

# Distributed Denial of Service Attack and Mitigation

## ReqView Software Requirements Specification

* ID	</> Upstream Traceability	Description	</> Implemented By	Custom Attributes
SRS-1		<h3>1 Introduction</h3> <p>Distributed denial of service attack(DDOS) is the second most cybercrime attack. The attack is done by different IP's on a particular node denying the services to the legitimate users.</p>		Type: Section
SRS-2		<h4>1.1 Purpose</h4> <p>Today, the internet is evolving at a very fast rate. We live in the world of Internet which has made great impact on computing and communications. Because of this the impact of DDoS attacks on internet security is growing excessively. These attacks hinder the services to the legitimate users.</p> <p>There are various ways by which attacks are done like flooding, (slow), etc</p> <p>Here, we propose a model which will detect and mitigate TCP and HTTP flood attacks in a timely manner and in very efficient way. But to detect them we have to first make a system which will do these attacks.</p>		Type: Section
SRS-3		<h4>1.2 Scope</h4> <ul style="list-style-type: none"><li>Name: Distributed Denial of Service Attack and Mitigation</li><li>Purpose: To help reduce the effect of denying the services to a legitimate user and prevent losses faced by the companies due to downtime of the servers.</li><li>Objective: Using traffic analysis and expected incoming traffic to detect a DDoS attack and the prevent/ mitigate it by denying access to the illegitimate traffic.</li><li>Goals:<ol style="list-style-type: none"><li>Detecting DDoS attacks.</li><li>Mitigate/prevent DDoS attack.</li><li>Secure network from illegitimate traffic.</li><li>Ensure rapid access to legitimate traffic.</li></ol></li></ul>		Type: Section
SRS-5		<h4>1.3 Product perspective</h4> <p>With rapid growth of networking communications, there is threat to financial data, business analytics data, etc through DDoS attacks. The goal of our system will be to detect and mitigate this attacks, so that victim must not be affected. Because if a system goes down for a moment, it may pose great loss. Since many application layer protocols want don't their data to be lost and have a guaranteed delivery if the packets, TCP is mostly the underlying protocol, so our main aim will be to handle TCP flooding SYN/ACK attacks.</p>		Type: Section
SRS-6		<h5>1.3.1 System interfaces</h5> <p>The application runs in the latest version of Chrome or Firefox browser on Windows, Linux and Mac.</p>		Type: Section
SRS-7		<h5>1.3.2 User interfaces</h5> <p>GUI depicting the coming packets one by one and shows the number of attacks happened in timebound frame.</p> <p>Also it will give the graphical view of the traffic on the system.</p>		Type: Section


* ID	</> Upstream Traceability	≡ Description	</> Implemented By	⚙ Custom Attributes
SRS-8		<b>1.3.3 Hardware interfaces</b> All devices like Personal Computers, Mainframe Computers with Linux or Windows Operating System.		⚙ Type: Section
SRS-9		<b>1.3.4 Software interfaces</b> <ul style="list-style-type: none"> <li>Operating system: Windows or Linux (32-64 bit)</li> <li>Database system: MySQL</li> <li>Backend: JAVA</li> <li>Frontend: JAVA</li> <li>Dependencies: WireShark</li> </ul>		⚙ Type: Section
SRS-10		<b>1.3.5 Communications interfaces</b> <ul style="list-style-type: none"> <li>High level use of socket programming</li> <li>Use http, icmp, tcp, protocols</li> <li>To detect the packets, packet sniffing is done for all layers</li> </ul>		⚙ Type: Section
SRS-11		<b>1.3.6 Memory constraints</b> It requires memory to store the packets. Also the dynamic memory to store the IP address of attacker(if detected) for short period of time and then free the memory.		⚙ Type: Section
SRS-12		<b>1.3.7 Operations</b> <ul style="list-style-type: none"> <li>This software will be compatible with Linux or Windows with JDK (32-64bit)</li> <li>The system will not interrupt any other process though it will run continuously.</li> <li>This software will be developed in JAVA.</li> </ul>		⚙ Type: Section
SRS-13		<b>1.3.9 Interfaces with services</b> Socket Programming Interface.		⚙ Type: Section
SRS-14		<b>1.4 Product functions</b> <ol style="list-style-type: none"> <li>Demonstrating DDoS Attack: It will perform DDoS Attack on one node in the network where other attackers may also attack at same time.</li> <li>DDoS attack detection: By analysing the packets coming on node, software will detect the attack</li> <li>DDoS attack Mitigation: After analysing and detecting attack, there is a need to firewall the packets coming from IP address of attacker for short period of time.</li> </ol>		⚙ Type: Section
SRS-15		<b>1.5 User characteristics</b> <ol style="list-style-type: none"> <li>Network Administrators</li> <li>Cloud Networking</li> <li>Independent Servers</li> <li>Companies, institutions, etc</li> </ol>		⚙ Type: Section
SRS-16		<b>1.6 Limitations</b> <ol style="list-style-type: none"> <li>To segregate attack traffic from legitimate user traffic.</li> <li>To detect all types of attacks .</li> <li>MAC Spoofing is difficult to handle.</li> <li>DNS Spoofing will not be maintained</li> </ol>		⚙ Type: Section
SRS-17		<b>1.7 Assumptions and dependencies</b> <ul style="list-style-type: none"> <li>Attackers are distributed by IP Spoofing.</li> <li>Internet Connection</li> <li>JAVA Gcc</li> <li>WireShark</li> <li>Server System</li> </ul>		⚙ Type: Section

* ID	</> Upstream Traceability	≡ Description	</> Implemented By	⚙️ Custom Attributes
SRS-18		<h2>1.8 Definitions</h2> <ul style="list-style-type: none"><li>• DDOS ATTACK:  A distributed denial-of-service (<i>DDoS</i>) <i>attack</i> is a malicious attempt to disrupt normal traffic to a web property by distributed system.</li><li>• DOS ATTACK:  A Denial-of-Service (<i>DoS</i>) <i>attack</i> is an <i>attack</i> meant to shut down a machine or network, making it inaccessible to its intended users.</li><li>• IP Spoofing:  IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of impersonating another computing system.</li><li>• MAC Spoofing:  MAC spoofing is a technique for changing a factory-assigned Media Access Control (<i>MAC</i>) <i>address</i> of a network interface on a networked device.</li><li>• HTTP FLOOD ATTACK:  HTTP flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application</li><li>• TCP FLOOD ATTACK:  TCP SYN/ACK flood is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.</li></ul>		⚙️ <i>Type:</i> Section
SRS-18		<h2>1.9 Acronyms and abbreviations</h2> <p>DDoS: Distributed-Denial of Service</p> <p>DoS: Denial of Service</p> <p>HTTP(S): Hyper Text Transfer Protocol (Secure)</p> <p>TCP: Transport Control Protocol</p> <p>ICMP: Internet Control Message Protocol</p> <p>RFC: Request For Comments</p> <p>IP: Internet Protocol</p> <p>MAC: Media Access Protocol</p> <p>SYN: Synchronize</p> <p>ACK: Acknowledgement</p>		⚙️ <i>Type:</i> Section
SRS-20		<h2>2 Requirements</h2>		⚙️ <i>Type:</i> Section
SRS-21		<h3>2.1 External interfaces</h3> <ul style="list-style-type: none"><li>• Operating Systems - All Operating Systems with a java compiler</li><li>• Database Used - MySQL</li><li>• Java Compiler</li></ul>		⚙️ <i>Type:</i> Section

* ID	</> Upstream Traceability	≡ Description	</> Implemented By	⚙ Custom Attributes
SRS-22		<h2>2.2 Functions</h2> <ul style="list-style-type: none"> <li>Creating a DDoS Attack: <p>The software provides a feature to create a DDoS attack. However it should be noted that this feature is for testing/checking the security of server against DDoS attacks and should not be used for any illegal purpose.</p> </li> <li>Detecting a DDoS Attack: <p>The software has a feature of detecting a DDoS attack. It detects an attack when there is enormous incoming traffic, more than what it experiences usually. It detects when there is traffic from a machine with a spoofed IP address, or even multiple machines sending malicious traffic, to deny service to the legitimate users and/or to breakdown the server. It distinguishes the spoofed IP address from the real ones by checking the MAC addresses of the incoming traffic.</p> </li> <li>Mitigating: <p>The software service to reduce the severity of the DDoS attack. This feature of mitigation ensures that the attack causes no or minimum damage to the server in addition of providing access to the genuine users. The mitigation is done by restricting the access to spoofed IP addresses.</p> </li> </ul>		⚙ Type: Section
SRS-23		<h2>2.3 Usability requirements</h2> <ul style="list-style-type: none"> <li>Rapid action is taken on detection of an attack.</li> <li>The UI is simple and precise.</li> <li>Shortcuts can be provided to for rapid interaction with the user(Network Administrator).</li> </ul>		⚙ Type: Section
SRS-24		<h2>2.4 Performance requirements</h2> <ul style="list-style-type: none"> <li>The detection of an attack is very rapid. Earlier the attack detected, lesser is the severity of the attack.</li> <li>Accurate distinguishment is made between legitimate and illegitimate traffic.</li> </ul>		⚙ Type: Section
SRS-25		<h2>2.5 Logical database requirements</h2>		⚙ Type: Section
SRS-26		<h2>2.6 Design constraints</h2>		⚙ Type: Section
SRS-27		<h2>2.7 Standards compliance</h2> <ul style="list-style-type: none"> <li>The software is in accordance with the RFC(Request For Comments) of the networking protocols.</li> <li>The software doesn't violate the standards of the ISPs.</li> </ul>		⚙ Type: Section
SRS-28		<h2>2.8 Software system attributes</h2> <p>The software will be reliable. The server admins can be able to trust the software for protection against DDoS attacks.</p>		⚙ Type: Section
SRS-29		<h2>3 Verification</h2> <p>There will be a proper and accurate verification so that under no circumstances, a legitimate user be denied or restricted to the services.</p>		⚙ Type: Section

SRS-30

## 4 Supporting information

 Type: Section

### End Users:

- **Content Delivery Networks (CDNs) :**

CDNs are the target of a large no. of DDoS attacks.

- **Banks:**

In today's world, where we are going to a cashless state, all the transactions are carried over Internet and the bank servers always need to be up to allow transactions. If it goes down even for a smaller time, it would result to havoc.


- **Companies:**

Servers of all leading companies need to be up all the time and provide access to legitimate users rapidly.

- **All servers, websites, etc.**

SRS-31

## 5 References

 Type: Section

<https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019/>  
(<https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019/>)

[https://en.wikipedia.org/wiki/DDoS\\_mitigation](https://en.wikipedia.org/wiki/DDoS_mitigation)  
([https://en.wikipedia.org/wiki/DDoS\\_mitigation](https://en.wikipedia.org/wiki/DDoS_mitigation))