**Project Design Phase-I**
**Proposed Solution Template**

| | |
|---|---|
| Date | 25Th October 2023 |
| Team ID | TEAM 1.5 |
| 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) | To address the challenges of detecting unknown threats, reducing false positives, enabling real-time detection, improving adaptability, ensuring scalability, integrating with existing systems, and complying with ethical and regulatory requirements in the ever-evolving landscape of cybersecurity. |
| 2. | Idea / Solution description | The AI-enhanced Intrusion Detection System is a cutting-edge cybersecurity solution that uses advanced AI and machine learning to detect known and unknown threats, reduce false positives, provide real-time monitoring, adapt to evolving threats, ensure scalability, integrate with existing systems, and comply with ethical and regulatory requirements. It offers organizations a powerful and adaptable defense against modern cybersecurity challenges. |
| 3. | Novelty / Uniqueness | • Advanced AI Models: Utilizing cutting-edge AI and ML for comprehensive threat detection.<br>• Anomaly Detection: Identifying unknown threats by recognizing abnormal behavior.<br>• Real-time Response: Swiftly reacting to security incidents, reducing potential damage.<br>• Continuous Learning: Adapting and improving over time for enhanced accuracy.<br>• Reduced False Positives: Minimizing the burden on security teams through AI-driven precision.<br>• Scalability: Built to handle growing data volumes and network traffic.<br>• Integration and Compliance: Seamlessly integrating with existing systems while adhering to ethical and regulatory standards. |
| 4. | Social Impact / Customer Satisfaction | This AI-enhanced IDS not only enhances cybersecurity but also promotes peace of mind by protecting sensitive data and systems. It reduces the risk of breaches, leading to higher customer satisfaction and trust in organizations that deploy it. |
| 5. | Business Model (Revenue Model) | The revenue model for the AI-enhanced IDS is based on a subscription-based service, where organizations pay a recurring fee for ongoing access to the system's threat detection, monitoring, and response capabilities. This model ensures a steady stream of income and allows for continuous updates and support. |
| 6. | Scalability of the Solution | The system is designed for easy scalability, capable of handling increasing data volumes and network traffic as organizations grow, ensuring long-term effectiveness and adaptability. |