**Name- Priyanshu Sharma**

**Reg. No.-21BCI0364**

**1.Title of the project:**

Network Packet Filtering Using Advanced ML Techniques

**2.Problem Statement**

The challenge at hand is to create a machine learning-based system for filtering network packets using data from Wireshark. Traditional packet filtering techniques rely on static rules and signatures, which often fail to detect sophisticated or novel cyber threats, leading to either missed attacks or unnecessary blocking of legitimate traffic. This project seeks to develop an intelligent, real-time filtering mechanism that can effectively discern between malicious and benign network packets. By analysing the complex and unstructured data captured by Wireshark, the system will use advanced machine learning models to detect patterns and anomalies indicative of cyber threats. The goal is to enhance the accuracy and efficiency of network security measures, reducing the occurrence of false positives and negatives while ensuring the system can adapt to new types of attacks across various network environments. This approach aims to provide a more resilient and dynamic defence mechanism against the ever-evolving landscape of cyber threats.

**3. Base Paper**

**DOI:**[**10.1109/COMSNETS56262.2023.10041315**](https://doi.org/10.1109/COMSNETS56262.2023.10041315)

**4. Objective of the project**

The primary objective of this project is to design and implement an advanced machine learning-based system for network packet filtering that leverages data captured by Wireshark. The system aims to enhance the security of network infrastructures by providing an intelligent, adaptive, and real-time mechanism for identifying and filtering out malicious packets. Unlike traditional methods that rely on predefined rules and signatures, this system will utilize sophisticated machine learning models to detect patterns and anomalies within the network traffic, distinguishing between normal and potentially harmful activities. The system's goal is to minimize false positives—where legitimate traffic is incorrectly flagged as malicious—and false negatives—where actual threats go undetected. By achieving this, the project seeks to ensure a more secure and efficient network environment, capable of responding to the constantly evolving nature of cyber threats.

**5. Motivation of the project**

The motivation for this project arises from the growing complexity and sophistication of cyber threats, which challenge the effectiveness of traditional network security measures. Standard packet filtering techniques, which typically depend on static rules, signatures, and known attack patterns, are increasingly inadequate in the face of advanced persistent threats, zero-day exploits, and other novel attack vectors. These conventional approaches often lead to two major issues: missed detections of new or sophisticated attacks, and the unnecessary blocking of legitimate network traffic, which can disrupt normal business operations.

Given these challenges, there is a pressing need for a more dynamic and intelligent approach to network security. Machine learning offers a powerful solution by enabling the analysis of large volumes of network data to uncover hidden patterns and subtle anomalies that might indicate a cyber threat. By applying machine learning models to the data captured by Wireshark—a widely-used tool for network analysis—this project aims to create a filtering system that can not only detect known threats but also adapt to emerging ones in real-time.

The ability to enhance the accuracy of threat detection and reduce false alarms will significantly improve the reliability of network security systems. This is particularly crucial as organizations increasingly rely on digital infrastructures, making the need for robust, adaptive, and efficient security measures more critical than ever. The project aspires to contribute to this goal by developing a system that not only addresses the limitations of existing methods but also sets a new standard for intelligent network defence mechanisms.