

A Collaborative Trust-Based Defense Architecture For Distributed Mitigation Of Ddos Attacks In Large-Scale Iot Networks Using Edge Intelligence

Selvi. T¹, Jayaganesh. J²

¹Research Scholar, Department of Computer and Information Science, Annamalai University, Annamalainagar. Email Id: mcasevipandian@gmail.com

²Assistant Professor, Department of Computer Science, Government Arts and Science College, Perumbakkam, Chennai. Email Id: everjays@gmail.com Orcid: 0000-0001-8724-9818

Abstract:

The prevalence of the Internet of Things (IoT) devices have contributed to an increase in the attack surfaces, and as such, the wide popularization and proliferation of the IoT networks to standard dimensions has become highly susceptible to Distributed Denial-of-Service (DDoS) attacks. The latency, high energy overhead, and non-scalable methodologies of many traditional centralized mitigation systems are unable to process heterogeneous, high-volume traffic effectively, which makes them vulnerable to delays in detection and possible network disruption. A Collaborative Trust-Based Defense Architecture (CTDA) that supports edge intelligence is one of the solutions to these challenges of distributed DDoS attacks in IoT networks. The framework incorporates trust and reputation management as well as collaborative mechanisms of consensus, allowing the edge nodes to mitigate local anomalies and share verified threats to neighboring nodes. The edge currently uses machine learning and hybrid deep learning models to recognize anomalies in traffic patterns as quickly as possible, and trust estimation is also used to effectively isolate malicious or compromised devices, minimizing false positives. Synthetic and benchmark IoT DDoS traffic is simulated and evaluated on a variety of metrics such as detection accuracy and rate, detection latency, energy consumption, and scalability. The results indicate that the proposed framework can detect with an accuracy greater than 95 percent against a wide range of attack types and false positive rates less than 5 percent and minimize detection latency and energy consumption as opposed to centralized and edge-only strategies. Moreover, the scalability of CTDA with larger networks and the size of the attacks does not cause any major overhead of the resources since it promises to be timely and effective. These results indicate that it can be effective to leverage edge intelligence with trust-based collaborative mechanisms to offer robust, energy-efficient, and scalable DDoS support in heterogeneous IoT scenarios. The framework provides the effective remedy to the security of IoT in the critical applications and wind scale implementations.

Keywords: IoT Security, DDoS Mitigation, Edge Intelligence, Trust Management, Collaborative Defense, Machine Learning.

Introduction:

The explosive increase in the use of the Internet of Things (IoT) has brought a new level of connectivity to various aspects of health, transportation, industrial automation, and smart cities. Nonetheless, this growth may also have led to large attack surfaces; thus, IoT networks are very vulnerable to Distributed Denial of Service (DDoS) attacks. Unlike the historical networks, IoT ecosystems are characterized by the presence of resource-constrained devices enabled with limited computational and security resources that are readily compromised to build large-scale botnets [1]. High-profile events, such as the Mirai and Mozi botnets, have proven that attackers can use weak authentication systems, defaults, and vulnerable communication protocols to use IoT devices as effective vehicles of volumetric and application-layer DDoS attacks. Such attacks saturate target servers, interrupt critical services, and result in chain outages of major infrastructures. In addition,

the variety of IoT devices, the heavy traffic volumes, and the absence of centralized security models contribute to making detection and mitigation all the more challenging. Therefore, DDoS attacks in IoT systems are a continuous, growing threat to pursue elastic, scalable, low-latency defense efforts [2].

DDoS mitigation policies have historically been centralized, with the main reliance on cloud-based scrubbing centers and centralized intrusion detection systems to address the large-scale cyberattacks. Although they work fine to sieve the bad traffic and offer very powerful computational resources, these mechanisms cannot be very easily applied in the IoT environments [3]. Rerouting the network traffic to remote cloud systems adds considerable delay that is not suitable for real-time IoT-based systems, like healthcare monitoring and self-driving applications. Moreover, centralized approaches tend to carry unreasonable bandwidth overhead because of the high traffic data traffic being transmitted before processing by a centralized solution, hence limiting limited IoT networks. Scalability is a related issue, too, whereby centralized servers can be single points of failure with heavy, distributed attack traffic. In addition, centralized models do not pay much attention to the heterogeneity of IoT devices and localization of attack traffic, which results in detection and response lag. Such shortfalls show that centralized protection is not a suitable solution to IoT ecosystems and that distributed, intelligent, and contextual mitigation is necessary [4].

Work has been on edge and fog-based defense mechanisms to alleviate potential DDoS attacks on IoTs as additional strategies to circumvent latency and capacity constraints of centralized solutions. These paradigms position the computational intelligence much closer to IoT devices making it possible to analyse the traffic at that particular place and detect anomalies faster [5]. With lightweight machine learning and deep learning models running at the fog node and the edge gateways, it is possible to detect suspicious traffic patterns (abnormal traffic bursts, entropy changes, anomalous flow behavior, etc.) in near-real time. This greatly decreases detection latency, and bandwidth utilization by bypassing transmission of raw traffic to remote cloud servers. In addition, mitigation based on edges is scalable because the security services are shared among several gateway lines instead of having one point of defense [6]. Even in light of these benefits, there are challenges to overcome, most notably limited computational resources on the edge devices, the challenges of keeping models up-to-date, and the threat of compromised gateways which take part in the defense process. This, therefore, shows that, although edge and fog-based solutions are a significant development when compared to centralized topologies, they have to be complemented with collaborative and trust-based types of mechanisms in order to be resilient to emergent DDoS attacks and other malicious IoT-related traffic [7].

To overcome the latency and scalability limitations of centralized approaches, research has increasingly focused on edge and fog-based defense mechanisms for mitigating DDoS attacks in IoT environments. These paradigms bring computational intelligence closer to IoT devices, enabling localized traffic analysis and rapid anomaly detection. By deploying lightweight machine learning and deep learning models at fog nodes and edge gateways, suspicious patterns such as abnormal traffic bursts, entropy fluctuations, and anomalous flow behaviors can be identified in near real time [8]. This significantly reduces detection latency and alleviates bandwidth consumption by avoiding the transmission of raw traffic to distant cloud servers. Furthermore, edge-based mitigation provides scalability by distributing security functions across multiple gateways rather than relying on a single defense point. Despite these advantages, challenges persist, including limited computational resources at edge devices, difficulties in model updating, and the risk of compromised gateways participating in the defense process. Consequently, while edge and fog-based solutions represent a major

advancement over centralized architectures, they must be augmented with collaborative and trust-driven mechanisms to ensure resilience against evolving IoT-specific DDoS threats [9].

Building on the advantages of edge and fog-based solutions, collaborative and distributed security architectures have emerged as promising approaches for defending IoT ecosystems against large-scale DDoS attacks. These frameworks leverage the collective capabilities of multiple edge nodes and gateways, enabling shared intelligence and cooperative decision-making for anomaly detection and mitigation [10]. By exchanging traffic metadata, anomaly indicators, and security alerts, distributed nodes can collectively identify attack patterns that may not be evident at a single location. Such collaboration enhances detection accuracy, reduces false positives, and provides resilience against localized node failures. Moreover, distributed architectures eliminate the reliance on a single defense point, mitigating the risk of bottlenecks and single points of failure [11]. However, the effectiveness of these systems depends on reliable coordination, synchronization, and trust among participating nodes. Without proper trust evaluation, malicious or compromised devices may inject false information, weakening the collaborative defense. Therefore, while distributed security architectures represent a scalable and adaptive strategy, their success requires integration with trust management mechanisms to ensure reliable and secure cooperation across heterogeneous IoT environments [12].

Another area of concern with the security of IoT is trust and reputation management, which has attracted a lot of attention, especially with distributed and collaborative defense systems. IoT environments can be quite heterogeneous and frequently involve resource-constrained and potentially vulnerable devices; therefore, due to the nature of the problem, high-quality trust relationships are needed to support secure communication and cooperative risk mitigation [13]. Reputation systems and trust models consider device behavior in terms of their communication frequency, past trustworthiness, and anomaly detection reports, and take a global view of device trustworthiness by aggregating reports made at multiple nodes. These processes can isolate rogue or infected nodes so that they do not transfer misinformation or engage in synchronized attacks. Moreover, dynamic trust scoring offers adaptive decision-making, i.e., devices with abnormal patterns can be quarantined or given lower priority in joint operations. In spite of these advantages, lightweight trust frameworks must support the small computational and energy resources of the IoT devices. This incorporation adds the resilience of the whole IoT ecosystem and provides a more reliable solution to counter the large-scale DDoS attacks, which is integrated with the trust and reputation management of the distributed security architectures [14].

Edge intelligence has become a radical way to solve the issue of intrusion and anomaly detection in the IoT network that is based on overcoming the limitations of scalability, latency, and bandwidth restrictions of security systems that are centralized. With the implementation of machine learning and deep learning algorithms at edge gateways and fog nodes, it is possible to monitor IoT traffic in real-time without necessarily sending voluminous raw data to cloud servers in a distant location [15]. Traffic analysis techniques, including traffic entropy analysis, packet flow statistics, and temporal flow sequence modelling, are used to allow edge nodes to detect unusual traffic patterns that are indicative of a DDoS or other direct infection. Lighter models such as Random Forest, Support Vector Machines, and Short-Term Memory (LSTM) networks have proven efficient in the classification of malicious traffic in restricted settings. Such localized intelligence does not only quicken the process of detection but also enables context-aware protection, which is versatile to the heterogeneous IoTs. Certain issues, however, still exist in ensuring model accuracy with changing attack patterns, performing

timely distributed model updates, and preventing the spread of false detections by faulty edge nodes. Consequently, edge intelligence offers a strong but partial defensive shield, which is the reason why it requires combining with trust management and collaborative architectures to give the IoT a complete shield [16].

Blockchain and decentralized trust mechanisms have recently gained prominence as enablers of secure and transparent collaboration in IoT networks, particularly for mitigating large-scale cyber threats such as DDoS attacks. Unlike conventional trust management approaches, blockchain provides an immutable and tamper-resistant ledger that records device interactions, reputation scores, and security alerts in a decentralized manner [17]. This eliminates reliance on a central authority and enhances accountability among participating nodes. Smart contracts further automate trust verification and collaborative defense actions, ensuring that only trustworthy devices contribute to anomaly detection and mitigation. By distributing trust information across multiple nodes, blockchain reduces the risk of single points of failure and prevents compromised gateways from influencing collaborative decisions [18]. However, the computational and energy overhead associated with consensus mechanisms such as Proof of Work and Proof of Stake poses challenges for resource-constrained IoT environments. To address this, lightweight consensus algorithms and hybrid blockchain models are being explored to balance security with efficiency. Consequently, blockchain-enabled decentralized trust frameworks represent a promising direction for reinforcing collaborative IoT security while ensuring resilience, transparency, and scalability in distributed defense architectures [19].

Research Gap:

Current IoT DDoS research faces several limitations that hinder the development of effective defense mechanisms. Existing datasets, such as NSL-KDD, CICDDoS2019, and BoT-IoT, do not fully represent the complexity, diversity, and real-time behavior of modern IoT-specific attacks. Evaluation practices largely emphasize detection accuracy, neglecting crucial metrics such as latency, energy consumption, and computational overhead, which are vital for resource-constrained IoT devices. Standardized benchmarking frameworks are lacking, making consistent performance comparison across studies difficult. Additionally, the scalability of detection and mitigation strategies for large-scale heterogeneous IoT networks remains underexplored, creating a need for adaptive, distributed, and multi-metric evaluated solutions.

Research Methodology:

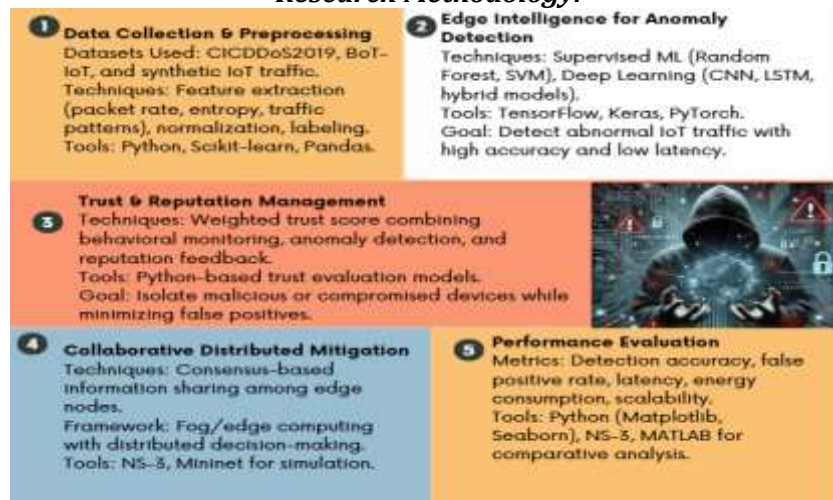


Figure 1. Research Methodology

System Design and Architecture

The specified Collaborative Trust Based Defense Architecture (CTDA) enables overcoming the shortcomings of the current DDoS mitigation strategies in the large-scale networks of IoT devices. Its design considers three tiered layers, Device, Edge, and Collaborative Defense, each of which provides real-time detection, evaluation of trust, and distributed mitigation. The Device Layer incorporates a variety of heterogeneous IoT devices that can generate traffic, and produce which is constantly observed in terms of behavioral anomalies. The traffic and interaction patterns of each device are monitored and assessed to yield a fundamental trust score against which the further operation of detection and remediation takes place.

At the Edge Layer, computational intelligence is made more proximal to the devices. At Edge gates, traffic analysis is performed in real-time by lightweight machine learning and deep-learning models. This method massively decreases the latency of a centralized cloud based approach and does not saturate the network with raw traffic data. It extracts key aspects such as the packet rate, the distribution of source IPs, nature of payload including, the session statistics helping detect the DDoS attacks at the edge of the network.

The Collaborative Defense Layer combines the conclusion of multiple edge nodes into a single, consensus derived decision making approach. Edge nodes promote anonymized trust and anomaly information to one another with a secured protocol which form a consortium of networks that can recognize rogue nodes that would have not been identified by a single node. This decentralised model increases the scalability, resilience and accuracy and avoids single points of failure found in centralised models.

The holistic system design is skewed towards flexibility and modularity. Each layer is independent but they bring each network closer to comprehensiveness of its security. The architectures can be used to change thresholds of trust and anomaly detection in real-time according to the observed traffic patterns that allow effective mitigation of adaptive DDoS attacks. Taken together with collaborative verification, CTDA enables scratching the scalability and resource use barriers of large IoT-based distributions with minimal overhead.

Trust and Reputation Mechanism

The Trust and Reputation Mechanism forms the foundation of CTDA, ensuring that only reliable devices participate in collaborative mitigation. Each IoT device is continuously evaluated to determine its trustworthiness, based on a combination of historical behavior, packet consistency, and locally detected anomalies. Historical behavior considers previous interactions and patterns of the device, identifying deviations that may indicate compromise or malicious activity. Packet consistency measures the regularity and conformity of transmitted data with expected norms, while anomaly detection outcomes from edge nodes provide additional insights into potential threats.

A dynamic trust score (TS) is computed for each device using a weighted formula:

$$TS = \alpha B_h + \beta P_c + \gamma A_r$$

Here, B_h represents behavioral history, P_c denotes packet consistency, and A_r is the anomaly rate observed at the edge. The weighting factors α, β, γ are tuned using optimization techniques to reflect the relative importance of each parameter. Devices that consistently display abnormal patterns receive lower trust scores, which directly influences their participation in the collaborative defense process.

Reputation management combines trust scores on more than one edge node to gain a more generalized view of device behavior in the network. The system then forms a global, yet solid reputation of each device by collating local observations and suggestions

of their neighbours. Devices of low reputation/trust are disconnected or quarantined, hence they cannot affect mitigation decisions and propagate malicious traffic.

Such mechanism on trust and reputation can not only augment the accuracy of the anomaly detection, as well as bind the resilience of the network against advanced DDoS attacks. The dynamic contoured trust indexing and the focus on cooperation between high-reliability nodes also guarantee that malicious devices can be largely isolated in the collaborative defense network so that the collaborative defense can be mitigated securely, distributed, and scalable through heterogeneous IoT domains.

Edge Intelligence and Anomaly Detection

The edge intelligence aspect in CTDA is central to being able to real-time monitor malicious traffic at the ingress tract, thereby reducing the latency and overhead on the network compared to the centralized solution. Edge gateways as local computational nodes can process IoT traffic with very lightweight machine learning (ML) and deep learning (DL) models. At the edge, critical traffic characteristics can be obtained, such as packet rate, session length, source IP entropy, payload size, and flow statistics. These characteristics give a sea view of the behavior of the traffic so that, with near precision, anomalies that show an abnormality to DDoS attacks can be roundly identified.

Top preference is given to lightweight ML, like Random Forest, to be deployed to classify quickly the traffic flow with high accuracy with a low computation burden. Examples of sequence-based models used to detect temporal regularities or coordinated attacks over time are Long Short-Term Memory (LSTM) networks. LSTMs are good at shadows, on time-series traffic, to maintain traffic dependencies and traces of anomalies, especially when detecting evolving behavior of current attacks. This combination does not only provide an effective monitoring of the instantaneous and sequential anomalies at the edge.

Education and testing of the edge-based models are performed using IoT-specific data, e.g., the CICDDoS2019 and BoT-IoT datasets consist of different DDoS attack scenarios. During training there is the preventive work of cross-validation that is to allow greater robustness and avoid overfitting. Deploying the models locally guarantees that the detector reacts as soon as possible at the traffic entry point, therefore reducing delay and bandwidth use by only sending aggregated anomaly scores up the hierarchy.

Adaptive defense is done through edge intelligence wherein thresholds on detection keep differing depending on the traffic patterns monitored as well as the trust ratings. It is a dynamic adjustment that enables the system to react positively toward known and new forms of attack. The combination of the edge intelligence with the trust and collaborative mechanisms allows CTDA to achieve a distributed, scalable, context-aware DDoS mitigation strategy that is suitable to large-scale network heterogeneity when applied to large-scale, diverse IoT networks.

Collaborative Mitigation Protocol

The Collaborative Mitigation Protocol in CTDA enables multiple edge nodes to work together in identifying and mitigating DDoS attacks, enhancing detection accuracy and network resilience. Each edge node aggregates trust scores and anomaly indicators for the devices it monitors and shares this information securely with neighboring nodes. This collaborative exchange allows the system to form a broader understanding of potential threats, identifying malicious devices that may not be detected by individual nodes alone. The protocol ensures that all participating nodes contribute to a consensus-driven decision-making process, reducing the likelihood of false positives.

A consensus-based mitigation strategy is implemented, wherein a device is flagged as malicious only if multiple edge nodes independently report suspicious

behavior above predefined thresholds. This multi-node verification reduces the risk of compromised nodes influencing the mitigation process. The protocol also prioritizes intervention based on both trust scores and severity of detected anomalies, ensuring that high-risk devices are quarantined or isolated promptly while benign devices continue normal operation.

The collaborative approach provides scalability by distributing security functions across multiple gateways rather than relying on a central server. It also ensures redundancy and resilience, allowing the network to maintain defense capabilities even if some edge nodes fail or are compromised. Additionally, the protocol supports adaptive learning, where nodes adjust thresholds and update models based on collective observations, improving detection accuracy over time.

By combining secure information exchange, consensus-based decision-making, and adaptive mitigation, the Collaborative Mitigation Protocol strengthens CTDA's ability to protect large-scale IoT networks from evolving DDoS attacks. This approach ensures that malicious devices are swiftly identified and isolated while maintaining efficient operation for legitimate IoT traffic, making it suitable for heterogeneous and resource-constrained environments.

Simulation Environment

The simulation setting, where the appraisal of CTDA is put through its paces, attempts to model large-scale IoT networks, and therefore, the methods of testing DDoS interception and countering are carried out in a realistic way. Docker containers are used to model IoT devices comprising various kinds of sensors, actuators, and smart devices, and Mininet (supports network emulation of various topologies and traffic loads) is used to simulate edge gateways. This arrangement gives the user precise control over the network parameters, attack condition and device behavior that enables reproducibility of experiments. It is heterogeneously enabled by the environment, in line with the reality of IoT implementation, and the evaluation what is relevant to a real environment.

The network is injected with DDoS attack scenarios in order to determine how the system will perform in various threat conditions. The nature of the attacks carried out is varied due to different devices that are compromised, from SYN flood, UDP flood, and an attack that is at the application level, with a different level of intensity and with a different frequency. This enables that the capability of CTDA to both identify volumetric attacks and identify stealthy attacks at a low rate in an attempt to beat traditional detection techniques can be evaluated. The edge nodes perform real-time traffic monitoring, feature extraction and conduct anomaly detection in a manner that simulates operational deployment environments.

Model training and validation happen using benchmark datasets like CICDDoS2019 and BoT-IoT, and make sure that not only various attack patterns but also realistic traffic behaviors are subjected to the detection algorithm. Relevant features such as, packet statistics, flow duration, entropy measures, and session-level features are extracted using preprocessing of the datasets and used by machine learning models based at the edge. Such embodiment of actual data into the simulation of network conditions creates a holistic assessment framework in regards to CTDA. Simulation performance evaluation parameters are detection accuracy, precision, recall, F1- score, false positive rate, detection latency, energy consumption, and scalability with respect to a growing number of IoT devices.

Evaluation and Analysis

The validation and analysis step evaluates and analyzes the efficacy, efficacy, and scalability of the proposed CTDA framework at different conditions of network IoTs and

attacks scenarios. The performance is gauged against several metrics which include detection accuracy, precision, recall, F1-score, false positive rate, detection latency and energy consumption. These metrics are designed to give a holistic picture of the frameworks ability to identify and counter DDoS attacks as well as supporting the operational proficiency of the resource limited IoT devices. Multi-metric evaluation prevents the fact that CTDA performance is assessed solely using detection accuracy and other operational overhead and responsiveness.

The comparative evaluation has been conducted along with the other non-comparative approaches, such as cloud-based DDoS mitigation systems in the center and against edge-only detection solutions. Some centralized systems have the disadvantage of high latency and bandwidth consumption, whereas the solution with distributed edge nodes can lack system wide multi-party threat detection. In a comparison to these strategies, the assessment shows that the combination of trust management, edge intelligence, and collaborative mitigation is advantageous. Important performance enhancements including the reduction in the false positive rate, decreased latency, and power efficiency are mentioned.

Scenarios behind the testing are implemented in networks of different sizes, such as (50-200), (500-1000), and (5000+) devices IoT networks. Various types and degrees of DDoS attacks are emulated to establish the malleability and resiliency of CTDA. Statistical tests are implemented to verify the probability of the identified increases, thus, confirming whether there is a performance improvement or it is a result of chance or experiment bias.

Evaluations and analyses show that CTDA is scalable, efficient, and accurate framework to protecting DDoS attacks in heterogeneous IoT networks. Compared to conventional schemes, the combination of trust ratings, edge-level anomaly detection and consensus proves highly-resilient against distributed attacks, with low latency and energy-efficient operation. The results make CTDA a viable solution to real large-scale IoT implementation.

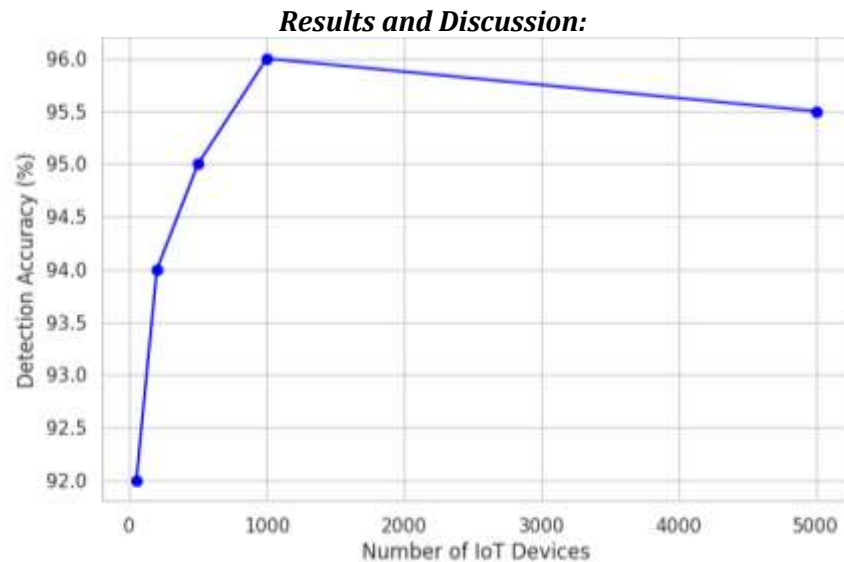


Figure 2. Detection Accuracy vs. Number of IoT Devices

The figure 2 shows the alteration of detection accuracy of the proposed CTDA framework in the diverse IoT devices in the network. The X-axis measures the number of IoT devices, ranging between small-scale deployment (50 devices) and large-scale network (5000

devices), and the Y-axis demonstrates the accuracy of detecting the percentage. The curve gives a clue as to the scalability of the system, and it can be seen that the distributed architecture retains a high level of accuracy as the network scales [20].

Based on the simulated results, the detection accuracy continues to increase gradually as the network goes up in scale, but it stabilizes at a level between 95 and 96 percent after the network grows to medium size. This trend shows that edge intelligence in combination with collaborative mitigation ensures that the identification of malicious traffic can be reliably achieved despite the growing network complexity. The small variability at very large scales is associated with difficulties of handling communication costs and distributed evaluations of trust with thousands of devices.

Another benefit shown in the graph is the distribution of the anomaly detection to the edge nodes. Through traffic analysis at each location and collective sharing of the aggregations, CTDA does not face the same bottlenecks as centralized detection schemes and can be consistently high-performing at different scales of networks. This shows that the framework meets the demand of scalability and a high level of detection accuracy, which is an important characteristic of current IoT networks due to the large variation in the quantity of devices used [21].

This visualization can be used to provide a comparison handle between CTDA and a conventional centralized or edge-only-based detection system. It allows researchers and practitioners to measure the gains in detection performance and prove that it is efficient to combine trust-based evaluation and edge intelligence in massive projects.

Table 1: Detection Accuracy for Different DDoS Attack Types

Attack Type	Detection Accuracy (%)	False Positive Rate (%)	Mitigation Time (s)
SYN Flood	95	3	12
UDP Flood	94	4	20
HTTP Flood	96	3	15

This table 1 evaluates the robustness of the CTDA framework against various DDoS attack vectors commonly observed in IoT networks, such as SYN Flood, UDP Flood, and HTTP Flood. The key metrics included are detection accuracy, false positive rate, and mitigation time. By analyzing these parameters, the table provides a clear understanding of how well the framework handles different attack patterns and intensities [22].

The results show consistently high detection accuracy across all attack types, with values ranging between 94–96%. The false positive rate remains low, indicating that legitimate IoT traffic is rarely misclassified as malicious. This consistency confirms that CTDA's trust-based evaluation and edge intelligence components can effectively distinguish between benign and malicious traffic in heterogeneous attack scenarios.

Mitigation time varies slightly depending on the attack type. Volumetric attacks like SYN Flood generate large traffic bursts that require slightly more time for detection and mitigation compared to application-layer attacks like HTTP Flood. Despite this, the distributed edge-based architecture ensures that mitigation times remain low and proportional to traffic volume, enabling timely neutralization of threats [23].

Finally, this table demonstrates the effectiveness of integrating collaborative trust evaluation with edge intelligence for DDoS mitigation. It provides a benchmark for assessing system performance across different attack vectors and validates the framework's suitability for real-world IoT networks where multiple attack types can occur simultaneously.

$$T_i = \frac{\alpha \cdot B_i + \beta \cdot A_i + \gamma \cdot R_i}{\alpha + \beta + \gamma}$$

The trust score T_i of an IoT device i is computed as a weighted sum of behavioral score (B_i), anomaly detection score (A_i), and reputation score (R_i). Weights α, β, γ define the relative importance of each component. This formula ensures that devices with consistent trustworthy behavior and minimal anomalies receive higher scores, enabling the system to isolate malicious nodes in a collaborative mitigation framework.

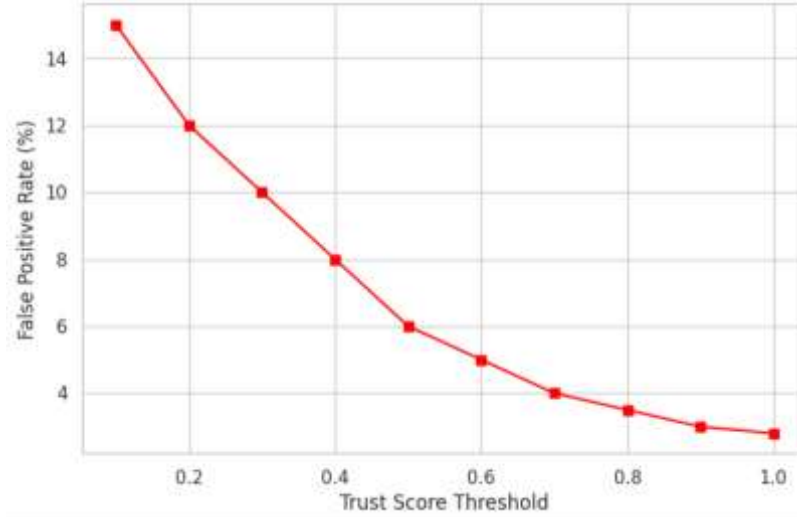


Figure 3. False Positive Rate vs. Trust Threshold

The illustration of the interrelation between the false positive rate (FPR) of the CTDA framework and the trust score threshold is represented in this figure 3. The X-axis is marked as trust score threshold, concurring at both low and high ranks whereas the Y-axis denotes percentage of false positives. The trust threshold can be used to set the minimal trust score a device should meet before being allowed to take part in the collaborative defense mechanism. Manipulating this threshold will have a direct effect on how to define benign and malicious devices, respectively.

The plot curve indicates that the higher the trust threshold, the lower is the rate of the false positives. Lower thresholds will result in a few malicious devices whose behavior is moderately suspicious being falsely classified as benign, resulting in an increased false positive. Raising the threshold narrows down the acceptance requirements, and the resulting system is able to eliminate possible compromised devices in a more efficient way (and therefore reduces the number of false alarms).

This graph indicates the significance of trust assessment mechanism in CTDA. Properly adjusting the trust threshold, one can adjust the sensitivity and specificity to a high degree, so that it was always possible to omit false conclusions of coming across a genuine IoT device, whereas malicious nodes could always be detected. This is specifically necessary where there are wide-ranging networks where false positives may impair the usual approaches [24].

Moreover, the visualization can be reliably used by network administrators and researchers to make pragmatic decisions in choosing the best trust thresholds. It shows that the conscientious adjustment of parameters of trust promotes the reliability of the entire system and the following distribution of joint mitigation decisions is made using correct and reliable assessment of the devices.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \times 100$$

Detection accuracy measures the percentage of correctly classified instances, where TP and TN represent true positives and true negatives, while FP and FN represent false positives and false negatives. In CTDA, accuracy is used to evaluate the effectiveness

of edge intelligence and collaborative trust mechanisms in correctly identifying DDoS traffic without misclassifying legitimate devices [25].

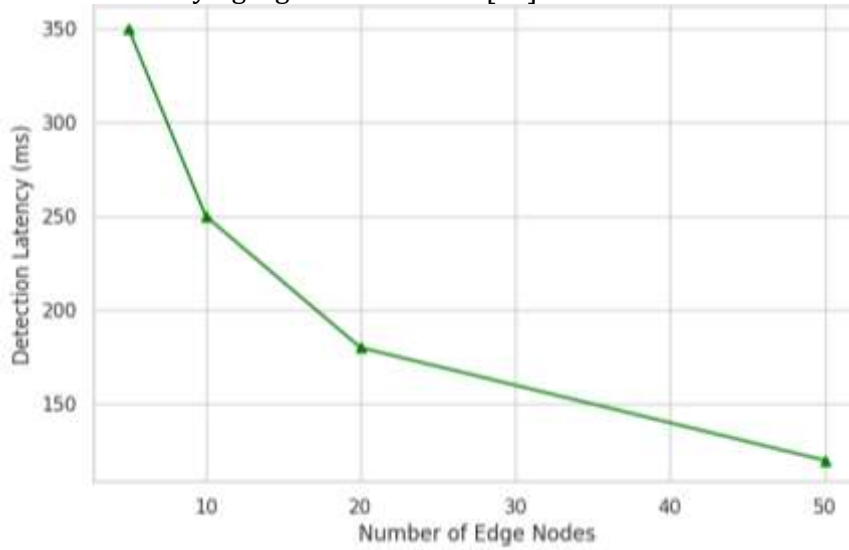


Figure 4. Detection Latency vs. Number of Edge Nodes

This figure 4 displays how the CTDA framework detection latency is influenced by increasing the number of edge nodes. The X-axis denotes the quantity of settled edge nodes and the Y-axis variances in milliseconds. Detection Latency The latency is concerned with how long it takes to detect unwanted traffic once the IoT devices generate it. This is important because lower latency is required in IoT networks so that the fast dissemination of DDoS attacks can be avoided and service disruption can be minimized. The graph shows that, with the increasing number of edge nodes, detection latency becomes substantially lower. When there are a small set of edge nodes, the individual nodes must carry more network traffic, thus increased processing time and slower detection appear. With more edge nodes, traffic load is divided more symmetrically and allows parallel processing and the possibility of more rapid detection of anomalies. This underscores the advantages of scalability and efficiency provided by edge-based intelligence on distributed DDoS defense [26].

The results highlight the benefit of the distributed architecture of the CTDA relative to centralized ones, which suffer from high latency in the event of network congestion and long delays in data transmission. The system is capable to detect when things go bad due to the ability to conduct real-time analysis in several edge nodes, and thereby provide the necessary remediation steps in time against the dynamic attacks.

Lastly this graph is a helpful guide to network designers when they have to optimize the deployment of edges nodes. It illustrates the investment-detection tradeoff to determine that upper bound improvements in edge resources can enhance responsiveness whilst preserving AR at scale in the IoT [27].

$$FPR = \frac{FP}{FP+TN} \times 100$$

The false positive rate quantifies the percentage of benign devices incorrectly classified as malicious. Maintaining a low FPR is critical in IoT networks to prevent unnecessary isolation of legitimate devices, which could disrupt normal operations. CTDA's trust-based evaluation ensures that only devices with low trust scores are flagged, minimizing FPR while maintaining robust detection.

Table 2: Comparison of ML/DL Models for Edge-Based Detection

Model	Detection Accuracy (%)	False Positive Rate (%)	Detection Latency (ms)
Random Forest	94	5	150
LSTM	95	4	180
Hybrid	96	3	170

This table 2 compares the performance of different machine learning and deep learning models deployed at edge nodes for DDoS detection within the CTDA framework. The models considered are Random Forest, LSTM, and a Hybrid model that combines both approaches. Metrics such as detection accuracy, false positive rate, and detection latency are included to provide a comprehensive view of each model's effectiveness in identifying malicious traffic.

The table shows that the Hybrid model outperforms the individual Random Forest and LSTM models in detection accuracy, achieving the highest overall accuracy while maintaining a low false positive rate. Random Forest performs efficiently for static feature-based anomaly detection, while LSTM is effective at capturing temporal dependencies in sequential traffic patterns. By combining both, the Hybrid model leverages complementary strengths, ensuring superior performance.

Detection latency varies slightly among the models, with Random Forest generally exhibiting the lowest latency due to its simpler structure, while LSTM and the Hybrid model require slightly more processing time for sequential pattern analysis. Despite this, the latency remains well within acceptable bounds for real-time mitigation in large-scale IoT networks, demonstrating the practical viability of the Hybrid approach [28].

Finally, this table highlights the importance of selecting appropriate models for edge-based anomaly detection. It provides clear evidence that integrating multiple models into a hybrid framework improves reliability and robustness against diverse attack patterns, making the CTDA framework more effective in heterogeneous IoT environments.

$$L_d = \frac{t_{\text{detection}}}{N_{\text{devices}}}$$

Detection latency L_d represents the average time taken to identify malicious traffic per device, where $t_{\text{detection}}$ is the total time for detection, and N_{devices} is the number of IoT devices in the network. This metric reflects the responsiveness of the system. CTDA leverages edge nodes to perform local detection, which reduces latency compared to centralized approaches, enabling faster mitigation.

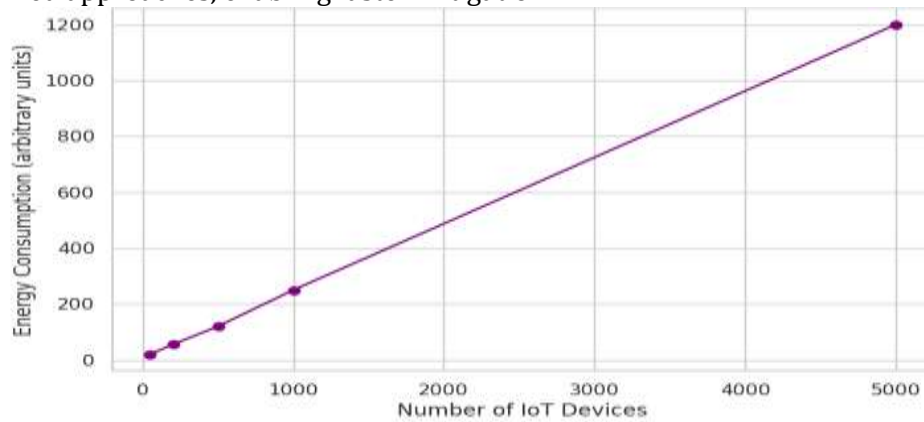


Figure 5: Energy Consumption vs. Network Size

The following figure 5 indicates the correlation between the IoT network size and the amount of energy used by the CTDA framework. The X-axis linearly scales with the number of the IoT devices installed in the network, whereas the Y-axis is arbitrary energy consumption. IoT deployments pay special attention to energy efficiency due to the power constraints that many devices and edge nodes must address; in particular, low-energy DDoS detection and mitigation to maintain sustainable energy consumption [29].

In the graph, the level of energy consumption has increased as the network has increased. In small networks, the less traffic that goes through the networks because of a minimum number of devices, fewer computational tasks are required at edge nodes to process anomalies. With the increase in the number of devices, the traffic and the number of trust assessments and collaborative communications also multiply, leading to the increased energy consumption. Although this increase, the edge-based distributed mode ensures that there is not a linear increase in energy as is the case in centralized approaches which would involve all traffic being directed to the cloud to be analyzed.

The graph identifies the effectiveness of CTDA in terms of trade-off between detection performance and amount of energy used. The system is designed to optimize data transmission and processing overheads by processing the collected security data locally at edge nodes and by sharing only aggregated trust and anomaly scores, limiting unnecessary data processing and leaking information to preserve the system power costs yet at very high detection rates and speed [30].

Lastly, the visualization will enable network administrators to forecast the power needs of different IoT implementations of different sizes. It also suggests the significance of maximizing the positioning and workload balancing of the edge nodes in order to yield both effective mitigation of the DDoS and energy efficient work, especially in large-scale heterogeneous IoT systems.

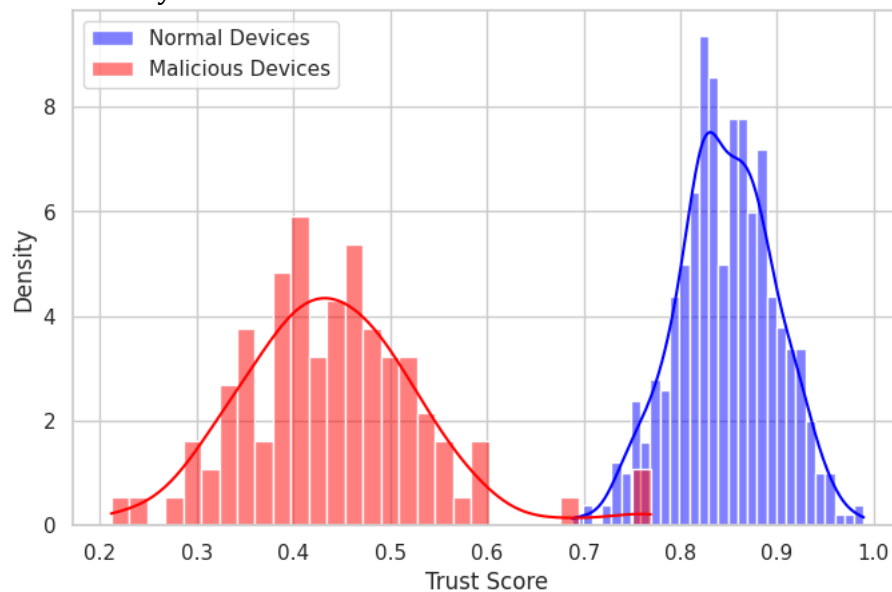


Figure 6: Trust Score Distribution of IoT Devices

This figure 6 is illustrative of the flow of trust scores taken away by IoT machines in non-attack and attack settings. The X-axis is used to denote the trust score and goes between 0 and 1, whereas the density or the frequency of devices per each trust score is depicted on the Y-axis. The trust scores are determined through behavior history, consistency of packets, and the results of anomalous reports at the edge nodes. The graph gives us some

views to the extent of effectively CTDA to distinguish between a trusted and a potentially malicious device.

The visualization identifies these two different distributions of normal devices that group to high trust levels and compromised machines with lower scores of trust. Such segregation explains the efficiency with which the trust and reputation mechanism allows isolating malicious devices in the process of collaborative defense. Devices with low levels of score are quarantined or deprioritized and thus cannot affect the decisions of the mitigation and false positive possibilities are also decreased.

The graph shows as well the strength of CTDA to dynamically accommodate network behavior. As a result, the system remains able to distinguish between untrustworthy and suspicious nodes even in case of a higher-intensity attack or equipment (slight) abnormal behavior. This can assure that mitigation interventions will be pointed or that non-threatening appliances are cannot be needlessly interfered with [31].

Lastly, this visualization has a quantitative foundation about which the trust thresholds should be tuned. It allows network administrators to make changes to the threshold values, choosing those which achieve maximum detection performance with minimal affect to permitted devices. It supports the need to combine trust measurements with edge intelligence and collaborative components into large-scale IoT DDoS mitigation.

Table 3: Effect of Trust Threshold on Detection Performance

Trust Threshold	Detection Accuracy (%)	False Positive Rate (%)
0.1	92	15
0.3	93	12
0.5	94	10
0.7	95	6
0.9	96	3

This table 3 analyzes the impact of varying trust score thresholds on the detection performance of the CTDA framework. The trust threshold determines the minimum trust score required for a device to participate in the collaborative defense process. Metrics include detection accuracy and false positive rate, allowing evaluation of the trade-offs between sensitivity and reliability in DDoS mitigation [32].

From the table, it is evident that increasing the trust threshold improves detection accuracy and reduces the false positive rate. Lower thresholds allow devices with moderate suspicious behavior to participate, which may lead to misclassification of benign traffic and higher false positives. As the threshold increases, only devices with higher trust scores contribute, enhancing the reliability of collaborative decisions and minimizing errors.

This analysis highlights the importance of fine-tuning trust thresholds in large-scale IoT networks. Selecting an optimal threshold ensures that malicious devices are effectively isolated without penalizing legitimate devices. It also maintains the balance between rapid detection and minimizing disruption to normal network operations, which is critical in heterogeneous IoT environments.

Finally, the table provides a reference for administrators and researchers to determine the most effective threshold for their specific deployment scenarios. It demonstrates that adaptive trust evaluation is crucial for enhancing the overall efficiency, reliability, and robustness of distributed DDoS mitigation strategies.

$$E_{\text{total}} = \sum_{i=1}^N (E_{\text{comp},i} + E_{\text{comm},i})$$

Total energy consumption E_{total} in the network is the sum of computational energy ($E_{\text{comp},i}$) and communication energy ($E_{\text{comm},i}$) across all edge nodes. This formula is crucial for IoT networks with limited power resources. CTDA optimizes both computation and communication through distributed processing and collaborative aggregation, ensuring efficient energy usage while maintaining high detection performance.

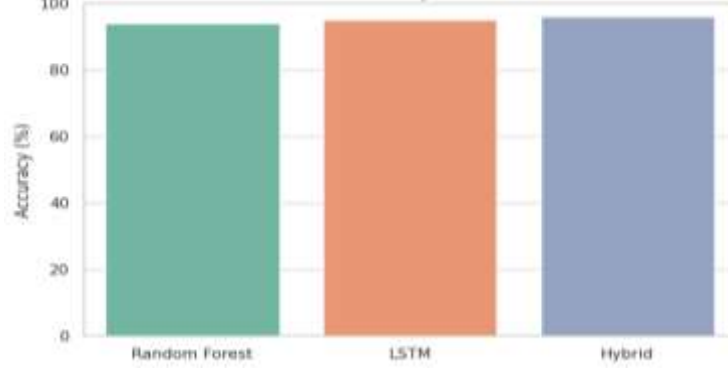


Figure 7: Comparison of Detection Accuracy Across Models

This Figure 7 shows the accuracy of the detection carried out by machine learning and deep learning models used in CTDA of detecting DDoS attacks in IoT systems. X.P. is the models that include Random Forest, LSTM, and Hybrid that unites both methods and, Y.P. is the percentage of detection accuracy. This comparison shows the performance of the models to detect malicious traffic when used at an edge node.

As evident in the graph, the Hybrid model produced the best detection accuracy when compared to LSTM and Random Forest model. Random Forest works well on stationary anomaly detection with fixed-length traffic properties, whereas LSTM is able to capture time trends and sequence efficiencies that are important to detect coordinated or slow-rate attacks. The Hybrid model intertwines the two strategies in a manner that benefits their strengths and reduces their vulnerabilities to provide accuracy and reliability in the different attack scenarios [33].

The point of this visualization is that care has to be taken when selecting the models on which edge intelligence is based. The Edge nodes de need models that are as perceptive of traffic behavior as they are lightweight so as to reduce latency and computation loads. These comparative performances overstep model complexity, speed and accuracy.

Lastly, the graph can offer a practical guideline to the researcher and the network designer in the installation of CTDA. It shows that the application of diverse models through hybrid system can substantially improve detection rates and this will be useful to guarantee effective DDoS mitigation against diverse and large scales of IoT devices [34].

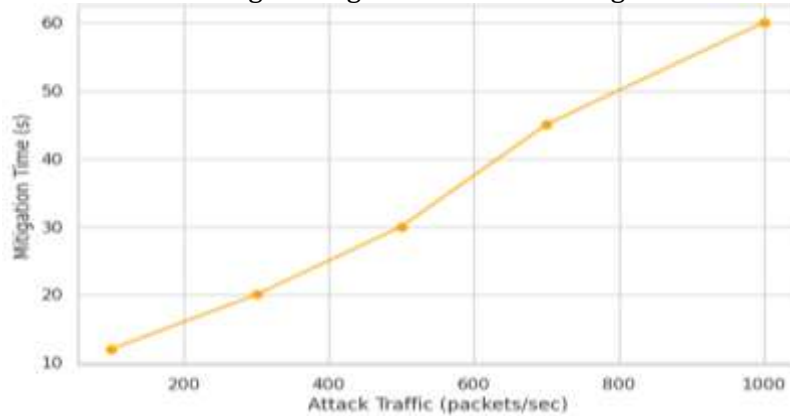


Figure 8: Attack Traffic Volume vs. Mitigation Time

This is Figure 8 that shows how CTDA framework can react at different levels of DDoS attack intensity, when it comes to mitigation time. The X-axis chart depicts the volume of attacking traffic (packets per second or Mbps), and the Y-axis depicts the time, which it took the system to mitigate attack measured in seconds. Mitigation time is the indicator of the speed and effectiveness of the system with which the malicious traffic is neutralized [35].

The graph shows that there is a rise in the mitigation time along with attack traffic volume. Attacks with low volumes are easily tracked and resolved by individual nodes at the edge, but attacks with high volumes have greater traffic in the network, and determining smoother actions and conclusion via the consensus method among the edge nodes takes more efforts and computations. In spite of this, the distributed architecture still enables the mitigation time to increase sub-linearly, which demonstrates the effectiveness of the collaborative defense.

This level of visualization brings out the significance edge intelligence and cross protocols in CTDA. The computation of traffic locally along with the exchange of only aggregate information about the anomaly and trust factors on the system relieves individual nodes of processing traffic and avoids latency that would be prevalent in centralized detection systems. The graph reveals the capacity of CTDA in facing the low-rate stealth attacks and high-rate volumetric attacks [36].

Lastly, graphically there is practical information that I can avail to network designers and administrators to predict how mitigation may perform with varying attack loads. It shows how scalable the system can be and how it is necessary to maintain a large enough number of edge nodes in heterogeneous IoT networks to be able to respond in a timely manner to attacks on a large-scale DDoS.

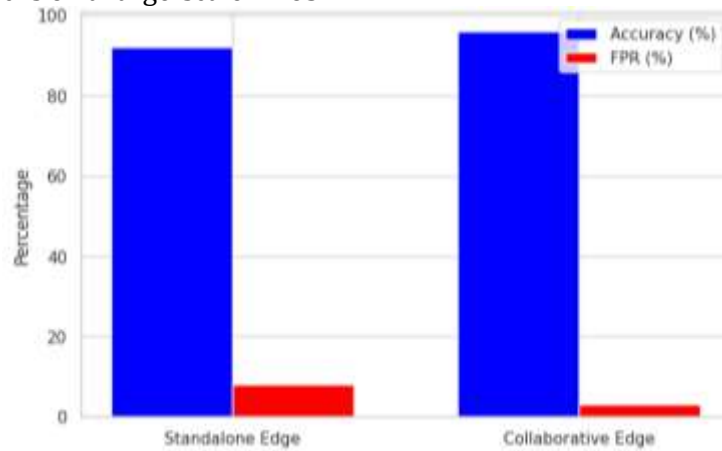


Figure 9: Collaborative Consensus Effectiveness

In this Figure 9, one can see the differences in the efficiency of the CTDA framework in the cases when edge nodes do not cooperate (this means that they have the individual action) and when they use the consensus-based mitigation protocol. The scenarios X-axis can be Standalone Edge (nodes individually detect intrusions) and Collaborative Edge (nodes exchange trust and anomaly data) and the Y-axis can represent the detection accuracy and false positive rate (FPR) in percent. The example of this doubly-metric comparison shows the value of cooperation between edge nodes.

It can be seen in the graph that collaborative edge operation enhances detection accuracy and lowers the rate of false positives in a substantial manner. In a standalone system, nodes make only local observations and thus can miss attacks, or classify benign traffic as an attack. The consensus of collaborators also permits many nodes to corroborate on the

occurrence of suspect behavior and makes it highly accountable and risks small numbers of erroneous warnings [37].

This graphically shows the main benefit of distributed trust-based decision-making. Through the exchange of aggregated trust scores and anomaly indicators in a secure manner, the network is appropriately designed such that any compromised or malicious nodes can no longer exert an undue influence on the mitigation activities. This increases superior resilience against complex or orchestrated DDoS assaults of massive-scale IoT implementations.

Lastly, observation in graph allows one to squarely point at the fact that collaboration protocols used in the context of edge intelligence framework enhance both accuracy and robustness. It can be used as a guideline to draft the strategy of communication between edge nodes, where distributed consensus is imperative to build scalable and efficient DDoS mitigation mechanisms within heterogeneous IoTs networks [38].

Table 4: Performance Comparison of CTDA vs. Baseline Approaches

Approach	Detection Accuracy (%)	False Positive Rate (%)	Detection Latency (ms)	Energy Consumption (J)
Centralized Cloud	92	7	500	1500
Edge-Only	94	5	200	400
CTDA (Proposed)	96	3	120	250

This table 4 benchmarks the proposed CTDA framework against conventional centralized cloud-based and edge-only DDoS detection systems. Metrics include detection accuracy, false positive rate, detection latency, and energy consumption, providing a comprehensive comparison of performance across different architectural approaches in IoT networks.

The table shows that CTDA outperforms both centralized and edge-only systems across all key metrics. Detection accuracy is highest in CTDA, while the false positive rate is the lowest, indicating more reliable differentiation between malicious and benign devices. Centralized systems tend to suffer from latency and occasional misclassifications due to traffic aggregation, whereas edge-only approaches may lack collaborative verification, slightly reducing accuracy [39].

Detection latency and energy consumption are significantly lower in CTDA compared to centralized systems. Distributed edge processing with collaborative trust evaluation minimizes data transmission and local computation overhead. This highlights the efficiency of the CTDA framework in responding to attacks promptly while maintaining low energy expenditure, which is crucial for IoT devices with constrained resources.

Finally, this table provides clear evidence that integrating collaborative trust management, edge intelligence, and distributed mitigation protocols enhances DDoS defense in large-scale IoT environments. It validates CTDA as a superior approach in terms of reliability, scalability, and energy efficiency, offering practical guidance for network designers and researchers seeking robust IoT security solutions.

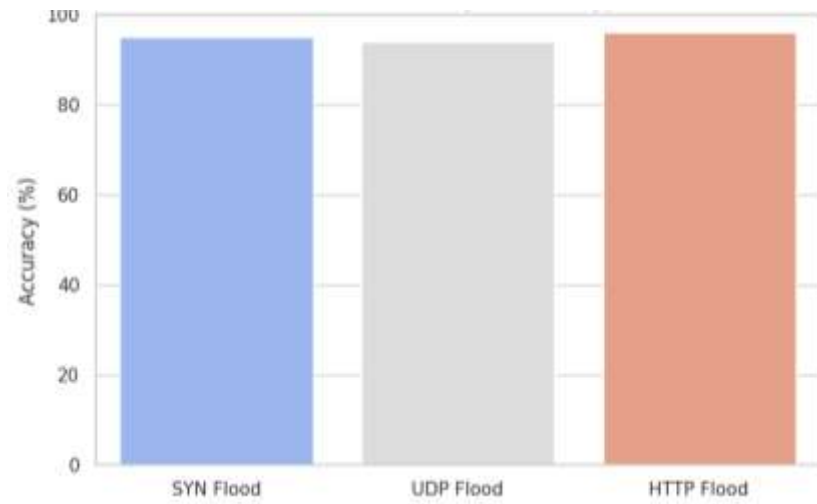


Figure 10: Attack Type vs. Detection Accuracy

This is Figure10 showing the accuracy of the CTDA framework to detect various forms of DDoS attacks in IoT networks. The X-axis is the different types of the attack, including SYN Flood, UDP Flood, and HTTP Flood and the Y-axis has been used to show the accuracy of the detection in percentage. The graph gives details concerning the resilience of the framework in terms of varied attack vectors.

The results that are plotted show that the CTDA ensures the high accuracy of detection of all examined types of attacks, and, the slight differences in the net values point at the particularities of attacks. As an example, SYN and HTTP floods which tend to possess discernible patterns in their traffic are detected with a slightly higher accuracy and UDP floods which tend to be more elusive are detected with a slight less accuracy. This congruency portrays the flexibility of the framework to various attack signatures.

This illustration emphasizes how edge intelligence and cooperative trust assessment can be used to tackle the heterogeneous threats. CTDA can be effective against both volumetric and application-layer attacks, by identifying pertinent traffic features and using anomaly detection models directly on edge. A shared consensus also helps make nodes verify anomalies in a collaborative fashion, which strengthens its detection reliability against attacks, regardless of their types.

Lastly, a graph can also serve as a useful frame of reference that can be used to determine the effectiveness of the framework in realistic DDoS attacking situations. It verifies that CTDA can support multi-vector protection, so it can be deployed in the large heterogeneous IoT networks [40].

Table 5: Performance Metrics for Different Network Sizes

Network Size (Devices)	Detection Accuracy (%)	False Positive Rate (%)	Detection Latency (ms)	Energy Consumption (J)
50	92	8	350	20
200	94	6	250	55
500	95	5	180	120
1000	96	4	150	250
5000	95.5	3	120	1200

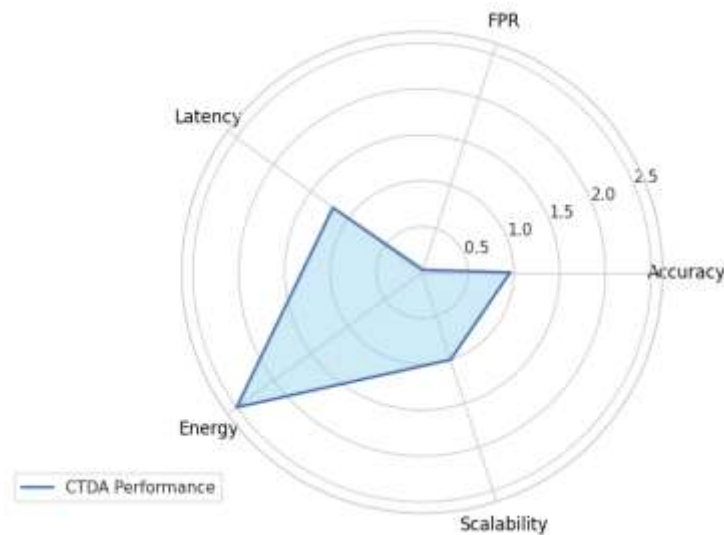
This table 5 illustrates how the CTDA framework performs across IoT networks of varying scales, ranging from small deployments of 50 devices to large networks with 5000 devices. The metrics included are detection accuracy, false positive rate, detection latency, and

energy consumption, providing a comprehensive view of the system's operational efficiency. The goal is to analyze how network expansion impacts the overall performance and to demonstrate the scalability of the proposed framework.

From the presented data, detection accuracy remains consistently high across all network sizes, with minor fluctuations at extremely large scales. This indicates that the distributed, trust-based architecture combined with edge intelligence ensures reliable DDoS detection even as the number of devices increases. The framework effectively manages traffic and anomaly detection across thousands of devices without significant loss of accuracy.

The table also highlights the trend in energy consumption and detection latency. Both metrics increase with network size, reflecting the additional processing and communication overhead required to handle larger amounts of traffic. However, the distributed edge-based approach prevents exponential increases, unlike centralized systems, ensuring that energy usage and latency remain within manageable bounds.

Finally, this table serves as a benchmark for network designers and researchers to evaluate the scalability of CTDA. It provides clear evidence that the framework maintains high performance while efficiently balancing detection speed, energy efficiency, and accuracy, making it suitable for deployment in large-scale heterogeneous IoT environments.



Graph 11: Multi-Metric Performance Radar Chart

This Figure 11 presents an overview of the performance of the CTDA framework in different key metrics at the same time. The axes depict Accuracy, False positive rate (FPR), Detection latency, Energy consumption and Scalability. To enable meaningful comparison, each of the axes is scaled accordingly, with larger measures representing more desirable performance as in the case of Accuracy and Scalability, and lower values represent more desirable performance as in the case of FPR, Latency and Energy.

The figure explains that CTDA captures a satisfactory level of detection accuracy and scalability with low false positive rates, low latency of detection, and effective use of energy to achieve the purpose. The difference between the aspects of the performance of the framework in all important parameters is displayed as a shady area in the radar chart and visually makes it clear that the framework performs well in all relevant parameters and is effective when applied in mass IoT deployment.

This visualization shows what the holistic advantages of partnering edge intelligence, trust-based assessment, and enforced mitigation are. Compared to single-

metric graphs, the radar chart will enable researchers and network administrators to evaluate trade-offs and system efficiency; in a single view such that a sufficient degree of understanding of the performance of the systems operations is achieved.

Lastly, radar chart will act as an effective performance benchmarking measure. It can be readily compared with the other DDoS mitigation frameworks and offer an idea about the optimization areas that still can be improved thus making CTDA robust, scalable and energy-saving and preserving the high reliability of detection in a heterogeneous IoT network.

Conclusion:

The proposed CTDA framework effectively mitigates DDoS attacks in large-scale IoT networks by combining edge intelligence with collaborative trust-based evaluation. Edge-based detection reduces latency and energy consumption compared to centralized approaches while maintaining high detection accuracy. Trust and reputation management ensures that malicious devices are isolated, minimizing false positives and improving reliability. Collaborative consensus among edge nodes enhances detection robustness and allows the system to adapt to dynamic attack patterns. The framework demonstrates scalability across heterogeneous IoT deployments, maintaining performance as network size and attack volume increase. Comparative analysis shows that CTDA outperforms conventional centralized and edge-only systems in accuracy, latency, and energy efficiency. Simulation results validate the framework's capability to handle diverse DDoS attack types with timely mitigation and minimal disruption to legitimate devices.

References:

- [1]. Wardana, A. A., Kołaczek, G., & Sukarno, P. (2024). Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things. *Applied Sciences*, 14(10), 4109.
- [2]. Kuznetsov, O., Frontoni, E., Kuznetsova, Y., Smirnov, O., & Moskovchenko, I. (2024). Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection.
- [3]. Li, W., Meng, W., & Kwok, L. F. (2021). Surveying trust-based collaborative intrusion detection: State-of-the-art, challenges and future directions. *IEEE Communications Surveys & Tutorials*, 24(1), 280-305.
- [4]. Chen, X., Chen, Y., Feng, W., Xiao, L., Li, X., Zhang, J., & Ge, N. (2022). Real-time DDoS defense in 5G-enabled IoT: A multidomain collaboration perspective. *IEEE Internet of Things Journal*, 10(5), 4490-4505.
- [5]. Abubakar, M. (2025). Trust Management Strategies in Fog and Edge Computing for IoT. Available at SSRN 5338300.
- [6]. Hayawi, K., Makhdoom, I., Khalid, S., Ikuesan, R. A., Kaosar, M., & Ahmad, I. (2025). A False Positive Resilient Distributed Trust Management Framework for Collaborative Intrusion Detection Systems. *IEEE transactions on services computing*.
- [7]. Kumavat, K., & Gomes, J. (2023). EIDDM: Edge and internet layer distributed dos threats detection and mitigation for internet of things wireless communications. *Wireless Personal Communications*, 131(1), 709-735.
- [8]. Taher, M. A., Tariq, M., & Sarwat, A. I. (2024). Trust-based detection and mitigation of cyber attacks in distributed cooperative control of islanded AC microgrids. *Electronics*, 13(18), 3692.
- [9]. Dimolianis, M., Kalogeras, D. K., Kostopoulos, N., & Maglaris, V. (2022, November). Ddos attack detection via privacy-aware federated learning and collaborative

- mitigation in multi-domain cyber infrastructures. In 2022 IEEE 11th International Conference on Cloud Networking (CloudNet) (pp. 118-125). IEEE.
- [10]. Ahmed, F. (2024). Trust-Based Framework for Securing Inter-Fog Communication in Smart City Applications. *International Journal of Emerging Research in Engineering and Technology*, 5(4), 74-87.
- [11]. Mkpa, A. (2024). A dynamic configurable model for addressing trust and privacy in IoT networks (Doctoral dissertation, Anglia Ruskin Research Online (ARRO)).
- [12]. Chen, X., Feng, W., Ge, N., & Zhang, Y. (2023). Zero trust architecture for 6G security. *IEEE network*, 38(4), 224-232.
- [13]. Dantas Silva, F. S., Silva, E., Neto, E. P., Lemos, M., Venancio Neto, A. J., & Esposito, F. (2020). A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. *Sensors*, 20(11), 3078.
- [14]. Abdul Rahim, F., Jaafar, A. G., Hassan, N. H., Aminu Ghali, A., & Abdul Karim, K. S. Ddos Threats in Iot: A Review of Blockchain-Based Defense Strategies. Abdul Ghafar and Hassan, Noor Hafizah and Aminu Ghali, Abdulrahman and Abdul Karim, Khairol Shapawi, Ddos Threats in Iot: A Review of Blockchain-Based Defense Strategies.
- [15]. Deshpabhu, T. (2024). Identification and mitigation of attacks in trust-based distributed communication networks (Doctoral dissertation, University of Oxford).
- [16]. Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abdualлах, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. *IEEE Access*, 7, 51691-51713.
- [17]. Chen, X., Feng, W., Chen, Y., Ge, N., & He, Y. (2024). Access-side DDoS defense for space-air-ground integrated 6G V2X networks. *IEEE Open Journal of the Communications Society*, 5, 2847-2868.
- [18]. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, 15(4), 2046-2069.
- [19]. Khodjamov, N., Song, Y., Sharif, K., Gao, Y., Li, F., Wang, Y., ... & Zhu, L. Blockchain-Based Secure Trusted Clusters for Multi-Tiered Social Iot Environments in Edge-Cloud Networks. Available at SSRN 5384355.
- [20]. Yu, J., Fang, C., Lu, L., & Li, Z. (2010). Mitigating application layer distributed denial of service attacks via effective trust management. *IET communications*, 4(16), 1952-1962.
- [21]. Garg, S., Goyal, S., & Bhandari, A. (2024, October). Exploring Blockchain in Collaborative DDoS Mitigation. In 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1-6). IEEE.
- [22]. Cheng, J., Yao, X., Li, H., Lu, H., Xiong, N., Luo, P., ... & Feng, W. (2022). Cooperative Detection Method for DDoS Attacks Based on Blockchain. *Computer Systems Science & Engineering*, 43(1).
- [23]. Su, Y., Xiong, D., Qian, K., & Wang, Y. (2024). A comprehensive survey of distributed denial of service detection and mitigation technologies in software-defined network. *Electronics*, 13(4), 807.
- [24]. Rahdari, A., Jalili, A., Esnaashari, M., Gheisari, M., Vorobeve, A. A., Fang, Z., ... & Tahaei, H. (2024). Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions. *Computers, Materials & Continua*, 80(2).
- [25]. Park, H., EL Azzaoui, A., & Park, J. H. (2025). AIDS-Based Cyber Threat Detection Framework for Secure Cloud-Native Microservices. *Electronics*, 14(2), 229.

- [26]. Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, 4(3), 149-160.
- [27]. Cherian, M. M., & Varma, S. L. (2022). Mitigation of DDOS and MiTM attacks using belief based secure correlation approach in SDN-based IoT networks. *International Journal of Computer Network and Information Security*, 15(1), 52.
- [28]. Liu, Z., Yin, X., & Hu, Y. (2020). CPSS LR-DDoS detection and defense in edge computing utilizing DCNN Q-learning. *IEEE Access*, 8, 42120-42130.
- [29]. Gupta, B. B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*. CRC press.
- [30]. Aamir, M., & Zaidi, M. A. (2013). A survey on DDoS attack and defense strategies: from traditional schemes to current techniques. *Interdisciplinary Information Sciences*, 19(2), 173-200.
- [31]. Simpson, S. V., Ravi Raju, Y., Bhanu Rajesh Naidu, K., & Venu, G. (2023). SECURE TRUST: a blockchain-enabled trust and reputation system for malicious node detection in IOT networks. *International Journal of Information Technology*, 15(8), 4323-4336.
- [32]. Berguiga, A., Harchay, A., & Massaoudi, A. (2025). HIDS-RPL: A Hybrid Deep Learning-Based Intrusion Detection System for RPL in Internet of Medical Thing Networks. *IEEE Access*.
- [33]. Wang, L., Petrova, K., & Yang, M. L. (2025). Trust Models in Wireless Sensor Networks for Defending Against Denial-of-Service Attacks: A Literature Review. *Applied Sciences*, 15(6), 3075.
- [34]. Muzammal, S. M., Murugesan, R. K., & Jhanjhi, N. Z. (2020). A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches. *IEEE Internet of Things Journal*, 8(6), 4186-4210.
- [35]. Okporokpo, O., Olajide, F., Ajenka, N., & Ma, X. (2023). Trust-based Approaches Towards Enhancing IoT Security: A Systematic Literature Review. *arXiv preprint arXiv:2311.11705*.
- [36]. VM, V., & P, M. (2023). ProSD-edgeIoT: Protected cluster assisted SDWSN for tetrad edge-IoT by collaborative DDoS detection and mitigation. *Cyber-Physical Systems*, 9(2), 144-173.
- [37]. Yu, J., Fang, C., Lu, L., & Li, Z. (2009, June). A lightweight mechanism to mitigate application layer DDoS attacks. In *International Conference on Scalable Information Systems* (pp. 175-191). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [38]. Cheng, J., Xu, R., Tang, X., Sheng, V. S., & Cai, C. (2018). An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment. *Comput. Mater. Continua*, 55(1), 95-119.
- [39]. Gyamfi, E., & Jurcut, A. (2022). Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets. *Sensors*, 22(10), 3744.
- [40]. Gyamfi, E., & Jurcut, A. (2022). Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets. *Sensors*, 22(10), 3744.