M.Sc. Computer Science with specialization in Artificial Intelligence (2023-’25 Batch)

SEMESTER II MINOR PROJECT ABSTRACT

TOPIC

AI-Powered System for Analyzing Cyber Attack Patterns, Attackers, Techniques, Tactics, and Procedures

PROJECT DESCRIPTION

In today's era, the widespread usage of Android applications in daily life has introduced a significant potential for cyber incidents. These incidents often stem from vulnerabilities present within Android apps, which can lead to various cyber threats. To address this challenge, we propose an approach for analyzing Android applications and detecting Android malware by leveraging the sequence of system calls made by these apps.

We began by collecting a diverse set of Android apps from the Play Store, which we subsequently subjected to thorough analysis and tracing using tools such as Monkey and strace. By tracing the system calls made by these apps, we aimed to gather comprehensive information for malware analysis.

The collected sequences of system calls were then utilized to develop a robust Android malware detection model based on transformer-based architectures, particularly leveraging BERT (Bidirectional Encoder Representations from Transformers). By employing BERT, we aimed to effectively capture the intricate patterns and behaviors indicative of malware presence within the sequences of system calls.

Furthermore, to enhance the interpretability and transparency of our detection model, we incorporated explainability techniques to elucidate the decisions made by the model.

TEAM MEMBERS

1. Abhinand I (Reg No. 34423003)
2. Minhaj P (Reg No. 34423021)
3. Sabin Santhosh (Reg No. 34423030)