Final Year Project Proposal Defense

# VPN SpyGlass

Unveiling Network Shadows: Unmasking VPNs with VPN Spyglass

**Advisor**: Dr. Mehdi Hussain
**Co-Advisor**: Dr. Arsalan Ahmad

**Team Members:**

Hassan Abdullah 337275
Sameen Mubashar 346848

# Overview

- Introduction
- Problem Statement
- Literary Review
- Value Proposition
- Initial Phases Before Development
- Technologies
- Software Development Implementation
- Project Milestones
- Work Division
- Costing

# Introduction

01 Importance of network security

02 Encrypted Network Traffic Analysis

03 Need to detect VPN usage

04 P4 Language

# Problem Statement

## Problem 1

The proliferation of VPNs poses a challenge to network administrators, as these tools can bypass security measures and access restricted content. This poses security risks, violates agreements, and slows network performance

## Problem 2

Existing methods often struggle to identify VPN traffic due to encryption and masking techniques employed by VPN services.

# Literary Review

## Works in the Network Analytics And SDN

| RESERCH PAPER | YEAR/AUTHOR | GOAL | METHOD USED | LIMITATION |
|---|---|---|---|---|
| Characterization of Encrypted and VPN Traffic using Time-related Features | 2016<br>Gerard Draper-Gil, Arash Habibi Lashkari, Mohammad Saiful Islam Mamun and Ali A. Ghorbani | Effectiveness of flow-based time-related features to detect VPN traffic and to characterize encrypted traffic into different categories, according to the type of traffic. | C4.5 decision tree and KNN | 1. Proposed set of time-related features achieving accuracy levels around 80%.<br>2. Require Labelled Dataset of previous Network Packet History |
| Detection of VPN Network Traffic | 2022<br>Avnish Goel, Apoorv Kashy, B. Devesha Reddy | Detecting and classifying the network traffic as VPN/Non-VPN over the standardized Dataset using various Machine Learning algorithms. | Multilayer Perceptrons (MLPs) and Random Forest Model | 1. The precision and recall for the same were 0.99907 and 0.92849 respectively.<br>2. Require Labelled Dataset of previous Network Packet History |
| A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures | 2021<br>EVA PAPADOGIANNAKI, SOTIRIS IOANNIDIS | Examine the literature that deals with network traffic analysis and inspection after the ascent of encryption in communication channels | Use traditional deep packet inspection systems | Only for Normal traffic. Not for VPN. |
| Lightweight Anti DDoS Security Tool: Edge Level Filtering in SDN using P4 | 2023<br>Masumi Arafune; Bhargavi Goswami; Manasa Kulkarni; Nagarajan Venkatachalam | Defense mechanism by enabling edge-level filtering without involving the control plane. | By implementing filtering functions in edge switches, it can provide an efficient and effective defense layer in SDN network systems so that SDN switch can become the first line of defense against packet injection attacks. | 1. Only for DDoS Attack<br>2. Isolates Data Plan from control Plane |

# Value Proposition

The value of our project lies in its potential to significantly enhance network security and policy enforcement. By providing network administrators with a tool that can accurately identify and monitor VPN usage full filling few UNSDGs , organizations can:

01 **Prevent data breaches.**

02 **Industry, Innovation, and Infrastructure**

03 **Peace, Justice, and Strong Institutions**

04 **Sustainable Cities and Communities**

# Project Development Methodology / Architecture

# Initial Phases Before Development

01 Understanding existing VPN detection systems

02 Understanding BMV2 and P4 working

03 Requirements engineering for web interface

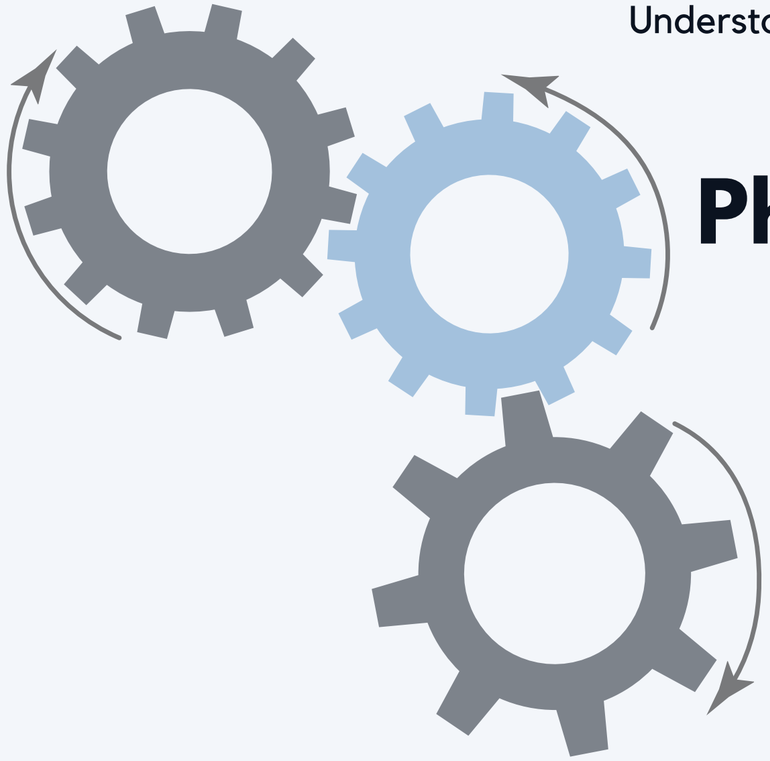
# Technologies

- ReactJS
- Django
- Python
- P4 Language
- Mininet
- ONOS
- OpenFlow
- Wireshark

# Implementation

## Phase 1

Detection of VPN traffic using Deep Packet Inspection based on their IP, Port Number, and Packet Length. Understand P4, BMV2, and OpenFlow.



## Phase 2

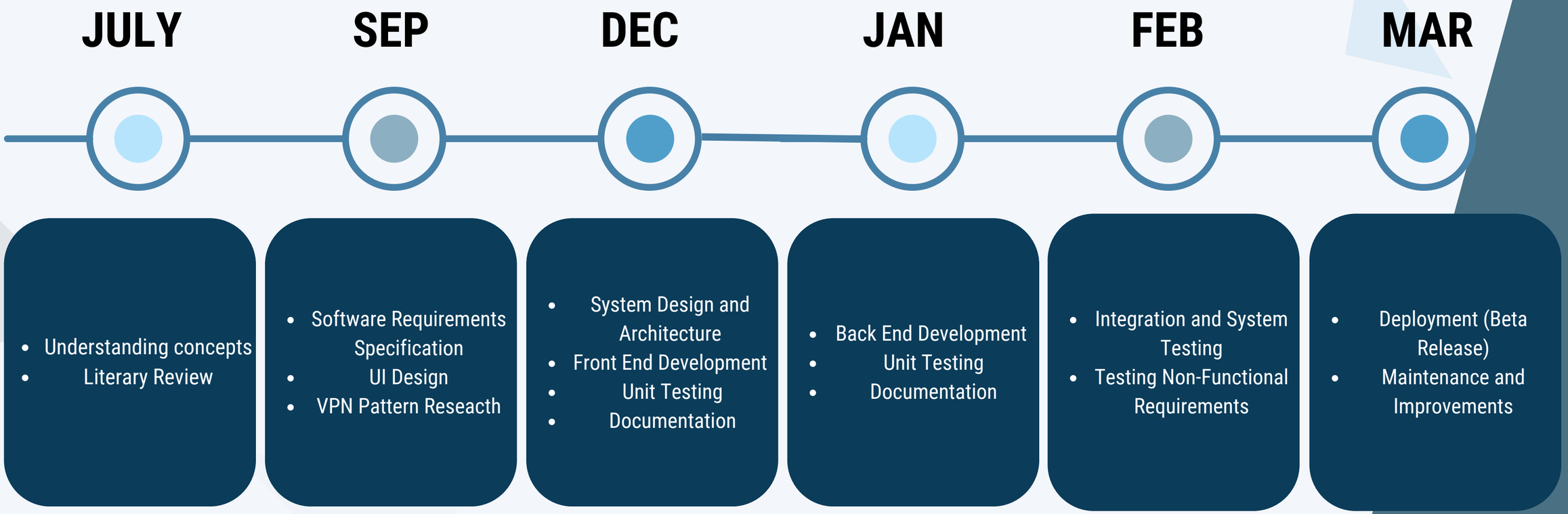
Development of Web Page. Setting up of implementation environment.

## Phase 3

Implementation of code on BMV2 switch and integrating with the webpage.

# Project Milestones and Deliverables

# Project Timeline



# Work Division

- Environment Setting.
- Implementing Mininet Topology and OpenFlow
- Backend Development, Testing, and Documentation
- Deployment

**Hassan**

- UI Design
- Frontend Development, Testing, and Documentation
- Non-functional Requirements Testing

**Sameen**

- P4 Program
- Pattern detection of VPNs
- SRS and SDS
- Maintenance and Improvement

**Mutual**

# Costing

| ITEM | COST |
| --- | --- |
| Domain for 1 year | PKR 1300 |
| System to set up virtual Switch | PKR 60,000 |
| (**Optional**) Edgecore DCS802-12.8T Programmable Data Center Switch | $ 32,000 |

# Thank You

For Your Attention

## Any Questions?