Project Design Phase – I

Date	20 October 2023
Team ID	2.5
Project Name	Malware Detection and Classification
Team Members	- Hardik Kankane - Anondita Dutta - Elisabeth Varghese

Project Solution

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	The problem we aim to address is the need for an efficient and accurate system to detect and classify malware in real-time. Current malware detection methods often struggle to keep pace with evolving malware types and threats, leaving systems vulnerable to attacks and data breaches.
2.	Idea / Solution description	The project aims to develop a state-of-the-art Malware Detection and Classification system that leverages machine learning and artificial intelligence. This system will not only detect the presence of malware but also classify it into specific threat categories. By analyzing the characteristics and behavior of malware, our solution will enable swift and accurate threat identification, allowing organizations and individuals to take proactive measures to safeguard their systems and data

3.	Novelty / Uniqueness	This project is unique because of its ability to continuously adapt to emerging malware threats. Our system will employ advanced machine learning algorithms that evolve with the changing threat landscape. It will also incorporate real-time threat intelligence feeds to stay up to date with the latest malware strains. This adaptability and proactiveness in addressing new threats are what make our system novel and unique.
4.	Social Impact / Customer Satisfaction	The impact of our project extends beyond cybersecurity experts and organizations. It directly benefits individuals who rely on secure online interactions and transactions. By preventing malware infections, our system contributes to the protection of personal and financial information, ultimately enhancing customer satisfaction and peace of mind. Moreover, organizations can safeguard their reputations, customer trust, and financial stability.
5.	Business Model (Revenue Model)	The business model for our project is based on a subscription-based service for organizations and individuals. It will offer different subscription tiers based on the level of protection and support required. Additionally, it may explore partnerships with cybersecurity service providers to integrate our solution into their offerings. This revenue model ensures sustainable growth while delivering value to our customers.
6.	Scalability of the Solution	The system will be designed to scale horizontally, allowing it to accommodate a growing volume of data and increasing demand for malware detection and

		classification. This scalability ensures that the solution remains effective as it expands to protect a larger user base and address the evolving landscape of cybersecurity threats.