Abstract

Twitter, FACEBOOK are very famous social networking site utilized by billions of individuals to exchange the data to one another. To communicate with one another over the long separation it is used. At the same time it additionally attracts the attacker in doing diverse assaults or get the data being imparted by their clients. Twitter users can send the messages to one another as tweets, that tweets have the size impediment of greatest 140 characters. So to share the large information addresses to that pages is used by providing links of that pages. And for this purpose URL shorting is used. Attackers send the suspicious URLs in tweets and move the clients to malignant pages. These URLs can also be shared on Facebook with followers and friends. This paper introduces a Near REAL TIME APPLICATION to detect the suspicious URLs which are shared on twitter’s public timeline. This application collects the tweets, extracts the features correlated to the URL redirect chain, and with the help of training classifier it classifies the URLs as Suspicious and Benign.

Index Terms

Computer Science  Networks

Keywords

Suspicious URL, Twitter, URL redirection, conditionnel redirection, classification.