International Journal of Applied Mathematics

Volume 38 No. 8s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A2M: ADAPTIVE MULTI-LAYERED DEFENCE MECHANISM AGAINST DDOS ATTACKS WITH MINIMAL SERVICE DOWNTIME

Sujit Sutradhar[1*], Joy Lal Sarkar[2]

[1*,2]Faculty of science & Technology, ICFAI University Tripura,

Abstract

This paper presents DDoS-A2M, an adaptive multi-layered DDoS defence system using Random Forest, CNN, and Hybrid CNN + LSTM at the perimeter layer, transport layer, and application layer that caters to multi-vector DDoS while ensuring quality of service. The DDoS-A2M approach is evaluated using the CICDDoS2019 dataset and CAIDA 2007 dataset, achieving an accuracy of 94.54%, a precision of 95.60%, and a recall of 94.54%; an F1-score of 93.77%, and MTTM (Mean Time to Mitigate) of 1.38 milliseconds at 2.0% CPU and 64.1% memory utilisation. The consolidated ROC analysis confirmed near-1.0 AUC performance across all 18 categories of DDoS attacks. The DDoS-A2M approach proved capable of generally performing above 92% accurate detection time with very little latency. DDoS-A2M provides an effective, scalable, and reliable intelligent multi-layered DDoS defence model for practical networks.

Keywords: *DDoS Detection, Adaptive Defence, Multi-Layered Security, Machine Learning, Network Resilience.*

1. Introduction

Adaptive Multi-Layer Defence Mechanism Against DDoS attacks encompasses an effective strategy to mitigate service disruption & DDoS attacks and is paramount in the field of computer science engineering [1]. With the increase in web applications and cloud storage, it is crucial to offer service continuity [2]. DDoS attacks can overload networks processing requests from multiple clients, resulting in denial-of-service, downtime and loss of revenue. This framework outlines automated defences, network-level rate limiting, intelligent traffic filtering, behavioural analysis, AI-based detection process, all enabled to show behavioural adaptation during attack behaviour, presence of action ability while defending or mitigating attack behaviour to ensure service availability and resiliency [3,4].

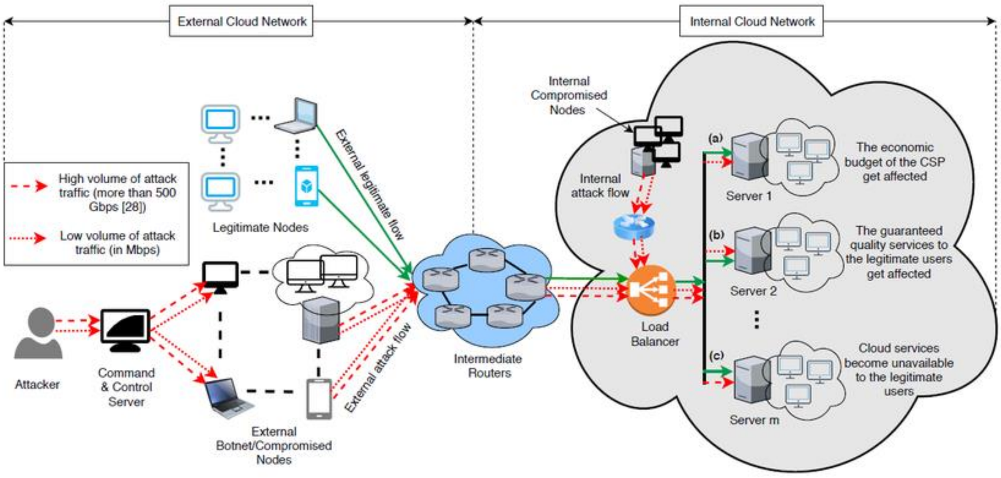
External Cloud Network
Internal Cloud Network
High volume of attack traffic (more than 500 Gbps [28])
Low volume of attack traffic (in Mbps)
Legitimate Nodes
External legitimate flow
Attacker
Command & Control Server
External Botnet/Compromised Nodes
External attack flow
Intermediate Routers
Internal Compromised Nodes
Internal attack flow
Load Balancer
(a)
Server 1
The economic budget of the CSP get affected
(b)
Server 2
The guaranteed quality services to the legitimate users get affected
(c)
Server m
Cloud services become unavailable to the legitimate users

Fig. 1: Scenario of DDoS attack under a cloud computing environment [5]

Received: August 15, 2025

DDoS attacks in cloud settings make use of both internal compromised nodes and external botnets from command-and-control servers that produce bad traffic aimed at routers and application load balancers to exhaust all resources and disrupt legitimate services as shown in Fig.1. These attacks include a combination of (1) volumetric attacks (UDP floods, amplification), (2) protocol attacks (SYN floods, split-packet), and (3) application-layer attacks that vilify and replicate the same behavior seen from legitimate users making detection and mitigation challenging, as in the cases of massive data flow illustrated from the 1.35 Tbps GitHub attack in 2018 and the 2.3 Tbps AWS attack in 2020 [9,6]. Regular single-layer DDoS defences, such as static rules, firewalls, and intrusion prevention systems, by themselves often do not address multi-vector DDoS attacks enough to prevent mitigation delays, false positives, and service downtimes [12,7]. In response, this work presents an adaptive multi-layered DDoS defense mechanism that integrates across several layer of defensive solutions including real-time mitigation, machine learning based traffic analyzation and anomaly detection across network, transport and application layers that automatically adapt to evolving threats, legitimize relevant traffic, learn and adapt across traffic patterns and networks, and ensuring low false positive rates, scalable and practical deployability [14,8]. The research objectives are: (i) to identify and characterise the DDoS attack patterns using historic datasets, (ii) to develop an integrated detection architecture that utilises signature-based detection, anomaly detection, and behavioural detection to identify threats in real-time, and (iii) to evaluate adaptive response strategies for various intensity levels of attack. Evaluation will be based on detection accuracy, false positive rate, latency, and system recovery time to ensure an overall evaluation of detection and mitigation. The rest of the paper is structured as follows: Section II addresses a review of prior work and identifies limitations to traditional defences; Section III presents the proposed framework; Section IV describes the implementation in all layers; Section V evaluates the performance of the system; and Section VI will conclude with contributions and directions for future work.

2. Literature Review

Recent research indicates that AI, along with a multi-layered architecture, is essential to DDoS defence. Sheibani et al. [18,9] proposed a three-layer IDS using SDN controllers that are distributed and make use of a self-organising map that is used in conjunction with a double deep Q-network that is used to reposition switches. These methods resulted in balancing among the SDN controllers and continued DDoS defence. Xu et al. [10] developed an SDN-based framework for power networks that used Rényi entropy in conjunction with multi-level CNNs and satisfied detection metrics. Verma et al. [11] analysed the collateral damage of cloud DDoS attacks and provided mitigation responses. Sudar et al. [12] proposed a GenAI hybrid defence using transformers, GANs, autoencoders, and unmonitored rules, improving detection rates while reducing false positives. Shah et al. [13] focused on multi-layered defence (whether in technology or human implemented) coupled with an AI filtering approach to maintain service availability. Akroma et al. [14] describe AI being used for real-time detection when dealing with an evolving attack vector. Carter et al. [15] provide a review of DDoS advances and trends. Bharathi et al. [16] focus on how attacks can physically exploit cloud-specific and general cloud service countermeasures. Swati et al. [17] suggested for IIoT, the Moving Target Defence for IIoT, for fast response efforts and resource availability. Afraji et al. [18] categorised attacks relative to explainable AI and transparent deep learning-based systems. While advancements are occurring, conventional defences still have limited layer coverage, static rules, and cannot adapt in real-time, leaving gaps in scalability, trust, and efficiency. The proposed framework, however, bridges those gaps through adaptive, multi-layered, AI-supported approaches for cloud-native and IIoT environment frameworks.

Received: August 15, 2025

3. Research Methodology

A systematic, layered, and iterative approach plans and evaluates an adaptive defence mechanism that will reduce service downtime during multi-vector DDoS attacks. The multi-stage, rigorous research methodological approach, which is shown in Fig. 2, ensures a robust and viable option that captures scalability and practical relevance while achieving scientific rigour.

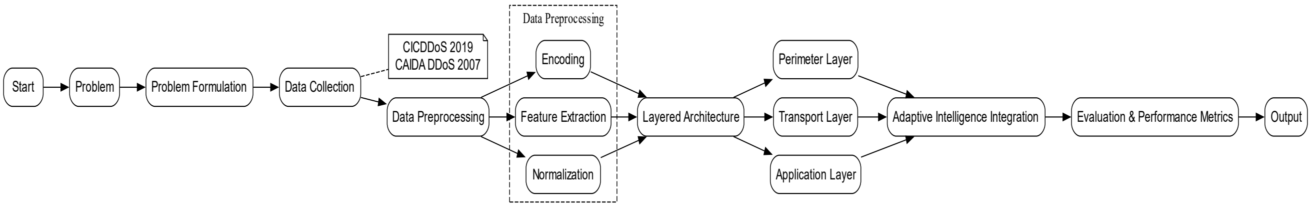

Fig. 2: Proposed Adaptive Multi-Layered Defence Methodology Block Diagram

The proposed approach is intended to design and test an adaptive multi-layered defence framework to mitigate multi-vector DDoS attacks and avoid service degradation in cloud and IoT environments. The process begins with the identification of the problem, in which DDoS attacks are becoming increasingly sophisticated with volumetric, protocol and application attack vectors, and static or single-layered defences are insufficient to protect against a multidimensional threat. Data collection will occur from historical datasets and real-world datasets, all of which provide a diverse representation of attacks for training and evaluation. The preprocessing stage will involve traffic normalisation, feature extraction, label encoding, dimensionality reduction, and temporal aggregation, which utilises time-windowing to maintain a high standard of input for machine-learning models. With that in mind, the input model will require formulas like $x' = \frac{x - x_{min}}{x_{max} - x_{min}}$ regarding normalisation, entropy calculation, $H(X) = -\sum_x p(x) \, log \, p\,(x)$ and dimensionality reduction $X_{\text{reduced}} = XW$. The defence structure is organised into three architecture layers, perimeter, transport, and application-based, to address volumetric, protocol-transport-based, and stealthy application attacks, respectively, using techniques such as signature-based filtering, entropy-based anomaly detection, deep learning based models (CNN, Random Forest), and a hybrid behavioural-based profiling. All three layers interact with a central Adaptive Intelligence Integration module using math, dynamically tuning thresholds, applying rule-based heuristics, and learning to detect in the real world and mitigate. The collective detection model can be mathematically represented as: $CapP_{detection} = 1 - \prod_{i=1}^{3}(1 - P_i)$ By stressing robustness throughout, the performance evaluation metrics are detection accuracy, false positive and negative rates, mean time to remediation, service availability, resource overhead, and the ability to scale with varying traffic. This methodology integrates an iterative preprocessing approach with layered defense and adaptive intelligence, resulting in a solution that is scalable, reliable, and context-sensitive, with the ability to perform efficiently to detect and remediate various DDoS attack vectors while maintaining continuous service availability that can be applied in practice and provides a scientifically sound framework that is compliant with IEEE standards for cybersecurity research.

4. Algorithm for DDoS Detection

Algorithm 1: Adaptive Multi-Layered Defense Mechanism Against DDoS Attacks

1. **INPUT:** Real-time network traffic stream T
2. **Initialize:**

- Load pre-trained models: RF_Model, CNN_Model
- Activate Perimeter, Transport, and Application Layers
- Initialize Adaptive Intelligence Engine, rules, and thresholds.

3. **Preprocessing**

- Remove noisy/incomplete packets

- Normalize numerical features; encode categorical features
- Apply dimensionality reduction (PCA/correlation filtering)
- Apply dimensionality reduction (e.g., PCA, correlation filtering)
- Segment traffic into time windows

4. **Perimeter Layer Filtering:**

- For each packet p ∈ T:
  - If volumetric attack signature → flag as potential DDoS
  - Else → forward to Transport Layer

5. **Transport Layer Detection:**

- Analyse the pack
- If suspicious → flag for mitigation as suspicious
- Else → forward to Application Layer

6. **Application Layer Classification:**

- Extract high-level features from the session
- Predict using RF_Model
- If confidence is low - or if traffic is complex:
- If DDoS detected - then, Mitigate
- else Allow traffic

7. **Procedure Trigger_Mitigation(p):**

- Block source IP via SDN/firewall
- Update adaptive rules and thresholds
- Log event for analysis

8. **Adaptive**

- Periodically retrain models if performance drops

9. **Performance Evaluation Metrics:**

- Detection of adversary intentions, accuracy of detection, false positives and false negatives, mean time to mitigation, service disruption time, system overhead

OUTPUT: Final traffic classification and triggered mitigation

5. Results & Discussion

This comprehensively evaluates the performance of our proposed A2M framework utilising multiple metrics: accuracy, precision, recall, F1-score, and efficiency to confirm the performance of our proposed models, especially in varying attack scenarios and traffic types. Our efforts are to demonstrate that our framework can be performed uniformly and adaptively shift from static thresholds to adaptive thresholds, and employed to characterise tuning thresholds. Overall, this section indicates how effective our proposed framework will be at detecting and deterring attacks in real-world environments.

Table 1: Comparative Performance of Machine Learning Models in Detecting DDoS Attacks Using CICDDoS2019 Dataset

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Random Forest	91.84	91.71	91.84	91.77
KNN	91.60	91.53	91.60	91.50
MLP	93.21	91.06	93.21	91.75
CNN	93.13	92.93	93.13	91.62
Hybrid CNN+LSTM	92.56	90.43	92.56	91.03

Received: August 15, 2025

Table 1 shows that all five models detect DDoS attacks effectively with minimal service impact. MLP leads at 93.21% accuracy, followed by CNN at 93.13%. Random Forest and KNN exceed 91%, while hybrid CNN + LSTM reaches 92.56% with 91.03% F1-score, demonstrating strong detection and service continuity.

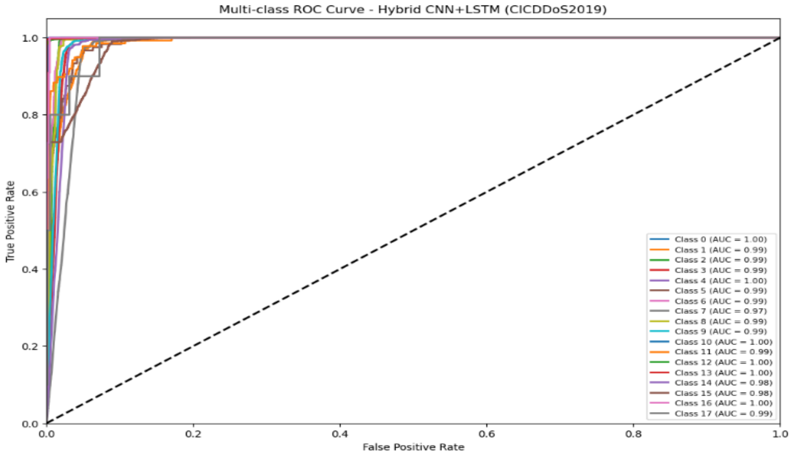

Fig.3: Multi-Class ROC Curve of Hybrid CNN+LSTM Model on CICDDoS2019 Dataset

The capability of the Hybrid CNN + LSTM model to classify 18 different types of DDoS attacks is depicted in Fig.3. The model exhibits an acceptable level of identification according to the AUC values, as the great majority of these values are close to 1.0. The model establishes a positive True Positive Rate while demonstrating a very low False Positive Rate. AUC cannot be mistaken for random chance, where AUC = 0.5. The accuracy across a wide range of classes indicates that the A2M defence mechanism can trust that different types of DDoS attacks will be accurately detected and services will remain up and effectively manage the network.

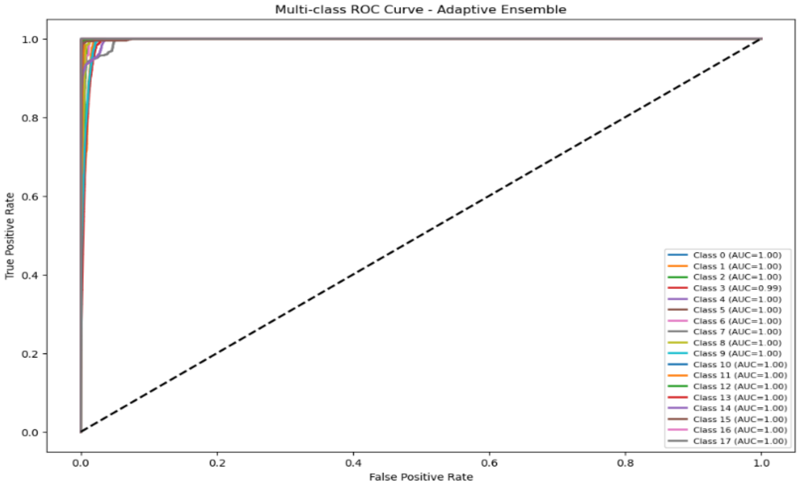

Fig.4: Multi-Class ROC Curve of Adaptive Ensemble Model on CICDDoS2019 Dataset

The Adaptive Ensemble Model's excellent classification performance across the different DDoS attack classes is shown in Fig.4, with an AUC equal to 1.00 on nearly all classes, as well as 0.99 for class 3, indicating excellent discrimination capabilities from the model. The upturn in curve form, coupled with minimal movement away from the top-left corner of the plot, demonstrates the ability of the model to effectively and accurately detect threats, and is highly aligned with the A2M framework's goal of maintaining a high level of accuracy and minimal downtime for impacted service

Table 2: Comprehensive Performance and Resource Efficiency of Adaptive Multi-Layer Ensemble Model

Metric	Value
Accuracy	94.54%
Precision	95.60%
Recall	94.54%
F1-Score	93.77%
MTTM (ms per record)	1.38
CPU Usage (%)	2.0
Memory Usage (%)	64.1
Total False Positives	4714
Total False Negatives	4714

The Adaptive Multi-Layer Ensemble in Table 2 has detection accuracy (94.54%) and precision (95.60%) values higher than other models, which also demonstrate a good trade-off complete with recall (94.54%) and F1-score (93.77%) values while still accurately identifying DDoS threats; the operation is efficient, as reflected by the relatively low Mean Time to Mitigate (MTTM) value of 1.38 ms per event, along with a low CPU usage value of (2.0%), and moderate memory usage (64.1%). Even with a total of 4714 false positive and false negative events, which may lean toward the moderately destructive nature of the data, overall performance does support a role in the A2M framework goals of providing adaptive layered defence without significantly harming the operational continuity of service.

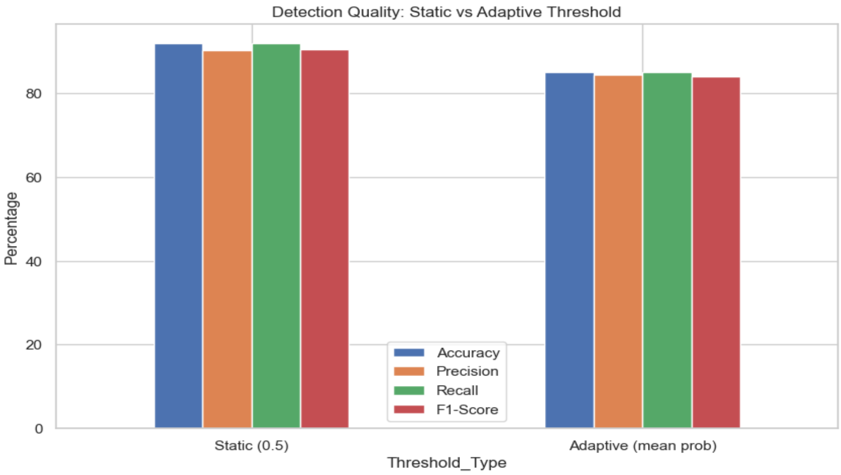

Fig.5: Comparison of Detection Quality Between Adaptive and Static Thresholds

Fig.5 illustrates the operationally effective DDoS detection threshold criteria in the static criterion (0.5) and adaptive (mean probability) option. In both cases of static and adaptive thresholds, the accuracy, precision, recall, and F1-scores are sufficiently greater than 80%. The adaptive thresholds adapt marginally better to the dynamic attack patterns as developed than the static thresholds. The allowance for changes in thresholds brings `adaptability´ to the A2M by increasing detection assurance and improving service availability.

Table 3: Threshold Sensitivity for DDoS Detection Performance

Threshold Type	Accuracy	Precision	Recall	F1-Score
Static (0.5)	92.70%	92.66%	92.70%	92.66%
After Tuning	90.25%	92.63%	90.25%	89.03%

Received: August 15, 2025

As shown in Table 3, there are differences in performance due to the static threshold of 0.5 and the post-tuning threshold. The precision hovered around 92.63% while the accuracy decreased slightly from 92.70% to 90.25% indicating there was no impact on the diversity of threat detection. When the threshold was adjusted slightly, recall and F1-score dropped, indicating some compromise in sensitivity. On the whole, these findings show, some flexibility of threshold needs to be applied while balancing detection quality and service limitations in the A2M framework.

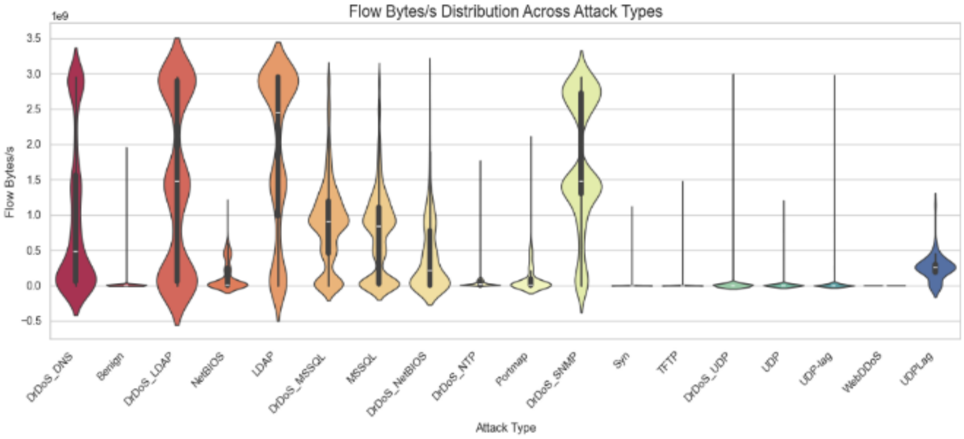

Fig.6: Distribution of Flow Bytes per Second Across DDoS Attack Types

The rate of bytes per second for attack and benign traffic is shown in Fig.6 to have opposing characteristics. DDoS_LDAP, DDoS_MSSQL, and DDoS_UDP have larger and wider distributions indicative of volumetric attacks that lead to substantial traffic spikes and bursts. Benign traffic has smaller, lower distributions, indicating that the model performs well at distinguishing between normal and malicious flows. Collectively, these results validate the adaptive capacity of the A2M framework to accurately classify varied DDoS behaviours.

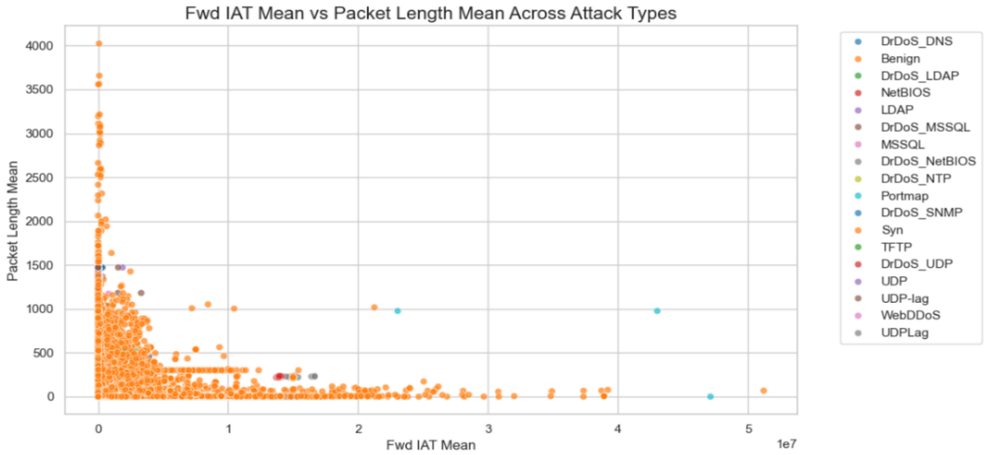

Fig.7: Scatter Plot of Forward Inter-Arrival Time Mean vs Packet Length Mean Across DDoS Attack Types

The distributions of Fwd IAT Mean and Packet Length Mean for DDoS attacks and benign traffic are illustrated in Fig.7. Most forms of attack are fast at sending their packets and have a small packet size, indicating high-throughput DDoS. A few outliers might suggest more sneaky or complicated attacks. The clearly-defined separation of benign and attack traffic provides the A2M framework with flow-based characteristics to help law enforcement agents identify threats in an accurate and adaptive way.

6. Conclusion

The Adaptive Multi-Layered Defence Mechanism (A2M) framework illustrates that it is possible to precisely detect and remediate several different types of DDoS attacks from one autonomously operating architecture that minimises service downtimes. Testing of our framework demonstrates 94.54% accuracy, 95.60% precision, as evaluated against both the CICDDoS2019 dataset, a public dataset from the University of CAIDA in 2007; additionally, we demonstrate a low Mean Time to Mitigation (MTM) of 1.38 ms for each record evaluated, showing both operational efficiency and scalability. Robustness is ensured through adaptive thresholds, ensemble intelligence, and multi-level analysis. Our designs demonstrate low undifferentiated resource usage despite dynamic and adaptive thresholds, joining multiple users and multiple layers, all with adaptive thresholds for evaluating evolving attack patterns. Future work will focus on improving real-time orchestration-based cloud network environments, integrating federated learning and blockchain-based trust validation, in addition to extending deployment in IoT and 5G edge environments to secure heterogeneous and large-scale systems from future DDoS threats.

REFERENCES

[1]. Haseeb-Ur-Rehman, Rana M. Abdul, Azana Hafizah Mohd Aman, Mohammad Kamrul Hasan, Khairul Akram Zainol Ariffin, Abdallah Namoun, Ali Tufail, and Ki-Hyung Kim. "High-speed network DDoS attack detection: A survey." *Sensors* 23, no. 15 (2023): 6850.

[2]. Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." *IEEE Communications Surveys & Tutorials* 15, no. 4 (2013): 2046-2069.

[3]. Apostu, Alexandru, Silviu Gheorghe, Andrei Hîji, Nicolae Cleju, Andrei Pătraşcu, Cristian Rusu, Radu Ionescu, and Paul Irofti. "Detecting and Mitigating DDoS Attacks with AI: A Survey." *arXiv preprint arXiv:2503.17867* (2025).

[4]. Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." *Computer networks* 44, no. 5 (2004): 643-666.

[5]. Agrawal, Neha, and Shashikala Tapaswi. "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges." IEEE Communications Surveys & Tutorials 21, no. 4 (2019): 3769-3795.

[6]. Li, Qing, He Huang, Ruoyu Li, Jianhui Lv, Zhenhui Yuan, Lianbo Ma, Yi Han, and Yong Jiang. "A comprehensive survey on DDoS defense systems: New trends and challenges." *Computer Networks* 233 (2023): 109895.

[7]. Talla, Rajasekhar Reddy, Aditya Manikyala, Md Nizamuddin, Hari Priya Kommineni, Srinikhita Kothapalli, and Arjun Kamisetty. "Intelligent Threat Identification System: Implementing Multi-Layer Security Networks in Cloud Environments." *NEXG AI Review of America* 2, no. 1 (2021): 17-31.

[8]. Falowo, Olufunsho I., Murat Ozer, Chengcheng Li, and Jacques Bou Abdo. "Evolving malware & DDoS attacks: Decadal longitudinal study." *IEEE Access* (2024).

[9]. , Morteza, Savas Konur, Irfan Awan, and Amna Qureshi. "A Multi-layered defence strategy against DDoS attacks in SDN/NFV-based 5G mobile networks." Electronics 13, no. 8 (2024): 1515.

[10]. Xu, Kai, Zemin Li, Nan Liang, Fanchun Kong, Shaobo Lei, Shengjie Wang, Agyemang Paul, and Zhefu Wu. "Research on Multi-Layer Defense against DDoS Attacks in Intelligent Distribution Networks." Electronics 13, no. 18 (2024): 3583.

[11]. Verma, Priyanka, Nitesh Bharot, John G. Breslin, Mukta Sharma, Nisha Chaurasia, and Ankit Vidyarthi. "Uncovering collateral damages and advanced defense strategies in cloud environments against DDoS attacks: A comprehensive review." Transactions on Emerging Telecommunications Technologies 35, no. 4 (2024): e4934.

[12]. Sudar, K. Muthamil. "ADVANCED HYBRID GENERATIVE AI MODELS FOR MULTI-LAYERED DETECTION AND DEFENSE AGAINST DDOS ATTACKS." ICTACT Journal on Soft Computing 15, no. 3 (2025).

[13]. Shah, Syed Rajab Ali. "Preventing Distributed Denial of Service (DDoS) Attacks in Cloud Networks." *Global Perspectives on Multidisciplinary Research* 5, no. 3 (2024): 64-69.

[14]. Akroma, Abdulssalam Jomah, and Rabee Hamza Gareeb. "Leveraging Artificial Intelligence for Enhanced Detection and Mitigation of DDoS Attacks." مجلة شمال إفريقيا للنشر العلمي (NAJSP) (2025): 36-42.

[15]. Carter, Samuel. "Inside a Distributed Denial of Service (DDoS) Attack: Anatomy, Impact, and Defense Strategies." International Journal of Social Trends 2, no. 4 (2024): 1-7.

[16]. Bharathi, M., T. Aditya Sai Srinivas, D. Rohini, S. Shaankari, and M. Aishwarya. "Virtual Clouds, Real Threats: DDoS Attacks Reviewed and Mitigated."

[17]. Swati, Sangita Roy, Jawar Singh, and Jimson Mathew. "Securing IIoT systems against DDoS attacks with adaptive moving target defense strategies." *Scientific Reports* 15, no. 1 (2025): 9558.

[18]. Afraji, Doaa Mohsin Abd Ali, Jaime Lloret, and Lourdes Peñalver. "Deep Learning-Driven Defense Strategies for Mitigating DDoS Attacks in Cloud Computing Environments." *Cyber Security and Applications* (2025): 100085.