|  |  |  |
| --- | --- | --- |
|  | **TABLE OF CONTENTS** |  |
|  |  |  |
|  | **ABSTRACT** | **ix** |
|  | **LIST OF FIGURES** | **x** |
|  | **ABBREVIATIONS** | **xi** |
|  | **1 INTRODUCTION** | **1** |
|  | 1.1  The Emerging Threat of DDoS Attacks for Cloud Environments | 1 |
|  | 1.2  Impact of Real-time Detection and Mitigation | 1 |
|  | 1.3  DDoS Protection System with AWS and Machine Learning | 2 |
|  | 1.4  Contribution and Future Prospects | 3 |
|  | **2      LITERATURE SURVEY** | **4** |
|  | 2.1  Challenges of DDoS Attacks in Cloud Environments | 4 |
|  | 2.2  AWS-Based Solutions for DDoS Mitigation | 5 |
|  | 2.3  Role of Machine Learning in DDoS Defense | 5 |
|  | 2.4  Innovative Architectures for Cloud Security | 6 |
|  | 2.5  Conclusion | 6 |
|  | **3      SYSTEM ARCHITECTURE AND DESIGN** | **7** |
|  | 3.1  Layered Architecture Overview | 7 |
|  | 3.1.1  Traffic Data Generation Layer | 7 |
|  | 3.1.2  Anomaly Detection Layer | 7 |
|  | 3.1.3  Load Simulation and Testing Layer | 7 |
|  | 3.1.4  Mitigation Layer | 8 |
|  | 3.1.5  Monitoring and Report Layer | 8 |
|  | 3.2  Core Components | 8 |
|  | 3.2.1  Traffic Data Simulation and Anomaly Detection | 8 |
|  | 3.2.2  Load Testing Framework | 9 |
|  | 3.2.3  Cloud Based Mitigation | 9 |
|  | 3.3  Scalability and Performance Considerations | 9 |
|  | 3.3.1  Scalability | 9 |
|  | 3.3.2  Low Latency Operations | 9 |
|  | 3.3.3  Adaptability | 9 |
|  | 3.4  Integration with AWS Infrastructure | 10 |
|  | 3.4.1   CloudWatch Monitoring and Alerts | 10 |
|  | 3.4.2   EC2 Deployment and Management | 10 |
|  | 3.4.3 Legacy System Compatibility | 10 |
|  | 3.5  Validation of System Design | 10 |
|  | 3.6  Summary | 11 |
|  | **4       METHODOLOGY** | **12** |
|  | 4.1  Addressing Cloud Security using AI and Cloud Native Techniques | 12 |
|  | 4.2  Synthetic Traffic Data Generation | 12 |
|  | 4.3  Anomaly Detection using Machine Learning | 13 |
|  | 4.4  Load Testing with Apache JMeter | 14 |
|  | 4.4.1  Simulation of Realistic Traffic | 14 |
|  | 4.4.2  DDoS Attack Resilience Test | 14 |
|  | 4.5  Cloud Integration with AWS | 15 |
|  | 4.5.1  Deploying on AWS | 15 |
|  | 4.5.2  Traffic Monitoring with CloudWatch | 15 |
|  | 4.5.3  Auto Scaling and Load Balancing | 15 |
|  | 4.6  Validation and Mitigation Strategies | 17 |
|  | 4.6.1   Simulation of Attack Scenarios | 17 |
|  | 4.6.2   Mitigation with Blocking Mechanisms | 17 |
|  | 4.6.3   Performance Evaluation | 17 |
|  | 4.7  Summary | 17 |
|  | **5        CODING AND TESTING** | **18** |
|  | 5.1  Traffic Data Generation | 18 |
|  | 5.1.1   Pseudocode | 18 |
|  | 5.1.2  Testing the Traffic Data Generation | 19 |
|  | 5.2  Anomaly Detection with Isolation Forest | 19 |
|  | 5.2.1   Pseudocode | 19 |
|  | 5.2.2   Testing Anomaly Detection | 20 |
|  | 5.3  Load Testing with Apache JMeter | 20 |
|  | 5.4  Cloud Integration with AWS | 21 |
|  | 5.4.1  AWS CloudWatch Setup | 21 |
|  | 5.4.2  Testing AWS CloudWatch Alerts | 21 |
|  | 5.5  Auto Scaling and Load Balancing | 21 |
|  | 5.5.1  Testing Auto Scaling and Load Balancing | 21 |
|  | 5.5.2  Testing Load Balancer Behaviour | 22 |
|  | 5.6  System Validation and Performance Evaluation | 22 |
|  | **6        RESULT AND DISCUSSIONS** | **23** |
|  | 6.1  Introduction | 23 |
|  | 6.2  Results | 23 |
|  | 6.2.1  Accuracy during training of the ML Model | 23 |
|  | 6.2.2   Results of Validation | 24 |
|  | 6.2.2.1  Validation Accuracy | 24 |
|  | 6.2.2.2  Confusion Matrix | 24 |
|  | 6.2.3   Mitigation Strategy | 25 |
|  | 6.2.3.1  Traffic Filtering and Rate Limiting | 25 |
|  | 6.2.3.2  Performance Metrics | 25 |
|  | 6.3  Visualization of Results | 26 |
|  | 6.3.1  Performance Metrics | 26 |
|  | 6.3.2   Confusion Matrix | 26 |
|  | 6.3.3   AWS CloudWatch | 27 |
|  | 6.3.4   AWS Resource Usage | 27 |
|  | 6.4  Discussion | 28 |
|  | **7        CONCLUSION AND FUTURE ENHANCEMENT** | **29** |
|  | 7.1  Summary of Findings | 29 |
|  | 7.1.1  DDoS Detection with AWS and ML | 29 |
|  | 7.1.2  Real-Time Mitigation on AWS | 30 |
|  | 7.1.3  Performance and Scalability | 30 |
|  | 7.2  Future Improvements | 30 |
|  | 7.2.1   Real-Time Mitigation Enhancements | 30 |
|  | 7.2.2  Broadening Attack Scenarios | 31 |
|  | 7.2.3   Scalability and Distributed Architecture | 31 |
|  | 7.2.4   Adaptive Learning for Evolving Attacks | 31 |
|  | 7.2.5   Integration with other Security Tools | 32 |
|  | 7.3  Conclusion | 32 |
|  | **REFERENCES** | **33** |
|  | **APPENDIX** |  |
|  | **A CONFERENCE PUBLICATION** | **37** |
|  | **B CONFERENCE PLAGIARISM REPORT** | **38** |