ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

Surveying Ensemble-Based Approaches for Detecting DDoS in Internet of Things Environments

Abdulrahman Tunde Alabelewe[1*]; Rupert Waboke, William[2]; Serestina Viriri[2]; Adeyinka Samson[1]; Obunike Arinze Ubadike[1]; Omotayo Paul Ale[1]

[1]Department of Cybersecurity, Faculty of Computing, Air Force Institute of Technology, Kaduna, Nigeria
[2]School of Computer Science, College of Agriculture, Engineering and Science, University of Kwazulu-Natal, Durban, South Africa

Corresponding Author: Abdulrahman Tunde Alabelewe[1*]

Publication Date: 2026/04/17

Abstract: The Internet of Things (IoT) is becoming popular in recent times. This evolution has created more cybersecurity threats, particularly Distributed Denial of Service (DDoS) attacks. Several studies have achieved success in using single machine learning algorithms with impressive results. But DDoS attacks have become sophisticated and complex, and successful attacks have increased in recent times. Research has suggested the use of the ensemble learning technique, which promises to be more effective in mitigating these complex attacks. The study examines the vulnerabilities in IoT architectures that expose them to DDoS attacks, analyzes traditional machine learning approaches and their limitations, and evaluates the effectiveness of various ensemble learning methods, which include bagging, stacking, boosting, and voting techniques. The analysis reveals that ensemble techniques achieve superior detection accuracy and adaptability compared to standalone approaches while addressing the computational constraints inherent in IoT environments. This review contributes to the ongoing discussion about the development of effective cybersecurity solutions for increasingly complex and vulnerable IoT ecosystems.

Keywords: *Internet of Things, DDoS Attacks, Ensemble Learning, Voting Classifier, Stacking Classifier, Machine Learning, Cybersecurity.*

How to Cite: Abdulrahman Tunde Alabelewe; Rupert Waboke, William; Serestina Viriri; Adeyinka Samson; Obunike Arinze Ubadike; Omotayo Paul Ale (2026) Surveying Ensemble-Based Approaches for Detecting DDoS in Internet of Things Environments. *International Journal of Innovative Science and Research Technology*, 11(4), 930-942. https://doi.org/10.38124/ijisrt/26apr311

I. INTRODUCTION

The Internet of Things (IoT) is a wireless interconnection of physical devices, including computing devices, mechanical and digital machines, objects, animals, or people that allows data to be collected, sent, and stored without requiring human-to-human or human-to-computer interaction. Within the last two decades this technology has evolved by enabling connectivity between diverse devices to communicate autonomously and transfer data over networks (Kiran, 2019). According to Alam, (2018), there will be over 75 billion IoT devices by 2025, this expansion has created unprecedented security challenges. This massive growth in IoT technology has necessitated robust security measures to protect against vulnerabilities and potential attacks. The number and diversity of IoT devices, with their limited security features, present a complex and growing cybersecurity landscape (Al-Sarawi et al., 2020). IoT devices are usually characterized by limited computational resources, heterogeneous architectures, and often inadequate security measures; this has made them attractive targets for cyber attackers.These factors create vulnerabilities that attackers can exploit, potentially leading to data breaches, unauthorized access, and even physical damage to systems (Sasi et al., 2024). Among various cyber threats, Distributed Denial of Service (DDoS) attacks represent one of the most significant risks to IoT ecosystems. These attacks exploit the vulnerabilities in IoT devices to overwhelm target systems with malicious traffic, disrupting services and potentially causing substantial financial and operational damage (Gupta & Dahiya, 2021).

Several high-profile DDoS attacks throughout the years have had a substantial impact on cybersecurity

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

measures, technological advancement, and public awareness of the flaws in internet infrastructure. Notable instances include the Panix SYN flood of 1996, Mafiaboy's assaults in 2000, the Spamhaus incident in 2013, the Dyn assault in 2016, and the GitHub breach in 2018. Recent assaults include the 2020 AWS DDoS and the 2023 exploit of HTTP/2 vulnerabilities (Kabanda et al., 2023).

The Dyn DDoS attack in 2016 was one of the most major, focusing on IoT devices. Dyn, a major DNS provider that serves Twitter, Spotify, Reddit, and Netflix, was affected. The attack was carried out using the Mirai botnet, which was made up of hijacked IoT devices, with a peak speed of 1 Tbps, making major websites unreachable for hours. It revealed flaws in IoT security, possibly compromising devices with insufficient protection, and highlighted the critical role DNS providers play in sustaining internet infrastructure (Kirda & Ristenpart, 2017).

Traditional security mechanisms are often insufficient in IoT environments because IoT devices have limited resources and face constant, evolving threats. The resource constraints of IoT devices, such as low processing power, memory, and battery life, make them vulnerable to attacks that consume these resources. Additionally, the dynamic nature of IoT environments, with constantly changing devices and networks, means that traditional security approaches, which often rely on fixed configurations, struggle to adapt to new vulnerabilities and attack patterns (Szymoniak et al., 2025). The increasing complexity of cyber threats has prompted the development of increasingly sophisticated and adaptive detection techniques. Machine learning tools, especially ensemble learning techniques, are emerging as promising options for increasing detection accuracy and lowering false alarms (Fasial Sharif, 2024).

This study gives a complete overview of the use of ensemble learning approaches for detecting DDoS attacks in IoT contexts. The research starts by looking at IoT designs and their vulnerabilities, followed by DDoS assaults in IoT settings. An examination of standard machine learning algorithms and their limitations for DDoS detection is then presented. The study then delves into the fundamentals of ensemble learning for improving DDoS detection, evaluates relevant research and the performance of different algorithms, discusses the discoveries and gaps in the literature, and finally concludes.

II. ARCHITECTURE OF THE INTERNET OF THINGS AND ASSOCIATED SECURITY VULNERABILITIES

The rapid proliferation of Internet of Things (IoT) devices presents significant environmental and security challenges, including data privacy breaches, weak authentication, lack of encryption, and vulnerabilities in firmware and software. These challenges are exacerbated by the rise of remote work, the expansion of IoT devices in various sectors, and the increasing sophistication of cyber attacks (Baniya et al., 2024)

IoT systems function by integrating hardware and software to collect, process, and act upon data . The hardware elements include sensors, bridges, routing mechanisms, data acquisition modules, data processing units, and communication modules. Figure 1 show a block diagram of an IoT-based system. Devices such as Arduino boards and Raspberry Pi computers commonly serve as the foundations for IoT implementations, with the former providing specialized functionality and the latter offering more comprehensive computing capabilities (Sivaji et al., 2022).

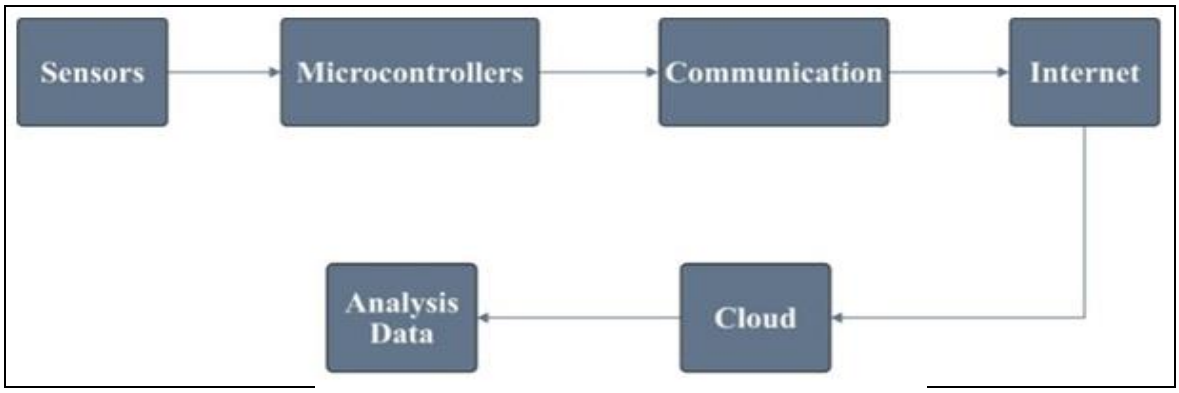

Fig 1 Block Diagram of IoT-Based System (Gupta et al., 2022)

IoT software architecture typically comprises three fundamental layers: the perception layer, the network (transportation) layer, and the application layer as shown in figure 2 (Domínguez-Bolaño et al., 2022). Each layer serves specific functions in the IoT ecosystem, from data collection and processing to network communication and user interaction. Each architectural layer within IoT systems presents unique security challenges that warrant careful consideration. The perception layer, also known as the sensor layer of physical layer is the foundation layer of the IoT system. This layer is responsible for data collection and processing, which is achieved through the integration of various sensors employing technologies such as Radio-Frequency Identification (RFID), Global Positioning System (GPS), and Wireless Sensor Networks (WSN), exhibits vulnerability to physical attacks, denial of service attacks, and routing attacks (Kavre et al., 2019). Physical attacks target hardware components and typically require proximity

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

to the network. Denial of Service (DoS) attacks overwhelm systems with excessive traffic, thereby preventing legitimate users from accessing services. Routing attacks manipulate routing information to redirect network traffic, potentially leading to data interception or alteration (Singh & Jain, 2024).

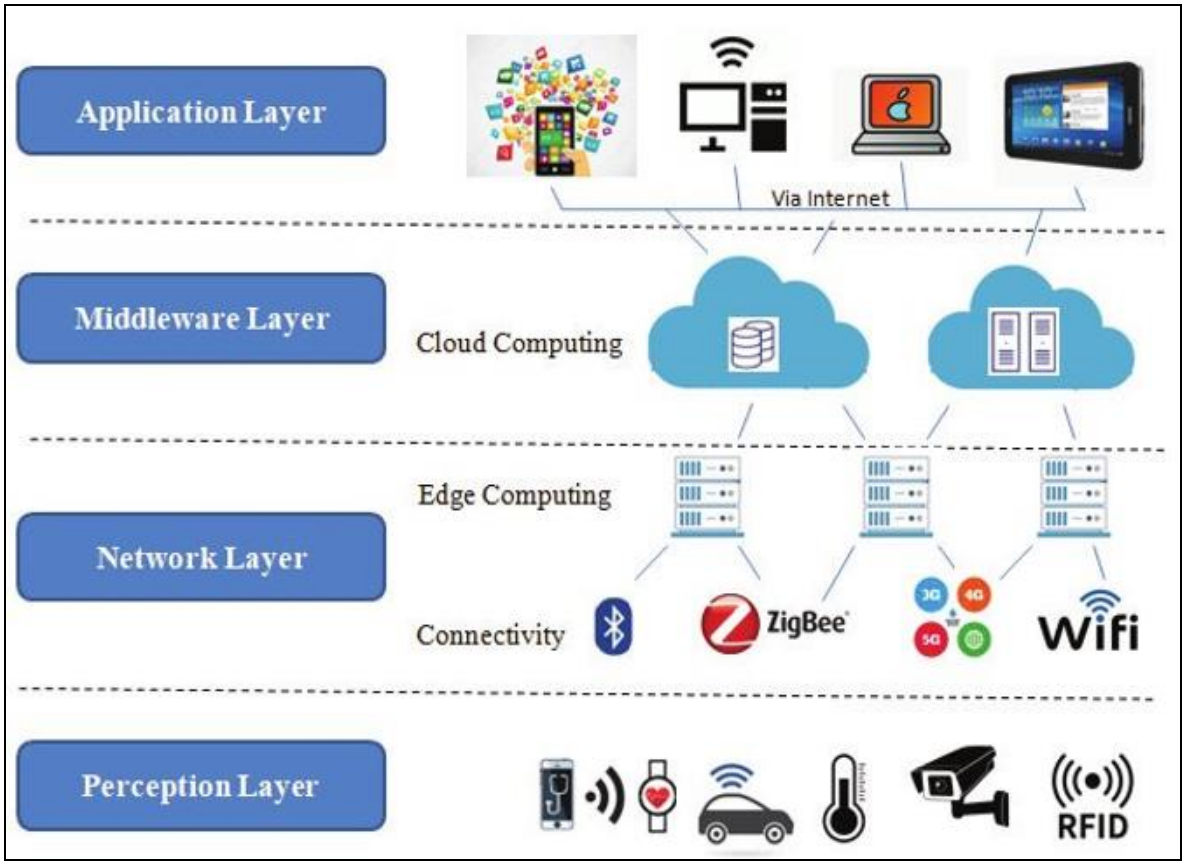

Fig 2 Four Layers of IoT Architecture (Kavre et al., 2019)

The transportation layer, which is an extension of the functionality of the perception layer, is crucial for reliable data transfer by collecting data across the communication systems. This layer faces security challenges, including routing attacks implemented through techniques such as Internet Protocol (IP) spoofing and man-in-the-middle attacks. Furthermore, this layer is particularly susceptible to DoS attacks due to inadequate security protections, the substantial number of connected devices, and inherent connectivity issues (Jahangeer et al., 2023). The application layer, positioned at a higher level in the architecture, delivers specific services to end-users by transforming raw data into actionable information. This layer is vulnerable to various attacks, including data theft, authentication breaches, and application-specific vulnerabilities (Sasi et al., 2024). The lack of standardised protocols in IoT systems creates significant security vulnerabilities across all architectural layers. Each layer, from device to cloud, presents unique challenges, including those related to data processing, detection of threats, and actuation of responses (Sebestyen et al., 2025). This lack of standardization hinders interoperability, creating gaps that can be exploited at various layers, ultimately compromising the overall security of the IoT ecosystem. This study, therefore, reviews ensemble learning techniques for enhanced DDoS attack detection in IoT environments.

III. DDOS ATTACKS IN IOT ENVIRONMENTS

Internet of Things (IoT) devices constitute particularly attractive targets for Distributed Denial of Service (DDoS) attacks due to several intrinsic vulnerabilities. IoT devices typically operate with minimal computational power, basic security mechanisms, and diverse architectures, rendering them susceptible to exploitation (Abomhara et al., 2015; Nazir et al., 2023). Additionally, many IoT devices employ default credentials and weak authentication mechanisms, which facilitate unauthorized access and potential enrollment into botnets. This makes them easy targets for attackers who can then control these devices to perform malicious activities, such as DDoS attacks . The communication infrastructure of IoT systems frequently relies on unencrypted or weakly encrypted communication protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), exposing them to interception and manipulation (Gelgi et al., 2024). Furthermore, the inherent resource constraints of IoT devices, particularly limited processing power and memory, impede the implementation of sophisticated security software, thereby establishing IoT devices as weak links within broader security architectures (Gupta & Quamara, 2020). Many IoT devices operate with outdated firmware, which significantly increases their vulnerability to cyberattacks. Exploiting these outdated systems allows

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

attackers to compromise the devices and potentially use them as entry points to larger networks (Bakhshi et al., 2024).

DDoS attacks targeting IoT environments are unique due to the nature of compromised IoT devices forming botnets. These botnets, composed of interconnected devices with weak security, can generate overwhelming traffic to overwhelm target systems. This makes identifying and mitigating these attacks particularly challenging. (Wazzan et al., 2021). These compromised devices are frequently exploited for reflection and amplification attacks, wherein small queries generate disproportionately large traffic volumes directed at targets. Domain Name System (DNS) and Network Time Protocol (NTP) amplification represent common techniques employed in these attacks (Ismail et al., 2021). Additionally, attackers increasingly focus on the application layer of IoT devices to disrupt services, a strategy that presents significant detection challenges as the malicious traffic often mimics legitimate traffic patterns (Liu et al., 2021). Command and Control (C&C) architectures, whether centralized or decentralized, enable attackers to coordinate large-scale DdoS operations with maximum impact (Ahmad & Alsmadi, 2021). The consequences of DdoS attacks on IoT ecosystems extend beyond immediate service disruption to encompass significant financial losses, reputational damage, and potential compromises of sensitive data.

IV. MACHINE LEARNING APPROACHES FOR DDOS DETECTION

Machine learning (ML) techniques have been widely applied to enhance intrusion detection in traditional network environments. However, their implementation in IoT contexts presents unique challenges due to resource limitations and the heterogeneous nature of IoT devices, limited computational power, memory, and energy, making it difficult to deploy complex ML models. In addition, the diverse nature of IoT devices, with varying protocols, hardware, and operating systems, further complicates the creation of uniform security strategies (Kikissagbe & Adda, 2024).

Several machine learning algorithms have proven effective in detecting Distributed Denial-of-Service (DDoS) attacks, with techniques like Support Vector Machines (SVMs), Random Forests, Decision Trees, K-nearest neighbour and logistic regression, among others, demonstrating high accuracy. These algorithms leverage various facets of machine learning and data analysis to identify patterns indicative of DDoS attacks (Abiramasundari & Ramaswamy, 2025). However, these algorithms encounter significant limitations when implemented within Internet of Things (IoT) environments for security purposes. Single-algorithm approaches frequently demonstrate inadequate adaptability to evolving attack patterns, thereby limiting their effectiveness against emerging threats . This adaptability challenge represents a critical vulnerability in rapidly changing threat landscapes characteristic of IoT ecosystems. Furthermore, many conventional machine learning algorithms necessitate substantial computational resources, creating implementation challenges within the resource-constrained environments typical of IoT devices . This resource limitation significantly restricts the deployment of sophisticated detection mechanisms across distributed IoT architectures.

Individual algorithms often exhibit strong performance on specific datasets while failing to generalize effectively across diverse IoT environments with varied traffic patterns (Heidari & Jamali, 2022). This generalization limitation undermines the universal applicability of single-algorithm solutions. Additionally, single-model implementations frequently struggle to establish an optimal balance between false positives and false negatives, thereby compromising either detection accuracy or operational efficiency (Pandey et al., 2023). This precision-recall balance represents a persistent challenge in practical deployment scenarios.

Computational demands associated with complex algorithms may impede real-time detection capabilities, which constitute a critical requirement for effective Distributed Denial of Service (DDoS) mitigation in IoT contexts (Chohan et al., 2023). These real-time processing limitations potentially create windows of vulnerability during which attacks may progress undetected. These collective limitations underscore the necessity for more adaptive and computationally efficient approaches to DDoS detection within IoT environments, prompting increased research interest in ensemble learning techniques that can address these complex challenges.

V. ENSEMBLE LEARNING FOR ENHANCED DDOS DETECTION

Ensemble learning emerges as a promising approach to address the limitations of traditional machine learning methods in Internet of Things (IoT) security contexts. By strategically combining multiple models, ensemble techniques achieve superior detection performance while maintaining computational efficiency appropriate for IoT environments.

Ensemble learning is fundamentally grounded in the "wisdom of the crowd" principle, which posits that combining the outputs of diverse models frequently yields better performance than any single constituent model (Elliott & Anderson, 2023). This improvement in performance derives from several complementary mechanisms:

Ensembles effectively reduce bias through the aggregation of models with differing biases, thereby producing more accurate overall predictions (Yang et al., 2023). This bias reduction is particularly valuable in heterogeneous IoT environments where traffic patterns vary significantly. Additionally, by averaging multiple model predictions, ensembles mitigate variance through reducing the impact of noise and outliers in the data (Sasi et al., 2024). Ensemble methods also enhance stability, demonstrating resilience to fluctuations in training data and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

ensuring more reliable and consistent predictions across varying operational conditions (Shtayat et al., 2023).

Numerous notable ensemble methods are documented in the literature, including voting, bagging, boosting, and stacking. These techniques integrate many machine learning models to enhance overall predictive accuracy and resilience (Mishra et al., 2025). Ensemble approaches are very beneficial in security for functions such as intrusion detection, virus analysis, and fraud detection. Voting is the most basic ensemble approach that involves aggregating predictions from several models, often by majority voting for classification or averaging for regression. Bagging, or bootstrap aggregating, generates numerous models from various bootstrapped subsets of the training data and then consolidates their predictions, often by averaging or voting. Boosting, conversely, constructs models progressively, with each model endeavouring to rectify the flaws of its predecessor. Examples are AdaBoost and gradient boosting. The ultimate stacking technique simultaneously trains numerous models and then employs a meta-learner to amalgamate their predictions, hence optimising the utilisation of the basic models' outputs (Mohammed & Kora, 2023).

VI. RELATED WORK AND RESEARCH GAPS

The use of ensemble machine learning techniques has gained significant popularity recently. The popularity arises from the use of the strengths of diverse combining algorithms to enhance the resultant system. This enhancement has resulted in improved accuracy, robustness, and generalisation capabilities in prediction models. As a result, several researchers are progressively using ensemble approaches, including voting, bagging, boosting, and stacking, to address intricate issues across diverse fields. This paper analysed current research that used ensemble techniques to create algorithms for detecting and preventing Distributed Denial of Service (DDoS) attacks in an IoT environment.

Das et al. (2019) ensembled four supervised machine learning classifiers, which include Artificial Neural Network (ANN), Support Vector Machine (SVM), K-Nearest Neighbours, and Decision Tree. The classifiers were combined using a majority voting method to enhance the robustness of the detection based on the DDoS attack patterns. The model was trained with the NSL-KDD dataset and validated with the 10-fold cross-validation technique to compare with the individual classifiers and the ensemble model. The performance of the model was evaluated using accuracy, true positive rate, false positive rate, precision, recall, F-measure, and ROC curve. The ensemble technique significantly outperforms individual classifiers in the detection of DDoS attacks. The study concludes that the system precisely detects 99.77% of DDoS attacks, with a false positive rate of around 0.23%.

Oluwole et al. (2022) presented an ensemble bagging method utilising decision trees as the foundational estimators, which is effective for the real-time detection and prevention of DDoS attacks in IoT settings. The study employed bagging to reduce variability and prevent overfitting by training multiple iterations of a classifier on various random segments of the dataset. The CICDoS2019 dataset comprises 50 million records that include both DDoS and benign traffic data, utilised for the purposes of training and testing. The evaluation of the model's performance involved the use of various metrics, including classification accuracy, precision, recall, F1-score, Matthews Correlation Coefficient (MCC), false positive rate (FPR), and false negative rate (FNR). The model demonstrated exceptional performance across all datasets, attaining a classification accuracy of 99.75%. The findings indicate a precision rate of 99.99%, a recall rate of 99.76%, and an F1 score of 99.87%, alongside a low false positive rate of 4.42% and a false negative rate of 0.24%. The study concludes that the ensemble bagging classifier demonstrated superior performance compared to other ensemble models.

Al-Haija & Al-Dala'ien (2022), like Das et al. (2019), used the voting mechanism to combine three decision tree-based algorithms. The algorithms consist of AdaBoosted Decision Trees, RUSBoosted Decision Trees, and Bagged Decision Trees. The method leverages the strength of each of the algorithms and, on evaluation using the N-BaIoT-2021 dataset, detects both normal and botnet attacks in various IoT devices. The study claimed to have achieved a detection accuracy of 99.6% and demonstrated its effectiveness in identifying botnet attacks.

The adaptive framework was proposed by Aslam et al. (2022) to detect and mitigate Distributed Denial of Service (DDoS) attacks within Software-Defined Networking (SDN) environments in the IoT devices. The research employed an ensemble voting mechanism to integrate outcomes from multiple classifiers, including support vector machines, naive Bayes, random forests, k-nearest neighbours, and logistic regression. The framework's performance was assessed through simulations of SDN-enabled IoT networks and was reported to have attained better detection accuracy, precision, recall, and F1 scores, surpassing earlier DDoS detection methods.

Abdulla & Hasoun (2022), in their study, demonstrate the efficacy of ensemble techniques to enhance detection accuracy and minimise false alarm rates in network attacks. This study analyses ensemble methods, including bagging, boosting, and stacking, which integrate multiple classifiers to enhance accuracy. The study compared the performance of both homogeneous and heterogeneous ensemble methods for detecting DoS and DDoS attacks. Various machine learning algorithms, including Support Vector Machine (SVM), K-Nearest Neighbours (KNN), Decision Trees (DT), and Random Forest (RF), were used for the experimental study. The dataset used for the study was the CICIDS 2017 and NSL-KDD with the confusion matrix for model evaluation. This work demonstrates that hybrid or ensemble learning models exhibit superior performance compared to single-algorithm models in the detection of DoS and DDoS attacks. In another study, Beulah and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

Pitchai Manickam (2022) aim to enhance the accuracy of detection and reduce false positives by integrating Support Vector Machine (SVM) and Logistic Regression (LR) classifiers through the use of a voting classifier. This model obtained an accuracy rate of 99.2%.

To further demonstrate the effectiveness of ensemble techniques, Alotaibi & Ilyas (2023) used voting and stacking to enhance detection of DDoS attacks in IoT settings. This study included four supervised machine learning models: Random Forest (RF), Decision Tree (DT), Logistic Regression (LR), and K-Nearest Neighbours (KNN), which were combined using stacking and voting techniques. The models were assessed based on accuracy, precision, recall, and F1 score. The results indicate that the stacking ensemble approach surpassed the voting method, with an accuracy of 98.64%. in contrast to 96.63% for voting. However, both the voting and stacking methods achieve an acceptable accuracy.

Aljebreen et al. (2023) introduced a method for detecting distributed denial of service (DDoS) attacks with a snake optimiser ensemble learning approach (DDoSA-SOEL). The snake optimiser method was used for feature selection, and ensemble learning included three deep learning models: Long Short-Term Memory (LSTM), Bidirectional LSTM (BiLSTM), and Deep Belief Network (DBN), using the Adadelta optimiser for hyperparameter tuning. The model was evaluated and validated using benchmark datasets, and its performance was compared with other recently developed models using several metrics. The DDoSA-SOEL technique had an average accuracy of 99.81% on the test dataset, surpassing several current models.

Pandey & Mishra (2023) examines the difficulties associated with imbalanced datasets and the need for effective feature selection in DDoS detection. The research used six machine learning classifiers: Random Forest (RF), Naïve Bayes (NB), Support Vector Machine (SVM), AdaBoost, eXtreme Gradient Boosting (XGBoost), and Gradient Boosting (GB) methods, with feature selection conducted by additional tree classifiers. The research used the CICDDoS2019 dataset, which comprises traffic data pertinent to DDoS assaults using the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), often employed in IoT networks. Ensemble sampling strategies substantially mitigated the class imbalance in the dataset, resulting in enhanced detection performance. In the same vain Aswad et al. (2023) integrate Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM)-RNN, Convolutional Neural Network (CNN), and Bidirectional LSTM (BiLSTM) to develop a robust DDoS detection system. The CICIDS2017 dataset was used for the training and evaluation of the models, including an extensive collection of network traffic data with annotated examples of diverse assaults. The models were assessed for accuracy, precision, recall, and F-measure to ascertain their efficacy in identifying DDoS assaults. The CNN-BiLSTM hybrid model achieved an optimal accuracy of 99.76%, demonstrating great precision (98.90%) and recall (99.60%), indicating its efficacy in accurately distinguishing between normal and malicious traffic.

Ahmim et al. (2023) provide another hybrid model that integrates several deep learning architectures, including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Deep Autoencoders, and Deep Neural Networks (DNNs). The concept of integrating these diverse forms of deep neural networks is to use their distinct characteristics to get superior performance. The CIC-DDoS2019 dataset, which meets all the criteria for an intrusion detection dataset, was used to assess the model. The findings indicate that the assembled deep learning model surpassed many established machine learning and deep learning models for true positive rate, accuracy, false alarm rate, average accuracy, and average detection rate.

Laiq et al. (2023) evaluate the efficacy of many ensemble learning classifiers, such as XGBoost and a hard-voting ensemble including Support Vector Machine (SVM), Decision Tree (DT), and Naive Bayes (NB), in identifying DDoS assaults. The research used the Edge-IIoT dataset, including traffic data from more than 10 IoT devices and 14 protocol-related assaults gathered via a sophisticated seven-layer testbed. An ensemble technique using hard voting was executed by amalgamating the predictions of SVM, DT, and NB classifiers and assessed by conventional classification metrics to ascertain their efficacy in identifying DDoS assaults. The research indicated that XGBoost surpassed the hard-voting ensemble classifier by 11% regarding accuracy. The ensemble method exhibited enhanced detection accuracy relative to singular classifiers, underscoring the advantages of integrating several models. The Edge-IIoT dataset enabled the creation of a realistic simulation of IIoT traffic and attack scenarios, enhancing the relevance of the findings to real-world contexts.

Bhadauria et al. (2024) present an ensemble learning framework that integrates various supervised machine learning techniques, including Random Forest, Support Vector Machine (SVM), and AdaBoost, to address DDoS attacks. The research employs network traffic datasets comprising both normal activity and DDoS attacks. The models were evaluated using metrics including accuracy, precision, recall, and F1-score to determine their effectiveness in detecting DDoS attacks. Ensemble learning methods exhibited superior detection rates for DDoS attacks relative to individual machine learning models. The ensemble models demonstrated effectiveness in managing different types of DDoS attacks, suggesting their applicability in practical scenarios. The results indicate that the application of ensemble learning techniques can improve the security of network infrastructures through the provision of more precise and dependable DDoS detection mechanisms.

Anis & Shohrab Hossain (2024) developed an ensemble machine learning approach by integrating three models derived from four traditional machine learning algorithms through hard ensemble voting. The algorithms comprise K-Nearest Neighbours (KNN), Support Vector

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

Machine (SVM), Decision Tree (DT), and Naive Bayes (NB). The experiment's outcome is determined through the evaluation of precision, recall, F1-score, and accuracy. The experiments demonstrate that the features selected via the feature importance technique attained a maximum accuracy of 98.86% when utilised with the ensemble voting classifier comprising KNN, SVM, and DT. The ensemble model exhibited high precision, recall, and F1-score, reflecting its efficacy in detecting DDoS attacks. The ensemble method improved the model's robustness by addressing the limitations of individual classifiers.

Das et al. (2024) developed two distinct ensemble frameworks: one that incorporates supervised learning algorithms and another that utilises unsupervised learning algorithms for the detection of DDoS attacks. The supervised ensemble framework comprises logistic regression, support vector machines, naïve Bayes, decision trees, and neural network classifiers. The unsupervised ensemble framework incorporates One-Class SVM utilising linear and polynomial kernels, Isolation Forest, Elliptic Envelope, and Local Outlier Factor. The framework integrated the outcomes from both ensemble models to establish a comprehensive detection system capable of recognising both familiar and unfamiliar attack patterns. The hybrid ensemble model's effectiveness was assessed using benchmark datasets, and its performance was compared to existing detection methods. The hybrid ensemble model exhibited enhanced efficacy in identifying DDoS attacks relative to standalone classifiers. The unsupervised ensemble framework effectively identified zero-day attacks, which are typically challenging for conventional signature-based detection systems to detect. The proposed model demonstrated consistent high performance across all three benchmark datasets, reflecting its robustness and generalisability. The hybrid ensemble method demonstrated superior performance compared to various established DDoS detection techniques regarding detection accuracy and false positive rates.

(Mante & Kolhe, 2024) Develop a model that combines various tree-based classifiers, including decision trees, random forests, and gradient boosting machines, to utilise their distinct advantages. The outputs from individual classifiers are integrated through an ensemble method, such as majority voting or weighted averaging, to derive the final prediction. The models are assessed through metrics such as accuracy, precision, recall, F1-score, and area under the curve (AUC) to evaluate their efficacy in identifying DDoS attacks. The ensemble model exhibited enhanced efficacy in identifying DDoS attacks relative to standalone classifiers, attaining greater accuracy and reduced false positive rates.

Kachavimath and Narayan (2025) developed an ensemble machine learning framework combining Hist Gradient Boosting Classifier and XGBoost through soft voting. The selected the best features by incorporating random forest classifier. The model's was evaluated using accuracy, precision, recall, F1-score. The experimental results demonstrated that the ensemble classifier performed better than individual classifiers. This study agrees with the conclusion of Das et al. (2024).

Raza et al. (2025) compared the performance of the ensemble algorithm that combines XGBoost and random forest with six individual classifiers. The six algorithms include Convolutional Neural Network (CNN), XGBoost, HistGradient Boosting Classifier, Random Forest, Decision Tree, and Long Short-Term Memory (LSTM). The experimental results show that the ensemble classifier outperformed the individual modes. The findings were consistent with the findings of other studies.

Alabelewe et al. (2025) compared the performance of voting and stacking ensemble classifiers that combine Random Forest, Decision Tree, Logistic Regression, and K-Nearest Neighbours algorithms. The experimental results on the CIC-IoT2023 dataset show that the voting classifier achieved 99.39% accuracy with 190.99ms inference time, while the stacking classifier reached 99.40% accuracy with 224.96ms inference time . Both ensemble methods outperformed individual classifiers, with the stacking classifier reducing false negatives by 17.5% and the voting classifier reducing false alarms by 64%. The findings were consistent with previous studies, demonstrating that ensemble approaches significantly enhance DDoS detection capabilities in IoT environments.

These studies demonstrate that ensemble learning is an effective approach for DDoS detection, particularly when combined with domain-specific feature selection.

Table 1 Summary of Ensemble Learning Techniques for detection of Distributed Denial of Service Attack in IoT Environments

Author	**Year**	**Dataset**	**Ensemble Classifier**		**Ensemble technique**	**Feature Selection Algorithm**
			Supervised	Unsupervised		
Das et al.	2019	NSL-KDD	C4.5, kNN, NN, SVM	NA	Majority voting	Manual, domain-knowledge-driven reduction:
Oluwole et al.	2022	CICDoS2019	Bagged, Random Forest, AdaBoost, Gradient Boosted, Decision Trees	NA	Bagging (Bootstrap Aggregating)	Minimal manual pre-processing. 5 non-numeric columns were dropped
Al-Haija & Al-Dala'ien	2020	N-BaIoT-2021	Bagged, AdaBoosted,	NA	Soft Voting. (Aggregation)	Correlation Coefficient Score

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

			RUSBoosted, and bagged			(Pearson)
Aljebreen et al.	2023	BOT-IOT	long short-term memory, bidirectional long short-term memory, deep belief network	NA	Simple averaging	Snake optimizer (SO)
Pandey & Mishra	2023	CICDDoS2019	Random Forest , Näıve Bayes , support vector machine, AdaBoost, eXtreme Gradient Boosting and Gradient Boosting	NA	Random under sampler and ADAptive SYNthetic (ADASYN)	Pearson correlation coefficient & Extra Tree classifier
Ahmim et al.	2023	CIC-DDoS2019	Convolutional Neural Networks , Long Short-Term Memory , Deep Autoencoder, and Deep Neural Networks	NA	Cascade / multi-level fusion (no voting or averaging).(deep learning)	None
Laiq et al.	2023	Edge-IIoT	SVM, Decision Tree, and Naive Bayes	NA	hard voting	Manual
Anis & Hossain	2024		K-Nearest Neighbors , Support Vector Machine , Decision Tree , and Naive Bayes	NA	hard ensemble voting	ANOVA, mutual information, and feature importance
Das et al.	2024	NSL-KDD, UNSW-NB15, and CICIDS2017	Logistic Regression, Support Vector Machine, Decision Tree, Naive Bayes with Gaussian function, Neural Network,	One-class SVM with linear kernel, one-class SVM with polynomial kernel, isolation forests, elliptic envelope, local outlier factor.	Stacking ensemble	Used dataset-specific filter sets taken from literature. (FS-7 for NSL-KDD, chi-square for UNSW-NB15)
Mante & Kolhe	2024	Bot-IoT, CICIoT2023, and DS2OS	Decision Tree , Extra Tree , Random Forest, and Extreme Gradient Boosting		Voting and Stacking	Wrapper approach tuned per ensemble: Voting: Step-Forward Feature Selection (SFS) reduces to 18 features. Stacking: Average tree-based feature-importance reduces to 9 features.
Kachavimath and Narayan	2025	InSDN	Histogram-based Gradient Boosting XGBoost		Soft-voting ensemble	Multistage Filter (Top 20 for Select KBest ANOVA F-value Random-Forest feature importance)
Raza et al.	2025	CIC IoT-2023	XGBoost Histogram Gradient-Boosting		Soft-voting ensemble	AI-based importance Mutual-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

			Classifier			information score Correlation filter
Alabelewe et al.,	2025	CIC IoT-2023	Random Forest Decision Tree Logistic Regression K-Nearest Neighbors		Voting Ensemble Stacking Ensemble	Correlation filter Mutual-information ranking PCA

Table 2 Performance Evaluation of Some Common Ensemble Classifiers

	Classifier		**Dataset**	**Ensemble Method**	**Accuracy %**	**Precision %**	**Recall %**	**F1 score %**
Das et al. 2019	Ensemble	C4.5, k-nearest neighbors, Neural Network, support vector machine	NSL-KDD	Majority voting	99.77	97.9	97.9	97.9
Das et al. 2019	Individual Classifiers	C4.5		MLP	96.5%	96.5%	97.3	96.9
		k-nearest neighbors		SMO	95.7	96.0	96.6	96.3
		Neural Network		IBK	97.8	97.9	97.9	97.9
		support vector machine		J48	97.9	97.9	97.9	97.9
Oluwole et al 2022	Ensemble	Bagged, Random Forest, AdaBoost, Gradient Boosted, Decision Trees	CICDoS2019	Ensemble Bagging with Decision-Tree base learner	99.75	99.99	99.76	99.87
Al-Haija & Al-Dala'ien 2020		Bagged, AdaBoosted, RUSBoosted, and bagged	N-BaIoT-2021	Multiclass	99.6	98.4	97.1	97.7
Aljebreen et al. 2023	Ensemble	Long short-term memory, bidirectional long short-term memory, deep belief network	BOT-IOT	DDAD-SOEL ensembl	99.81	99.59	99.61	99.60
Pandey & Mishra 2023	Pearson correlation coefficient	Random Forest , Näıve Bayes , support vector machine, AdaBoost, eXtreme Gradient Boosting and Gradient Boosting	CICDDoS2019	AdaBoost, eXtreme Gradient Boosting and Gradient Boosting	100	100	100	100
Ahmim et al. 2023	Deep Learning	Convolutional Neural Networks , Long Short-Term Memory , Deep Autoencoder, and Deep Neural Networks	CIC-DDoS2019	NA	80.75	98.74	97.1	97.7
Laiq et al. 2023	Ensemble	SVM, Decision Tree, and Naive Bayes	Edge-IIoT	Hard Voting	88.77	88.80	88.80	88.80
Das et al. 2024		Logistic Regression,	NSL-KDD, UNSW-NB15,	Combined ensemble	99.90	99.90	99.90	NA

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

		Support Vector Machine, Decision Tree, Naive Bayes with Gaussian function, Neural Network,	and CICIDS2017					
Mante & Kolhe 2024		Decision Tree , Extra Tree , Random Forest, and Extreme Gradient Boosting	Bot-IoT, CICIoT2023, and DS2OS	Stacking Ensemble	99.30	99.12	98.84	99.06
Kachavimath and Narayan 2025		Histogram-based Gradient Boosting XGBoost	InSDN	Voting Ensemble	99.99	100	99.99	99.99
Raza et al. 2025		XGBoost Classifier Histogram Gradient-Boosting Classifier	CIC IoT-2023	XGBoost / Random-Forest soft-voting ensemble	87			
Alabelewe et al., 2025		Random Forest Decision Tree Logistic Regression K-Nearest Neighbors	CIC IoT-2023	Stacking Ensemble	99.40	99.9	99.9	99.9

VII. DISCUSSION FOR FURTHER RESEARCH

Despite the significant advancements documented in the literature, several critical research gaps remain in the application of ensemble learning for DDoS detection in IoT environments:

- *Dataset Utilization Limitations*

While promising results have been demonstrated on various datasets, the application of ensemble learning approaches on contemporary datasets like CIC-IoT2023 remains largely unexplored. This gap is particularly significant given the continuously evolving nature of DDoS attacks and the need for current benchmarks that accurately reflect modern attack vectors and IoT device characteristics. The CIC-IoT2023 dataset presents unique characteristics, including traffic from diverse IoT device types, realistic network conditions, and contemporary attack patterns that may challenge existing ensemble approaches in ways not captured by older benchmark datasets.

Existing studies predominantly utilize datasets like NSL-KDD, UNSW-NB15, and Bot-IoT, which, while valuable, may not fully represent current IoT-specific attack landscapes. This temporal gap in dataset utilization potentially limits the generalizability of research findings to contemporary operational environments. The research community would benefit substantially from systematic evaluations of ensemble learning techniques across multiple contemporary datasets to establish their robustness and applicability to current threat landscapes.

- *Resource Constraint Considerations*

Existing research often fails to adequately address the computational demands of ensemble methods in resource-constrained IoT environments. While several studies report detection latencies and training times, few provide comprehensive analyses of memory utilization, energy consumption, and scalability characteristics—factors critical for practical IoT deployments. This limitation is particularly pronounced in edge-deployment scenarios where computational resources are severely restricted.

A comprehensive approach balancing detection accuracy with computational efficiency across the entire computational spectrum of IoT devices (from severely constrained edge devices to more capable gateway systems) remains absent from the literature. Future research should systematically quantify resource requirements across different ensemble configurations and develop adaptive approaches that can dynamically adjust ensemble complexity based on available resources and threat severity.

- *Performance Trade-off Quantification*

The literature reveals insufficient understanding of the precise trade-offs between detection accuracy and computational efficiency in ensemble-based approaches. While individual studies often report both performance metrics and computational requirements, systematic analyses that quantify these relationships across multiple ensemble configurations, dataset characteristics, and operational contexts are notably absent. This gap becomes critical in IoT contexts where real-time detection capabilities are essential, yet processing resources remain limited.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

The research community would benefit from mathematical models or empirical frameworks that predict performance-efficiency trade-offs for different ensemble configurations, enabling informed design decisions based on specific operational requirements. Such frameworks should consider not only traditional performance metrics like accuracy and precision but also IoT-specific considerations like energy efficiency and communication overhead.

- *Algorithm Integration Optimization*

The potential for combining high-performing algorithms like decision trees and random forests with complementary classifiers through ensemble techniques has not been thoroughly investigated using contemporary IoT attack datasets. While existing studies demonstrate the effectiveness of various ensemble combinations, systematic analyses of algorithm selection strategies, optimal ensemble sizes, and integration mechanisms specifically optimized for IoT security applications remain limited.

This gap is particularly notable given the distinctive characteristics of IoT network traffic, which often exhibits periodicity, device-specific patterns, and protocol constraints not typically present in conventional network environments. Research exploring algorithm integration strategies specifically designed to leverage these IoT-specific traffic characteristics could yield significant advancements in detection performance.

VIII. CONCLUSION

This review has examined the application of ensemble learning techniques for enhancing DDoS attack detection in IoT environments. Our analysis reveals that ensemble methods offer significant advantages over traditional single-algorithm approaches, particularly in addressing the unique challenges of IoT security.

Ensemble learning techniques, especially voting and stacking classifiers, demonstrate superior detection accuracy and adaptability compared to individual machine learning algorithms. By combining the complementary strengths of multiple models, these approaches can achieve higher detection rates, lower false positives, and improved generalization across diverse attack patterns. This makes them particularly well-suited for the dynamic and heterogeneous nature of IoT environments.

However, implementing ensemble learning in resource-constrained IoT devices presents significant challenges. The computational overhead of combining multiple models must be carefully balanced against detection accuracy to ensure practical deployability. Future research should focus on developing lightweight ensemble architectures specifically designed for IoT constraints, potentially through model compression techniques and optimized algorithm selection.

Additionally, the effectiveness of ensemble methods on contemporary datasets like CIC-IoT2023 warrants further investigation. As attack patterns evolve and new vulnerabilities emerge, continuous evaluation and refinement of ensemble approaches will be essential to maintain detection efficacy.

The integration of deep learning with ensemble techniques presents another promising direction. While traditional machine learning algorithms provide the foundation for current ensemble methods, incorporating deep learning models could potentially capture more complex attack patterns and further enhance detection capabilities.

Finally, federated learning approaches could address the distributed nature of IoT ecosystems, enabling collaborative model training across devices while preserving data privacy. This approach could significantly improve the scalability and adaptability of ensemble-based detection systems.

In conclusion, ensemble learning offers a powerful framework for enhancing DDoS attack detection in IoT environments. By addressing the identified research gaps and pursuing these future directions, the cybersecurity community can develop more robust and efficient protection mechanisms for increasingly complex IoT ecosystems.

REFERENCES

[1]. Abdulla, N., Nazanin, & Hasoun, K., Rajaa. (2022). Review of Detection Denial of Service Attacks using Machine Learning through Ensemble Learning. *Iraqi Journal for Computers and Informatics*, *48*(1), 13–20. https://doi.org/10.25195/ijci.v48i1.349

[2]. Abiramasundari, S., & Ramaswamy, V. (2025). Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms. *Scientific Reports*, *15*(1), 13098. https://doi.org/10.1038/s41598-024-84879-y

[3]. Abomhara, M., Koien, G. M., & Department of Information and Communication Technology, University of Agder, Norway. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

[4]. Abu Al-Haija, Q., & Al-Dala'ien, M. (2022). ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks. *Journal of Sensor and Actuator Networks*, *11*(1), 18. https://doi.org/10.3390/jsan11010018

[5]. Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. *Internet of Things*, *14*, 100365. https://doi.org/10.1016/j.iot.2021.100365

[6]. Ahmim, A., Maazouzi, F., Ahmim, M., Namane, S., & Dhaou, I. B. (2023). Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model. *IEEE Access*, *11*, 119862–119875. https://doi.org/10.1109/ACCESS.2023.3327620

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

[7]. Alabelewe, A. T., Ahmad, M. A., Aliyu, A. A., Ibrahim, M., Ahmed, A. M., & Abdulkadir, S. (2025). Enhanced DDoS Attack Detection in IoT Environments Using Voting and Stacking Ensemble Learning: Implementation and Performance Analysis. UMYU Scientifica, 4(2), 142-157. https://doi.org/10.56919/usci.2542.017

[8]. Alam, T. (2018). A reliable communication framework and its use in Internet of Things (IoT). International. *Journal of Advanced Computer Science and Applications*, *9*(12), 1–9.

[9]. Alotaibi, Y., & Ilyas, M. (2023). Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security. *Sensors*, *23*(12), 5568. https://doi.org/10.3390/s23125568

[10]. Al-Sarawi, S., Anbar, M., Abdullah, R., & Al Hawari, A. B. (2020). Internet of Things Market Analysis Forecasts, 2020–2030. *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 449–453. https://doi.org/10.1109/WorldS450073.2020.9210375

[11]. Anis, A., & Shohrab Hossain, Md. (2024). DDoS Attack Detection Using Ensemble Machine Learning. In M. Pandit, M. K. Gaur, & S. Kumar (Eds.), *Artificial Intelligence and Sustainable Computing* (pp. 531–546). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-0327-2_39

[12]. Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., Chelloug, S. A., Elaziz, M. A., Al-Qaness, M. A. A., & Jilani, S. F. (2022). Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT. *Sensors*, *22*(7), 2697. https://doi.org/10.3390/s22072697

[13]. Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors*, *24*(2), 708. https://doi.org/10.3390/s24020708

[14]. Baniya, P., Agrawal, A., Abid, K., Nath, J., Chaudhary, B. K., & Kunwar, B. (2024). The Internet of Things: Security Challenges and Opportunities. *2024 3rd International Conference on Power Electronics and IoT Applications in Renewable Energy and Its Control (PARC)*, 153–158. https://doi.org/10.1109/PARC59193.2024.10486356

[15]. Bhadauria, S., Aildasani, N., Kushwaha, J. P., & Gauttam, H. (2024). DDoS Attacks Detection using Ensemble Learning. *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–6. https://doi.org/10.1109/ICCCNT61001.2024.10724315

[16]. Das, S., Ashrafuzzaman, M., Sheldon, F. T., & Shiva, S. (2024). Ensembling Supervised and Unsupervised Machine Learning Algorithms for Detecting Distributed Denial of Service Attacks. *Algorithms*, *17*(3), 99. https://doi.org/10.3390/a17030099

[17]. Das, S., Mahfouz, A. M., Venugopal, D., & Shiva, S. (2019). DDoS Intrusion Detection Through Machine Learning Ensemble. *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 471–477. https://doi.org/10.1109/QRS-C.2019.00090

[18]. Domínguez-Bolaño, T., Campos, O., Barral, V., Escudero, C. J., & García-Naya, J. A. (2022). An overview of IoT architectures, technologies, and existing open-source projects. *Internet of Things*, *20*, 100626. https://doi.org/10.1016/j.iot.2022.100626

[19]. Elliott, D. L., & Anderson, C. (2023). The Wisdom of the Crowd: Reliable Deep Reinforcement Learning Through Ensembles of Q-Functions. *IEEE Transactions on Neural Networks and Learning Systems*, *34*(1), 43–51. https://doi.org/10.1109/TNNLS.2021.3089425

[20]. Fasial Sharif. (2024). *The Role of Ensemble Learning in Strengthening Intrusion Detection Systems: A Machine Learning Perspective*. Unpublished. https://doi.org/10.13140/RG.2.2.10798.93766

[21]. Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., & Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors*, *24*(11), 3571. https://doi.org/10.3390/s24113571

[22]. Gupta, B. B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges, and Countermeasures* (1st ed.). CRC Press. https://doi.org/10.1201/9781003107354

[23]. Gupta, B. B., & Quamara, M. (2020). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*, *32*(21), e4946. https://doi.org/10.1002/cpe.4946

[24]. Gupta, P., Krishna, C., Rajesh, R., Ananthakrishnan, A., Vishnuvardhan, A., Patel, S. S., Kapruan, C., Brahmbhatt, S., Kataray, T., Narayanan, D., Chadha, U., Alam, A., Selvaraj, S. K., Karthikeyan, B., Nagalakshmi, R., & Chandramohan, V. (2022). Industrial internet of things in intelligent manufacturing: A review, approaches, opportunities, open challenges, and future directions. *International Journal on Interactive Design and Manufacturing (IJIDeM)*. https://doi.org/10.1007/s12008-022-01075-w

[25]. Ismail, S., Hassen, H. R., Just, M., & Zantout, H. (2021). A review of amplification-based distributed denial of service attacks and their mitigation. *Computers & Security*, *109*, 102380. https://doi.org/10.1016/j.cose.2021.102380

[26]. Kachavimath,V A, Narayan D G, (2025). An Efficient DDoS Attack Detection in SDN using Multi-Feature Selection and Ensemble Learning, Procedia Computer Science, Volume 252, 2025, Pages 241-250, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.12.026.

[27]. Jahangeer, A., Bazai, S. U., Aslam, S., Marjan, S., Anas, M., & Hashemi, S. H. (2023). A Review on the Security of IoT Networks: From Network Layer's Perspective. *IEEE Access*, *11*, 71073–71087. https://doi.org/10.1109/ACCESS.2023.3246180

[28]. Kabanda, R., Byera, B., Emeka, H., & Mohiuddin, K. T. (2023). The History, Trend, Types, and Mitigation

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr311

of Distributed Denial of Service Attacks. *Journal of Information Security*, *14*(04), 464–471. https://doi.org/10.4236/jis.2023.144026

[29]. Kavre, M., Gadekar, A., & Gadhade, Y. (2019). Internet of Things (IoT): A Survey. *2019 IEEE Pune Section International Conference (PuneCon)*, 1–6. https://doi.org/10.1109/PuneCon46936.2019.9105831

[30]. Kikissagbe, B. R., & Adda, M. (2024). Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. *Electronics*, *13*(18), 3601. https://doi.org/10.3390/electronics13183601

[31]. Kiran, D. R. (2019). Internet of Things. In *Production Planning and Control* (pp. 495–513). Elsevier. https://doi.org/10.1016/B978-0-12-818364-9.00035-4

[32]. Kirda, E., & Ristenpart, T. (2017). *Proceedings of the 26th USENIX Security Symposium: August 16-18, 2017, Vancouver, BC, Canada*. USENIX Security Symposium, Berkeley, CA. USENIX Association.

[33]. Laiq, F., Al-Obeidat, F., Amin, A., & Moreira, F. (2023). DDoS Attack Detection in Edge-IIoT using Ensemble Learning. *2023 7th Cyber Security in Networking Conference (CSNet)*, 204–207. https://doi.org/10.1109/CSNet59123.2023.10339784

[34]. Liu, X., Yu, W., Liang, F., Griffith, D., & Golmie, N. (2021). Toward Deep Transfer Learning in Industrial Internet of Things. *IEEE Internet of Things Journal*, *8*(15), 12163–12175. https://doi.org/10.1109/JIOT.2021.3062482

[35]. Mante, J., & Kolhe, K. (2024). Ensemble of Tree Classifiers for Improved DDoS Attack Detection in the Internet of Things. *Mathematical Modelling of Engineering Problems*, *11*(9), 2355–2367. https://doi.org/10.18280/mmep.110909

[36]. Mishra, D., Tripathi, S. M., Chaurasia, A., & Chaurasia, P. K. (2025). A Review on Ensemble Learning Methods: Machine Learning Approach. *International Journal of Research Publication and Reviews*, *6*(2), 3795–3803. https://doi.org/10.55248/gengpi.6.0225.0971

[37]. Mohammed, A., & Kora, R. (2023). A comprehensive review on ensemble deep learning: Opportunities and challenges. *Journal of King Saud University - Computer and Information Sciences*, *35*(2), 757–774. https://doi.org/10.1016/j.jksuci.2023.01.014

[38]. Nazir, A., He, J., Zhu, N., Wajahat, A., Ma, X., Ullah, F., Qureshi, S., & Pathan, M. S. (2023). Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets. *Journal of King Saud University - Computer and Information Sciences*, *35*(10), 101820. https://doi.org/10.1016/j.jksuci.2023.101820

[39]. Oluwole, O. N., Adigwe, W., & Oghenefego Ogwara, N. (2022). Distributed Denial of Service Attack Detection and Prevention Model for IoT based Computing Environment using Ensemble Machine Learning Approach. *International Journal of Network Security & Its Applications*, *14*(4), 39–53. https://doi.org/10.5121/ijnsa.2022.14403

[40]. Pandey, N., & Mishra, P. K. (2023). Detection of DDoS attack in IoT traffic using ensemble machine learning techniques. *Networks and Heterogeneous Media*, *18*(4), 1393–1409. https://doi.org/10.3934/nhm.2023061

[41]. Raza, M S, Sheikh, M. N. A. , and Hwang, I.-S. “Ensemble Learning-Based DDOS Attack Recognition in IoT Networks”, Comput. Networks Commun. , vol. 3, no. 2, pp. 73–83, Jul. 2025.

[42]. Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*, *2*(6), 455–513. https://doi.org/10.1016/j.jiixd.2023.12.001

[43]. Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2025). A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. *Computers*, *14*(2), 61. https://doi.org/10.3390/computers14020061

[44]. Shtayat, M. M., Hasan, M. K., Sulaiman, R., Islam, S., & Khan, A. U. R. (2023). An Explainable Ensemble Deep Learning Approach for Intrusion Detection in Industrial Internet of Things. *IEEE Access*, *11*, 115047–115061. https://doi.org/10.1109/ACCESS.2023.3323573

[45]. Singh, C., & Jain, A. K. (2024). A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network. *E-Prime - Advances in Electrical Engineering, Electronics and Energy*, *8*, 100543. https://doi.org/10.1016/j.prime.2024.100543

[46]. Sivaji, C., Ramachandran, M., Prasanth, V., Sriram, S., & Sowmiya, S. (2022). Application of Arduino Devices in various IOT Application. *Renewable and Nonrenewable Energy*, 39–45. https://doi.org/10.46632/rne/1/1/7

[47]. Szymoniak, S., Piątkowski, J., & Kurkowski, M. (2025). Defense and Security Mechanisms in the Internet of Things: A Review. *Applied Sciences*, *15*(2), 499. https://doi.org/10.3390/app15020499

[48]. Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research. *Applied Sciences*, *11*(12), 5713. https://doi.org/10.3390/app11125713

[49]. Yang, Y., Lv, H., & Chen, N. (2023). A Survey on ensemble learning under the era of deep learning. *Artificial Intelligence Review*, *56*(6), 5545–5589. https://doi.org/10.1007/s10462-022-10283-5