**PHISHING WEBSITE DETECTION USING MACHINE LEARNING**

**ABSTRACT**

Phishing is quite a popular form of cyber-attacks these days in which the user is made to visit illegitimate websites. In these websites, the user can be tricked into revealing his sensitive information such as username, passwords, bank details, card details, etc. Thus, it has been used quite a lot by phishers to obtain a user’s credentials. The phishing URLs look almost similar to the legitimate ones but actually differ in some respect. In our method, we make use of only the information about the URL of a website to determine whether the website is a phishing website or not. Thus, there is no need of actually visiting a website to determine whether it is phishing or not. This also allows the user to not visit the phishing websites and expose themselves to malicious codes that it may carry. Also, we discuss how meta data of the URLs can be used to determine whether the URL is phishing or not. Random forest algorithm can then be applied to a dataset having such features that contain the meta data of the URLs. Random forest algorithm offers the advantage of not overfitting the data as well

**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 : Dual Core I5 Speed : 3.5 Ghz

Ram : 8 GB(min)

Hard Disk : 320 GB

**Software Requirements:**

Operating System : Windows 10

Coding Language : Python

Dataset

Jupyter Notebook

Machine Learning Libraries