**Software Requirements Specification**

**Topic** - DDoS Protection System for Cloud

**Team** – Saksham Dharmik (112215157)

Deepesh Patil (112215055)

Naman Goyal (112215120)

Tanishq Ingole (112215076)  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Table of Contents :**

**1. Introduction**1.1 Purpose  
1.2 Document Conventions  
1.3 Intended Audience and Reading Suggestions  
1.4 Project Scope  
1.5 References

**2. Overall Description**2.1 Product Perspective  
2.2 Product Features  
2.3 User Classes and Characteristics  
2.4 Operating Environment  
2.5 Design and Implementation Constraints  
2.6 User Documentation  
2.7 Assumptions and Dependencies

**3. System Features**3.1 DDoS Detection  
3.1.1 Description and Priority  
3.1.2 Stimulus/Response Sequences  
3.1.3 Functional Requirements

3.2 DDoS Mitigation and Recovery  
3.2.1 Description and Priority  
3.2.2 Stimulus/Response Sequences  
3.2.3 Functional Requirements

**4. External Interface Requirements**4.1 User Interfaces  
4.2 Hardware Interfaces  
4.3 Software Interfaces  
4.4 Communications Interfaces

**5. Other Nonfunctional Requirements**5.1 Performance Requirements  
5.2 Safety Requirements  
5.3 Security Requirements  
5.4 Software Quality Attributes

**6. Other Requirements**Appendix A: Glossary  
Appendix B: Analysis Models  
Appendix C: Issues List

**1. Introduction**

1.1 Purpose  
This document provides the requirements for the DDoS Protection System for Cloud. The system shall detect, mitigate and recover from DDoS attacks on cloud-hosted web applications so that high availability and security are guaranteed.

1.2 Document Conventions  
Conventions used in this document are as follows:  
• High-priority requirements are marked as [High].  
• The functional and non-functional requirements are numbered as REQ-X, where X is a unique identifier.

1.3 Intended Audience and Reading Suggestions  
This SRS is intended for software developers, system architects, cybersecurity experts, project managers, and testers. The overview of Section 2 and the detailed system features in Section 3 will be of more interest to the readers.

1.4 Project Scope  
The system shall equip tools for the detection and protection of cloud-hosted websites from various kinds of DDoS attacks. Minimum down time and automatic recovery mechanisms should be ensured. Cybersecurity aspects for the developed solution shall be emphasized with as little involvement of machine learning as possible.

1.5 References  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2. Overall Description**

2.1 Product Perspective  
The system is to be integrated into a cloud-hosted environment in which the web application is to be protected against several DDoS attacks. This should be designed in such a way that it would function effectively in a larger security infrastructure.  
  
2.2 Product Features  
• Real-time detection of DDoS attacks  
• Automatic mitigation through filtering traffic and rate limiting  
• Recovery with minimum possible downtime for high availability  
• Logging and reporting of attack patterns

2.3 User Classes and Characteristics  
• System Administrators: These shall be concerned with activities in the monitoring and reacting to security alerts.  
• Security Analysts: Analyze attack patterns and responses for system improvements.

2.4 Operating Environment  
• Cloud-based infrastructure, such as AWS, Azure, GCP.  
• Web-based user interfaces.  
• Distributed database systems for logging and analysis.

2.5 Design and Implementation Constraints  
• Should be compliant with GDPR for user data security.  
• Should operate on widely used cloud platforms.

2.7 Assumptions and Dependencies  
• The underlying cloud infrastructure provides support for basic load balancing and network firewall.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**3. System Features**

3.1 DDoS Detection  
3.1.1 Description and Priority  
The system shall use anomaly detection methods to identify suspicious patterns of traffic that may indicate a DDoS attack.  
**Priority**: High

3.1.2 Stimulus/Response Sequences  
• The system is fed incoming traffic.  
• It analyzes patterns for spikes from single IPs, unusual traffic behavior, and geolocation clustering.  
• The system flags the traffic as suspicious.

3.1.3 Functional Requirements  
• REQ-1: The system shall detect suspicious volumes of traffic originating from individual ranges of IP addresses.  
• REQ-2: Log unusual traffic behavior (e.g. continuing peaks every 10 minutes).

3.2 DDoS Mitigation and Recovery  
3.2.1 Description and Priority  
System shall, immediately after the detection of the attack, automatically trigger mitigation mechanisms and ensure quick restoration of services.   
**Priority**: High

3.2.2 Stimulus/Response Sequences  
• Upon the system detecting an ongoing attack.  
• Mitigation shall be done - that is, filtering out harmful traffic.  
• Recovery of services shall be aimed at with respect to continuity of the website.

3.2.3 Functional Requirements  
• REQ-3: Rate-limiting needs to be performed on suspicious traffic.  
• REQ-4: Within 2 minutes after an attack is stopped, the system needs to recover.  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**4. External Interface Requirements**

4.1 User Interfaces  
System monitoring shall be provided via a web-based dashboard, which includes real-time attack alerts and the health status of the system.

4.2 Hardware Interfaces  
The system shall interface with cloud standard hardware, such as load balancers, firewalls.

4.3 Software Interfaces  
• The system shall interface with cloud platforms, such as AWS, Azure, etcetera, using their API to manage traffic.

4.4 Communications Interfaces  
• The system will use HTTP/HTTPS protocols to communicate data between services.  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**5. Other Nonfunctional Requirements**

5.1 Performance Requirements  
The system shall be able to handle up to 1 million requests per second during attack mitigation.

5.2 Safety Requirements  
Mitigation action shall not disrupt legitimate traffic unless it is absolutely necessary.

5.3 Security Requirements  
All logs shall be encrypted, and all communications with APIs shall use secure protocols.

5.4 Software Quality Attributes  
• Average: 99.99% uptime.  
• Usability: Easy management interface to get the overview of the current status of the attack quickly  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
6. Other Requirements  
• The system shall be integrated with natively developed cloud security services.  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Appendix A: Glossary  
• DDoS: Distributed Denial of Service  
• Mitigation: Explanatory steps or processes which have aims to reduce impacts in some ways  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_