Project Design Phase-I
Proposed Solution Template

Date	25 October 2023
Team ID	Team 4.2
Project Name	Network Anomaly Detection using AI
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 poses a substantial challenge to network security. Traditional signature-based intrusion detection systems are often ineffective against novel and adaptive attack methods. Failing to detect these network anomalies can lead to data breaches, system downtime, and financial losses.
2.	Idea / Solution description	Our project proposes the development of an advanced network anomaly detection system that leverages state-of-the-art machine learning and deep learning algorithms. This system will continuously analyse network traffic, logs, and endpoint data to identify deviations from normal behaviour. It will use unsupervised learning techniques and heuristics to detect known and unknown anomalies in real-time. The solution will offer a user-friendly dashboard for security analysts to investigate and respond to detected anomalies promptly.
3.	Novelty / Uniqueness	What sets our solution apart is the incorporation of cutting-edge deep learning techniques, including neural network architectures such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs). These algorithms excel in identifying complex, time-series anomalies, making our solution highly effective against previously unseen threats. Additionally, the system will continuously adapt and learn from new data, ensuring it remains up-to-date in detecting evolving attack methods.

4.	Social Impact / Customer Satisfaction	The successful implementation of our solution will significantly enhance network security, reduce false alarms, and improve operational efficiency. This will lead to greater customer satisfaction among organizations seeking robust cybersecurity solutions. Moreover, by safeguarding sensitive data and critical infrastructure, our project will contribute to the broader social goal of protecting digital assets and privacy.
5.	Business Model (Revenue Model)	We intend to monetize the solution through a subscription-based model. Organizations can choose from various subscription tiers based on the scale of their network. Additionally, we will offer professional consulting services to assist with the integration and fine-tuning of our system. We plan to establish partnerships with managed security service providers and offer licensing options for on-premises deployments. These revenue streams will support ongoing development and support.
6.	Scalability of the Solution	Our solution is designed with scalability in mind. It can seamlessly adapt to networks of all sizes, from small businesses to large enterprises. The underlying AI algorithms are highly parallelizable, allowing for efficient processing of increasing data volumes. We are also considering international expansion and integration with cloud-based solutions to facilitate cross-industry scalability.