

# **Project Proposal and Synopsis for CS-757**

**a) Name of Project Title and Group Member Names**

**Project Title:** Secure Network Environment Implementation

**Group Members:**

Akshit Chhikara, CO21306

Chetan Kumar, CO21315

**b) Name of the Proposed Guide**

**Proposed Guide:** Prof. R.B. Patel (Final decision to be taken by the department)

**c) One Paragraph Explaining Your Expected Work**

**Abstract:**

The project aims to implement key cybersecurity principles to create a secure and resilient network environment. The focus will be on deploying a custom firewall to monitor, filter, and control incoming and outgoing network traffic based on predefined security rules. This firewall will act as the first line of defence, blocking unauthorized access while allowing legitimate communications.

Additionally, the project will utilize proxy and reverse proxy servers to manage and secure data flow between clients and servers. The proxy server will serve as an intermediary, protecting the identity and structure of the internal network, while the reverse proxy server will handle incoming requests, distributing them to the appropriate servers and enhancing load balancing and security.

Furthermore, the project will integrate Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) using Suricata. Suricata will continuously monitor network traffic for signs of suspicious activities, such as unusual data patterns or unauthorized access attempts, and generate alerts for further investigation. The IPS capabilities of Suricata will take proactive measures to block or mitigate identified threats, ensuring that malicious activities are stopped before they can cause harm.

The primary goal of this project is to ensure the integrity, confidentiality, and availability of data within the network by providing robust protection against a wide range of cyber threats. By combining a custom firewall, proxy servers, and Suricata IDS/IPS, the project aims to create a multi-layered security architecture that can effectively safeguard the network from both internal and external threats.