Problem statement: AI-Powered Threat Detection

Team name: The Qubits
Team members: Karthik Sriram V, Akhilesh T S, Ramya K, Elizabeth Jomy
Institute name: SASTRA University

Abstract:

The emergence of zero-day assaults and ransomware underscores the need for strong AI-driven threat detection systems as cybersecurity threats keep changing. To quickly detect and neutralize new threats, this model provides an artificial intelligence algorithm with real-time network traffic monitoring. To obtain important details including source and destination IP addresses, communication protocols, and other relevant metadata, the suggested system uses feature extraction techniques on network packets. To distinguish between potentially harmful activity and typical network behavior, a machine learning model trained on labeled datasets uses these properties as input.

With a focus on speed, our AI-powered solution is engineered to combat ransomware and zero-day exploits effectively. It monitors network behaviors and traffic using lightweight algorithms, with an emphasis on quick threat detection and containment. The system employs machine learning models to discern possible ransomware behaviors and attacks and employs basic anomaly detection techniques to identify suspicious activities. To improve detection capabilities, Our solution interfaces with threat intelligence streams that are accessible to the general public. When a threat is identified, automated procedures are triggered to lessen its effects. Organizations can strengthen their cyber defenses thanks to the solution, which prioritizes continual learning and adaptation.

The suggested approach places a strong emphasis on ongoing learning and adaptation, enabling a proactive defense mechanism against the ever-changing nature of cyber threats. The adaptable nature of the model guarantees a smaller window of opportunity for attackers by quickly eliminating threats in real time. Additionally, the system is built to be flexible and scalable, accommodating the ever-changing landscape of cyber threats and offering a strong foundation for improving overall cybersecurity posture. In an era where cyber threats pose immediate and complex risks to digital infrastructure and sensitive data, the proposed methodology addresses the need for quick detection and response.