Project Design Phase-I

Proposed Solution Template

Project Name	"AI-Enhanced Intrusion Detection System"

Proposed Solution Template:

S.No.	Parameter	Description
1	Problem Statement (Problem to be solved)	The problem is to develop an **AI-based intrusion detection system** that accurately identifies cyber threats in real-time while minimizing false positives to ensure efficient and reliable network security.
2	Idea / Solution description	The proposed solution is a machine learning-driven Intrusion Detection System (IDS) that analyzes network traffic patterns to detect abnormal behavior and potential intrusions. It will use a combination of: • Anomaly detection algorithms • Behavioral pattern recognition • Real-time adaptive learning • Explainable AI (XAI) for transparent alerts The system will prioritize threats based on risk levels, reduce noise from false positives, and integrate with existing security infrastructure for automated response.
3	Novelty / Uniqueness	• Incorporates self-learning models that adapt to new and evolving threats. • Uses explainable AI to provide clear reasons behind each alert, unlike traditional black-box models. • Features false-positive reduction techniques, improving efficiency and analyst trust. • Can be extended to cloud and multi-cloud environments, a rare feature in standard IDS tools.
4	Social Impact / Customer Satisfaction	• Reduces cybercrime risks for organizations and protects sensitive user data. • Enhances the efficiency of security teams by reducing unnecessary alerts. • Promotes digital safety and trust in both public and private sectors. • Offers a user-friendly dashboard, increasing customer satisfaction and ease of use.

5	Business Model (Revenue Model)	• SaaS-based subscription model for enterprises. • Tiered pricing plans based on features (e.g., number of nodes, cloud integration, auto-mitigation). • Consulting and customization for large organizations. • Option for freemium version with basic features for small businesses or educational use.
6	Scalability of the Solution	• Built on a modular microservices architecture for easy scaling across large networks. • Can be deployed on-premises or in the cloud, depending on user requirements. • Supports integration with SIEM tools, firewalls, and DevOps pipelines. • Future-ready for IoT and smart infrastructure applications as threats evolve.