Project Design
Proposed Solution

Date	24 October 2023
Team ID	Team-591527
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)	Unauthorized access to networks poses a significant security risk, as firewalls and traditional security measures may not be sufficient to protect against determined attackers.
2.	Idea / Solution description	The solution we have developed is a sophisticated AI-enhanced Intrusion Detection System (AI-IDS), which is intended to more accurately and efficiently identify security threats early on. It offers a complete solution to network security by fusing artificial intelligence, machine learning, and real-time monitoring.
3.	Novelty / Uniqueness	The project's distinctiveness stems from its concentration on tackling a particular and frequently disregarded facet of network security: home network security. Its user-centric design, platform-specific tailoring, iterative development, and transparent testing distinguish it as a unique addition to the intrusion detection systems sector.
4.	Social Impact / Customer Satisfaction	By improving digital security, decreasing downtime, safeguarding privacy, empowering people, promoting digital literacy, saving money, encouraging community collaboration, assuring health and safety, and aiding in the development of critical cybersecurity skills, the project's development of an NIDS for Windows-based home networks can have a significant positive social impact. In the end, it creates a digital environment that is safer and more secure for people as well as communities.
5.	Business Model (Revenue Model)	In addition to improving cybersecurity for individual users, the creation of a network intrusion detection system (NIDS) for Windows-based home networks has the potential to yield major business benefits. These benefits include increased market share, increased revenue, decreased incident rates, customer confidence, and the encouragement of cybersecurity awareness and education. Companies taking part in this initiative have the chance to improve their financial line and users' digital safety.
6.	Scalability of the Solution	Scalability is a critical aspect of any AI-Enhanced Intrusion Detection System (AI-IDS) solution, as it ensures that the system can handle increasing data volumes, network traffic, and computational requirements as an organization or network expands. Here are some key considerations for ensuring the scalability of your AI-IDS solution:

		1. **Horizontal Scaling:** 2. **Load Balancing:** 3. **Distributed Data Storage:** 4. **Elastic Resource Allocation:** 5. **Real-time Analysis:** 6. **Interoperability:** 7. **Efficient Data Processing:** 8. **Scalable Machine Learning Models:** 9. **Scalable Storage Infrastructure:** 10. **Scalable Alerting and Reporting:** 11. **Resource Monitoring and Management:** 12. **Security and Access Controls:**.