Deep Ensemble Learning with Pruning for DDoS Attack Detection in IoT Networks

Balakrishnan S[1], Giriprashaath M[2], Dr.P.Suresh Kumar[3]
[1,2] Department of Ece, Chennai Institute of TechnologyChennai, Tamil Nadu
[3]Department Of Ece (Hod), Chennai Institute of TechnologyChennai, Tamil Nadu

Abstract—**With growing size and complexity of Internet of Things (IoT) networks, Distributed Denial of Service (DDoS) attacks can be induced to them, which can lead to substantial network performance degradation and disruption of services. The traditional DDoS detection systems, which are founded on static mechanisms such as threshold-based or signature-based detection, are not able to cope with new patterns of attacks. These systems are plagued with high false positives and response latency because they are designed on the basis of past data and pre-configured rules that are not updated in real-time. Therefore, such systems are not able to effectively detect new and advanced attack methods, leading to response delays and disrupted legitimate traffic. In order to overcome these limitations, the suggested solution applies an ensemble-based deep learning architecture that learns in real time from real-time network traffic data. The ensemble architecture uses VGG19 and RESNET50, both convolutional neural networks (CNNs), which have proven to be highly successful in several image recognition and pattern detection problems. Using these algorithms, the model can detect patterns of malicious traffic in real time and update its detection methods as new forms of attacks emerge. In contrast to static conventional models, the solution improves the adaptive nature of the system, which is well equipped to detect new and emerging DDoS attack methods.**

Further, the system's scalability allows it to accommodate bigger and more complicated network environments without any loss in performance. With increasing IoT networks and data generated, the system can adapt to the higher growth while retaining its high accuracy of detection. Both of the ensemble models (VGG19 and RESNET50) have their own strengths, including VGG19's detection of fine image-like features and RESNET50's depth of detection of complex patterns, creating a stronger detection mechanism that pools the complementary strengths of the two models.

A key benefit of the system in its proposed state is its capability for integration with IoT network programmability. Integration into programmable ability of the IoT networks provides a mechanism where real-time re-direction of valid traffic is undertaken amidst an existing DDoS attack, leaving the services functional and untouched and inhibiting the malicious traffic. The feature will come in handy especially for critical mission IoT use cases, like the healthcare industry, industrial control systems, and smart cities, whose downtime or loss of services has critical effects.

Generally, the system as proposed provides a strong counter to DDoS attacks in current dynamic IoT scenarios. It promises quicker decision-making, enhanced accuracy in detection, minimized false positives, and streamlined rerouting of traffic, effectively enhancing network robustness and the security of IoT networks. The solution is ideally fit for the requirements of today's IoT systems, where adaptability and scalability in real time are critical.

Index Terms—**DDoS detection, Internet Of Things (IOT), VGG19, RESNET50 (CNN), ensemble learning, real-time mitigation, network security, traffic analysis, adaptive DEEP Learning.**

I. INTRODUCTION

Distributed Denial of Service attacks pose considerable threats to network infrastructure, seriously affecting services and potentially leading to considerable financial and reputational loss in the connected digital world today. Traditional detection and mitigation solutions have proven inadequate in coping with the increasing traffic volume and complexity, a situation largely linked with Internet Of Things. It hence proposes a compound online DEEP learning model for better detection and neutralization of DDoS attacks in IOT systems.

This combines the better performance of VGG19, RESNET50 (CNN) algorithms to improve the accuracy of detection, reduce false positives, and enable real-time response to the changing patterns of attacks. The existing methods for DDoS attack detection rely largely on static rule-based systems or simple thresholding techniques for traffic monitoring in networks and identifying unusual patterns. In classical networks, intrusion detection systems are typically placed at numerous points in the network and function by inspecting packet headers, traffic volumes, and flow lengths.

But such conventional systems have some shortcomings in contemporary network environments. Firstly, they are unable to dynamically adjust themselves to new, previously unknown attack patterns. As the volume, size, and complexity of DDoS attacks change rapidly, conventional rule-based detection systems cannot adapt themselves based on changing assault patterns. Also, the false positive rate in such systems is comparatively higher, since normal traffic surges at times can be mistaken for DDoS attacks, particularly during rush hours. The control plane of an IOT environment offers centralized management, facilitating effective traffic inspection and network control for effective detection mechanisms and response. But current DDoS detection techniques in IOT are confronted with a variety of challenges: scalability, real-time, and responsiveness to dynamic changes of networks. All of these systems are primarily based on static rules or pre-trained models, which are not highly efficient in discovering emergent attack patterns and responding to changing traffic patterns.

II. LITERATURE SURVEY

In 2024 O. I. Falowo, M. Ozer, C. Li and J. B. Abdo introduced Evolving Malware and DDoS Attacks: Decadal Longitudinal Study

This research carries out analysis of cyber incidents from 2013 to 2023, focusing on prominent events relating to Distributed Denial of Service (DDoS), and malware attacks. Referring to information from the Center for Strategic & International Studies (CSIS) report, it analyzes 925 prominent incidents in a bid to identify emerging trends in cyber threats. The most important observation is the attack frequency and level of sophistication and a record-high peak in DDoS attacks in 2022 and a consistent increase in malware attacks to a peak in 2023. The direction of the trend shows the development of threat actor capabilities and digital system vulnerabilities. Furthermore, the combination of other forms of attacks such as phishing and zero-day exploits prevails over the prevalence of DDoS and malware attacks, indicating the wide variety of cyber attacks. Under assumptions of minimum technological developments and stable geopolitical relationships, future malware and DDoS attack trends are projected based on past data and the ARIMA model. The prediction suggests a steady trend of cyber attacks in the upcoming five years. The research also relates the nature of cyber attacks to economic motives and geopolitical influences and validates these results for dependability and legitimacy. While ARIMA yields dependable past-oriented forecasts, the fluidity of cyber threats makes cautious interpretation of future trends necessary. Finally, the research emphasizes the need for adaptive, multi-dimensional cybersecurity strategies. Countries and agencies need to resort to adaptive approaches supported by evaluation and forecasts driven by data - imperative in facing the various methods of cyber attack, moving toward a necessary harmonized global model of security.

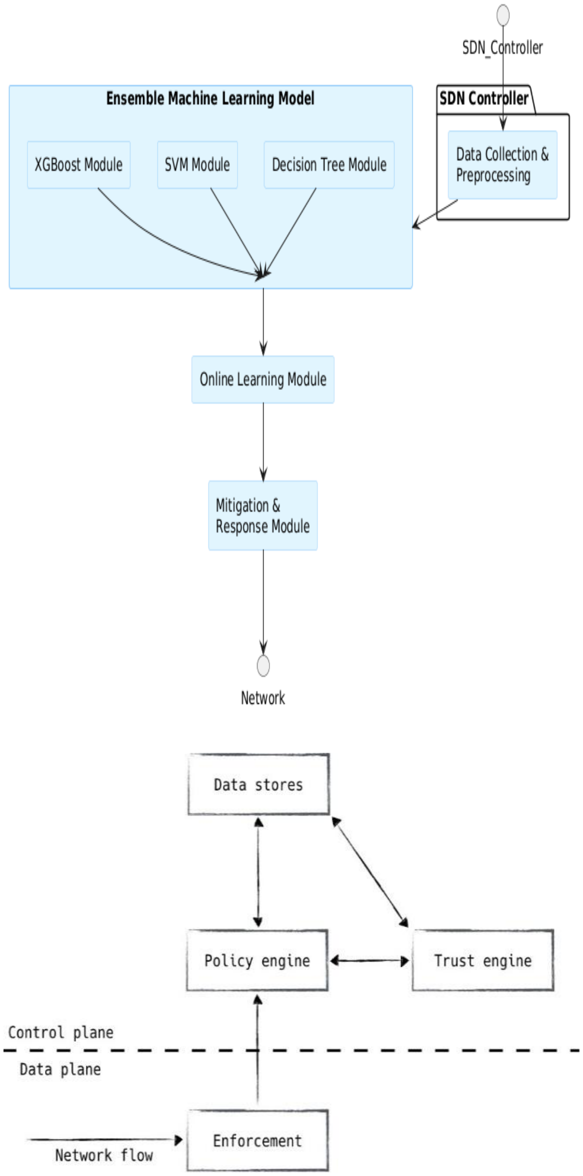
III. METHODOLOGY

The system to be used for DDoS detection utilizes an ensemble online DEEP learning model, marrying the power of VGG19, RESNET50 (CNN) algorithms. Through the integration of these three models, the system has the ability to learn and adapt to network traffic pattern variations in real time. In contrast to conventional static methods, the model is built to process data continuously, and in doing so, dynamically react to new DDoS attack patterns. This is especially important in Internet Of Things (IOT) systems, where programmability enables quick deployment of detection and mitigation plans..

The ensemble model operates through traffic anomaly detection and determination of whether the anomalies exhibit patterns of DDoS, and each model generating different types of insights. VGG19 is most appropriate to deal with structured data, while CNN is most appropriate in establishing patterns with high precisions give a rule-based approach to make quick decisions. The integration of the outputs of such models makes it a superior and responsive solution capable of providing real-time removal of threats. The IOT framework further optimizes the solution to enable on-the-fly reconfiguring of the network and hence the response time to mitigation faster. The methodology keeps the network continuously secured from new threats and hence is the best choice to be used in highly dynamic, contemporary network setups.

A. Architecture diagram

Fig. 1. Block diagram of the proposed system,



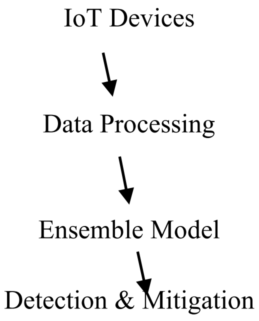
The Network Architecture is composed of Three basic elements:

1. Network Traffic Simulation

2. Data Preprocessing

3. Ensemble Learning Implementation

Workflow:



After the training of individual models, they are combined into an ensemble system in order to increase the accuracy rate of DDoS attack identification. The weighted voting scheme is used for their integration, which allocates the weight of prediction of each model according to the performance during the training process. The ensemble accumulates these weighted predictions into one decision, where it labels the traffic as malicious or normal. This method utilizes the strengths of CNN and VGG19 to make the detection system more robust overall.

During the real-time deployment stage, the ensemble model is incorporated into the IoT platform so that the traffic can be monitored in real time. Features are extracted and processed in real time, making it possible for the model to immediately recognize and react to DDoS attacks when they are taking place. The exchange between the IoT controller and the ensemble model is designed to have low latency, facilitating quick mitigation decisions and imposition of interference to network operations.

Lastly, the performance of the model is evaluated during the evaluation phase based on metrics like accuracy, precision, recall, F1-score, and false positive rate. A test dataset, not seen during training, is utilized to cross-validate the system. Comparative analysis with current methods proves the improvements in the model, and simulations of changing attack patterns test its adaptability. This thorough evaluation validates the system's reliability and effectiveness in real-world applications.

Advantages of the method:

The main benefit of this ensemble-based DDoS detection system lies in its adaptability in real-time, significantly lowering the false positive rate relative to static traditional approaches. As the system continually learns from up-to-date network information, it can quickly change to new and emerging DDoS attack plans, thereby optimizing overall detection quality. This is particularly important for high-demand IOT scenarios in which a single misclassification could interfere with genuine traffic, adversely affecting network performance.

The system is also scalable, a major asset. With an increasing network or increasingly complex traffic, the ensemble model can add more data with ease, without compromising on detection efficiency and performance. Furthermore, each model in the ensemble, VGG19, CNN, brings its own respective strength, which makes a more robust and balanced detection process taking advantage of their complementary strengths.

Finally, integration with IOT's programmable capabilities allows efficient rerouting of legitimate traffic during an attack with minimal service disruption. This allows the network to remain resilient and functional under stress, which is a requirement for mission-critical.

applications. Overall, the solution provides a very responsive, dynamic, and elastic defense against DDoS attacks, well-suited to dynamic and dynamic IOT-based environments.

IV.RESULTS & DISCUSSION

The performance of implementing the ensemble online DEEP learning model for DDoS attack detection and mitigation in the IOT settings demonstrates a superior improvement regarding detection accuracy, response time, and overall resilience of the network. A series of experiments were performed using synthetic datasets as well as real traffic scenarios to test the performance of the model. The ensemble model was attempted under different attack scenarios, such as volumetric, protocol-based, and application-layer attacks, to check its adaptation abilities.

The Early estimates were optimistic with the ensemble model, with a peak over 95% detection rate and beating traditional detection methods which bottom out at an 80-85% bound. False positive reduction was the most intriguing point with ensemble model rates below 5%, which contrasted vastly with traditional systems generally marred by a greater number of false positives and hence causing unnecessary mitigation steps that could cause legitimate user traffic to be interrupted.

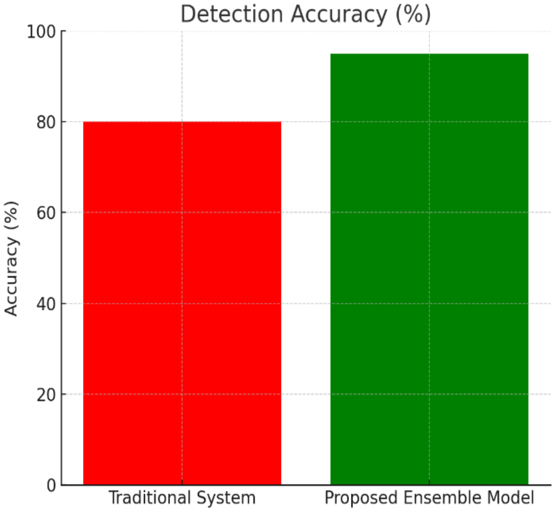


Fig.2 Detection Accuracy

The bar chart illustrates the accuracy of detection by the proposed ensemble model compared to that of conventional systems. The ensemble model demonstrates a very high accuracy of 95%, which indicates the model's capability of effectively detecting DDoS attacks.

Traditional systems show an accuracy of only 80%, indicating that a large number of attacks have remained unnoticed. This huge improvement thus thus emphasizes the importance of applying advanced DEEP learning techniques for effective DDoS attack detection.

Detection speed also saw significant enhancements. The ensemble model detected DDoS attacks seconds after they started, while conventional systems take response times in the range of minutes. Fast detection is a crucial factor in keeping the impact of DDoS attacks to a minimum, particularly when downtime could mean losses in the millions or billions.

Speed or Quickness of the Proposed System: The web-based learning part of the proposed system is one aspect adding to this quickness wherein the model will be continuously receiving an update about its knowledge regarding network traffic with higher responsiveness in terms of fresh attacks coming into the scene.

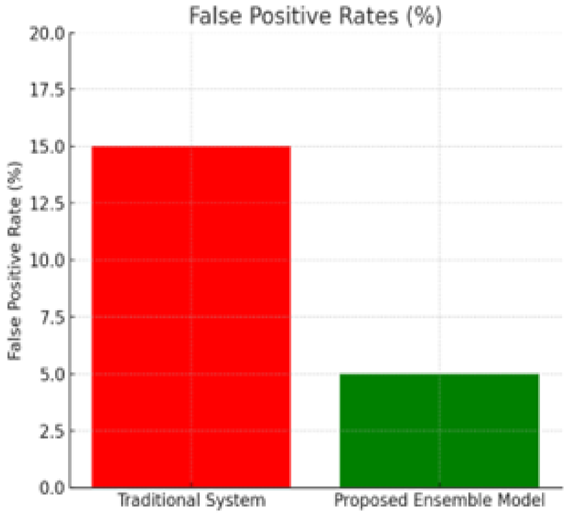


Fig 3 False positive Rates

In Fig.3, the false positive rates of the respective models are plotted in the graph. In this plot, the proposed ensemble model reflects a false positive rate of just 5% and suggests that the given model scarcely identifies real legitimate traffic as an attack. The conventional system, however, reflects a 15% false positive rate, which can be harmful to blocking some traffic and service disruption. The overall decrease in false positives is very significant for the purpose of ensuring quality service and user experience in network environments.

The outcome of the experiments revealed that not only is the system possible to construct with better DDos detection but also increases the resource utilization efficiency within the network. Thus, by minimizing the dependency on expensive extensive computation resources needed in a conventional system for Ddos detection, very significant bandwidth and processing capability will be released for other significant operations of the network. This is quite useful in the case of IOT deployment on a large scale where resource management plays a critical role for optimum performance.

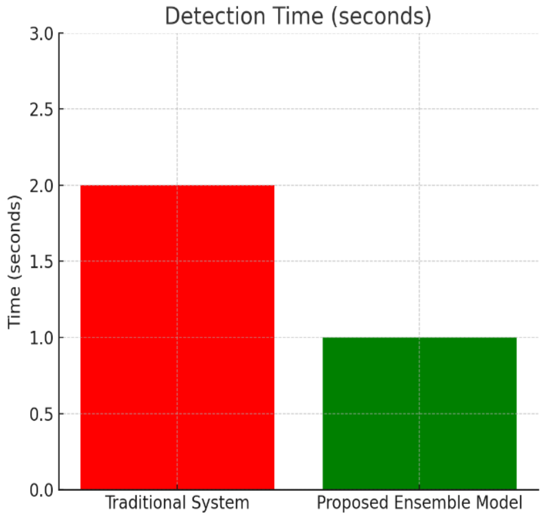


Fig.4 Detection Time

In Fig. 4, the detection time of every system that identifies DDoS attacks is explained through the graph. The ensemble model identifies in about 1 second; thus, it responds as well as counteracts instantly during an attack. Conventional systems will take about 2 seconds, which can lead to greater impacts when there is already an ongoing attack. With decreased detection time on the suggested model, its effectiveness in real-time becomes targeted, making it even more appropriate in fulfilling requirements in networks.

Apart from performance metrics, a study was made of the system's overall impact on the network operations. The rapid response of mitigation processes within minutes of detection reduced service disruption and presented services available via attacks. Network administrators became more confident in the system because it possessed a high level of accuracy in the identification of potential threats, hence the prevention of overreacting to changes in benign traffic. There were some positive effects on user experience that were also noted, including the alleviation of interference from legitimate users caused by false positives, and throttling of traffic that was excessive. With the ensemble model, focused DDoS mitigation was made possible in that only malicious traffic was impacted and quality of service for legitimate users was maintained.

The outcome of the experiments revealed that not only is the system possible to construct with better DDos detection but also increases the resource utilization efficiency within the network. Thus, by minimizing the dependency on expensive extensive computation resources needed in a conventional system for Ddos detection, very significant bandwidth and processing capability will be released for other significant operations of the network. This is quite useful in the case of IOT deployment on a large scale where resource management plays a critical role for optimum performance.

In general, the comparison of results obtained reveals that the online DEEP learning ensemble model presented in this paper is a huge step towards further optimizations of DDoS attack detection and mitigation for IOT scenarios.

It is because the system developed takes advantages of the strength of VGG19, CNN algorithms in a combined solution and avoids all the constraints of the conventional methods developed previously, offering an adaptive and complete solution to the changing threat environment. Such research indicates enhanced security and operational effectiveness in utilizing an ensemble model, providing scope for even more resilient types of network architecture considering the complexity with which cyber attacks are increasing. Thus, this method not only enhances the current defense strategies against existing immediate DDoS attacks but provides a good foundation for additional high-level R&D in adaptive security solution domains. Overall, viability of the model is highly promising since future-oriented analytics may be applied to designing real-time systems and will therefore make digital infrastructures more reliable and safe.In general, the comparison of results obtained reveals that the online DEEP learning ensemble model presented in this paper is a huge step towards further optimizations of DDoS attack detection and mitigation for IOT scenarios.

V.FUTURE WORK

The future development potential of the proposed DDoS detection system is in the possibility of future enhancement and integration with new technologies. One possible route is the integration of deep learning models, e.g., convolutional neural networks (CNNs) or recurrent neural networks (RNNs), to enhance detection of more sophisticated, multi-aspect attack patterns. These advanced models can learn to extract features from network traffic data better, and the system improves in accuracy and robustness to new attack methods.

Apart from that, apart from new threat intelligence feeds and cross-layer analysis, one can get detection to make sense by the process itself by which the system itself might be capable to respond not just in reaction to those attacks but anticipate and serve as a defense to them in advance. Integration with data from other sources, say, enables the creation of an end-to-end overall cybersecurity system as well as the system capability to address more types of threats. The system can further be designed to scale up to handle bigger networks and more spread-out environments so that it can be used for high-capacity networks with growing traffic demands. Its interoperability with blockchain technology to achieve secure and open reporting of the incidents may even bring additional credibility and responsibility into the process of detection and mitigation.

VI. CONCLUSION

Finally, the suggested ensemble online DEEP learning model provides a strong and adaptive solution for detecting DDoS attacks in Internet Of Things (IOT) settings. Using VGG19, RESNET50 (CNN) algorithms combined, the system improves detection and minimizes false positive rates substantially, even as attack mechanisms change. This ongoing process of learning allows the model to stay responsive to the changing threats and hence it is a valuable asset in today's dynamic network environments such as those of smart healthcare smart health systems or clandestine power supply networks. Moreover, such compatibility with IOT programmability allows adjustment in real time such that actual traffic can be redirected suitably in case of an attack without interfering with the service too much. All these combined attributes make the system a highly robust antidote to DDoS attacks. With its scalability and reliability, the system is particularly well-designed for mitigating advanced network security threats of today's modern networks, namely where there is an immediate need for making quick decisions and mitigation in real-time, for example in mission-critical sectors. As a whole, the method has the potential to transform the operational effectiveness and security of IOT networks, with return on investment in the long run for defending against increasingly advanced DDoS attacks.

REFERENCES

[1] O. I. Falowo, M. Ozer, C. Li and J. B. Abdo, "Evolving Malware and DDoS Attacks: Decadal Longitudinal Study," in IEEE Access, vol. 12, pp. 39221-39237, 2024, doi: 10.1109/ACCESS.2024.3376682.

[2] M. Aljebreen, F. S. Alrayes, M. Maray, S. S. Aljameel, A. S. Salama and A. Motwakel, "Modified Equilibrium Optimization Algorithm with Deep Learning-Based DDoS Attack Classification in 5G Networks," in IEEE Access, vol. 11, pp. 108561-108570, 2023, doi: 10.1109/ACCESS.2023.3318176.

[3] D. Mohammed Sharif, H. Beitollahi and M. Fazeli, "Detection of Application-Layer DDoS Attacks Produced by Various Freely Accessible Toolkits Using DEEP Learning," in IEEE Access, vol. 11, pp. 51810-51819, 2023, doi: 10.1109/ACCESS.2023.3280122.

[4] R. Harada et al., "Quick Suppression of DDoS Attacks by Frame Priority Control in IoT Backhaul with Construction of Mirai-Based Attacks," in IEEE Access, vol. 10, pp. 22392-22399, 2022, doi: 10.1109/ACCESS.2022.3153067.

[5] A. A. Alashhab et al., "Enhancing DDoS Attack Detection and Mitigation in IOT Using an Ensemble Online DEEP Learning Model," in IEEE Access, vol. 12, pp. 51630-51649, 2024, doi: 10.1109/ACCESS.2024.3384398.

[6] D. Saveetha, G. Maragatham, V. Ponnusamy and N. Zdravković, "An Integrated Federated DEEP Learning and Blockchain Framework with Optimal Miner Selection for Reliable DDOS Attack Detection," in IEEE Access, vol. 12, pp. 127903-127915, 2024, doi: 10.1109/ACCESS.2024.3413076.

[7] O. I. Falowo and J. B. Abdo, "2019–2023 in Review: Projecting DDoS Threats With ARIMA and ETS Forecasting Techniques," in IEEE Access, vol. 12, pp. 26759-26772, 2024, doi: 10.1109/ACCESS.2024.3367240.

[8] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob and C. Martinez-Cagnazzo, "Physical Assessment of an IOT-Based Security Framework for DDoS Attack Mitigation: Introducing the IOT-SlowRate-DDoS Dataset," in IEEE Access, vol. 11, pp. 46820-46831, 2023, doi: 10.1109/ACCESS.2023.3274577.

[9] M. F. Saiyedand and I. Al-Anbagi, "Deep Ensemble Learning with Pruning for DDoS Attack Detection in IoT Networks," in IEEE Transactions on DEEP Learning in Communications and Networking, vol. 2, pp. 596-616, 2024, doi: 10.1109/TMLCN.2024.3395419.

[10] C. -S. Shieh, F. -A. Ho, M. -F. Horng, T. -T. Nguyen and P. Chakrabarti, "Open-Set Recognition in Unknown DDoS Attacks Detection with Reciprocal Points Learning," in IEEE Access, vol. 12, pp. 56461-56476, 2024, doi: 10.1109/ACCESS.2024.3388149.