IoT Edge Cloud's whole architecture. With this design, data processing and analytics are brought closer to the sensors, IoT devices, and other interconnected systems that generate data. IoT Edge Cloud environments are ideal for applications like smart cities, driverless cars, healthcare monitoring, and industrial automation because they strive to lower latency, increase bandwidth utilisation, and improve real-time decision-making. The IoT Edge Cloud ecosystem is being employed in diverse domains, leveraging its potential to process and analyze data near the edge of the network. For example, in healthcare, wearable devices collect patient data and analyze it locally to provide immediate feedback, while critical information is sent to the cloud for further examination [5]. Similarly, smart cities use edge-enabled IoT devices for traffic monitoring, waste management, and energy optimization [6]. In the industrial sector, this environment supports predictive maintenance and process automation by analyzing sensor data at the edge, ensuring faster response times and reducing reliance on centralized data centers [7]. Figure 1 shows Edge Cloud IOT Environment.

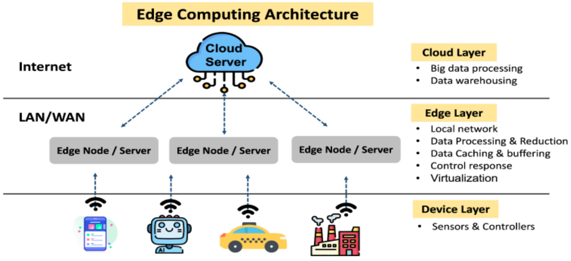

Figure : Edge computing architecture overview
Source : The research team

Figure 1 Edge Cloud IOT Environment

Despite its advantages, the IoT Edge Cloud environment is vulnerable to a range of security threats. The distributed and interconnected nature of this system creates multiple attack surfaces for adversaries. Cyberattacks can target IoT devices, communication networks, edge nodes, or cloud servers, endangering the system's confidentiality, availability, and integrity. These assaults have the potential to deliver malicious payloads, interrupt operations, or steal confidential information. Distributed Denial of Service (DDoS) assaults are a common form of attack [8], in which the attackers overload the network or edge nodes with traffic in order to interrupt services. Man-in-the-Middle (MitM) attacks use device-to-device communication interceptions to steal or alter data. [9]. Malware can infiltrate IoT devices or edge nodes, often exploiting weak authentication and unpatched vulnerabilities [10]. Data breaches target sensitive information stored or transmitted in the ecosystem, and ransomware can lock edge devices or cloud resources, demanding payment for release [11]. Physical attacks, such as tampering with IoT devices, add another layer of concern [12]. Recently, In Edge Cloud IoT contexts, machine learning (ML) and deep learning (DL) techniques have become effective tools for identifying and thwarting assaults. To find anomalous behaviours, such abnormal network traffic patterns, unauthorised access attempts, or strange device activity, these methods employ data-driven models. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are two examples of DL models that are excellent in identifying intricate and nuanced attack patterns. There are various benefits to using ML and DL to improve the security of IoT Edge Cloud settings. Large volumes of real-time data may be analysed by these models, which can also identify zero-day assaults that conventional rule-based systems could overlook. By constantly learning from fresh data, they adjust to changing threats and gradually increase the accuracy of their detections. Moreover, these techniques enable proactive threat mitigation, identifying vulnerabilities before they are exploited. By automating the detection and response processes, ML and DL reduce the reliance on human intervention, thereby increasing efficiency and reducing response times. The integration of ML and DL in IoT Edge Cloud security not only provides defenses against sophisticated cyberattacks but also ensures the reliability and resilience of this transformative technology. These advancements are pivotal in providing trust and enabling the widespread adoption of IoT Edge Cloud systems. Hence, this study focuses on exploring and evaluating ML and DL approaches presented recently for detecting cyberattacks in IoT Edge Cloud environments. Specifically, the contributions of this work are as follows:

- The study examines various ML and DL techniques that have been proposed for identifying and mitigating attacks in IoT environment, highlighting their strengths and limitations.
- The work employs the XGB model, a highly efficient gradient-boosting algorithm, to test its effectiveness in detecting attacks in an IoT environment.
- The detection performance of the XGB model is rigorously evaluated and compared against other existing attack detection approaches, providing valuable insights into its relative advantages.
- The study leveraged the publicly available “TON- IoT” dataset, ensuring that the results are tested on real-world data, thereby enhancing the practical relevance of the findings.

The manuscript is structured as follows. Section II provides a comprehensive review of various ML and DL approaches for attack detection, offering a broad perspective on existing techniques and their applications in IoT environments. Section III introduces the XGB model, going over its basic ideas, benefits, and suitability for handling attack detection duties. In Section IV, the performance and efficacy of the XGB model are assessed through the use of the "TON-IoT" dataset, where experimental results are examined and contrasted with those of other current methodologies. Section V wraps up the work by highlighting the main conclusions, pointing out its shortcomings, and suggesting other lines of inquiry. to enhance attack detection mechanisms in IoT Edge Cloud environments.

2. Literature Survey

This section presents the recent existing approaches presented for identifying attacks in IoT environment. A. R. Gad et al. [17], used the ToN-IoT realistic dataset, which was taken from a big, diverse IoT network. This study examined several machine learning techniques in both binary and multi-class classification problems. They used the Chi-square

(Chi2) technique for feature selection and the Class balancing using the synthetic minority oversampling approach (SMOTE). The results showed that the XGBoost approach performed better than the other ML techniques. Using a multi-class classification approach, I. Tareq et al. [18] built two intelligent network models, DenseNet and Inception Time, to identify cyberattacks. They started by evaluating these two networks' performance using three datasets: the UNSW2015 dataset, the Edge-IIoT dataset, and the ToN-IoT dataset, which includes heterogeneous data.. The outcomes were then contrasted by detecting multiple cyberattacks. The DenseNet multicategory classification model was used in extensive trials on common ToN-IoT datasets. With DenseNet, they achieved the best accuracy of 99.9%; however, we achieved the highest accuracy of 100% by employing the Inception Time technique. The best accuracy of 94.94% was obtained when the Inception Time technique was applied to the Edge-IIoT dataset. The Inception Time method, which had a 98.4% accuracy rate, was also used to evaluate the assaults in the UNSW-NB15 database. using an accuracy rate of 98.6% in the multicategory classification, the Inception Time model showed a small improvement when training using window sequences for the sliding window technique and a six-window size. A binary classification of normal and problematic IoT traffic was developed by Y. Alotaibi et al. [19] in order to improve the efficiency of the Intrusion Detection System (IDS). They used a variety of ensemble classifiers and supervised machine learning algorithms. Datasets of TON-IoT network traffic were used to train the suggested model. The four trained ML-supervised models that produced the most accurate results were K-Nearest, Random Forest (RF), Decision Tree (DT), and Logistic Regression (LR). neighbour (KNN). Two ensemble methods—voting and stacking—are fed these four classifiers. The effectiveness of the ensemble techniques on this classification task was compared and assessed utilising the evaluation measures. Compared to the individual models, the ensemble classifiers had a better accuracy. Ensemble learning techniques that make use of a variety of learning mechanisms with differing capacities were credited with this increase. Combining these techniques allowed them to decrease the frequency of classification errors while improving the accuracy of their forecasts. With an accuracy rate of 0.9863, the trial findings demonstrated that the framework may increase the IDS's efficiency. J. Li et al. [20], compared ML-based attack categorisation framework for IoT network intrusion detection system feature extraction and selection. Using binary and multiclass classification, it examined performance parameters such as accuracy, f1-score, and runtime, among others, on the diverse IoT dataset known as Network TON-IoT. Because there are fewer features, feature extraction performed better in detection than feature selection overall. Furthermore, extraction was less sensitive to variations in the number of features and demonstrated less feature loss than selection. On the other hand, feature selection took less time to train and infer models than its counterpart. Additionally, when the number of features varied, more space was needed to increase the accuracy of selection as opposed to extraction. This is true for both multiclass and binary classification. A. Almotairi et al. [21], addressed the difficulty of IDS in IoT by presenting a stack classifier model for IoT data that is built on heterogeneous machine learning. The model used ensemble modelling and feature selection to explore and improve important classification metrics for IoT data intrusion detection. The two main parts of this strategy were the creation of an ensemble model that combined many conventional machine learning models and the application of the K-Best algorithm for feature selection, which extracted the top 15 crucial characteristics. By combining these elements, classification performance was improved by utilising data from specific features and the combined power of each model. Their experiments contrasted the ensemble model with individual models using the "Tonne IoT dataset." The suggested ensemble technique demonstrated outstanding performance through thorough testing and comparisons, offering a solid way to strengthen IoT network security. In an IoT setting with constrained computer resources, Z. Wang et al. [22] presented BT-TPF, a knowledge-distillation-based IoT IDS model that can identify network assaults faced by IoT devices. A Siamese network was used by the suggested BT-TPF model to reduce the feature dimensionality of intricate, high-dimensional network traffic data. Furthermore, it employed Before using the trained Poolformer model as a classifier to identify network intrusion traffic, a large-scale Vision Transformer (ViT) model serves as a teacher model to direct a small-scale Poolformer model during training. In comparison to the huge model prior to knowledge distillation, the final tiny model created through this process only needed a minimum of 788 parameters, resulting in a 90% reduction in parameter count while retaining good detection accuracy. The BT-TPF model demonstrated above 99% accuracy on the CIC-IDS2017 and TON_IoT datasets, according to experimental results. Furthermore, as demonstrated by a number of evaluation measures, it demonstrated notable advantages above both contemporary state-of-the-art models and conventional DL techniques. S. A. Abdulkareem et al. [23], used feature importance, a An IoT/IIoT network traffic dataset's feature dimensions can be decreased using a filter-based feature selection technique for feature dimensionality reduction. After applying feature importance to the dataset, they additionally used lightweight stacking ensemble learning (SEL) to assess the reduced features and correctly identify network traffic records. The Edge-IIoTset dataset, which contains IoT and IIoT network records, was used in extensive studies. They demonstrated that feature importance resulted in a considerable reduction in training and testing time by 86.9% in the storage space required to store comprehensive network traffic data. Their classifier, which used the eight top dataset features, recorded 87.37%, 90.65%, 77.73%, and 80.88% in terms of accuracy, precision, recall, training, and test time. For its complete performance, it took 16.18 seconds and 0.10 seconds. Their suggested SEL classifier demonstrated negligible accuracy compromise in spite of the decreased features. In order to simplify the data, A. G. Ayad et al. [24] discussed feature selection techniques and the preprocessing phase for IoT datasets. The objective was to create an effective anomalous intrusion detection system (AIDS) that strikes a balance between quick detection times and high accuracy. They suggested a hybrid feature selection strategy that blended filter and wrapper techniques in order to accomplish this. This strategy was incorporated into a two-tier AIDS model. Their method divided network packets into two categories at level 1: normal and attack. Level 2 then further classed the attack to identify its particular type. The imbalance in these datasets was one important factor they took into account, and the Synthetic Minority Over-sampling Technique (SMOTE) was used to rectify it. They used benchmark datasets, BoT-IoT, TON-IoT, and CIC-DDoS2019, to assess the impact of the chosen features on the ML model's performance across various methods, including Decision Tree (DT), Random Forest (RF), Gaussian Naive Bayes (GNB), and k-Nearest Neighbour (KNN). According to the results, DT outperformed current AIDS diagnosis methods with high detection accuracy (99.82–100%) and quick detection periods (0.02-0.15 s). architectures for IoT networks and establishing its superiority in achieving both accuracy and efficient detection times. The study by A. R. Gad et al. [17] leveraged the TON-IoT dataset and employed Chi-square for feature selection and SMOTE for class balancing, enabling robust performance in both binary and multi-class classification tasks. The XGBoost model demonstrated superior accuracy compared to other ML methods, highlighting its potential in intrusion detection. However, the reliance on feature selection methods like Chi-square may limit its adaptability to dynamic datasets with evolving attack patterns. I. Tareq et al. [18] used DenseNet and Inception Time models for detecting cyber-attacks, achieving impressive accuracy rates, including 100% on the TON-IoT dataset. Their use of multiple datasets demonstrated the robustness of these models across different scenarios. However, the high computational cost of training deep networks like DenseNet and Inception Time can be a drawback, especially for resource-constrained IoT devices. Y. Alotaibi et al. [19] focused on enhancing intrusion detection systems using ensemble classifiers. By combining supervised ML models through voting and stacking, they achieved improved accuracy compared to individual classifiers. This method's key advantage lies in leveraging diverse learning mechanisms. However,reduction and lightweight stacking ensemble learning. This approach significantly reduced training and testing times while maintaining reasonable accuracy. Nevertheless, the accuracy compromise due to feature reduction highlights a potential trade-off between efficiency and detection capability, especially in identifying sophisticated attack patterns. Finally, A. G. Ayad et al. [34] proposed a hybrid feature selection method integrated into a two-level anomaly intrusion detection system (AIDS). This method achieved high accuracy and low detection times, particularly with Decision Tree classifiers. However, the approach's reliance on SMOTE for addressing data imbalance may introduce overfitting issues in real-world scenarios with highly imbalanced datasets, limiting its generalization capability. In the next section the XGB approach is presented.

3. Methodology

XGB is an advanced approach of gradient-boosting which optimizes performance and scalability [25]. It is particularly suitable for handling large datasets and complex tasks such as multiclass classification or detection. The main objective function in XGB is to combine the loss function and a regularization term as presented in Eq. (1).

$$\mathbf{L(\phi) = \sum N\ l\ (y, \hat{}y) + \sum K\ \Omega\ (f)(1)}$$

ensemble methods tend to be computationally expensive and may increase model complexity, i=1, k=1 making deployment on low-power IoT devices challenging. J. Li et al. [20] compared feature extraction and in Eq. (1). (yi, y i) is loss-function for predictions, y is true-label for ith instance, y   is anticipated likelihood vector for ith instance, Ω (f) is selection techniques for IoT network IDS and observed better performance with feature extraction regularization term for the kth ktree, N is no. ofmethods. The study offered insights into the trade-offs between detection accuracy and computational efficiency. While feature extraction provided superior detection performance, it required more storage and computational resources than feature selection, potentially limiting its feasibility for real-time

instances in dataset, K is no. of trees and ϕ is set of all parameters of the model. For multiclass detection or classification, the XGB loss function can be defined using Eq. (2).

$$\mathbf{l(y\ ,\hat{}y\ ) = -\sum C\ 1(y\ =c)\log\ (\hat{}y\ )}$$

applications. A. Almotairi et al. [21] introduced a heterogeneous ML-based stack classifier using feature selection and ensemble modeling. This approach showcased improved classification metrics and highlighted the importance of selecting relevant In Eq. (2), C is no. of classes, 1(yi=c) is indication- function, i.e., it will be 1 only when yi = c, else 0 features. While the ensemble model delivered robust performance, its complexity and dependence on otherwise and y is anticipated likelihood for class c selected   features may   limit   scalability   and for the i instance. The regularization in Eq. (1), i.e., generalization to new attack types or datasets. Z. Wang et al. [22] proposed a lightweight BT-TPF model for intrusion detection using knowledge distillation and a Siamese network. The model achieved high accuracy with minimal computational Ω(fk) is evaluated using Eq. (3).

$$\mathbf{\Omega\ f = YT + 1\ \lambda\ T\ w2}$$
$$\mathbf{k=2\ j=1}$$

requirements, making it suitable for resource-constrained environments. However, the model's reliance on large teacher networks during training may pose challenges in environments where initial resource availability is limited. S. A. Abdulkareem et al. [23] used feature importance for dimensionality In Eq. (3), T is no. of leaves in tree, wj is weight of jth leaf, Y is regularization-parameter for no. of leaves and λ is regularization parameter for leaf-weights.

4. Results and Discussion

For proposed work evaluation, a system with following specifications was utilized. The system was equipped with 16 GB RAM and an Intel i7 processor, which facilitated faster execution of computations and training of ML models. Windows 11 served as the operating system, providing a stable and efficient environment for the execution of the work. Python was used as the programming language to implement the entire framework. The performance metrics used to evaluate XGB included accuracy, precision, recall, and f-score which are evaluated using Eq. (4), Eq. (5), Eq. (6) and Eq. (7) respectively, where TN denotes true-negative, TP denotes true-positive, FN denotes false-negative and FP denotes false-positive.

$$\mathbf{Accuracy = \quad TP+TN}$$
$$\mathbf{TP+TN+FP+FN}$$

detection, and digital forensics. By providing a realistic representation of modern IoT and IIoT networks, the TON_IoT dataset serves as a valuable resource for researchers and practitioners aiming to enhance the security of interconnected devices and systems in the evolving landscape of Industry 4.0. The XGB model indicates that it is a reliable and efficient approach for detecting IoT intrusions. With an accuracy of 95.04%, XGB demonstrates its ability to correctly classify and detect a significant proportion of network traffic as either normal or malicious. This performance is further supported by its precision and recall values, both at 95.68%, highlighting the model's balanced capability to accurately identify TP while minimizing FP. The F-score of 95.44%, which combines precision and recall into a single metric, confirms the model's overall effectiveness in handling the classification task. The results illustrate that XGB is particularly adept at learning complex patterns in the data, owing to its

Precision = TP TP+FP

Recall = TP TP+FN

gradient-boosting mechanism, which iteratively (improves weak learners. While XGB's performance is robust, it falls slightly short compared to other models, such as Dense Net or ensemble methods like stacking classifiers, which have achieved near-perfect accuracy in similar tasks. This difference may be attributed to the model's dependency on hyper parameter tuning and the quality of feature engineering in the dataset used. Despite this, XGB remains a good model for IoT IDS

F - Score = 2×Precision×Recall

Precision+Recall The TON-IoT dataset [26] is a comprehensive collection of data designed to evaluate the performance of cybersecurity applications, particularly those utilizing artificial intelligence (AI) techniques such as ML and DL. Developed by the Cyber Range and IoT Labs at UNSW Canberra, this dataset reflects a realistic and large-scale Industry 4.0 network environment, encompassing Internet of Things (IoT) and Industrial IoT (IIoT) devices. The dataset comprises heterogeneous data sources, including telemetry data from various IoT and IIoT sensors, operating system logs from Windows and Linux platforms, and network traffic data. This diversity enables researchers to assess the effectiveness of AI-based cybersecurity solutions across different system layers, such as IoT devices, edge or fog computing nodes, and cloud services. To ensure the dataset's robustness, a variety of cyber-attack scenarios were simulated within the testbed environment. These scenarios encompass attacks like Denial of Service (DoS), Distributed Denial of Service (DDoS), and ransomware targeting web applications, IOT gateways, and computer systems. The dataset includes both raw and processed data, facilitating its use in developing and validating AI- driven cybersecurity applications, including intrusion detection systems, threat intelligence, malware due to its efficiency, scalability, and relatively lower computational requirements compared to DL models. Its ability to balance predictive performance with operational feasibility makes it a practical choice for real-world deployment in resource-constrained IoT environments. However, further optimization of hyper parameters and integration with ensemble strategies could enhance its performance, potentially closing the gap with other high-performing models. Figure 2 showssResults of XGB Model on TON-IOT Dataset

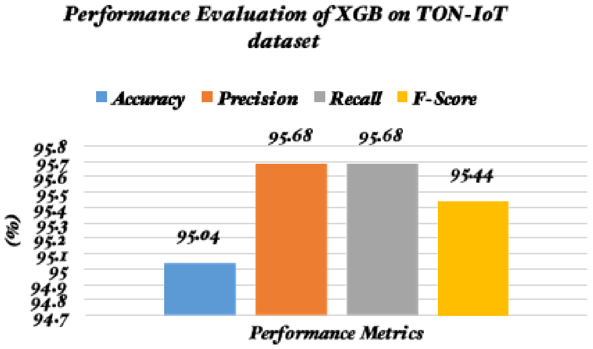

Figure 2 Results of XGB Model on TON-IOT Dataset

The comparative results as presented in Table 1 demonstrate the performance of various ML and DL models on IoT intrusion detection tasks, evaluated using metrics such as accuracy, precision, recall, and F-score. Among ML approaches, models like Decision Tree (DT), Random Forest (RF), and XGB consistently achieved high performance, with XGB demonstrating an accuracy of 98.6% in the study by [17]. K-Nearest Neighbor (KNN) also performed remarkably well with 98.1% accuracy, whereas Logistic Regression (LR) and Naive Bayes (NB) exhibited comparatively lower performance with accuracies of 77.7% and 71.1%, respectively. Adaptive Boosting (AB) underperformed significantly with only 39.9% accuracy, indicating its limitations in handling the complexity of IoT attack detection. DL models like DenseNet and Inception Time, explored by [18], showed exceptional performance, with DenseNet achieving an impressive accuracy of 99.65% and Inception Time reaching 98.57%. These results highlight the potential of DL models in cpturing complex patterns in IoT network data. DenseNet's F- score of 99.68% further reinforces its robustness for intrusion detection. Ensemble methods, such as stacking and voting classifiers presented by [19], also delivered promising results, with stacking achieving 98.64% accuracy, outperforming individual classifiers like DT and RF. Notably, the stacking classifier proposed in [21] achieved the highest accuracy of 99.99%, demonstrating the effectiveness of combining diverse models for improved predictive capability. The KNN model in the same study also achieved a near-perfect accuracy of 99.9%, showcasing its reliability for detecting IoT attacks. On the other hand, models like SVM and NB showed moderate performance, with SVM achieving 95.1% and NB reaching 80.46% accuracy. The integration of feature selection and advanced modeling techniques in [21] significantly enhanced the detection rates. Interestingly, while XGB demonstrated competitive performance in [17], achieving 98.6% accuracy, its performance in [21] was comparatively lower at 95.04%. This discrepancy underscores the influence of dataset characteristics and preprocessing techniques on model performance. Overall, the results emphasize the potential of leveraging advanced DL models and ensemble methods for IoT intrusion detection, while also highlighting the need for careful model selection and optimization to ensure robust and accurate predictions. Table 1 shows Comparative Study Table 2 shows Comparative Table

Table 1 Comparative Study

RF [19]	98.15	98.15	98.16	98.15
Stacking [19]	98.64	98.6	98.66	98.61
Voting [19]	96.63	96.59	96.51	96.6
RF [21]	98.2	98.19	98.19	98.19
NB [21]	80.46	87.45	80.45	81.44
SVM [21]	95.1	95.1	95.1	95.09
KNN [21]	99.9	99.9	99.91	99.9
Stack Classifier [21]	99.99	99.98	99.99	99.98
XGB Proposed	95.04	95.68	95.68	95.44

Table 2 Comparative Table

Model	Accuracy	Precision	Recall	F-Score
LR [17]	77.7	77.7	77.7	77.7
NB [17]	71.1	71.2	71.2	71.2
DT [17]	93.8	93.4	93.4	93.4
RF [17]	94	93.7	93.7	93.7
AB [17]	39.9	39.9	39.9	39.9
KNN [17]	98.1	97.9	97.9	97.9
SVM [17]	77.9	78	78	78
XGB[17]	98.6	98.3	98.3	98.3
Inception Time [18]	98.57	98.59	98.57	98.57
Densenet [18]	99.65	99.68	99.64	-
LR [19]	98.42	98.42	98.47	98.42
KNN [19]	98.28	98.28	98.29	98.3
DT [19]	97.44	97.44	97.44	97.44

Conclusion

The growing reliance on IoT and Edge Cloud environments has introduced significant cybersecurity challenges, necessitating robust mechanisms to detect and mitigate sophisticated attacks. This paper addressed this critical problem by exploring various ML and DL-based approaches for intrusion detection, emphasizing their strengths and limitations. A detailed analysis of existing methods highlighted the effectiveness of models like XGB, DenseNet, and ensemble classifiers in achieving high accuracy, precision, recall, and F-score on benchmark datasets such as TON-IoT. These approaches demonstrate how advancements in AI can significantly enhance the reliability and robustness of intrusion detection systems. The study also implemented and evaluated the XGB model, comparing its performance with other state-of-the-art approaches. While XGB exhibited strong predictive capabilities with an accuracy of 95.04%, its performance highlighted areas for improvement, particularly in comparison to ensemble methods and advanced DL models like DenseNet, which achieved near-perfect accuracy. The findings underscore the critical role of feature engineering, dataset characteristics, and model optimization in determining the efficacy of these approaches. The implications of this research extend to both academia and industry, offering insights into the selection and optimization of ML and DL models for

IoT security. The results demonstrate the potential for hybrid and ensemble approaches to address existing limitations and pave the way for more resilient IoT networks. Future work will focus on enhancing detection mechanisms through improved feature selection, model integration, and real-time deployment strategies in diverse IoT and Edge Cloud environments.

References

[1]. F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge Computing and Cloud Computing for Internet of Things: A Review," Informatics, vol. 11, no. 4, p. 71, Sep. 2024, doi: 10.3390/informatics11040071.

[2]. A. Al-Dulaimy et al., "The computing continuum: From IoT to the cloud," Internet of Things, vol. 27, pp. 101272–101272, Oct. 2024, doi: 10.1016/j.iot.2024.101272.

[3]. A. Biswas and H.-C. Wang, "Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain," Sensors, vol. 23, no. 4, p. 1963, Jan. 2023, doi: 10.3390/s23041963.

[4]. T. Nguyen, H. Nguyen, and Tuan Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," Journalofnetwork andcomputerapplications, pp. 103884–103884, Apr. 2024, doi: 10.1016/j.jnca.2024.103884.

[5]. K. Zovko, Ljiljana Šerić, T. Perković, H. Belani, and P. Solic, "IoT and health monitoring wearable devices as enabling technologies for sustainable enhancement of life quality in smart environments," JournalofCleanerProduction, vol. 413, pp. 137506–137506, May 2023, doi: 10.1016/j.jclepro.2023.137506.

[6]. K. Ahmed, Dr. M. Kumar Dubey, A. Kumar, and S. Dubey, "Artificial Intelligence and IoT Driven System Architecture for Municipality Waste Management in Smart Cities: A Review," Measurement: Sensors, p. 101395, Oct. 2024, doi: 10.1016/j.measen.2024.101395.

[7]. A. Ucar, M. Karakose, and N. Kırımça, "Artificial Intelligence for Predictive Maintenance Applications: Key Components, Trustworthiness, and Future Trends," Applied Sciences, vol. 14, no. 2, p. 898, Jan. 2024, doi: 10.3390/app14020898.

[8]. P. Kumari and A. K. Jain, "A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures," Computers&Security, vol. 127, p. 103096, Jan. 2023, doi: 10.1016/j.cose.2023.103096.

[9]. N. Sivasankari and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in iot network using regression modeling," AdvancesinEngineeringSoftware, vol. 169, p. 103126, Jul. 2022, doi: 10.1016/j.advengsoft.2022.103126.

[10].Basem Ibrahim Mukhtar, Mahmoud Said Elsayed, Anca Delia Jurcut, and M. A. Azer, "IoT Vulnerabilities and Attacks: SILEX Malware Case Study," Symmetry, vol. 15, no. 11, pp. 1978–1978, Oct. 2023, doi: 10.3390/sym15111978.

[11].T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges," Journal of Information and Intelligence, vol. 2, no. 6, Dec. 2023, doi: 10.1016/j.jiixd.2023.12.001.

[12].S. K. Sahu and K. Mazumdar, "Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance," Frontiers in Artificial Intelligence, vol. 7, p. 1397480, May 2024, doi: 10.3389/frai.2024.1397480.

[13].S. Yadav, H. Hashmi, D. Vekariya, Z. A. K. N, and V. F. J, "Mitigation of attacks via improved network security in IOT network environment using RNN," Measurement:Sensors, vol. 32, p. 101046, Feb. 2024, doi: 10.1016/j.measen.2024.101046.

[14].E. Ortiz-Ruiz, Juan Ramón Bermejo, Juan Antonio Sicilia, and J. Bermejo, "Machine Learning Techniques for Cyberattack Prevention in IoT Systems: A Comparative Perspective of Cybersecurity and Cyberdefense in Colombia," Electronics(Basel), vol. 13, no. 5, pp. 824–824, Feb. 2024, doi: 10.3390/electronics13050824.