National Institute of Technology Rourkela

Departmental Seminar

Seminar Title	: Malware Detector and Classifier using API Call Embedding and Graph Neural Networks
Speaker	: Rajneekant (222cs3383)
Supervisor	: Sumanta Pyne , PIC, Seminar, CS Dept.
Venue	: Seminar Room (CS114)
Date and Time	: 29 May 2024 (11:15 AM)

Abstract : The exponential rise in malware is a significant threat to the current hosts, and it necessitates robust detection and classification mechanisms. Traditional analysis methods like static and dynamic analysis do not successfully identify malware due to evasion techniques. Dynamic techniques can uncover behavior-hiding malware but require a sophisticated malware detector. Current malware detectors use API sequences for detection but overlook the significance of API arguments. To address the limitations, Levenshtein distance is proposed for evaluating the embedding of API calls and thereby enhancing the feature representation. Later, we construct a graphical network from API embeddings, and an appropriate graph neural network model is proposed to derive patterns from the provided graphical structures. The proposed malware detector/classifier achieves a 99.59% malware detection Matthews Correlation Coefficient score and a 74.39% malware classification Matthews Correlation Coefficient score. Overall, the proposed model aims to help understand malware behaviours, improve API call embedding, and detect stealthy malicious samples.