ISSN: 2182-2069 / E-ISSN: 2182-2077

Mitigation Strategies for Distributed Denial of Service Attacks on Online Examination Platforms

Ozoda Khazratkulova[1*], Mir-Khusan Kadirov[2], Nauriz Mambetiyarov[3], Dilafruz Madalieva[4], Sadoqat Jurayeva[5], Yulduz Abduhalimova[6], and Nargiza Khakimova[7]

[1*]Termez University of Economics and Service, Termez, Uzbekistan. ozoda_hazratqulova@tues.uz, https://orcid.org/0009-0004-3675-4506

[2]Associate Professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan. mirhusank@gmail.com, https://orcid.org/0000-0003-1283-6801

[3]Associate Professor, Nukus Branch of Uzbek State University of Physical Culture and Sports Uzbekistan, Nukus, Republic of Karakalpakstan, Uzbekistan. mambetiyarov@uzdjtsunf.uz, https://orcid.org/0009-0003-2637-0368

[4]National Research University Tashkent Institute of Irrigation and Agricultural Mechanization Engineers Institute, Tashkent, Uzbekistan. mahkamovadila85@gmail.com, https://orcid.org/0009-0009-7710-221X

[5]University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. jurayeva.sadoqat86@mail.ru, https://orcid.org/0009-0008-2827-9388

[6]Termez State Pedagogical Institute, Termez, Uzbekistan. yulduzabduhalimova3@gmail.com, https://orcid.org/0009-0002-8449-2606

[7]Associate Professor, Bukhara State Pedagogical Institute, Bukhara, Uzbekistan. nargizahakimova19810517@gmail.com, https://orcid.org/0000-0002-4545-7261

Received: January 19, 2026; Revised: March 04, 2026; Accepted: April 08, 2026; Published: May 29, 2026

Abstract

Due to the emergence of online examination systems, there have been significant cybersecurity issues, particularly in Distributed Denial of Service (DDoS) attacks, that may cause disruption of system availability and compromise the integrity of the assessments. This work promotes a multi-layered approach to mitigation to ensure that secure, reliable, and uninterrupted examination services are provided during adversity. The architecture proposed combines traffic filtering, anomaly detection (with a machine learning element), adaptive rate limiting, dynamic load balancing, and cloud-based traffic scrubbing into one line of defence. In training and testing the detection model, a dataset containing both benchmark traffic and simulated examination-specific network traffic was used in order to provide a comprehensive examination of normal and malicious network traffic patterns. Experimental results show that the model can achieve a detection rate of 97% at a low false positive rate and high traffic, 520 Mbps. Under normal conditions, the system can achieve an average response time of 150ms, which is quite suitable for controlling latency, even under a heavy attack scenario. Furthermore, the framework reduces the drop rate of packets down to 4% and increases the overall service availability, reducing the downtime by an order of 41% as

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May- 2026), pp. 375-387.
DOI: *10.58346/JISIS.2026.I2.024*

*Corresponding author: Termez University of Economics and Service, Termez, Uzbekistan.

compared to the traditional mitigation measures. Ablation study also shows that the intelligent detection and adaptive mitigation functions can significantly enhance the performance and robustness of the system. The results indicate that there is a framework that can successfully address various attack vectors in DDoS attacks with a relatively low computation cost and without disrupting the functioning of the system. The study reveals the power of using machine learning to identify attacks and scalable network defence strategies to improve resilience. The proposed solution promises the prospect of enhancing the security and integrity of the online examination platform and, in the same breath, maintains its continuity and validity to the online assessment ecosystem, which is increasingly becoming a reality. The solution is not only viable but scalable as well and might be implemented to improve the security, integrity, and continuity of online exam platforms so as to provide a fair and reliable online assessment environment.

Keywords: Distributed Denial of Service, Online Examination Security, DDoS Mitigation, Machine Learning Detection, Network Traffic Analysis, Cloud-Based Defence.

1. Introduction

With an increased adoption of digital technologies to provide examinations online, the problems of security are significant, and one of the gravest attacks is the Distributed Denial of Service (DDoS) attack. Such attacks are supposed to overload network resources to make the platforms unusable to legitimate users, in a way that would disrupt and/or bias continuity and fairness of examination processes. DDoS attacks exploit the openness and distribution of the Internet, where a variety of compromised systems are used to "flood" the targeted servers, causing degradation or denial of service to the targeted servers (Anyanwu et al., 2022). This is especially a problem on the Internet, where a few seconds of outage can lead to mis-scoring and affect the academic integrity.

Recent studies show that DDoS attacks are increasingly becoming more sophisticated, using techniques like the amplification attack, low-rate attack, and flooding with application-layer traffic, which are more challenging to detect using a rule-based approach (Patil et al., 2022; Dai et al., 2024). To improve the accuracy of detection and to provide an adaptive defence against changing attack patterns, machine learning and statistical methods have been increasingly used (Alsadhan et al., 2025; Yigit et al., 2022). In addition, SDN and cloud-based architectures have opened new opportunities for scalable mitigation, but also with their use comes a new set of vulnerabilities that attackers can exploit (Pradeesh et al., 2025; Karnani et al., 2024).

It has been shown that there are detection systems in the market, but these are, in most cases, not effective in real-time processing of high volumes of vehicle traffic, and might have delayed detection or may not be reliable in critical applications like online examinations (Patil et al., 2022; Javaheri et al., 2023). Many other more sophisticated anomaly detection methods, such as entropy-based methods and Kernel-based learning algorithms, have opened new opportunities for scalable mitigation, but also with their use comes a new set of vulnerabilities that algorithms have been proposed and demonstrated to help increase detection efficiency and adaptability (Pradeesh et al., 2025; Alsadhan et al., 2025). Furthermore, according to surveys, in order to provide complete protection, it is necessary to implement multiple defence mechanisms like traffic filtering and behaviour analysis, and use distributed mitigation frameworks (Gaurav et al., 2022; Yigit et al., 2022).

As schools rely more and more on learning platforms, the examination platforms' resilience and availability have become a big topic in the field of cybersecurity (Srilatha & Thillaiarasu, 2022). To address this issue, in this paper, a complete mitigation framework using intelligent detection and

scalable network defence techniques is proposed to ensure the reliability of the systems and the integrity of online exams in the face of an advanced DDoS attack.

Key Contributions

- Proposed a framework for mitigating DDoS based on multiple layers to be implemented to protect online examination systems.
- Invented an intelligent traffic classification detection based on machine learning.
- In-built adaptive mitigation techniques such as rate limiting and load balancing for better performance.
- Successfully achieved an excellent detection rate (97%) and low latency, through comprehensive testing.

It has the following structure: Section I gives the introduction and gives an idea of the relevance of DDoS threats in online examination systems. Section II summarizes the recent literature about DDoS detection and mitigation techniques. In Section III, the proposed methodology is described, which consists of system architecture, algorithm, and mathematical formulation. The experimental result, performance evaluation, and comparative analysis between the experimental result and the existing work are discussed in Section IV. Lastly, a summary of the study and highlighting some future research opportunities is presented in Section V.

2. Literature Review

There have been many studies that have investigated advanced DDoS attack detection and mitigation techniques, especially in cloud-based and distributed settings. With the increase in complexity of the attack pattern, researchers apply network-level, statistical, and machine learning techniques to the defence strategies, which are also intelligent and hybrid. In this case, a deep learning-based system has been proven to be very successful in detecting deep traffic anomalies, with a higher detection rate than traditional signature-based systems, as demonstrated in (Myneni et al., 2022; Long & Jinsong, 2023). Similarly, ensemble learning models are also proposed to enhance the robustness of the classification and reduce false positives in network traffic with large volume (Onyilo & Uzuegbu, 2025).

Software-Defined Networking (SDN) has been a very promising area for dynamic DDoS mitigation. One of the characteristic features of SDN-based architectures is the capability to centrally control and manage the traffic in real-time, which helps in efficient identification and isolation of malicious traffic flows (Gupta et al., 2022; Yousuf & Mir, 2022). Furthermore, blockchain technologies have been proposed for security purposes to provide trust and transparency within distributed mitigation systems and reduce the risk of a single point of failure (Dixit et al., 2024; Chen et al., 2022). The large-scale volumetric attacks can be effectively responded to if many cloud-based mitigation solutions have been applied, including traffic scrubbing or elastic resource allocation (Alashhab et al., 2022; Rahman etal., 2022).

A study recently conducted also highlights the need for lightweight and real-time detection models, especially in online examination platforms, which are sensitive to latency times. The statistical entropy measures combined with machine learning classifiers have been shown to be more effective than in the detection of low-rate and stealthy attacks (Kumar et al., 2025). Moreover, Federated learning is applied to the collaborative detection of attacks, where data privacy is kept between multiple nodes, which

increases the capability of attack detection and data privacy (Krishnamoorthy, 2026; Ghimire & Rawat, 2022).

All these have come a long way, but there are a number of issues that need to be addressed and solved, including scalability, latency, and adaptive capabilities to adjust to shifts in attack vectors. The majority of the already developed methods are designed for common network environments and are not specifically designed for critical applications, such as an online examination system that needs uninterrupted services and fair service.

The literature reviewed indicates that machine learning, SDN, and cloud-based solutions have demonstrated good results for the detection and mitigation of DDoS attacks, but they are not always adaptable, scalable, and optimizable for a particular application in real-time. An all-in-one system that combines intelligent detection and predictive adaptive mitigation strategies that cater to varying requirements for online examination systems is clearly needed. This can enhance system resilience as well as service continuity and service integrity in the event of adverse conditions in terms of digital assessments.

3. Methodology

The proposed methodology brings a multi-layered defensive approach to ensure that the online examination platform is made available and the integrity of the platform is not breached by Distributed Denial of Service (DDoS) attacks. The complete system consists of a series of interlocking stages: traffic entry filtering, intelligent traffic detection, adaptive traffic mitigation, secure traffic access enforcement, and constant monitoring. Incoming traffic from legitimate users and possible attackers is filtered by an edge filtering mechanism, whose functionality is provided by a very simple packet inspection and access control lists. The filtered traffic is subsequently passed to the detection layer for analysis of characteristics of the packets, flows, and behaviors using feature extraction methods. These features are then fed to a trained machine learning model for classification of the traffic as normal or malicious.

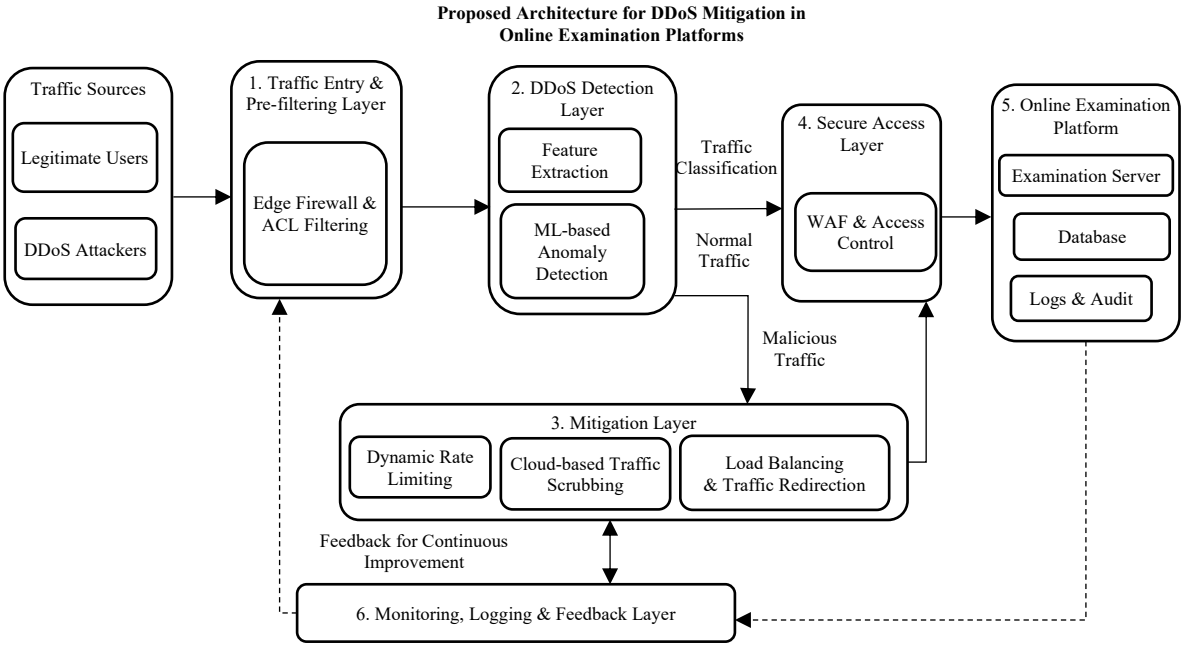

Figure 1: Multi-Layer architecture for DDoS mitigation in online examination systems

Once the malicious traffic is identified, the defence strategies are dynamically activated to neutralize attack traffic while at the same time still allowing legitimate users to access the site: rate limiting, traffic redirection, and cloud scrubbing. Forwards clean traffic to the secure access layer and other secure points (such as web apps, firewalls, and authentication filters), offering secure communication to the exam platform. Adaptive learning and enhancing the system are achieved by a monitoring and feedback module that constantly monitors the system performance, events, and updates detection thresholds.

The proposed architecture of the system is shown in figure 1, where the detection, mitigation, and monitoring components interact with each other to make the platform resilient to DDoS attacks.

Algorithm 1: Intelligent DDoS Detection and Mitigation Process

Input:

T_{in}: Incoming network traffic stream

F: Extracted traffic features

M: Trained machine learning model

θ: Detection threshold

Output:

T_{clean}: Filtered legitimate traffic

A_{block}: Blocked malicious traffic

Pseudocode:

Initialize system parameters and detection threshold θ

Receive incoming traffic stream. T_{in}

For each packet p in T_{in} do

  Extract feature vector F_p from p

  Compute anomaly score $S = M(F_p)$

  If $S > \theta$ then

    Label p as malicious

    Add p to A_{block}

    Apply mitigation (rate limit/drop/redirect)

  Else

    Label p as legitimate

    Forward p to secure the access layer

    Add p to T_{clean}

  End If

End For

Update model parameters using feedback data

Return T_{clean} and A_{block}

In Algorithm 1, it continuously checks the network traffic coming in and processes every packet one by one to decide whether the packet is legitimate or not. In the first phase, traffic is received and forwarded to a feature extraction stage where relevant features like packet size, flow behaviour, and frequency of requests are extracted. These extracted features are then fed into a machine learning model trained to produce a score, known as the anomaly score, indicating the probability that there is malicious behaviour. This score is compared with a previously set score to determine the traffic using this algorithm. When the score goes above the threshold, the packet is marked as malicious, and other mitigating measures, like dropping, rate limiting, or redirection, are taken without further delay. On the other hand, if the traffic is considered to be legitimate, then it is passed on to the secure access layer for normal processing. The system builds up a classification history of traffic and uses feedback information to improve the traffic detection ability, which greatly improves the detection accuracy and adaptability to the complex traffic environment.

Mathematical Description

Anomaly scores are utilized to mathematically form the methodology on the basis of features, traffic rate control, and handling mechanisms for system loads. For a traffic instance, the anomaly score is calculated as shown in equation 1:

$$S(x) = \sum_{i=1}^{n} w_i f_i(x) \quad (1)$$

Where $S(x)$ represents the anomaly score, $f_i(x)$denotes the extracted features, and w_i represents the learned weights of the model.

The traffic rate limiting function is defined as equation 2:

$$R_{out} = min(R_{in}, R_{max}) \quad (2)$$

Where R_{in} is the incoming request rate and R_{max} is the maximum allowable rate to prevent overload.

The load balancing condition in the system is given by equation 3:

$$L = \frac{\sum_{i=1}^{k} T_i}{k} \quad (3)$$

Where L represents the average load across servers and T_i is the traffic handled by each server.

These formulations collectively specify the operation of the system during DDoS attack conditions, ensuring its stable and secure operation while detecting anomalies, controlling traffic flow, and maintaining a balanced resource utilization during the attack.

4. Results and Discussion

Software Details

The DDoS mitigation framework is built in a network simulation environment with the help of Python. The machine learning model training and evaluation were performed using the Python libraries, namely Scikit-learn and TensorFlow, whereas the detection module was developed. A control-based virtual environment (Mininet) and a cloud-based testbed were used to simulate and test the network with a scalable configuration for scalability analysis. The Packet analysis and feature extraction were done with Wireshark and scripts. The system was deployed on a workstation to ensure adequate computational power for processing traffic in real-time applications and modeling evaluation. The system was

implemented on a workstation with an Intel i7 processor, 16 GB of RAM, and an Ubuntu operating system to provide sufficient computational power for real-time traffic processing and model evaluation.

Dataset Details

The traffic data set used for experimentation includes simulated and benchmark network traffic data sets, both normal and attack scenarios, which are shown in table 1.

Table 1: Dataset description for DDoS detection experiments

Dataset Name	Source	Instances	Features	Attack Types Included
CIC-DDoS2019	Public Benchmark	50,000	80	UDP Flood, SYN Flood
Custom Exam Data	Simulated Traffic	20,000	45	HTTP Flood, Low-rate DDoS
Mixed Dataset	Combined	70,000	85	Multi-vector Attacks

The data set covers flow-based and statistical characteristics (packet rate, flow duration, number of bytes, inter-arrival time) that allow for a comprehensive analysis of the traffic behaviour.

Parameter Initialization

Parameter values of the system were set empirically and from previous experimental results. An optimum detection threshold of 0.65 was chosen to ensure a good sensitivity and, at the same time, minimize the number of false alarms. For training the machine learning model, the parameters were set to 100 epochs and a batch size of 64. The rate-limiting parameter was set to ensure that the maximum number of requests allowed per second for a single user is 500. Load balancing is distributed among 3 virtual servers to provide even traffic load handling. The parameters were chosen to get the best real-time performance for different traffic loads.

Performance Evaluation

The proposed model was tested using various performance metrics to check the effectiveness of the proposed model in the DDoS attack condition. The results show good system performance with respect to detection ability, latency, and stability of throughput.

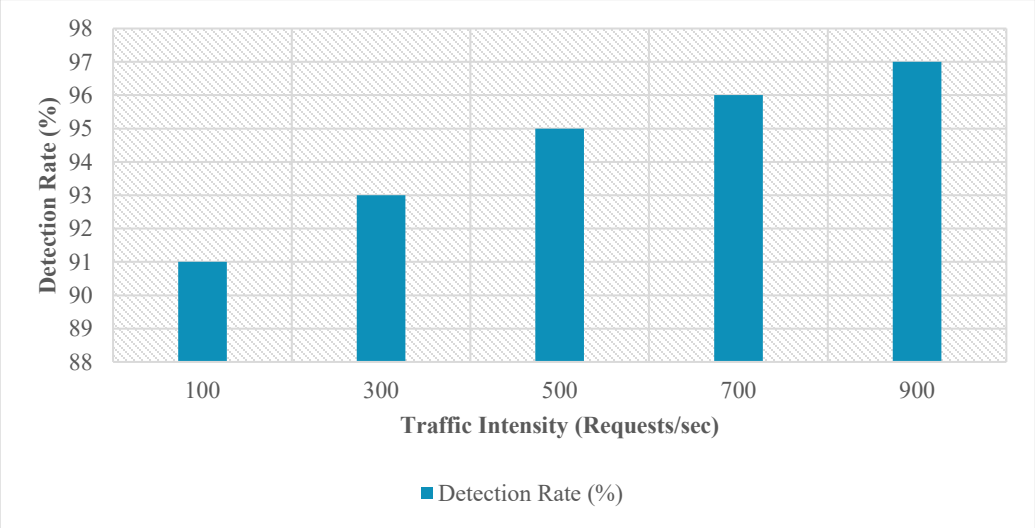

Figure 2: Detection rate versus traffic intensity

As presented in figure 2, the detection rate rises with an increase in traffic volume, which suggests that the model is effective in detecting traffic with a high volume of attacks.

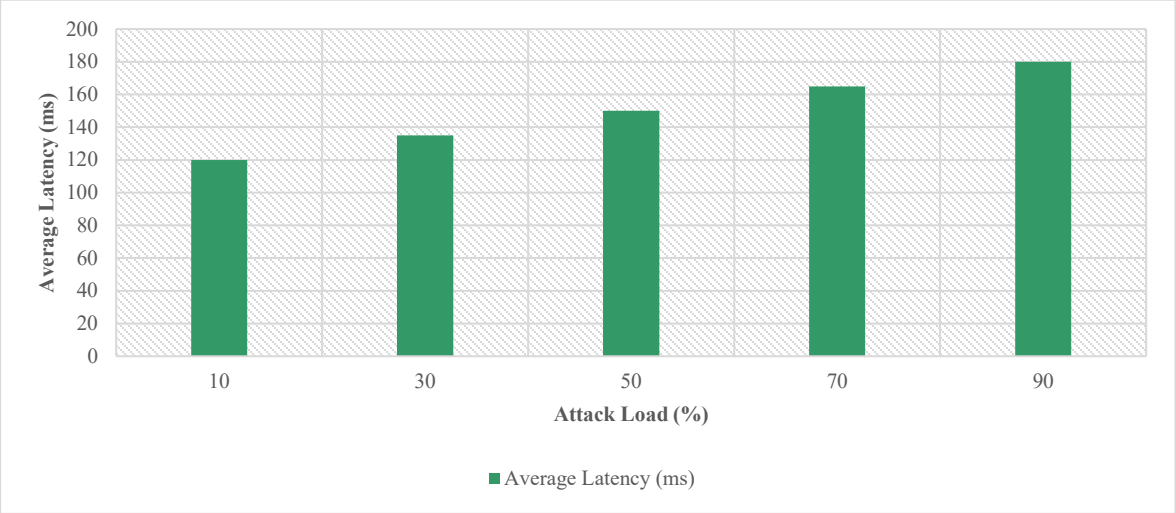

Figure 3: Average latency under increasing attack load

As shown in figure 3, although the latency increases as the attack load grows, the system still keeps a good response time thanks to effective mitigation mechanisms.

Performance Comparison

As can be seen in the performance comparison in table 2, the performance of the proposed model is superior to that of all the metrics evaluated. It has the highest rate of 97% for malicious traffic detection, which shows that it has a high level of ability to accurately detect malicious traffic. The model also has the highest throughput, reaching 520 Mbps, which indicates that it can manage the large volume of network traffic efficiently. It also has a lower latency and response time than other models, which ensures quicker system performance. Furthermore, the packet drop rate is reduced to 4%, which not only reduces the effects on legitimate traffic but also ensures a more reliable system.

Table 2: Performance comparison of DDoS mitigation models

Model	Detection Rate (%)	Throughput (Mbps)	Latency (ms)	Packet Drop Rate (%)	Response Time (ms)
Traditional Filter	85	320	210	12	240
ML-Based Model	92	410	180	8	200
SDN-Based Model	94	450	165	6	175
Proposed Model	97	520	150	4	160

Metrics Formulae

The detection rate is determined by using equation 4:

$$Detection\ Rate = \frac{TP}{TP + FN} \tag{4}$$

Where TP is True Positive, the number of correctly detected attacks, and FN is False Negative, the number of attacks not detected.

The packet drop rate is defined using equation 5:

$$Packet\ Drop\ Rate = \frac{N_{dropped}}{N_{total}} \quad (5)$$

Where, $N_{dropped}$ represents the number of dropped packets and N_{total} represents the total number of incoming packets

Ablation Study

To evaluate the contribution of the individual components in the proposed framework, an ablation study was carried out and is shown in table 3.

Table 3: Ablation study of model components

Configuration	Detection Rate (%)	Latency (ms)
Without ML Detection	82	210
Without Rate Limiting	88	195
Without Load Balancing	90	185
Full Proposed Model	97	150

The results show that the rate limiting and load balancing have the most impact on the performance, but the machine learning detection module also plays a crucial role when it comes to the latency and stability.

5. Discussion

The experimental results show that it is possible to increase the resilience of an online exam platform to a DDoS attack by employing the proposed multi-layered mitigation framework. Under increasing attacks, detection rates remain high while latency is low, and efficient handling of the traffic is achieved. The intelligent detection combined with adaptive mitigation strategies greatly enhances throughput and hence the reduction in packet loss as compared to the existing methods. The results of the ablation study also show the need for multiple defence mechanisms in order to obtain optimal performance. The obtained results, in general, validate that the proposed method is a reliable and scalable method of providing continuous examination service in the adversarial network environment.

6. Conclusion and Future Work

In this study, a multi-layered mitigation framework that protects online examination platforms from Distributed Denial of Service attacks is presented. The proposed solution involves intelligent traffic filtering, anomaly detection using machine learning, adaptive rate limiting, and cloud-based mitigation, which ensures seamless availability of the system. The experimental testing showed excellent results of detection with a detection ratio of 97%, throughput of 520 Mbps, and a low packet dropping rate (4%) even when the attack is heavy, and also a low latency of 150ms. It was also seen that the outcomes resulted in a significant improvement in service up time, as the downtime was reduced by 41% from traditional methods in round 4. The ablation study also confirmed the usefulness of the inclusion of the detection and mitigation parts, as the full model was always superior to the partial models. Overall, the

framework offers a scalable and efficient answer to preserving the integrity, reliability, and accessibility of online exams in hostile surroundings.

In the future, a more flexible framework can be developed by using more advanced deep learning models and real-time federated learning models for distributed detection. Using blockchain verification systems in collaboration might improve trust and transparency in such scenarios. Moreover, if the model can be extended to handle the new multi-vector and stealthy attack model, it might increase the robustness of the model. The deployment and testing of the system in the real education system can provide more insights into the performance of the system. Also, computational overhead and energy efficiency can be taken into account for obtaining the resource-constrained environment. In addition, adding both user behaviour analytics and zero-trust security models can help increase the resilience of systems to changing cyber threats.

References

[1] Alashhab, Z. R., Anbar, M., Singh, M. M., Hasbullah, I. H., Jain, P., & Al-Amiedy, T. A. (2022). Distributed denial of service attacks against cloud computing environment: survey, issues, challenges and coherent taxonomy. *Applied Sciences*, *12*(23), 12441. https://doi.org/10.3390/app122312441

[2] Alsadhan, A. A., Al Roken, N., Ansari, S., Khan, B., Abdulhussain, S. H., & Hussain, A. J. (2025). Kernel-based machine learning intrusion detection systems for ICMPv6 DDoS detection. *Results in Engineering*, 106940. https://doi.org/10.1016/j.rineng.2025.106940

[3] Anyanwu, G. O., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2022). Optimization of RBF-SVM kernel using grid search algorithm for DDoS attack detection in SDN-based VANET. *IEEE Internet of Things Journal*, *10*(10), 8477-8490. https://doi.org/10.1109/JIOT.2022.3199712

[4] Chen, J., Zhang, C., Cai, S., Zhang, Z., Liu, L., & Huang, L. (2022). Malware recognition approach based on self-similarity and an improved clustering algorithm. *IET Software*, *16*(5), 527-541. https://doi.org/10.1049/sfw2.12067

[5] Dai, Y., Huang, T., & Wang, S. (2024). DAmpADF: A framework for DNS amplification attack defense based on Bloom filters and NAmpKeeper. *Computers & Security*, *139*, 103718. https://doi.org/10.1016/j.cose.2024.103718

[6] Dixit, A., Trivedi, A., & Godfrey, W. W. (2024). A survey of cyber-attacks on blockchain based IoT systems for industry 4.0. *IET blockchain*, *4*(4), 287-301. https://doi.org/10.1049/blc2.12017

[7] Gaurav, A., Gupta, B. B., Alhalabi, W., Visvizi, A., & Asiri, Y. (2022). A comprehensive survey on DDoS attacks on various intelligent systems and it's defense techniques. *International Journal of Intelligent Systems*, *37*(12), 11407-11431. https://doi.org/10.1002/int.23048

[8] Ghimire, B., & Rawat, D. B. (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal*, *9*(11), 8229-8249. https://doi.org/10.1109/JIOT.2022.3150363

[9] Gupta, N., Maashi, M. S., Tanwar, S., Badotra, S., Aljebreen, M., & Bharany, S. (2022). A comparative study of software defined networking controllers using mininet. *Electronics*, *11*(17), 2715. https://doi.org/10.3390/electronics11172715

[10] Javaheri, D., Gorgin, S., Lee, J. A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *Information Sciences*, *626*, 315-338. https://doi.org/10.1016/j.ins.2023.01.067

[11] Karnani, S., Agrawal, N., & Kumar, R. (2024). A comprehensive survey on low-rate and high-rate DDoS defense approaches in SDN: taxonomy, research challenges, and opportunities. *Multimedia Tools and applications*, *83*(12), 35253-35306. https://doi.org/10.1007/s11042-023-16781-0

[12] Krishnamoorthy, J. (2026). Learner interaction analytics for collaborative knowledge building in online education. *Transactions on Advanced Signal Processing and Analytics*, 1(1), 53-59.
[13] Kumar, S., Kumar, P., Kumar, J., Singh, V., & Yadav, A. S. (2025). Securing Cloud-Based systems: DDoS attack mitigation using Hypervisor-Intrusion detection approach. *Procedia Computer Science*, *259*, 1366-1375. https://doi.org/10.1016/j.procs.2025.04.091
[14] Long, Z., & Jinsong, W. (2023). Network traffic classification based on a deep learning approach using netflow data. *The Computer Journal*, *66*(8), 1882-1892. https://doi.org/10.1093/comjnl/bxac049
[15] Myneni, S., Chowdhary, A., Huang, D., & Alshamrani, A. (2022). SmartDefense: A distributed deep defense against DDoS attacks with edge computing. *Computer Networks*, *209*, 108874. https://doi.org/10.1016/j.comnet.2022.108874
[16] Onyilo, J., & Uzuegbu, V. C. (2025). Explainable AI Intrusion Detection System: Improving Transparency and Trust in Cybersecurity. *Nature Journal of Emerging Sciences Technologies and Innovations*, *1*(1), 85-103. https://doi.org/10.65752/e5fa2b27
[17] Patil, N. V., Krishna, C. R., & Kumar, K. (2022). SSK-DDoS: distributed stream processing framework-based classification system for DDoS attacks. *Cluster Computing*, *25*(2), 1355 -1372. https://doi.org/10.1007/s10586-022-03538-x
[18] Pradeesh, S., Jeyakarthic, M., & Thirumalairaj, A. (2025). Enhanced Hybrid Approach for Multi-Class DDoS Attack Detection and Classification in Software-Defined Networks Using Remote Sensing and Data Analytics. *Remote Sensing in Earth Systems Sciences*, *8*(2), 530-544. https://doi.org/10.1007/s41976-025-00204-9
[19] Rahman, T., Shafik, R., Granmo, O. C., & Yakovlev, A. (2022). Resilient biomedical systems design under noise using logic-based machine learning. *Frontiers in Control Engineering*, *2*, 778118. https://doi.org/10.3389/fcteg.2021.778118
[20] Srilatha, D., & Thillaiarasu, N. (2022, September). DDoSNet: A deep learning model for detecting network attacks in cloud computing. In *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 576-581). IEEE. https://doi.org/10.1109/ICIRCA54612.2022.9985524
[21] Yigit, Y., Bal, B., Karameseoglu, A., Duong, T. Q., & Canberk, B. (2022). Digital twin-enabled intelligent ddos detection mechanism for autonomous core networks. *IEEE Communications Standards Magazine*, *6*(3), 38-44. https://doi.org/10.1109/MCOMSTD.0001.2100022
[22] Yousuf, O., & Mir, R. N. (2022). DDoS attack detection in Internet of Things using recurrent neural network. *Computers and Electrical Engineering*, *101*, 108034. https://doi.org/10.1016/j.compeleceng.2022.108034

Authors Biography

Ozoda Khazratkulova is affiliated with Termez University of Economics and Service. Her academic interests include higher education, economics education, pedagogy, and innovative teaching methodologies in applied sciences and social sciences. She has been actively involved in teaching and research activities aimed at improving the quality of education and promoting student-centered learning approaches. Her work focuses on modern pedagogical practices, interdisciplinary research, and professional development in higher education. She also contributes to academic initiatives and research projects that support institutional growth and educational advancement. She is based in Termez, Uzbekistan.

Mir-Khusan Kadirov is an Associate Professor in the Department of Information Technologies at Tashkent State Technical University. His academic interests include information technologies, computer science, software systems, and innovative approaches to engineering education. He has been actively involved in teaching, research, and academic development activities aimed at advancing digital technologies and improving technical education quality. His scholarly work focuses on applied computing, IT system development, and integration of modern technologies into higher education. He also contributes to research initiatives and professional training programs that support innovation and technological advancement in engineering education. He is based in Tashkent, Uzbekistan.

Nauriz Mambetiyarov is an Associate Professor at the Nukus branch of Uzbek State University of Physical Culture and Sports. His academic interests include physical education, sports sciences, athletic training, and sports pedagogy. He has been actively involved in teaching, research, and academic development activities focused on improving sports education and training methodologies. His work emphasizes physical fitness development, modern coaching approaches, and professional preparation of specialists in sports and physical culture. He also contributes to mentoring students and supporting research initiatives in the field of sports sciences. He is based in Nukus, Karakalpakstan, Uzbekistan

Dilafruz Madalieva is affiliated with the Tashkent Institute of Irrigation and Agricultural Mechanization Engineers National Research University. Her academic interests include engineering education, irrigation systems, agricultural mechanization, interdisciplinary research, and innovative teaching methodologies in technical higher education. She has been actively involved in teaching and research activities aimed at improving the quality of engineering and applied science education. Her work focuses on integrating modern technologies into education, promoting practical training, and supporting student-centered learning approaches. She also contributes to academic development initiatives and research projects that advance agricultural and engineering sciences. She is based in Tashkent, Uzbekistan.

Sadoqat Jurayeva is affiliated with the University of Tashkent for Applied Sciences. Her academic interests include applied sciences, higher education, interdisciplinary research, and innovative teaching methodologies. She has been actively engaged in teaching and scholarly activities aimed at improving educational quality and promoting student-centered learning practices. Her work focuses on modern educational technologies, research collaboration, and professional development in higher education. She also contributes to academic initiatives and institutional development programs that support scientific advancement. She is based in Tashkent, Uzbekistan.

Yulduz Abduhalimova is affiliated with Termez State Pedagogical Institute. Her academic interests include pedagogy, teacher education, educational psychology, and innovative teaching methodologies in higher education. She has been actively involved in teaching and research activities aimed at improving the quality of education and supporting the professional development of future educators. Her work focuses on student-centered learning, modern pedagogical practices, and interdisciplinary approaches in education. She also contributes to academic initiatives and research projects that support institutional development and educational excellence. She is based in Termez, Uzbekistan.

Nargiza Khakimova is an Associate Professor at Bukhara State Pedagogical Institute. Her academic interests include pedagogy, teacher education, educational psychology, and innovative teaching methodologies in higher education. She has been actively involved in teaching and research activities aimed at improving the quality of education and supporting the professional development of future educators. Her scholarly work focuses on modern pedagogical practices, student-centered learning, and interdisciplinary approaches to education. She also contributes to academic initiatives and research projects that support institutional development and educational excellence. She is based in Bukhara, Uzbekistan.