INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

R&D SHOWCASE 2021
Technology, Social Impact

Towards Identifying the Attacks exploiting Vulnerability in Text Data

ABSTRACTS

In the computer era lot of information gets shared via web applications. Although data transmission is convenient over time, it is still prone to many types of attacks. Attackers try to steal sensitive information from us like passwords, credit card details, etc. Cyber attacks are the most commonly happening attacks. These attacks occur due to the vulnerabilities that are present inside the software. There are several types of vulnerabilities that are present. This research focuses on the identification of vulnerabilities and suggests the proactive counter of attacks. The neutralization of attacks deals with the use of the machine learning algorithm. The model trained identifies the attack and classifies the attack into a specific category.

PURPOSE

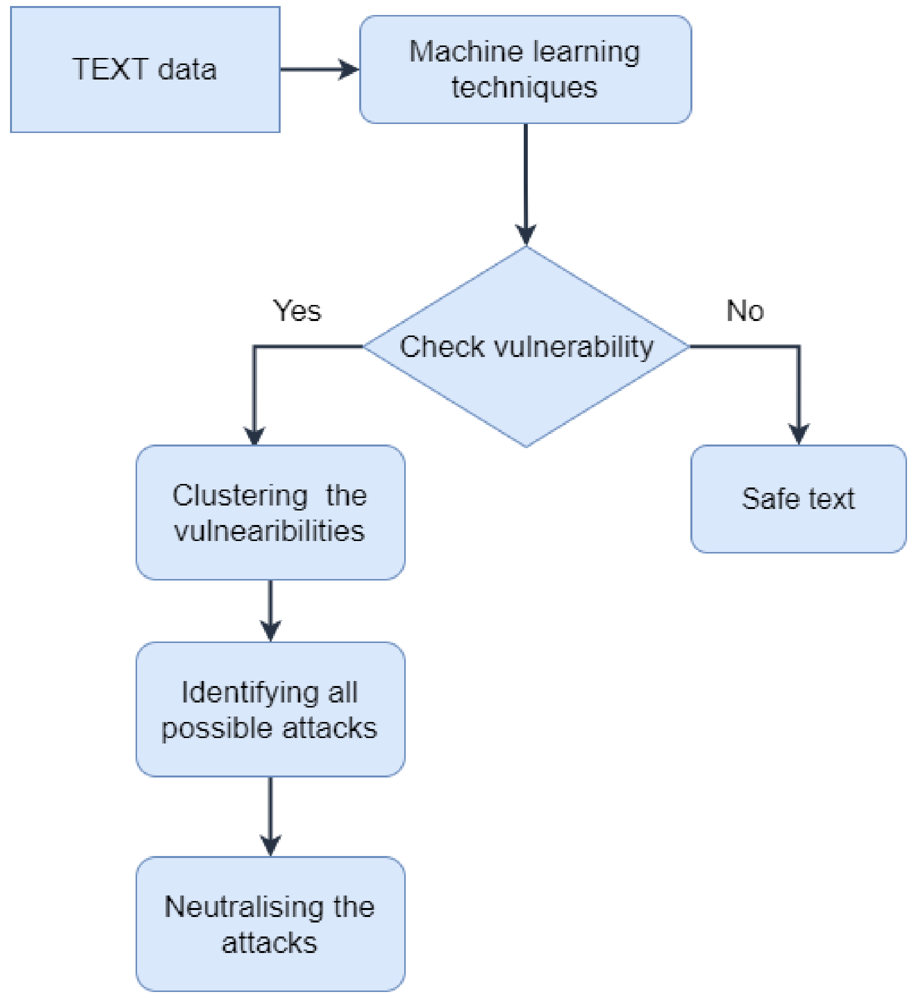
- The primary purpose of this research is to identify the vulnerabilities that are present in the system. Categorize the type of vulnerability, analyze all possible attacks, and take a proactive attack to handle them. All this analysis is done through the available text.
- Social Engineering attacks are one of the significant attacks where people couldn't identify it happening. Here the sensitive information has been collect as bits and pieces from different websites. Finally, all the parts are joined to a single image as a big picture.

OUTCOME

All the possible attacks through the text data that might happen could be identified based on their category, taking proactive measures to neutralize them. This helps in reducing the damage happening to the system.

METHOD

We would be using the machine learning technique and to detect the vulnerability. Based on the accuracy score of the attack. We would be using the clustering technique to categorize the attacks. Once the attacks are identified, we would be using traditional techniques to neutralize the attacks.



TEXT data

Machine learning techniques

Check vulnerability

Yes

No

Clustering the vulnearibilities

Safe text

Identifying all possible attacks

Neutralising the attacks

Authors: Sai Raju Ram Chander Chikkala, Lalit Mohan Sanagavarapu, Raghu Reddy Y

Research Center Name: Software Engineering Research Center