علي سمير كاظم
Mr.Mohammed Maithem Supervisor

Network Intrusion Detection System using Machine Learning

Abstract

evelopment and implementation of a network intrusion detection system (NIDS) using machine learning techniques offer significant potential in enhancing cybersecurity defenses. Through this project, we have demonstrated the feasibility and effectiveness of utilizing machine learning algorithms to detect and mitigate network intrusions in real-time Key points to consider in the conclusion of a network intrusion detection system project include: Effectiveness of Machine Learning: Evaluate the performance of the machine learning models in accurately identifying and classifying network intrusions. Highlight the achieved accuracy, precision, recall, and F1-score metrics. Robustness and Scalability: Discuss the robustness and scalability of the developed NIDS in handling large-scale network traffic and diverse types of attacks. Address any limitations or challenges encountered during the implementation process. Detection: Emphasize the importance of real-time detection capabilities in promptly identifying and responding to security threats. Highlight how machine learning enables rapid analysis and decision-making in dynamic network environments. Adaptability to New Threats: Highlight the ability of the NIDS to adapt and evolve in response to emerging cyber threats. Discuss strategies for continuously updating and improving the machine learning models to mitigate evolving attack techniques. Integration with Existing Systems: Discuss the integration of the NIDS with existing cybersecurity infrastructure and tools. Address compatibility issues and the seamless interoperability of the NIDS with network monitoring systems and security information and event management (SIEM) platforms.