MSc Cybersecurity and Digital Forensic

Module: Research Methods and Professional Development

Module Code: ACFA7004_LON

Assessment Component 1: Research Proposal

Submission Deadline: 1st May 2026, 14:00 (2PM)
Lecturer: Dr Suresh Shanmugasundaram

Title of Proposal: Adaptive AI/ML-Based Real-Time DDoS Detection and Mitigation for Computer Networks

Student Name: Shafee Ul Mahmud Chowdhury

Student Number: 243637

Table of Content

List of Figures 3
List of Tables 3
1. Introduction 3
1.1 Context and Background 3
1.2 Research Problem 5
1.3 Research Aim and Objectives 5
Aim 5
Objectives 6
1.4 Significance of the Research 6
2. Literature Review 6
2.1 Introduction to the Literature Review 6
2.2 Thematic Analysis of Existing Literature 7
2.2.1 Traditional DDoS Detection Techniques 7
2.2.2 Machine Learning-Based Detection 8
2.2.3 Deep Learning Techniques 9
2.2.4 Adaptive and Real-Time Detection Systems 9
2.3 Key Contributions and Research Gaps 10
2.4 Theoretical and Technical Frameworks 10
2.5 Relation to This Study 11
2.6 Literature Summary 11
3. Research Design and Methodology 12
3.1 Research Design 12
3.2 Research Methods and Materials 12
3.2.1 Methods 12
3.2.2 Materials 13
4. Expected Outcomes 14

4.1 Anticipated Results 14
4.2 Implications of the Research 15
4.3 Limitations 15
5. Timeline 16
6.Conclusion 17
7. References 18

List of Figures

Figure 1Classification of DDoS defense method. 4
Figure 2: Simulation Diagram 13
Figure 3: Gantt Chart Timeline 17

List of Tables

Table 1: Signature-Based vs. Anomaly-Based 7
Table 2: Comparison Between Traditional IDS and AI-Powered Adaptive IDS 9
Table 3: Intrusion Detection Datasets Comparison 14

1. Introduction

1.1 Context and Background

The fast growth of internet-based systems and information infrastructure has strongly raised the needs for network identification and protection. Consequently, cyberattacks against the availability of services have emerged as a major problem, in which Distributed Denial of Service (DDoS) attacks are the most serious threat. DDoS attacks work by sending excessive traffic towards a target, from many sources to make the targeted services unavailable for legitimate users [1]. The evolution of these attacks over the past few years, both in scale and complexity, poses significant detection and mitigation challenges [2].

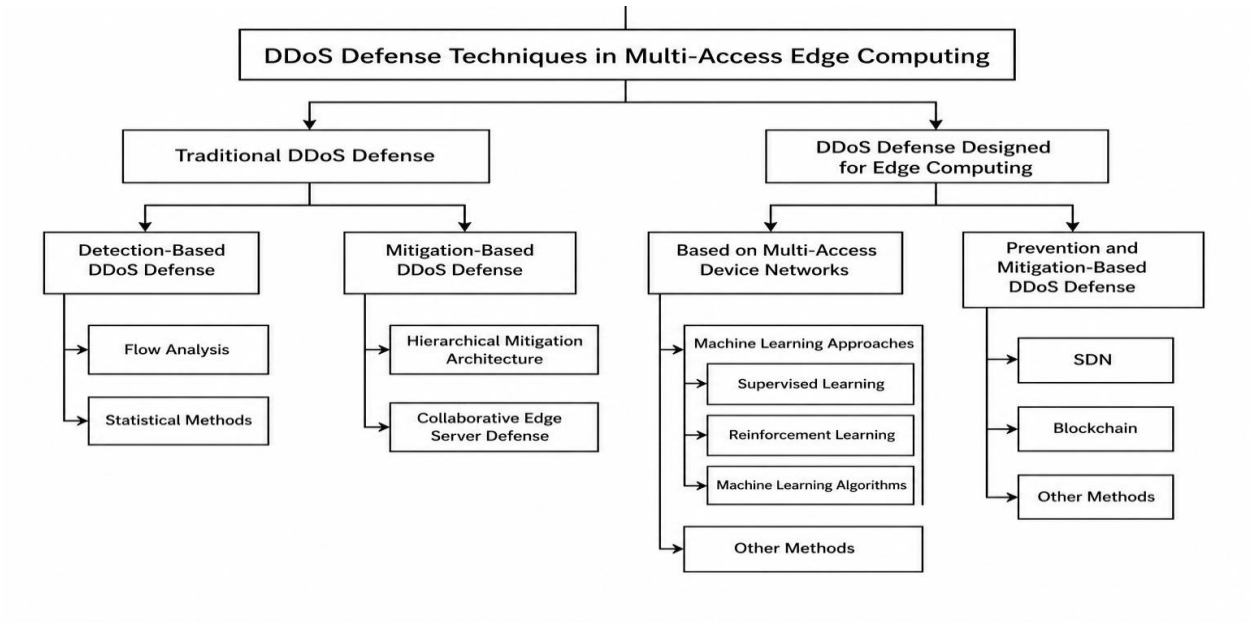

Figure 1Classification of DDoS defense method.

DDoS attacks have been, in general, volume based by nature - they target the high traffic volumes to exhaust the network resources exhaustively. However, today such attacks are increasingly multi-vector and combine volumetric, protocol and application-layer attacks in parallel [3]. The situation is only aggravated by the threat represented by botnets, i.e., networks of (potentially) thousands of compromised devices that can be instructed to launch different attacks at the same time [4]. Moreover, attackers are increasingly harnessing automation and artificial intelligence methods to improve attack designs that have made them adaptive and stealthy [5].

Traditional security mechanisms such as firewalls and rule based IDS use signature detection, which does not detect new or never seen threats [17]. As a result, researchers have been increasingly utilizing Artificial Intelligence (AI) and Machine Learning (ML) techniques for improved detection. ML models can process this vast amount of network traffic data, and they can infer what sort of anomaly corresponds to DDoS attacks [16].

Proposition of ML based methods is supported by extensive research work which prove that they are feasible for DDoS detection. Supervised learning algorithms i.e. Random Forest and Support Vector Machines (SVM) have been declared to achieve high levels of accuracy, often above 98%, especially in partitioned data domains [8]. Additionally, deep learning models like CNN based and LSTM networks enhance the feature extraction and classification [9].

Even though they have made significant strides, deploying ML-based systems in practice remains a challenge in real world networks. Most models are static and do not adapt to evolving threats, thus tending to underperform in the long run [10]. Moreover, the high-speed network traffic complicates their detection and its real-time mitigation is one ofthe primary challenges [11]. Hence, this research

emphasizes a system that is ai/ml based and will adapted to the possible threat, giving it an advantage of real time detection and mitigation.

1.2 Research Problem

Despite the great promise of research on DDoS detection using machine learning techniques, there are important challenges that limit their successful deployment at scale. The main reason is the existing models are non-adaptive. Many systems based on ML are trained over historical data sets, and unlike in our approach would not be able to update themselves in real-time [10].

False positives are also one of the biggest problems in such technology. In certain system models, such as banking and healthcare, it is essential that legitimate traffic remains unaffected by any service disruptions caused by misclassification degrades user experience [12]. This indicates that higher precision classification mechanisms are needed.

Another challenge lies in scalability. On the other hand, modern networks such as cloud and Internet of Things (IoT) systems produce high-volume data which requires rapid processing [13]. On the other hand, classic ML models usually fail to process such large-scale data in an appropriate time so they do not allow timely detection and response.

Nonetheless, most studies mostly emphasise on detection and not mitigation. Although detecting an attack is important, it is more crucial to have efficient countermeasures so that the availability of service can no longer be affected by the attacks [14]. Also, most of the existing systems do not have a tight integration between detection and mitigation which renders them only curative at best.

This statement of challenges starkly identifies the immediate research need for developing integrated, adaptive and real-time DDoS detection and mitigation framework. This can be addressed in this study through designing a system of applications that leverages cutting edge ML, as well as adaptively learns.

1.3 Research Aim and Objectives

Aim

Deep Learning and Machine Learning for Applications on DDoS An Adaptive AI/ML based Framework to Identify & Mitigate DDoS Attacks in Computer Networks

Objectives

1. To evaluate current DDoS detection systems and pinpoint their weaknesses [4].
2. To develop a training flexible machine learning model that is able to deal with changing attack patterns [10].
3. To perform the online classification of traffic with sophisticated ML algorithms [8].
4. To create an automated mitigation mechanism along with detection integrated [14].
5. Evaluation classified based on accuracy, precision, recall and F1-score[15].

1.4 Significance of the Research

This research adds to the literature in two main ways: it bridges the gap between academia and practical cybersecurity implementations. From an academic perspective, it moves the knowledge of adaptive machine learning techniques forward for network security by addressing shortcomings with static models [10]. This also helps in fusing detection and mitigation into a single paradigm.

Characterization: In practical sense, proposed system can be implemented on enterprise networks,where DDoS attacks are a real threat [13]. Better detection and mitigation capabilities will make these systems more reliable and secure.

Also, from a society perspective improving DDoS defences maintains accessibility to essential services: from healthcare and financial sectors through to government systems, ultimately strengthening our collective digital resilience.

2. Literature Review

2.1 Introduction to the Literature Review

This literature review intended to survey, critique, and analyze relevant work about DDoS detection and mitigation, especially using ML/AI-based approaches. This review will identify major trends, methodological advancements, and knowledge gaps in the field as a structured basis for the proposed research.

The review covers all literature from the years 2010 to 2025, which is a time period noted for rapid progress of AI in cybersecurity [4]. It consists of multiple sub domains such as traditional intrusion

detection systems, supervised and unsupervised machine learning approaches, statistical models, common deep learning models, and adaptive real-time frameworks [8]. Through a detailed analysis of these studies, the review outlines substantial contributions while also pointing out certain limitations that warrant an adaptive and integrated DDoS detection system [10].

2.2 Thematic Analysis of Existing Literature

2.2.1 Traditional DDoS Detection Techniques

Traditional DDoS detection methods are signature-based and consist of rules or patterns that identify types of malicious activities identified [1]. While these systems are effective against known attack types, they are not able to detect zero-day or evolving attacks [2].

Feature	Signature-Based	Anomaly-Based
Detection Principle	Matches known attack patterns	—
Effectiveness for Zero-Day	Low	High
Generate Fake alert or block	Low	High
Detection notification	Fast	Moderate
Maintenance	Frequent updates required for new signatures	Regularly train and tuning is needed for model
Adaptability	Static	Automatic but unstable
Learning Method	Rule-based	Statistical / Machine Learning

Table 1: Signature-Based vs. Anomaly-Based

In the above table it has shown that the features based comparison between Signature-Based and Anomaly-Based.

To tackle this limitation, anomaly-based detection approaches were proposed. [16] These techniques monitor unusual behavior, which enables them to detect unknown attacks [2]. But, the problem with

anomaly-based techniques is that they have high false grip because vibrant modify in traffic can be mistakenly labelled as attacks [4].

In addition, classical systems are static and cannot adapt to the changes in attack behavior [5]. Thus, they are not enough to mitigate contemporary DDoS attacks which exist under highly dynamic and intricate conditions.

2.2.2 Machine Learning-Based Detection

Therefore, since the approaches used to detect DDoS attacks require mastering and understanding so abandoned manual analysis of network traffic patterns together with machine learning have led to a remarkable improvement in detection performance [4]. The supervised learning algorithms like Random forest, Support Vector Machine (SVM), and Decision trees are widely applied because of their accuracy and robustness [3].

Criteria	Traditional IDS	AI-Powered Adaptive IDS
Detection Method	Signature or static anomaly-based	AI-driven (ML/DL) with real-time learning
Zero-Day Threat Handling	Poor (not detectable without prior signature)	Excellent (learns from behavior patterns)
Adaptability	Limited (manual updates required)	High (self-learning and model updating)
False Positive Rate	High (especially in anomaly-based models)	Lower (pattern recognition reduces false alarms)
Response Time	Delayed (requires signature matching or thresholding)	Real-time or near real-time
Scalability	Poor in dynamic environments	High scalability across cloud and edge environments
Privacy Considerations	Centralized data analysis	Supports decentralized and privacy-preserving approaches

Maintenance Requirement	Frequent manual tuning	Minimal – can auto-tune or adapt based on environment feedback

Table 2: Comparison Between Traditional IDS and AI-Powered Adaptive IDS

In particular, Random Forest reached more than 98% detection accuracy, which is why it is very used for DDoS detection [5]. Likewise, the SVM is proficient in high-dimensional data environments and good at classification [4].

When labelled data is not available, similar unsupervised learning methods include clustering and anomaly detection [6]. Nevertheless, these methods normally achieved worse accuracy with much more false positives in comparison with supervised approaches [2].

Although machine learning models offer such advantages, most of them are trained offline using static datasets and cannot dynamically adapt to new attack patterns [8].

2.2.3 Deep Learning Techniques

Deep learning approaches raise DDoS detection to new heights of effectiveness with data-centric models that leverage a multitude of automatic feature extraction from large datasets [7]. As a result, some key deep learning components such as CNNs for capturing spatial features in network traffic and LSTMs for modelling temporal dependencies [8] are also applicable here.

Such techniques are especially helpful in detecting complex and multi-vector attacks that are hard to identify with conventional methods [13] In addition, DNNs are applicable to large amounts of data effectively and compared with the traditional network environment [7].

At the same time, however, deep learning models have their fair share of challenges too. Both of these approaches are computationally intensive and need large data sets for training hence limiting their scalability [8]. Furthermore, the interpretability of ML models raises issues with regards to trust and transparency in decision making [4].

2.2.4 Adaptive and live traffi Detection Systems

New research has been focused on building of adaptive and live DDoS detection systems. These systems are expected to learn on continuous data stream and reflect the alterations in their models [10].

A notable improvement is through combining machine learning with Software Defined Networking (SDN) technology that allows dynamic observation and control of network traffic level [9]. Real-time response to threats is possible with SDN-based systems, and detection/mitigation efficiency is improved accordingly [9].

Adaptive frameworks have shown accuracy and real-time capabilities, with some studies achieving performance levels over 99% [10]. Nevertheless, these systems often encounter difficulties in terms of computational complexity and latency, as well as implementation complexity [8].

Moreover, most of the adaptive systems are mostly detection oriented and do not fully integrate mitigation component into flexible mechanisms rendering them largely useless in practice [6].

2.3 Key Contributions and Research Gaps

A number of important contributions in the arena of DDoS detection have been highlighted in the literature. The data up to October 2023 is used for training machine learning techniques, which greatly improve the accuracy of detections and reduce human reliance on rule-based systems [4]. Deep learning provides the ability to detect complex attacks [7]. Also, SDN-based frameworks enabled real-time monitoring and response [9].

Yet despite these advances, important gaps remain. One, a lot models are quite rigid and cannot adapt to dynamic change in threat [8]. Second, the deployment in real-time is still limited because most studies are focused on offline evaluation using static datasets high false positives rates still affect on the performance of anomaly systems [2].

Furthermore, existing solutions lack a systematic integration of detection and mitigation mechanisms [5], making them impractical. Scalability is another big issue, especially with current deep learning models that demand a lot of computational resources [8].

Such gaps reflect a growing necessity of an adaptive system capable of identifying notional targets and what real-time detection systems additionally need to do alongside mere automated mitigation.

2.4 Theoretical and Technical Frameworks

The theory behind DDoS detection research is founded on anomaly detection and classification theory. Anomaly detection attempts to find data that behaves significantly different from the normal behaviour, and classification models classify traffic into either benign or malicious classes [4].

Several machine learning algorithms are popularized in the literature from a technical perspective. Because of its wide applicability and robustness, Random Forest [3] is one of the most commonly

used algorithms to tackle datasets with many features. [4] Support Vector Machine is applicable to high-dimensional classification issues

Deep learning models, such as CNN and LSTM, enable advanced feature extraction and temporal analysis [7]. Also, SDN frameworks offer instantaneous observation and live supervision of the information transmissions [9].

Consequently, datasets such as CICDDoS2019, a labelled dataset with realistic network traffic data and various attack scenarios [11], are usually used for training and evaluation. Tools like Python, Scikit-learn and TensorFlow to implement ML models.

2.5 Relation to This Study

This research is built on literature by revealing the limitations of current DDoS detection systems. Although prior research have shown that high accuracy can be achieved using machine-learning and deep learning models, leading to a higher methodological richness of the results in some instances [8], based on empirical evidence they do not show convincing conclusions regarding adaptability and real-time responsiveness.

Tentative study describes a framework in which we can baseline the systems to be automated & the detection of major threats can be done through AI/ML based adaptive security. This system would learn from incoming data continuously and respond to changing attack patterns, unlike existing approaches [10].

Moreover, the paper is devoted to scalability and efficiency means that the high-quality of this system in large scale network environment like cloud and IoT systems [5]

The research addresses these gaps in contribution

2.6 Literature Summary

To sum up, DDoS detection has made great strides with application of machine learning and deep learning in the literature. Today, traditional approaches can only detect old attacks and become ineffective to modern types of attacks; in contrast ML based techniques provide a better effectiveness and adaptiveness [4].

Nevertheless, lack of adaptivity, high rates of false positives, a focus on scalability and low integration with mitigation strategies pose considerable challenges [8].

To overcome these challenges, this work proposes an holistic and adaptive DDoS detection and mitigation framework for real-time decision making that contributes to the state of-the-art in cybersecurity research.[20]

3. Research Design and Methodology

3.1 Research Design

This research adopts a Design Science Research (DSR) approach, which focuses on the development and evaluation of an artefact designed to solve a real-world problem [1]. In this study, the artefact is an adaptive AI/ML-based framework for real-time DDoS detection and mitigation. DSR is particularly suitable for this research because it enables the systematic design, implementation, and evaluation of innovative cybersecurity solutions [20].

Unlike purely theoretical analysis, this research requires the creation of a functional system capable of analysing network traffic and responding to attacks in real time. The DSR approach ensures that the proposed solution is both practically relevant and academically rigorous [18]. Furthermore, this approach supports iterative development, allowing the system to be refined based on evaluation results, which is essential when dealing with dynamic cybersecurity threats [3].

3.2 Research Methods and Materials

3.2.1 Methods

Quantitative research method is used in this study because it concerns with numerical analysis of network traffic data and machine learning models performance [4]. Quantitative methods are appropriate as they enable an objective measuring of classification accuracy, detection and false positive rates.

Our research strategy follows an experimental and software development approach in which several machine learning models are defined, implemented, and evaluated on benchmark datasets [5]. It is very useful to test the performance of DDoS detection systems based on AI in a controlled environment.

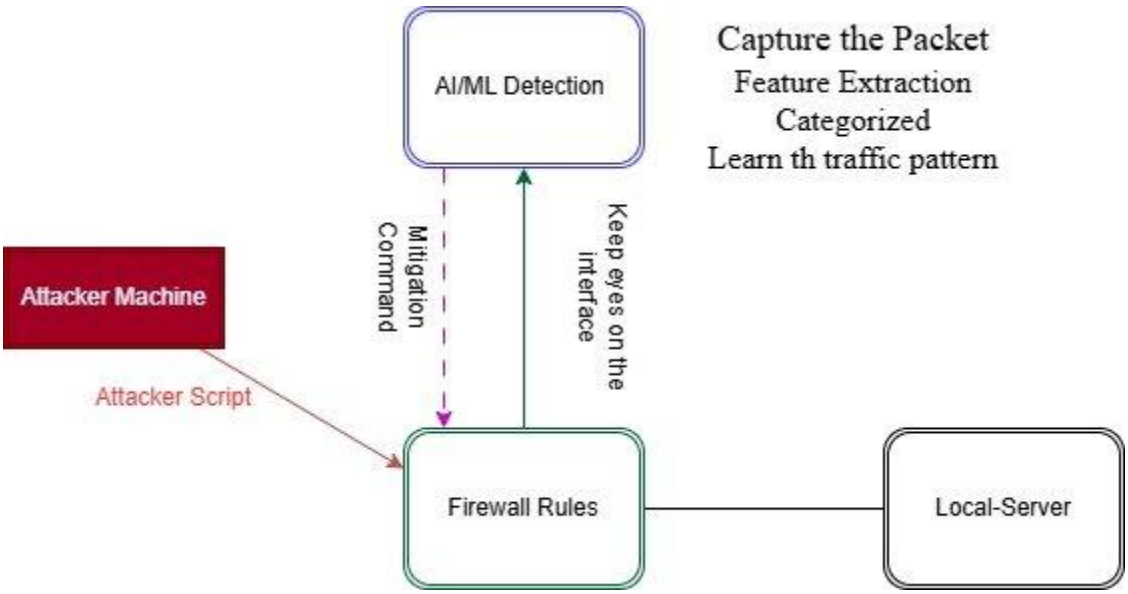

Figure 2: Simulation Diagram

Systems Architecture Based on [6], the proposed architecture has been divided into data collection, feature extraction, ML classification model, adaptive learning mechanism and mitigation module as illustrated in Figure 2. The classification module will incorporate classifiers such as Random Forest, Support Vector Machine (SVM) that achieved high detection accuracy in earlier studies [21]

For performance evaluation, data analysis will follow standard metrics in categorized including accuracy, precision, recall which are broadly used for measuring classification predictive performance [4]. Also, the evaluation of real-time performance will evaluate performance based on detection latency and system response time [8].

3.2.2 Materials

CICDDoS2017, CICDDoS2018, which is labelled network traffic data representing various types of DDoS [9]. Suitable for the training and evaluation of machine learning models [10], this dataset is popular among academic researchers and provides a realistic representation of attack cases.[14]

Dataset	Year	Attack Types	Traffic Type	Labeled	Modern Threats Included
KDD Cup 1999	1999	DoS, R2L, U2R, Probe	Simulated (DARPA)	Yes	No
NSL-KDD	2009	DoS, R2L, U2R, Probe	Refined KDD99	Yes	No
CICIDS2017	2017	DDoS, Botnet, Brute Force	Real-world (captured)	Yes	Yes
UNSW-NB15	2015	Fuzzers, Worms, Backdoors	Hybrid (real/simulated)	Yes	Yes
TON_IoT	2020	Reconnaissance, Injection	IoT/IIoT Traffic	Yes	Yes
BoT-IoT	2018	DDoS, Theft, Spoofing	IoT Network (realistic)	Yes	Yes

Table 3: Intrusion Detection Datasets Comparison

Python will be used as a programming language, together with the Scikit-learn and TensorFlow libraries, as these are widely used for machine learning/data analysis work [11].

Hardware requirements are either GPU enabled system or cloud computing platform [12], to process large dataset and train deep learning models efficiently.

Ethics: The datasets are obtained from publicly available sources, and do not involve personal or sensitive data that could result in non-compliance with guidelines for academic research.

4. Expected Outcomes

4.1 Anticipated Results

The expected results are predictive (not empirical) when this work is at the proposal stage, but based on previous research, it is expected that the adaptive AI/ML-based framework proposed in this paper will perform significantly well for both identification and reduction of DDoS attacks. In particular, it is anticipated that the system shall be able to attain an accuracy of detection above 98% which is comparable with other works[22] employing supervised leaning models such as Random Forest and Support Vector Machine (SVM).

Adaptive learning mechanisms will allow the model to adapt to learn attack behavior which is a still main limitation of static machine learning methods. Moreover, the new system is expected to lower false positive rates, which are due to anomaly based detection techniques [15].

In addition, the framework has stated that it will provide databases for real time traffic analysis and mitigation [22], which should result in lower response times during attacks as well as shortening service disruption. In conclusion, the performance of the proposed system is expected to be superior than the rule-based approach practices and provides a more robust and scalable cybersecurity solution [5].

4.2 Implications of the Research

The theoretical, practical and social implications of the findings are discussed. From the theoretical point of view, it adds to advancing adaptive machine learning in cybersecurity by integrating continuous progression mechanisms into DDoS detection models [6]. This could be useful for future study on self-learning and intelligent security systems.

In practical terms, the presented framework would be applicable in real-world environments including cloud computing [6], enterprise networks [20], and Internet of Things systems [7] that are significantly at risk of DDoS attacks. The incorporation of automated mitigation mechanisms is assumed to maximize network resilience, and consequently minimize downtime that matters most for sensitive industries.

Finally, this work provides an adaptable and scalable solution for the cybersecurity community by tackling existing detection systems limitations [13]. The reliance on commonly established datasets and reproducible procedures makes it optimal both scientifically as well as applied.

At the societal level, DDoS defence improves the resistance of critical digital infrastructure which is vital to almost all our economic and social activity [2]

4.3 Limitations

Limitations Along with the expected contributions, multiple limitations might limit this research output. The first hurdle is computational complexity, training such powerful machine learning and deep learning models on large-scale network traffic data [9]. This may need high-end hardware like GPU based system.

The second limitation comes from the dependency on benchmark datasets like CICDDoS2019. Despite their extensive usage, these datasets are not entirely representative of the realities in a network, and this could limit the generalizability of the results [10].

Moreover, real-time deployment is also accompanied by latency and system integration challenges; since high-speed networks demand rapid detection and reaction protocols [16]. The real-world complexity of implementing adaptive systems may also limit scalability.

Lastly, security models are as reactive as ever to emerging threats and therefore, the device may require continuous updates and retraining to stay effective .[13]

5. Timeline

The project is planned over a **16-week period (June to September)**, with clearly defined phases and milestones.

Weeks 1–2 : The **literature review** is conducted in this period, focusing on analyzing existing DDoS detection techniques and identifying research gaps. This forms the theoretical foundation of the study.

In **Weeks 3–4**, **data collection and preprocessing** are carried out using the CICDDoS2019 dataset, ensuring that the data is clean and suitable for model training.

Weeks 4–5: The **model development phase** involves designing and implementing machine learning algorithms such as Random Forest, SVM. This stage establishes the core detection framework.

Weeks 6–9: Extensive **testing and validation** are performed to evaluate model performance under different attack scenarios.

Weeks 10–11: The **evaluation phase** focuses on analysing results using metrics such as accuracy, precision, recall, and F1-score, ensuring the model meets performance expectations.

Weeks 11–14: During the **final report is written**, documenting methodology, findings, and analysis.

Weeks 15–16 : This period are dedicated to **review and refinement**, ensuring the research meets academic standards before submission.

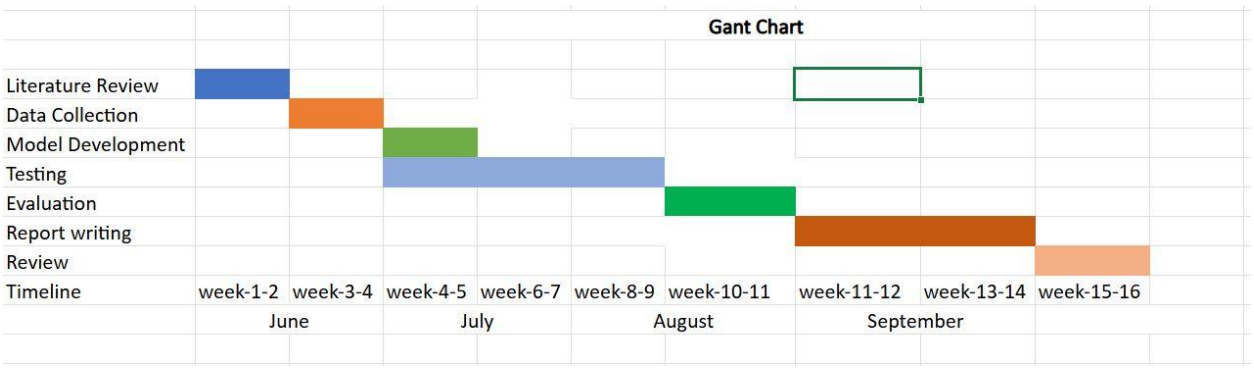

Figure 3: Gantt Chart Timeline

6.Conclusion

To conclude, this research indicates the rising difficulty of up-to-date DDoS assaults as well as the inadequacy stemming from old detection methods. Signature-based systems are only effective against previously discovered threats, while the anomaly-based method can detect unknown attacks but are not practical due to high false positives and less stability in dynamic environments. [3], [1]

This study state the usage of machine learning (ML) and detection of deep learning (DL) techniques is crucial as it increase the power of ML an DL to analyze traffic patterns in complex environments and detecting anomalies with very high accuracy. In practice, most existing models are static; they need to be trained using historical data before actually being launched for use, making them much more vulnerable to adaptations in attacking strategy. [4]

Our proposed research encompasses a potential solution to these limitations by proposing an adaptive framework powered by AI/ML, with improvements on timely detection and mitigation, which are automated. This allows for continuous learning from the network data enabling the system to adapt in real-time against emerging and complex threats while keeping low overheads through a decrease in false positives and enhanced response time. [19]

Moreover, the framework is built to scale accordingly and being deployed in modern world scenarios like cloud and IoT networks with large number of traffic. In general, this study provides a computer- and intelligence-based solution to network security enhancement contributing to the evolution of adaptive cybersecurity systems for future use.

7. References

[1] Suthar, F. and Patel, N., 2023. A survey on ddos detection and prevention mechanism

[2] Dantas Silva, F.S., Silva, E., Neto, E.P., Lemos, M., Venancio Neto, A.J. and Esposito, F., 2020. A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios

[3] R. R. Brooks, L. Yu, I. Ozcelik, J. Oakley and N. Tusing, "Distributed Denial of Service (DDoS): A History

[4] Ma, Y., Liu, L., Liu, Z., Li, F., Xie, Q., Chen, K., Lv, C., He, Y. and Li, F., 2024. A survey of DDoS attack and defense technologies in multiaccess edge computing.

[5] Kopp, D. and Hohlfeld, O., 2025, June. DDoS on Repeat: Measuring Pulse-Wave DDoS in the Wild.

[6] Waleed, A., Jamali, A.F. and Masood, A.., 2022. Which open-source ids? snort, suricata or zeek

[7] GUPTA, A.B., AKTER, S., ISLAM, M., JABED, M.M.I. and FERDOUS, J., 2023. Smart Defense: AI-Powered Adaptive IDs for Real-Time Zero-Day Threat Mitigation."

[8] Ganeshan, S. and Ramasamy, R.K., 2026. A Systematic Review of Machine-Learning-Based Detection of DDoS Attacks in Software-Defined Networks..

[9] Tang, T.A., Mhamdi, L., McLernon, D., Zaidi, S.A.R., Ghogho, M. and El Moussa, F., 2020. DeepIDS: Deep learning approach for intrusion detection in software defined networking.

[10] N. Mohamed, "DDoS Attacks Mitigation: A Review of AI-Based Strategies and Techniques," 2024 .

[11] Peng, J.C., Cui, Y.H., Qian, Q., Guo, C., Jiang, C.H. and Li, S.F., 2021. ADVICE: Towards adaptive scheduling for data collection and DDoS detection in SDN

[12] M. Fathian and A. Seifousadati, “Real-time DDoS detection,” 2026.

[13] Dritsas, E. and Trigka, M., 2025. A survey on cybersecurity in IoT

[14] J. Lansky et al., "Deep Learning-Based Intrusion Detection Systems: A Systematic Review,"

[15] Handelman, G.S., Kok, H.K., Chandra, R.V., Razavi, A.H., Huang, S., Brooks, M., Lee, M.J. and Asadi, H., 2019. Peering into the black box of artificial intelligence: evaluation metrics of machine learning methods

[16] Samariya, D. and Thakkar, A., 2023. A comprehensive survey of anomaly detection algorithms. Annals of Data Science

[17] Roshan, S., Miche, Y., Akusok, A. and Lendasse, A., 2018. Adaptive and online network intrusion detection system using clustering and extreme learning machines.

[18] Reis, I., Baron, D. and Shahaf, S., 2019. Probabilistic random forest: A machine learning algorithm for noisy data sets

[19] Santos, L., Gonçalves, R., Rabadao, C. and Martins, J., 2023. A flow-based intrusion detection framework for internet networks

[20] Kreutz, D., Yu, J., Esteves-Verissimo, P., Magalhaes, C. and Ramos, F.M., 2018. The KISS principle in software-defined networking: A framework for secure communications.

[21] R. R. Katta and V. Dorai, "AI-Agent-Based Autonomous Defense Against DoS/DDoS in AI Data Centers," 2025 International Conference on Computer and Applications (ICCA), Bahrain, Bahrain, 2025

[22] I. Najar, A.A. and Naik, S.M., 2025. DDoS attack detection using CNN-BiLSTM with attention mechanism.