Project Design Phase-I
Proposed Solution Template

Date	24 October 2023
Team ID	1.1
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)	The increasing sophistication of cyber threats and the constant evolution of attack techniques pose a significant challenge to the security of digital systems. Traditional intrusion detection systems often struggle to keep up with these dynamic threats, leading to a higher risk of successful cyberattacks. To address this problem, there is a need for an AI-enhanced intrusion detection system that can proactively detect and respond to emerging threats in real-time.
2.	Idea / Solution description	Our solution is an AI-enhanced intrusion detection system that leverages machine learning algorithms and artificial intelligence to monitor network traffic and system behaviour. This system continuously analyses data to identify potential threats, anomalies, and suspicious activities, allowing for real-time threat mitigation. It can adapt and self-improve, becoming more effective in detecting new and evolving attack patterns.
3.	Novelty / Uniqueness	What sets our AI-enhanced intrusion detection system apart is its ability to learn and adapt. By using deep learning and other AI techniques, it can recognize both known and previously unknown attack vectors. This adaptability makes it stand out in the field of intrusion detection, as it doesn't rely solely on predefined rules or signatures. It's capable of anomaly detection and behavioural analysis, which sets it apart from more traditional systems.

4.	Social Impact / Customer Satisfaction	It helps protect individuals, businesses, and organizations from cyber threats, safeguarding sensitive data and privacy. As the system is highly efficient and capable of real-time threat detection, it minimizes potential damage and financial losses due to cyberattacks. Customers will experience increased peace of mind, knowing that their digital assets are under the watchful eye of a highly intelligent and adaptive security system.
5.	Business Model (Revenue Model)	**Subscription Services**: Offer subscription-based access to the intrusion detection system, with tiered pricing for different levels of service and support. **Licensing**: License the technology to other cybersecurity companies or organizations that want to integrate it into their products or services. **Customization Services**: Provide customization and integration services for businesses with specific security needs. **Consulting and Training**: Offer consulting and training services to help organizations effectively implement and manage the system. **Data Analytics**: Analyse the data collected by the system to provide insights and reports to customers, helping them make informed security decisions.
6.	Scalability of the Solution	It can be deployed in small, medium, and large organizations, as well as cloud-based environments. The machine learning models can be trained on large datasets, making them adaptable to various use cases and industries. Additionally, as the system relies on cloud computing and AI technologies, it can easily scale up to handle increased data loads and traffic, ensuring its effectiveness in a rapidly evolving threat landscape.