# Securing the Internet of Things: A Comprehensive Examination of Machine and Deep Learning Approaches Against Denial of Service Attacks

Deepak Singh(✉) and R. Uma Mageswari

Vardhaman College of Engineering, Shamshabad, India
ds24098@gmail.com, r_uma@vardhaman.org

**Abstract.** The proliferation of Internet of Things (IoT) devices has revolutionized numerous industries, but it has also opened the door to sophisticated cyber threats, particularly Denial of Service (DoS) attacks. This review paper offers a thorough exploration of current methodologies employed in detecting and mitigating DoS attacks within IoT ecosystems, with a primary emphasis on the utilization of machine and deep learning techniques. Through a critical evaluation of the strengths, weaknesses, and limitations inherent in these approaches, this paper aims to identify gaps in existing research and propose innovative directions for future investigations. By addressing these research gaps, we aim to advance the field of DoS attack detection in IoT environments, enhancing the security and resilience of interconnected systems.

**Keywords:** DoS attacks · Deep Learning · Machine Learning · Benchmark-Dataset

## 1 Introduction

Denial of Service (DoS) [1] attacks stands as a formidable threat to the security and stability of Internet of Things (IoT) devices, marking a critical concern in the rapidly evolving landscape of digital connectivity. In essence, these attacks entail inundating an IoT device or network with an overwhelming influx of requests, intentionally causing a state of incapacitation where the system becomes unable to respond to legitimate traffic and can disrupt critical services, compromise data integrity, and cause financial losses. In the context of IoT, the consequences and risks associated with DoS attacks are amplified due to the interconnected nature of devices. For example, an attack on one device can have cascading effects on other devices within the network. Furthermore, compromised IoT devices can be weaponized as part of larger botnets [12] used for launching more sophisticated cyberattacks. With the proliferation of IoT devices [9] across diverse domains such as healthcare, smart cities, and industrial systems, the imperative to fortify these interconnected ecosystems against malicious disruptions


X. Cheng (Ed): BROADNETS 2024, LNICST 601, pp. 176–188, 2025.
https://doi.org/10.1007/978-3-031-81168-5_16

has become increasingly paramount. The sheer ubiquity of IoT devices, ranging from smart thermostats to industrial sensors, renders them susceptible to exploitation by malicious actors seeking to disrupt services or compromise data integrity. Consequently, the development and implementation of robust systems for detecting and preventing DoS attacks have become imperative in safeguarding the functionality and security of these interconnected devices. This review paper undertakes the task of delving into the realm of existing techniques aimed at detecting and preventing DoS attacks in IoT, with a specific focus on the application of machine and deep learning techniques. The rationale behind this exploration lies in the growing recognition of the potential of artificial intelligence (AI) methodologies to bolster cybersecurity defenses [2] in the intricate and dynamic landscape of IoT. Machine learning techniques, characterized by algorithms that learn patterns and make predictions based on data, have been at the forefront of endeavors to fortify IoT against DoS attacks. These methods leverage historical data to discern normal patterns of device behavior and can subsequently identify anomalies indicative of a potential DoS attack. The interpretability, scalability, and adaptability of machine learning approaches render them attractive in the context of IoT, where diverse devices with varying computational capacities and communication protocols [10] coexist. However, the efficacy of traditional machine learning techniques is not without its challenges. The intricate and evolving nature of DoS attacks, coupled with the diverse and dynamic data patterns within IoT environments, can pose difficulties in achieving high accuracy in detection. Machine learning models may struggle to keep pace with the sophistication of attacks, leading to potential vulnerabilities. In parallel, deep learning techniques, a subset of machine learning involving neural networks with multiple layers, offer a more intricate approach to DoS attack detection in IoT. These methods excel in extracting [2] complex features from raw data, potentially enabling them to discern subtle patterns indicative of an impending attack. The hierarchical representation of features learned by deep neural networks positions them as formidable tools for enhancing accuracy in the detection process. However, the advantages of deep learning come at a cost. The computational demands of training and running deep neural networks can be substantial, posing challenges in resource-constrained IoT environments. Moreover, the lack of interpretability in deep learning models raises concerns in cybersecurity contexts where understanding the rationale behind a detected threat is paramount for effective mitigation. In the pursuit of fortifying IoT against DoS attacks [11], it becomes imperative to critically evaluate and compare these machine and deep learning approaches. By dissecting their strengths, weaknesses, and limitations, this review aims to illuminate the current landscape of DoS attack detection in IoT. Through this exploration, we seek to identify research gaps that may pave the way for innovative solutions and future directions in augmenting the resilience of IoT ecosystems against the persistent and evolving threat of Denial of Service attacks. In doing so, the overarching goal is to contribute to the ongoing discourse on securing the interconnected future of IoT devices, ensuring their continued functionality and safeguarding against malicious disruptions.

## 2 Literature Review

In [5] a recent study, a team of researchers presented an innovative solution for detecting Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) networks. Published in 2021, their work introduces a lightweight machine learning (ML) model specifically designed for the complexities of IoT environments. This model leverages Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) algorithms to classify network traffic as normal or malicious. Impressively, the proposed model demonstrates high accuracy in detecting various DDoS attack types while maintaining low computational complexity—a critical factor for resource-constrained IoT devices. This research represents a noteworthy advancement in DDoS detection within IoT networks, showcasing the adaptability and effectiveness of machine learning techniques. The emphasis on a lightweight design acknowledges the computational limitations of IoT devices, making the proposed model a promising solution for enhancing security in the ever-expanding landscape of interconnected devices.

A 2022 survey [6] by N. D. B. Thang, D. T. Hoang, and D. M. Nguyen explores machine learning (ML) models for detecting Distributed Denial of Service (DDoS) attacks in IoT networks. Categorizing approaches by ML algorithms, data sources, and evaluation metrics, the study unveils diverse strategies with their respective strengths and limitations. This comprehensive overview identifies challenges, emphasizing the need for lightweight, adaptive, and privacy-preserving ML models. Recognizing the resource constraints in IoT, the call for lightweight models aligns with practical considerations. Adaptability addresses the dynamic nature of DDoS attacks, and the focus on privacy preservation responds to increasing concerns within the IoT ecosystem. As a snapshot of the current state and a guide for future research, this survey sets the stage for developing more robust and practical security solutions in the dynamic landscape of IoT-based networks.

A 2022 review [7] by S. Garg and S. Gupta delves into the application of Deep Learning (DL) for cyber threat detection in IoT networks, with a specific focus on the ever-pertinent issue of Denial of Service (DoS) attacks. This study meticulously explores various DL architectures, including Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Autoencoders, evaluating their effectiveness in the context of DoS attack detection. A key takeaway from the review is the emphasis on the necessity for domain-specific DL models. The unique characteristics and challenges inherent in IoT networks require tailored approaches to cyber threat detection. By underlining this need, the study provides valuable insights for researchers and practitioners, emphasizing the importance of crafting DL models that align with the intricacies of IoT environments. This tailored approach holds promise for enhancing the accuracy and adaptability of cyber threat detection mechanisms in the dynamic landscape of IoT networks.

In [8] their 2022 work, S. Mumtaz, S. I. Shohaimeh, and M. M. Mahmoud offer a comprehensive exploration of the applications, challenges, and future directions of Machine Learning (ML) and Deep Learning (DL) in the realm of IoT security and privacy. Focusing on areas such as DoS attack detection, the

study provides a nuanced overview of the advantages and limitations inherent in employing ML and DL techniques for safeguarding IoT environments. The research not only evaluates current applications but also extends its gaze toward the horizon of future developments. Notable among these prospective directions is the consideration of federated learning and reinforcement learning approaches. By acknowledging the evolving landscape of IoT security and privacy concerns, the study contributes to the ongoing discourse, offering valuable insights for researchers and practitioners seeking to fortify the robustness and privacy of IoT ecosystems.

## 3 Existing Detection Techniques for DoS Attacks in IoT

Detecting Denial of Service (DoS) attacks in the Internet of Things (IoT) realm is crucial to ensuring the security and functionality of interconnected devices. Various techniques have been proposed to address this challenge, each offering distinct advantages and considerations. Anomaly-based detection stands out as a prominent method, harnessing the power of machine learning algorithms to establish baseline behavior patterns within an IoT system or network. By comprehensively understanding normal operations, any deviations from these established norms are flagged as potentially malicious activities indicative of a DoS attack. This proactive approach enables the identification of novel attack vectors, making it a versatile solution for the dynamic landscape of IoT security. On the other hand, signature-based detection relies on predefined rules or signatures that match known patterns associated with specific types of attacks. While effective against familiar threats, this method may face limitations when confronted with previously unseen attack vectors. The rigidity of predefined signatures may result in false negatives when dealing with sophisticated and evolving DoS attack strategies [4]. Statistical analysis approaches bring a quantitative dimension to DoS attack detection in IoT environments. These techniques leverage statistical methods to discern abnormal network traffic patterns by comparing observed behavior with established norms. This data-driven approach enhances the detection capability, allowing for the identification of subtle deviations that may signify a potential DoS attack. However, the effectiveness of statistical analysis is contingent on the accuracy of the models and the ability to adapt to evolving attack tactics. Flow-based analysis introduces real-time detection capabilities by monitoring the flow of data packets within an IoT network. This method involves identifying anomalies or suspicious patterns that could indicate a DoS attack in progress. While offering a dynamic and responsive solution, flow-based analysis may require a sophisticated network infrastructure to efficiently process and analyze the vast amount of data generated by IoT devices.

## 4 Machine Learning Techniques for DoS Attack Detection in IoT

Machine learning techniques offer promising avenues for detecting DoS attacks in IoT devices [1]. Supervised learning algorithms, such as Support Vector Machines

(SVM) and Random Forests, can be trained on labeled datasets to classify network traffic as either legitimate or malicious. Unsupervised learning algorithms, including clustering algorithms like k-means or density-based techniques like DBSCAN, are capable of identifying anomalous patterns without the need for labeled data. Deep reinforcement learning can also be employed to develop adaptive detection systems that continuously learn from their environment and dynamically adjust their detection mechanisms. However, machine learning approaches face challenges related to feature engineering, high-dimensional data processing, interpretability of results, and adaptability to evolving attack strategies.

## 5 Deep Learning Techniques for DoS Attack Detection in IoT

Deep learning techniques have gained significant attention due to their ability to automatically extract meaningful features from raw data without explicit feature engineering [13]. Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks are commonly used deep learning architectures for detecting DoS attacks in IoT. These techniques excel at handling complex temporal dependencies in time-series data typically encountered in network traffic analysis. Furthermore, transfer learning can be leveraged by pretraining deep neural networks on large-scale datasets from other domains before fine-tuning them on specific target applications. Despite their success, deep learning models often require substantial computational resources and extensive amounts of labeled training data. Additionally, they may suffer from overfitting when faced with small or imbalanced datasets.

## 6 Comparative Analysis of Machine Learning vs Deep Learning Techniques

Machine learning (ML) and deep learning (DL) techniques have emerged as crucial tools in addressing the challenging task of detecting Denial of Service (DoS) attacks within the Internet of Things (IoT) ecosystem. Both approaches offer distinct advantages and drawbacks, necessitating a comprehensive comparative [5] analysis to guide the selection of the most suitable technique based on specific application requirements, dataset characteristics, and available computational resources. Machine learning techniques, characterized by algorithms that learn patterns from data, present notable advantages in interpretability, scalability, and adaptability to real-time scenarios. Interpretability, the ability to comprehend and explain the decision-making process, is a critical aspect in the context of DoS attack detection. Cybersecurity professionals need to understand the rationale behind flagged incidents to formulate effective mitigation

strategies. Machine learning models, by their nature, provide a more transparent view of their decision processes, facilitating interpretability. Scalability is another strength of traditional machine learning approaches. In the context of IoT, where deployments can be massive and diverse, the ability to scale detection mechanisms is paramount. Machine learning models can efficiently process large volumes of data, making them well-suited for addressing the challenges posed by the expansive nature of IoT networks. Moreover, machine learning models demonstrate adaptability to realtime scenarios. As the threat landscape evolves, the capacity to analyze and respond swiftly to emerging threats is crucial. Machine learning algorithms, when properly designed, can dynamically adjust to changing patterns, ensuring that the detection system remains effective in the face of evolving DoS attack strategies. However, traditional machine learning techniques have their limitations, particularly when faced with complex data patterns associated with sophisticated DoS attacks. The intricacies of such attacks may surpass the capabilities of conventional machine learning models to accurately capture and classify patterns, potentially compromising the overall accuracy of the detection system. Deep learning techniques, a subset of machine learning involving neural networks with multiple layers, offer a different set of advantages. One notable strength is their ability to extract intricate features from raw data, potentially leading to higher accuracies in DoS attack detection. The hierarchical representation of features learned by deep neural networks allows them to discern subtle and complex patterns that may evade traditional machine learning algorithms. Despite their potential for high accuracy, deep learning techniques come with computational trade-offs. The training and inference processes for deep neural networks, especially complex architectures like convolutional neural networks (CNNs) and recurrent neural networks (RNNs), demand substantial computational resources [14]. In resource-constrained IoT environments, where computational capabilities are often limited, the computational demands of deep learning can pose a significant challenge. Additionally, the interpretability of deep learning models is often criticized. The complex, nonlinear relationships learned by deep neural networks make it challenging to provide clear explanations for their decisions. In cybersecurity applications, where understanding the reasoning behind a detected threat is essential for effective response and mitigation, the lack of interpretability raises concerns. The choice between machine learning and deep learning techniques for DoS attack detection in IoT depends on a careful consideration of various factors. The specific requirements of the application, the characteristics of the dataset, the available computational resources, and the desired trade-offs between accuracy and interpretability all play crucial roles in this decision-making process (Table 1).

**Table 1.** Comparative Analysis of ML vs DL Techniques for DoS Attack Detection in IoT

| Criteria | Machine Learning (ML) | Deep Learning (DL) |
|---|---|---|
| Interpretability | Provides a transparent view of decision processes<br>Facilitates understanding for effective mitigation | Often criticized for lack of interpretability<br>Complex, nonlinear relationships hinder explanation |
| Scalability | Efficiently processes large volumes of data<br>Well-suited for massive and diverse IoT deployments | Computational demands may pose challenges in IoT<br>Resource-intensive, may be limiting in IoT settings |
| Adaptability | Dynamically adjusts to changing threat landscapes | Can discern subtle and evolving attack patterns |
| Accuracy | May struggle with complex data patterns | - Capable of higher accuracy, especially with intricate features |
| Computational Resources | Less demanding, suitable for various environments | Demands substantial computational resources |

## 7 Research Gap Analysis

In the realm of DoS attack detection within IoT, the current body of research, though marked by substantial strides, reveals discernible gaps that warrant attention and further exploration. While machine and deep learning techniques have shown promise in bolstering cybersecurity defenses, a nuanced examination of the existing literature underscores several areas where advancements are needed. One glaring research gap lies in the tendency of many studies to concentrate on specific types of DoS attacks or limited scenarios. The intricacies of the IoT landscape demand a more comprehensive understanding, encompassing diverse attack vectors and multifaceted aspects of the problem. Often, existing research falls short of addressing [6] the full spectrum of challenges posed by evolving DoS threats within the expansive IoT ecosystem. A holistic approach that considers the intersectionality of attack strategies, device heterogeneity, and communication protocols is essential for developing robust and adaptable detection systems. Moreover, the absence of standardized benchmark datasets poses a significant impediment to progress in the field. Many studies rely on datasets that may not authentically reflect the complexities of real-world IoT network traffic patterns across various application domains. The diversity of IoT applications, from healthcare to industrial systems, necessitates datasets that capture the nuances of distinct environments. Standardized benchmarks would facilitate fair and rigorous comparisons among different DoS detection systems, enabling researchers to assess the generalizability and efficacy of proposed methodologies across diverse scenarios. Furthermore, the ever-evolving nature of cyber threats [4] calls for adaptive detection systems capable of proactively identifying emerging attack vectors. As attackers continually refine and innovate their strategies

to circumvent existing defense mechanisms, the static nature of many current detection systems becomes a limitation. Future research endeavors should focus on developing dynamic and adaptive solutions that can autonomously evolve to counter new and sophisticated DoS attack techniques. This proactive stance is essential to stay ahead of the rapidly changing threat landscape in the IoT domain. In addressing these research gaps, the community can advance the field of DoS attack detection in IoT and contribute to the development of resilient and effective cybersecurity measures. Comprehensive studies that consider a broad spectrum of attack scenarios, coupled with the development of standardized benchmark datasets, would provide a solid foundation for evaluating the robustness and applicability of detection systems. Additionally, research efforts should prioritize the creation of adaptive detection mechanisms that can continuously learn and adapt to emerging threats, ensuring the sustained security of IoT ecosystems in the face of evolving cyber risks. As the Internet of Things continues to integrate into various aspects of daily life and industrial processes, closing these research gaps becomes imperative. The potential consequences of successful DoS attacks on critical IoT systems underline the urgency of advancing the state of knowledge and technology in this field. By addressing these gaps and pushing the boundaries of research, the community can contribute meaningfully to the ongoing efforts to fortify the security and resilience of IoT devices against the persistent and evolving threat landscape of Denial of Service attacks.

## 8 Proposed Solutions or Future Directions

To address these research gaps identified within existing literature on DoS attack detection in IoT using machine and deep learning techniques, several potential solutions or future directions can be explored:

### 8.1 Development of Comprehensive Benchmark Datasets

The creation of benchmark datasets is crucial for evaluating the effectiveness of DoS attack detection models. These datasets should be representative of diverse IoTapplications to ensure that the models can generalize well across different scenarios. Consideration should be given to various network traffic patterns, communication protocols, and device types. This will allow researchers to develop more robust and versatile models that can adapt to the dynamic nature of IoT environments (Table 2).

**Table 2.** Description of Datasets in IoT

| Dataset Name | IoT Applications | NetworkTraffic Patterns | Communication Protocols | Device Types |
|---|---|---|---|---|
| SmartHome Dataset | Smart Homes | Random | MQTT, CoAP | Sensors, Actuators |
| Iot Dataset | Industrial Iot | Periodic | OPC UA, modbus | PLCs, RFID readers |
| Health Dataset | Health care Iot | Bursty | HTTP, Bluetooth | Wearables, Medical Sensors |

### 8.2 Investigation Into Novel Algorithms or Methodologies:

Research efforts should focus on developing innovative algorithms or methodologies that go beyond existing approaches. This could involve exploring new features, designing adaptive learning strategies, or incorporating domain-specific knowledge. Emphasis should be placed on enhancing detection accuracy while simultaneously reducing false positives. This might involve the use of anomaly detection techniques, heuristic approaches, or leveraging the unique characteristics of IoT traffic.

**Exploration of Ensemble-Based Approaches:** Ensemble methods involve combining predictions from multiple models to improve overall performance. In the context of DoS attack detection, researchers could explore the integration of diverse machine and deep learning models [3]. Ensemble approaches can provide a more robust and reliable detection system by leveraging the strengths of different models and mitigating individual weaknesses. This could enhance the system's ability to detect various types of attacks. Ensemble-based approaches have gained popularity in various machine learning applications, including the field of cybersecurity, such as DoS (Denial of Service) attack detection. Combining predictions from multiple models can often lead to improved performance and robustness. Here's an exploration of ensemble methods in the context of DoS attack detection:

1. Model Diversity: Machine Learning Models: Researchers can integrate diverse machine learning models, such as decision trees, support vector machines, k-nearest neighbors, and random forests. Each model captures different patterns and characteristics of the data, contributing to the overall diversity of the ensemble.
   Deep Learning Models:Deep neural networks, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and other architectures can be included in the ensemble to leverage the representation learning capabilities of deep learning.
2. Heterogeneous Ensemble: Combining Different Paradigms: Combine machine learning and deep learning models in a heterogeneous ensemble. This can be particularly beneficial as machine learning models may excel in capturing certain features, while deep learning models can automatically learn intricate patterns from raw data.
3. Feature Engineering: Input Features:Experiment with different sets of input features for each model in the ensemble. Feature engineering techniques tailored to specific models can enhance their ability to detect anomalous patterns associated with DoS attacks.
4. Bagging and Boosting: Bagging (Bootstrap Aggregating):Use bagging techniques to train multiple models on different subsets of the dataset, introducing randomness and reducing overfitting. Random Forest is a popular bagging ensemble that combines multiple decision trees. Boosting: Explore

boosting algorithms like AdaBoost or Gradient Boosting, which focus on correcting the errors of individual models in the ensemble. Boosting can improve the overall performance by giving more weight to misclassified instances.

5. Voting Schemes: Majority Voting: Simple majority voting can be employed, where the most commonly predicted class among the ensemble members is chosen. Weighted Voting: Assign different weights to the predictions of each model based on their individual performance, allowing more influential models to contribute more to the final decision.
6. Ensemble Calibration: Calibrating Probabilities: Some ensemble methods provide probability estimates. Calibrate these probabilities to ensure they reflect the true likelihood of an instance belonging to a particular class. Well-calibrated probabilities can improve the reliability of the ensemble.
7. Dynamic Ensemble: Adaptive Approaches: Implement dynamic ensemble methods that can adapt over time. This is particularly useful in a dynamic environment where the characteristics of DoS attacks may change. Adaptive ensembles can automatically adjust their composition based on the evolving threat landscape.
8. Explainability: Interpretability: Consider the interpretability of the ensemble. While deep learning models may provide powerful predictive capabilities, their inherent complexity can make them less interpretable. Combining them with more interpretable machine learning models can enhance the overall explainability of the ensemble.
9. Dataset Augmentation: Data Augmentation: Augment the training dataset to increase diversity and improve the generalization of individual models. Techniques such as random sampling, noise injection, or synthetic data generation can be applied.
10. Cross-Validation: - **Ensemble Cross-Validation: ** Employ cross-validation techniques tailored to ensembles, such as Monte Carlo or bootstrap cross-validation, to obtain a more accurate estimate of the ensemble's performance.

By exploring these ensemble-based approaches, researchers can develop a robust and reliable DoS attack detection system that leverages the strengths of different models and enhances overall performance. The adaptability and versatility of ensemble methods make them well-suited for addressing the challenges associated with cybersecurity applications.

### 8.3 Integration of Explainable AI Methods

Deep learning models, particularly neural networks, are often viewed as "black boxes" because of their complexity. Integrating explainable AI methods is crucial for improving the interpretability of these models. Techniques such as attention mechanisms, feature importance analysis, and model-agnostic interpretability tools can help researchers and practitioners understand how the model arrives at its decisions. This is essential for building trust in the detection system and facilitating human understanding of detected threats. The integration of explainable

AI methods is indeed crucial for enhancing the interpretability of deep learning models, especially in the context of securing the Internet of Things (IoT) against Denial of Service (DoS) attacks. Here's a comprehensive examination of how various explainable AI techniques can be applied:

1. Attention Mechanisms: Explanation: Attention mechanisms in neural networks highlight specific parts of the input data that are deemed important for making a particular decision. This provides insights into which features the model is focusing on. Application: In the context of IoT security, attention mechanisms can be applied to identify and explain patterns in the network traffic or sensor data that contribute to the detection of potential DoS attacks. This can help in understanding the key indicators used by the model.
2. Feature Importance Analysis: Explanation: Feature importance analysis involves evaluating the contribution of each input feature to the model's output. This aids in identifying the most influential features in the decision-making process. Application: By conducting feature importance analysis, one can pinpoint the critical features in IoT data that contribute to the detection of DoS attacks. This information is valuable for refining the model and providing clear insights to stakeholders on what factors trigger an alert.
3. Model-Agnostic Interpretability Tools: Explanation: These tools are designed to interpret the predictions of any machine learning model, regardless of its underlying architecture. This helps in creating a more transparent understanding of model decisions. Application: For IoT security, using model-agnostic interpretability tools allows practitioners to apply various explainability techniques without being limited to the specifics of the deep learning model. This flexibility is important for ensuring compatibility with different IoT security models.
4. Lime (Local Interpretable Model-agnostic Explanations): Explanation: Lime is a technique that provides local explanations for individual predictions. It creates a locally faithful model around a specific instance to explain the decision made by the black-box model. Application: In the context of IoT, Lime can be used to generate explanations for specific instances of detected threats, allowing security analysts to understand the reasoning behind each decision and take appropriate actions.
5. Shapley Values: Explanation: Shapley values allocate contributions of each feature to the prediction based on its importance and interaction with other features. It ensures a fair distribution of credit across all features. Application: Applying Shapley values in the IoT security domain can help in understanding the collaborative impact of different features in identifying DoS attacks, ensuring a holistic view of the model's decision-making process.

By integrating these explainable AI methods, the interpretability of deep learning models can be significantly enhanced, fostering trust in the IoT security system and enabling effective collaboration between AI systems and human operators in the identification and mitigation of DoS attacks.

### 8.4 Incorporation of Active Defenses

Active defense mechanisms involve dynamically adapting the system's behavior in response to real-time threat intelligence. This could include adjusting network configurations, modifying access controls, or deploying countermeasures. Integration of threat intelligence feeds and collaboration with external security services can enhance the system's ability to respond proactively to emerging threats. Active defenses contribute to making the IoT environment more resilient against evolving DoS attack strategies (Fig. 1).

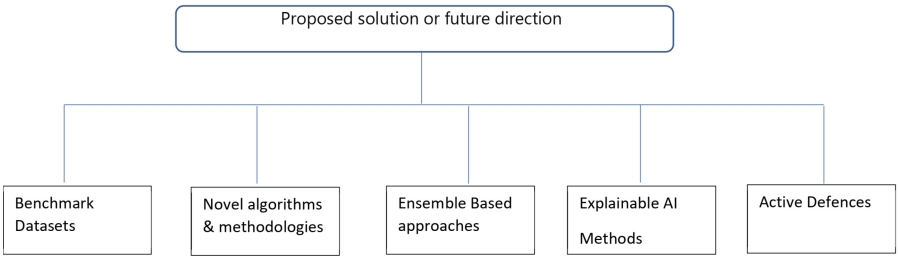


**Fig. 1.** simple representation shows each proposed solution or future direction

## 9 Conclusion

In conclusion, the detection and prevention of DoS attacks in IoT using machine and deep learning techniques play a critical role in ensuring the security and stability of IoT devices. By reviewing existing detection techniques, comparing machine learning and deep learning approaches, identifying research gaps, and proposing future directions, this paper highlights the need for further advancements in this field. Efforts to develop more accurate, efficient, scalable, and adaptive DoS attack detection systems will contribute to a safer IoT environment. Ultimately, the combination of machine learning, deep learning, and emerging technologies holds great promise for mitigating the risk posed by DoS attacks in IoT.

## References

1. Adedeji, K.B., Abu-Mahfouz, A.M., Kurien, A.M.: DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. J. Sens. Actuator Netw. **12**(4), 51 (2023)
2. Kazmi, S.H.A., Qamar, F., Hassan, R., Nisar, K.: Routing-based interference mitigation in SDN enabled beyond 5G communication networks: a comprehensive survey. IEEE Access (2023)

3. Jin, X., Bagavathiannan, M., Maity, A., Chen, Y., Yu, J.: Deep learning for detecting herbicide weed control spectrum in turfgrass. Plant Methods **18**(1), 94 (2022)
4. Iftikhar, S., Khan, D., Al-Madani, D., Alheeti, K., Fatima, K.: An intelligent detection of malicious intrusions in IoT based on machine learning and deep learning techniques. Comput. Sci. J. Moldova **30**, 288–307 (2022)
5. Al-Theeb, A.D., Al-Sagheer, A.A., Al-Othman, F.A.: A lightweight model for DDoS attack detection using machine learning techniques. IEEE Access **9**, 113119–113133 (2021)
6. Thang, N.D.B., Hoang, D.T., Nguyen, D.M.: DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions. IEEE Trans. Comput. Soc. Syst. **9**(3), 1017–1031 (2022)
7. Garg, S., Gupta, S.: Deep learning for cyber threat detection in IoT networks: a review. J. Netw. Comput. Appl. **196**, 103424 (2022)
8. Mumtaz, S., Shohaimeh, S.I., Mahmoud, M.M.: Machine and deep learning for IoT security and privacy: applications, challenges, and future directions. IEEE Internet Things J. **9**(11), 8328–8346 (2022)
9. Kumar, V., Paul, K.: Device fingerprinting for cyber-physical systems: a survey. ACM Comput. Surv. **55**(14s), 1–41 (2023)
10. Ali, S.A., Elsaid, S.A., Ateya, A.A., ElAffendi, M., El-Latif, A.A.A.: Enabling technologies for next-generation smart cities: a comprehensive review and research directions. Future Internet **15**(12), 398 (2023)
11. James, F., Ray, I., Medhi, D.: Worst attack vulnerability and fortification for iot security management: an approach and an illustration for smart home IoT. In: NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, pp. 1–6. IEEE (2023)
12. McNulty, L., Vassilakis, V. G.: IoT botnets: characteristics, exploits, attack capabilities, and targets. In: 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), pp. 350–55. IEEE (2022)
13. Gibert, D., Planes, J., Mateu, C., Le, Q.: Fusing feature engineering and deep learning: a case study for malware classification. Expert Syst. Appl. **207**, 117957 (2022)
14. Himeur, Y., Sayed, A., Alsalemi, A., Bensaali, F., Amira, A.: Edge AI for internet of energy: challenges and perspectives. Internet Things 101035 (2023)