Project Design Phase-I
Proposed Solution

Date	25 october 2023
Team ID	2.1
Project Name	MALWARE DETECTION AND CLASSIFICATION
Maximum Marks	2 Marks

Proposed Solution:

Our Project information in proposed solution:

f

S.No	Parameter	Description
1.	Problem Statement (Problem to be solved)	The problem at hand is the need to develop effective strategies and solutions to mitigate malware attacks in systems. Existing security measures often fall short of protecting devices and networks from sophisticated malware attacks.
2.	Idea / Solution description	In today's digital landscape, malware is a significant threat to the security of organizations' digital assets. The "Malware Detection and Classification the development of an advanced system that harnesses the power of artificial intelligence to identify and categorize different types of malware accurately. Organizations can bolster their cybersecurity defenses by leveraging cutting-edge AI techniques, proactively detecting malicious software, and enhancing their incident response capabilities
3.	Novelty / Uniqueness	In this paper, a framework has been developed to detect and classify different files (e.g exe, pdf, php, etc.) as benign and malicious using two level classifier namely, Macro (for detection of malware) and Micro (for classification of malware files as a Trojan, Spyware, Adware, etc.). We used for generating static and dynamic analysis report by executing files in the virtual environment. In addition, a novel model is developed for extracting features based on static, behavioral and network analysis using analysis report generated.Weak Framework is used to develop machine learning models by using training datasets.
4.	Social Impact / Customer Satisfaction	Annual Worldwide Economic Damages from Malware Exceed $13 Billion. Computer Economics recently conducted a survey of IT security professionals and managers on the frequency and economic impact of malware attacks on their organizations in the previous 12 months. Malware in action can consume a substantial amount of your computer's memory, leaving limited resources for other legitimate programs to use. This can lead to extremely sluggish performance of vital programs, like your Internet browser or operating system and a slow PC overall.
5.	Business Model (Revenue Model)	The malware to create and run a botnet is developed by developers and can be rented or sold to a botmaster. The devices needed to create the

		botnet are infected by malware distributors against a cost of less than 10 cents per infection. Data stolen from victims is stored by bulletproof hosting providers. Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015.
6.	Scalability of the Solution	A scalable malware detection system capable of detecting complex attacks is the need of time. This article discusses a scalable and distributed deep learning approach for malware detection using convolutional neural network and bidirectional long short-term memory (CNN-BiLSTM).