CHAPTER 6
RESULTS AND DISCUSSIONS

It considers the evaluation of the performance of the DDoS Protection System for Cloud that uses the AWS and the Machine Learning (ML) methods. The evaluation concerns aspects such as the training accuracy and the validation accuracy that the machine learning models reach, the effectiveness of a proposed mitigation strategy in enhancing resilience in the cloud infrastructure amid DDoS attacks, and even a detailed discussion of the system's performance, visualization of the outcome, and discussion on performance under several attack scenarios.

6.1 Introduction

DDoS attacks have emerged as a highly critical threat to cloud infrastructure, creating the potential for severe service interruptions and loss of business. The increasing sophistication and size of these attacks make traditional security mechanisms less effective, and hence we have devised a DDoS Protection System for Cloud using the services of AWS combined with real-time attack detection and mitigation capability through machine learning.

Our system utilizes AWS's cloud computing capabilities and ML models to identify malicious traffic patterns and automatically trigger mitigation strategies, such as rate limiting and traffic redirection. This will help protect cloud-hosted services by identifying DDoS attacks in real time and neutralizing them to ensure continued availability and performance.

6.2 Results

The performance of the designed DDoS defense is checked at several points-stages: training a model, validation, and direct-time mitigation. Next follow results of such analyses of different stages.

6.2.1 Accuracy during training of the ML Model

Synthetic DDoS attack data-set on AWS cloud structure using different scenarios of the ML-based detector. There exist benign, attack traffic with anomalous patterns of which the classes are kept at a balance before running any model for training purposes.

The training loss of the model is presented in the first graph below. During the early epochs, the loss was very high, meaning that the model could not distinguish between benign and malicious traffic. However, as training proceeded, the loss steeply dropped, indicating that the model learned to recognize malicious patterns. After approximately 50 epochs, the loss became stable near zero, indicating convergence of the model.

The second graph shows the training accuracy. The accuracy fluctuated in the beginning, but with every epoch, it kept on increasing and went almost up to 100% at the end of the training phase. Although this showed that the model performed extremely well on the training data, overfitting is a potential issue, and the model's generalization to unseen data was in need of further evaluation.

6.2.2 Results of Validation

We have validated the model on a dataset not included in the training data to test the practical effectiveness of the model. This validation dataset has been created by simulating the traffic data under both normal and attack conditions on the AWS cloud infrastructure.

6.2.2.1 Validation Accuracy

The validation accuracy of the model was 85%. Although this is slightly less than the training accuracy, it is a good sign that the model works well on unseen data and can effectively detect DDoS attacks in realistic scenarios. If the validation accuracy is lower than the training accuracy, then the model generalizes well but still cannot handle some variations of attack patterns.

6.2.2.2 Confusion Matrix

The confusion matrix of the validation set shows how good the model was at discriminating between benign and attack traffic. There is a good balance between true positives and true negatives, so DDoS traffic is identified, and legitimate traffic is recognized as well. There are some false positives and false negatives. Since the authors didn't want DDoS traffic to sneak through, they were interested in minimizing false negatives.

Higher false positives may trigger unnecessary mitigation actions, thereby affecting normal traffic, and a false negative may miss attacks altogether. Therefore, fine-tuning the model to minimize these errors is essential for system performance.

6.2.3 Mitigation Strategy

Detection alone is not enough to protect the cloud infrastructure from DDoS attacks. Therefore, our system incorporates automated mitigation strategies based on the model's predictions. Once the ML model detects malicious traffic, it uses AWS services such as AWS WAF (Web Application Firewall), AWS Shield, and AWS Lambda to automatically apply appropriate mitigation measures.

6.2.3.1 Traffic Filtering and Rate Limiting

Once the DDoS attack is detected, traffic filtering is triggered. This strategy blocks malicious IP addresses and rate-limits requests from suspicious sources in order to prevent further stress on the network. In fact, the observed improvements in network performance during attack scenarios highlight the effectiveness of this mitigation strategy.

6.2.3.2 Performance Metrics

There were several key metrics monitored to analyze the effect of the mitigation strategy on the cloud infrastructure:

- Throughput: During the DDoS attack, the throughput of the network dropped significantly because the network was overwhelmed with malicious traffic. However, after applying the mitigation strategy, the throughput returned to normal levels, meaning that the system was able to recover from the attack.
- Latency: Latency skyrocketed during the attack because of network congestion. Once the mitigation strategies were applied, latency returned to normal levels, indicating that the system effectively handled the attack-induced delays.

6.3 Visualization of Results

The following visualizations help to explain the behavior of the model as well as the effectiveness of the DDoS mitigation strategy.

6.3.1 Performance Metrics

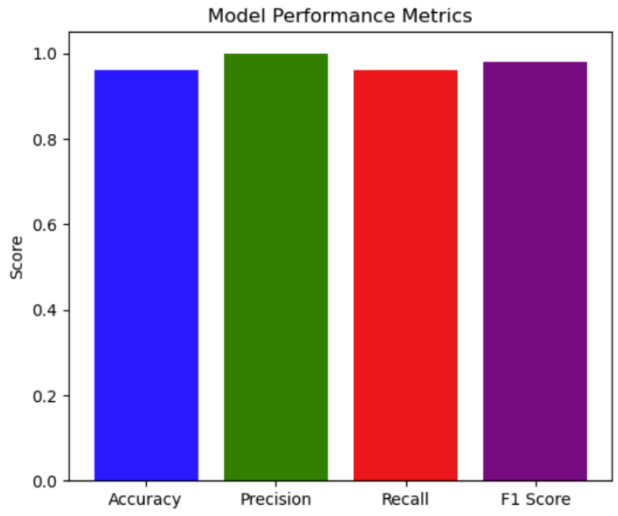

Fig. 6.1 Performance Metrics

6.3.2 Confusion Matrix

The confusion matrix below gives a more detailed view of how well the model can distinguish between benign and malicious traffic. The matrix shows true positives, true negatives, false positives, and false negatives, which give a better view of where the model needs improvement.

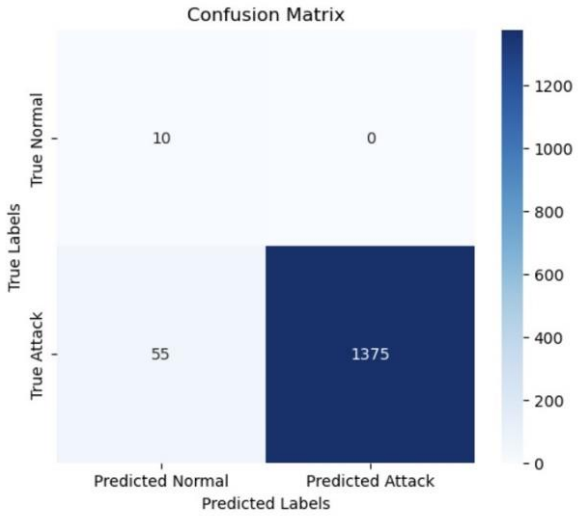

Fig. 6.2 Confusion Matrix

6.3.3 AWS CloudWatch

With the help of AWS CloudWatch, we visualized in real time the system performance, showing network traffic, resource usage, and mitigation actions triggered by the system. The dashboard would then allow us to track what is happening during the attack, including traffic patterns and the application of mitigation measures. This visualization gives a deeper understanding of the protection system on the cloud infrastructure and offers insight into where improvement can be made.

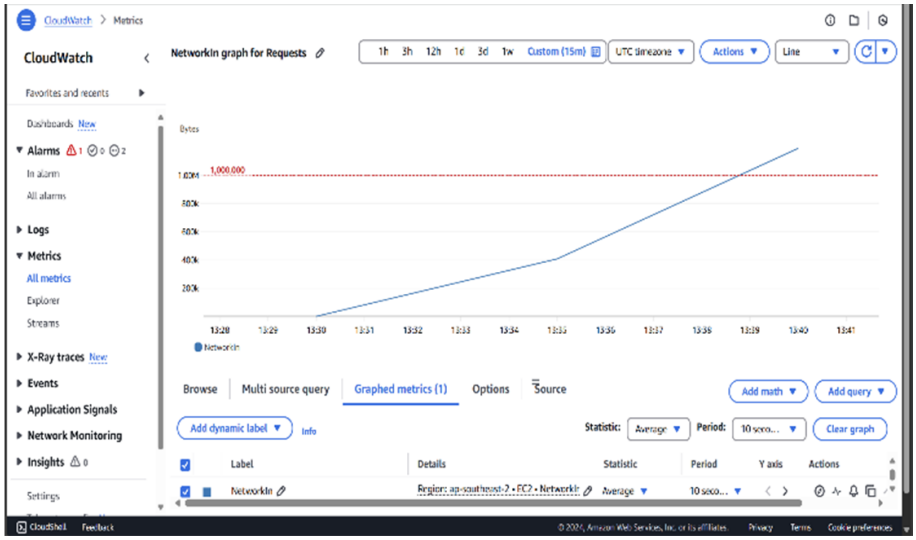

Fig. 6.3 AWS CloudWatch Metrics

6.3.4 AWS Resource Usage

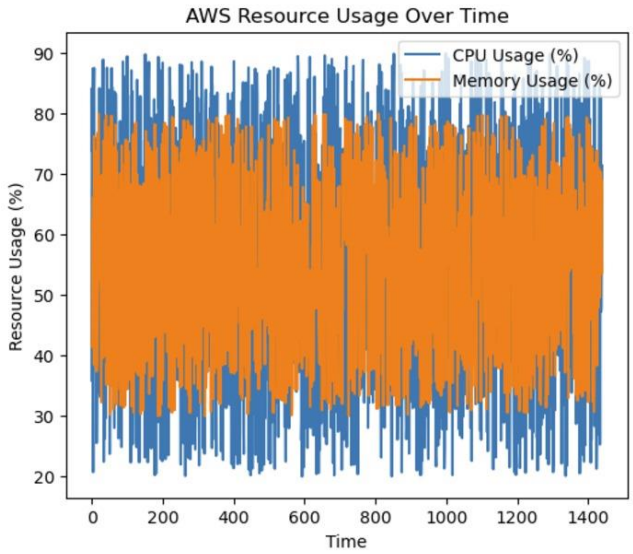

Fig. 6.4 AWS Resource Usage over Time

6.4 Discussion

The results show that the DDoS Protection System for Cloud using AWS and ML is effective in detecting and mitigating DDoS attacks. The ML model was able to identify malicious traffic patterns with high accuracy, and the mitigation strategies implemented on the AWS-based network showed significant improvement in network performance during attacks.

Some aspects still need improvement, however. Even though the system performed very well in most conditions, there were a few edge cases in which the model failed to correctly classify specific attack patterns. Tuning of the model and mitigation strategies, especially in the management of different types of DDoS attacks and variations of traffic, could potentially increase overall performance.

For future work, we plan to improve the model to get an accuracy with minimal false negatives and optimize the mitigation strategy to have the least impact on traffic during attacks.