**DATA-DRIVEN DEFENSE: MACHINE LEARNING PARADIGM FOR CYBER ATTACK DETECTION**

**Abstract:**

In a world where cyber threats increasingly endanger digital networks and systems, the significance of robust cyber security measures cannot be overstated. This project focuses on enhancing cyber security through the implementation of machine learning algorithms for the detection of cyber attacks. The methodology involves the analysis of network data to identify potential threats by establishing correlations among various variables. By leveraging machine learning, the accuracy and efficiency of cyber attack detection are significantly improved, thereby fortifying the security of digital networks and systems. The cyber attack data utilized in this study is sourced from the University of New South Wales (Australia). The dataset obtained from the Cyber Range Lab of UNSW Canberra, comprises two sets of training and testing data. It encompasses records of nine distinct types of cyber attacks, including **Fuzzers, Analysis, Backdoors, DoS (Denial of Service), Exploits, Generic, Reconnaissance, Shellcode, and Worms**. Each attack type represents a unique threat vector, ranging from exploiting vulnerabilities to disrupting system functionality. The proposed approach empowers organizations to proactively identify cyber threats by employing advanced machine learning techniques. Through the analysis of diverse attack scenarios, the model can adapt and evolve, ensuring robust detection against a broad spectrum of cyber threats. This research contributes to the ongoing efforts to strengthen cyber security practices and serves as a valuable resource for organizations seeking to safeguard their digital infrastructure.