Project Title: AI enhanced Intrusion Detection System

Research Focus: Cybersecurity

Abstract:

For years now, networks have been one of the main investments organisations of all sizes make to protect their networks, user, and data. In today's hyper-connected digital landscape, the need for robust cybersecurity measures is more critical than ever. The "**AI-Based Intrusion Detection System**" project presents an innovative solution poised to redefine the way we safeguard our networks and digital assets. Leveraging cutting-edge artificial intelligence and machine learning technologies, this system offers continuous monitoring and adaptive threat detection, significantly enhancing network security.

The answer to "what is intrusion" is typically an attacker gaining unauthorized access to a device, network, or system. Cyber criminals use increasingly sophisticated techniques and tactics to infiltrate organizations without being discovered. This includes common techniques like:

- Address Spoofing
- Fragmentation
- Pattern Evasion
- Coordinated attack

Encrypting data, using firewalls to prevent unauthorized traffic entering the network, employing antimalware solutions and a variety of other tools are upheld as a standard for more or less every organization, and are used to detect cyber attacks and ultimately stop them.

Simply put, **IDS** is a software-based system used to detect and respond to malicious behaviour from outsiders or unauthorized attempts from within a network. It can detect malicious activities like virus and malware attacks as well as threats like phishing, brute force, DDoS and more. The IDS sends alerts to IT and security teams when it detects any security risks and threats. Our AI-based Intrusion Detection System is engineered to excel in various aspects of cybersecurity, making it a formidable defense against an evolving spectrum of threats. It operates in real-time, tirelessly analyzing network traffic and user behaviour patterns to swiftly identify potential security breaches, reducing the window of vulnerability in the face of cyberattacks. By leveraging the power of IDS + AI together, autonomous systems are able to protect a network better than ever before, allowing IT administrators to rest with the assurance that their cyber infrastructure is safe from threats and malicious activity. The combination also provides greater visibility across the network by collecting data from multiple sources and providing comprehensive situational awareness. This enables you to quickly detect potential threats and take action in real-time before they escalate into major issues.