# **Log Generation In Firewall**

***Kirshna Paresh Raichura, Sreejha, Harshavardhini, Vishnupargavan***

***I-Year CSE(AIML)***

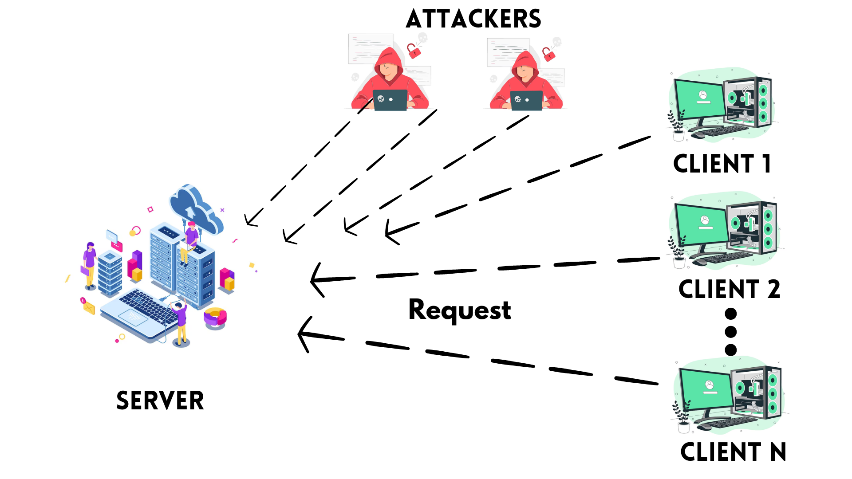
**1.Objective**

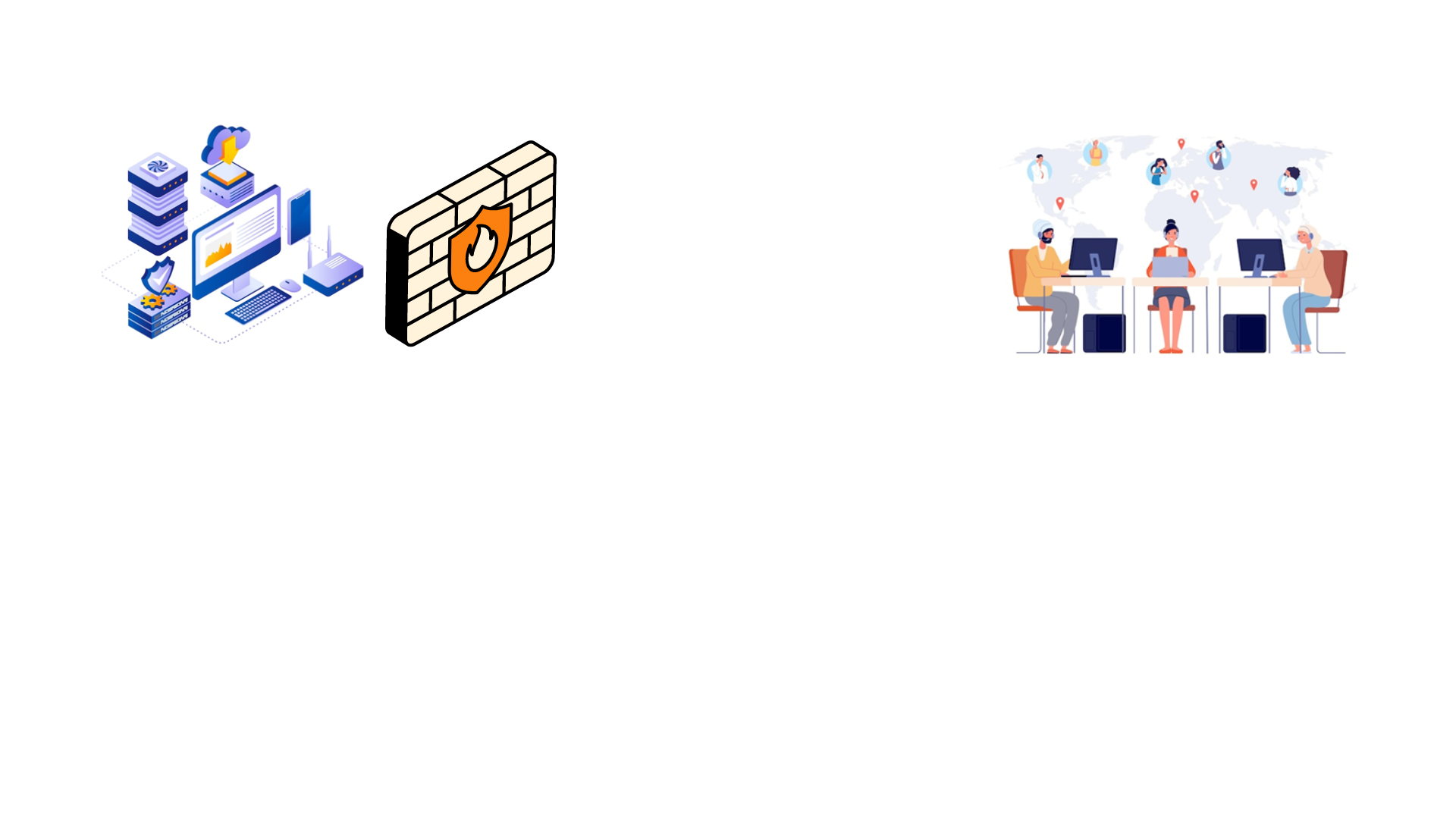
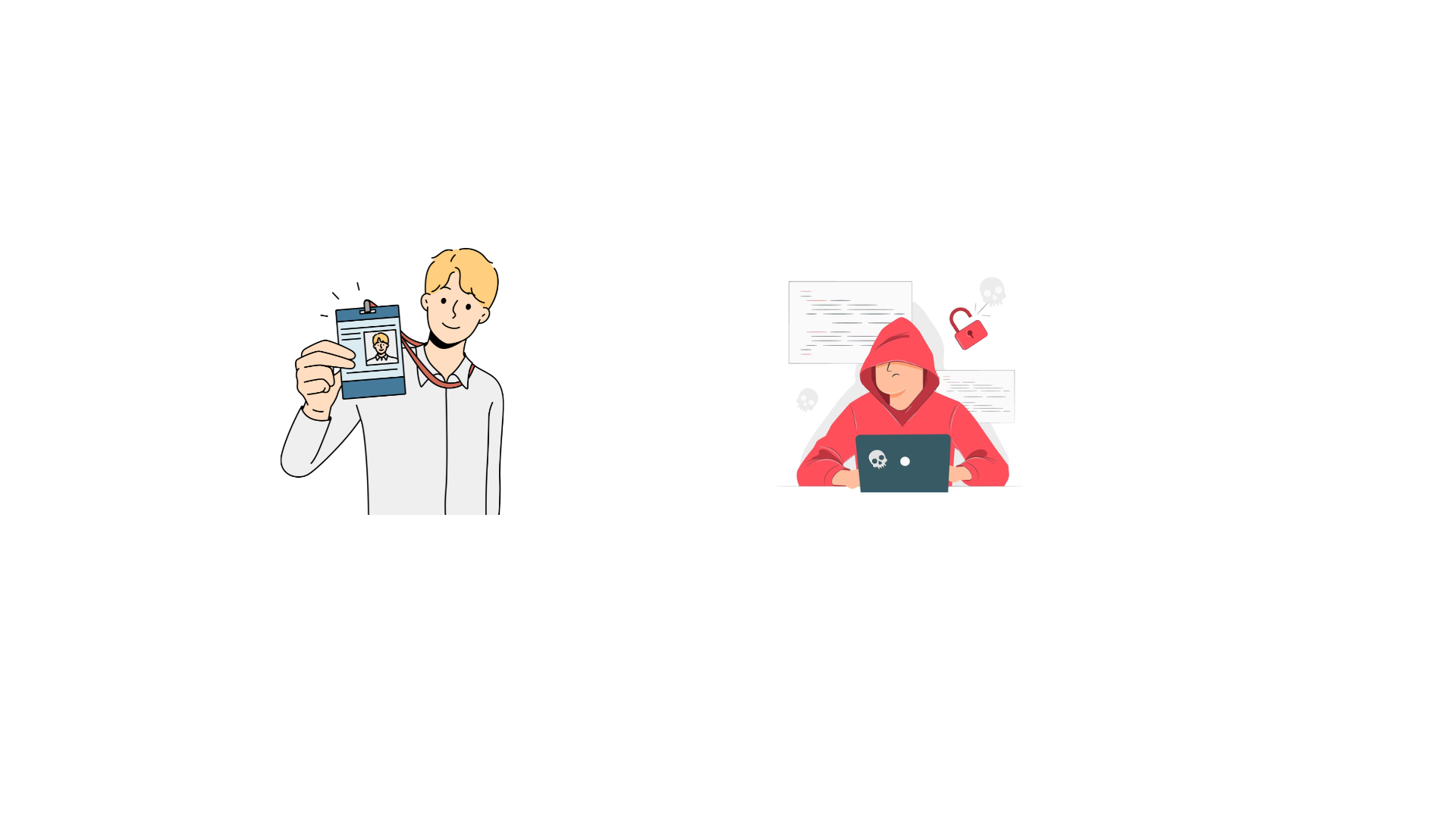
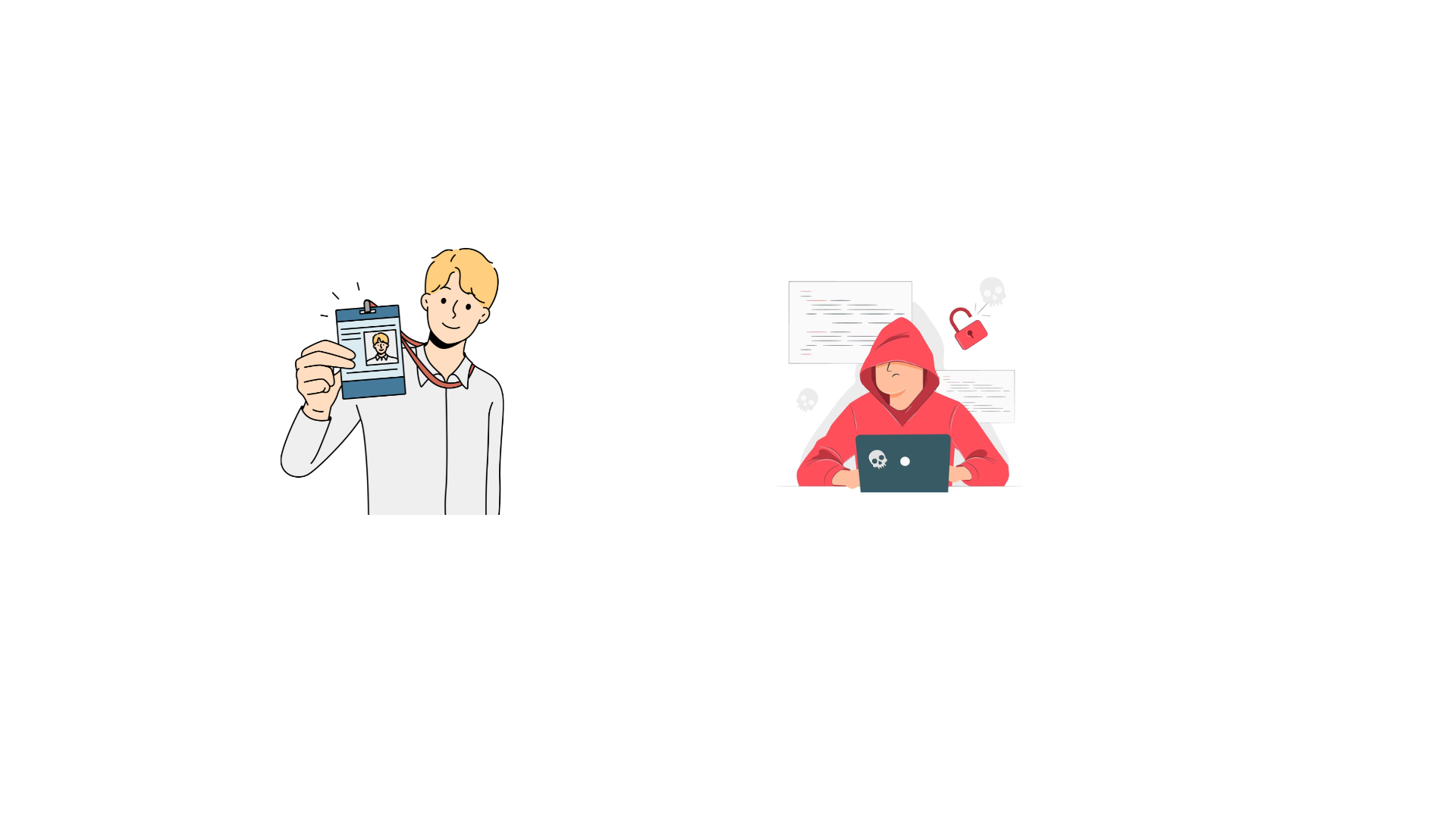
* The objective of our project is to develop a firewall that can effectively detect Denial of service attack (DDoS) attacks and provide timely host alerts, enhancing network security by mitigating the risks associated with these attacks.

**2.Abstract**

* The protection of a network is important so as to manage the traffic into and out of the environment. To achieve this, firewall is installed, which monitors the networking environment and also to protect. There are some firewalls which also offer the visibility of the source of the presumed attack and also the of traffic coming into the environment. Always a firewall is designed in such a way to configure by using the rules. For a successful impact of the firewall, a ruleset is augmented with a successful logging feature. The logging feature records the type of the activity happens in the firewall, analyzes the environment and keeps in track of the traffic. Also helps in notifying the users of the unusual environment. The logs keeps the information such as the source and the destination IP addresses, the protocols implemented and the port numbers attached.

**3.** **Overall Architecture**

****

 ****

**CLIENTS**

**SERVER**

**REQUEST**

**FIREWALL**

GENERATE LOGS

**GENUINE CLIENTS**

**ATTACKERS**

**Architecture**

**4.Conclusion**

Through this we can be notified about the attack on our website or application which helps us to save our web or applications or our personal information from external attacking source.

**References**

* https://web.archive.org/web/20131124235452/http://hackerspace.lifehacker.com/how-to-defend-yourself-against-mitm-or-man-in-the-middl-1461796382
* https://www.crowdstrike.com/cybersecurity-101/man-in-the-middle-mitm-attacks/
* https://www.quora.com/topic/Man-in-the-Middle-communications-attack