Ministry of Higher Education and

Scientific Research

University of Babylon

College of Information Technology

Security department

Intrusion Detection System on Machine Learning

A Project

Submitted to the University of Babylon / College of information technology / security department in Partial Fulfilment of the Requirements of the bachelor's degree in Security

Prepared by

Mojtaba saad jasim

Supervised by

Assist. Lec. Shahad A. Hussein

Abstract

Development and implementation of an intrusion detection system (IDS) 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 intrusions in real-time Keypoints to consider in the conclusion of an 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 IDS in handling large-scale 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 IDS 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 IDS with existing cybersecurity infrastructure and tools. Address compatibility issues and the seamless interoperability of the IDS with network monitoring systems and security information and event management (SIEM) platforms.