**Phase-1 Submission Template STUDENT NAME: MANISHA M**

**REGISTER NUMBER: 731123205032**

**INSTITUTION: GOVERNMENT COLLEGE OF ENGINEERING, ERODE**

**DEPARTMENT: B TECH INFORMATION TECHNOLOGY**

**DATE OF SUBMISSION: 26/04/2025**

# 1.Problem Statement

Cyber threats, such as malware, intrusions, and data breaches, pose significant risks to organizations. Traditional security measures often struggle to detect these threats in real-time. This project aims to develop an anomaly detection system that identifies unusual patterns in network traffic, which may indicate potential cyber threats.

# 2.Objectives of the Project

# To design and implement an anomaly detection system for network traffic.

# To identify and classify different types of cyber threats based on detected anomalies.

# To evaluate the effectiveness of the anomaly detection system in real-time scenarios.

# To provide actionable insights and alerts for network administrators.

# 3.Scope of the Project

# Focus on analyzing network traffic data to detect anomalies.

# Limit the study to specific types of cyber threats, such as DDoS attacks, unauthorized access, and data exfiltration.

# Develop a prototype system that can be tested in a controlled environment.

# Provide recommendations for integrating the system into existing security frameworks.

# 4.Data Sources

# Network traffic logs from firewalls and routers.

# Publicly available datasets, such as the CICIDS (Canadian Institute for Cybersecurity Intrusion Detection System) dataset.

# Synthetic data generated to simulate various cyber threat scenarios.

# 5.High-Level Methodology

# DATA COLLECTION: Gather network traffic data from various sources.

# DATA PREPROCESSING: Clean and preprocess the data to remove noise and irrelevant information.

# FEATURE EXTRACTION: Identify key features that can help in detecting anomalies.

# MODEL DEVELOPMENT: Use machine learning algorithms to build the anomaly detection model.

# MODEL EVALUATION: Test the model using validation datasets and assess its performance.

# DEPLOYMENT: Implement the model in a real-time monitoring system and provide alerts for detected anomalies.

# 6.Tools and Technologies

# PROGRAMMING: Python

# LIBRARIES: Scikit-learn, Pandas, NumPy, TensorFlow/Keras

# VISUALIZATION: Matplotlib, Seaborn

# TRAFFIC ANALYSIS: Wireshark, Tcpdump

# ENVIRONMENT: Jupyter Notebook, Google Colab, or Anaconda

# 7.Team Members and Roles

1. MANISHA M – Project Leader
2. BHUVANIHA N C – Data Collection
3. SAVITHA K – Machine Learning Engineering
4. PRIYANKA G – Evaluation Analyst