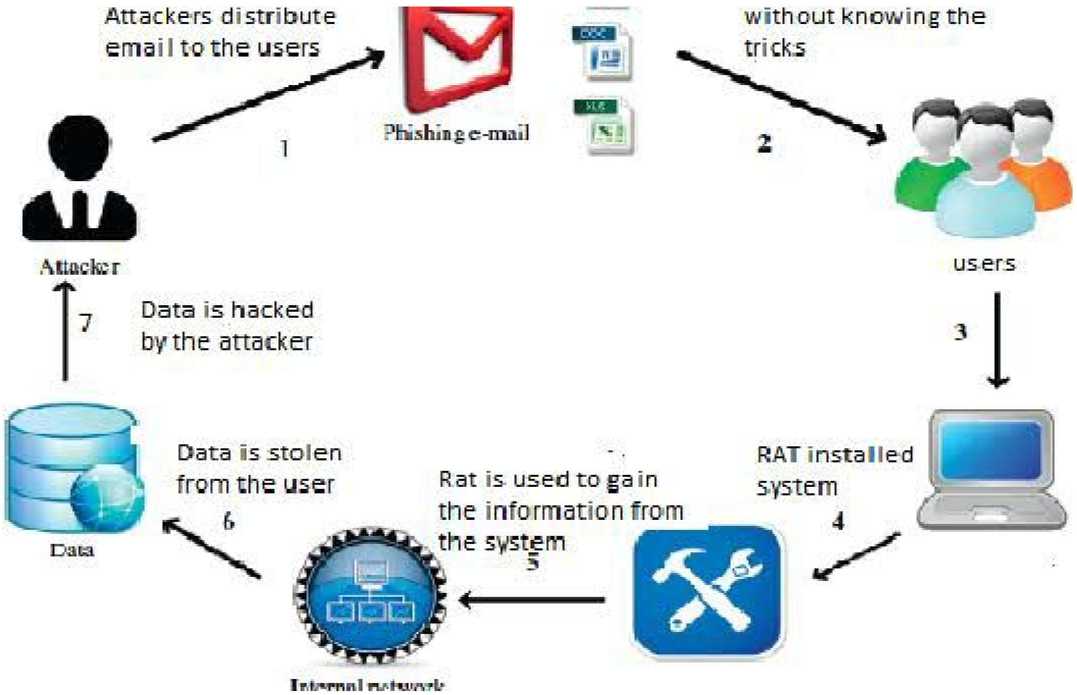
Embathy Map Canvas



List Of Problem Statement

● A phishing site attack is still dangerous for inexperienced internet user to give the attackers his or her private confidential information.

●The traditional methods for detecting phishing attacks are ineffective, with only around 20% of phishing attacks being detected.

●Even on small datasets, ML methods produce better performance, but at a cost of scalability and time.
● Heuristic methods for detecting phishing have a high rate of false positives.

●While IoT gadgets have access to classified resources, their features and security architectures are not yet mature, making them an extremely obvious target for attackers.

- An all-encompassing phishing site attack detection solution could be built in the future to recognize and block malicious websites without the involvement of the user.

- If a website requests login details or confidential information, a system or smart web plug-in solution can verify the site's legitimacy and notify the owner (organization, company, etc.) in advance.

- The growth of phishing attacks is huge due to the covid19 because everything is online and the detection of these attacks is very low.

- This means that we have to work more on the detection of phishing attacks.

- Machine learning is one of the good approaches for detecting phishing attacks..

- This paper compares various research for each machine learning technique in terms of detecting phishing attacks and discusses the benefits and drawbacks of each methodology.

- This paper presents a detailed list of existing phishing attack threats as well as potential research directions in this sphere.

- The DNN, LSTM, CNN, is the best technique for detection of phishing attacks which achieves the best accuracy on the base of the small dataset and low features for phishing URL detection.