**PHISHING WEB SITES FEATURES CLASSIFICATION BASED ON**

**MACHINELEARNING**

**ABSTRACT:**

Phishing is one of the most common and most dangerous attacks among cybercrimes. The main aim of these attack is to hack the user information by accessing the credentials that is used by individuals and any of the organizations. Phishing web sites contains various hints among their contents and web browser-based information. The victim’s confidential data is expected by the phishing sites by deriving them to surf a phishing web sites that resembles to legitimate websites, which is one of the criminal attacks prevailing in the internet. Phishing websites is similar to cyber threat that is targeting to get all the credential-based information accessed from the credit cards and social security numbers. The purpose of this project is to perform Extreme Learning Machine (ELM) based classification. There are different types of features based on web pages. Hence, to prevent phishing attacks we must use a specific web page feature. Here, a model based on Machine Learning techniques like Naïve Bayes is used to detect phishing web pages.

**EXISTING SYSTEM:**

Phishing is a Web-based attack that seduces end users to visit fake websites and give away personal information such as user id and password. Phishing web pages are formed by fraudulent people to copy a web page from an original one. These phishing web pages are very similar to the original ones. Technical tricks and social engineering are extensively joined together for beginning a phishing attack. An important view of online security is to protect users from phishing attacks and fake website. Intelligent methods can be used to develop fake web pages. For this reason, internet users whether have enough experience in information security or not might be cheated. Phishing attacks can be launched via sending an e-mail that seems to be sent from a trusted public or private organization to users by attackers. Attackers get the users to update or verification their information by clicking a link within the e-mail. Other methods such as file sharing, blogs, and forums can be used by attackers for phishing. There are many ways to fight phishing including legal solutions, education, and echnical solution. Nowadays, information and communication tools are used in a manner that is very dense with information. For this purpose,various solution methods for various problem types have been developed.

**PROPOSED SYSTEM:**

An important view of online security is to protect users from phishing attacks and fake website. Intelligent methods can be used to develop fake web pages. For this reason, internet users whether have enough experience in information security or not might be cheated. Phishing attacks can be launched via sending an e-mail that seems to be sent from a trusted public or private organization to users by attackers. Attackers get the users to update or verification their information by clicking a link within the e-mail.Other methods such as file sharing, blogs, and forums can be used by attackers for phishing. There are many ways to fight phishing including legal solutions, education, and technical solution. Nowadays, information and communication tools are used in a manner that is very dense with information. For this purpose, various solution methods for various problem types have been developed.

**SYSTEM REQUIREMENTS:**

**Hardware Requirements:**

Processor : I3 processor onwards

Ram : 4 GB(min)

Hard Disk : 340 GB

**Software Requirements:**

Operating System : Windows 10

Coding Language : Python

IDE : Jupyter NoteBook

Dataset