Project Design Phase-I
Proposed Solution

Project Name	AI-Enhanced Intrusion Detection System
Maximum Marks	2 Marks

Proposed Solution Template:

Project team shall fill the following information in proposed solution template.

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Traditional intrusion detection systems rely heavily on static rules and known threat signatures, making them ineffective against new and sophisticated cyber-attacks. These systems also generate excessive false positives, overwhelming security teams and delaying incident response.
2.	Idea / Solution description	The proposed solution is an AI-powered Intrusion Detection System that uses machine learning algorithms to detect and classify malicious activities within network traffic in real time. It combines anomaly detection and signature-based methods, with a self-learning model that improves continuously using updated data. The system will include automated responses and a user-friendly dashboard for threat monitoring.
3.	Novelty / Uniqueness	Unlike traditional IDS tools, this system adapts to new threats through machine learning, significantly reduces false positives, and includes automated responses to threats. Its modular architecture allows for easy integration and scaling. The continuous learning component makes it more resilient to zero-day attacks.
4.	Social Impact / Customer Satisfaction	The solution enhances the cybersecurity posture of organizations, helping prevent data breaches and service disruptions. It contributes to safer digital environments, protects user privacy, and reduces the workload on security analysts — increasing satisfaction among clients and users.
5.	Business Model (Revenue Model)	The solution can be offered as a **subscriptionbased SaaS** (Security-as-a-Service) model for SMEs or licensed for larger enterprises. Additional revenue can come from premium features like advanced analytics, priority support, and integration with third-party tools.

6.	Scalability of the Solution	The system is designed to be scalable across various organization sizes — from small networks to enterprise-level infrastructures. Its cloudcompatible architecture allows deployment in onpremise, cloud, or hybrid environments, and supports adding new detection modules or data sources as needed.