**PHISHING WEBSITE DTECTION**

**OBJECTIVE:**

The main objective of this application is to investigate a specific problem of whether it is valuable or not to use machine learning techniques to predict the type of website.

**ABSTRACT:**

Phishing is a common attack on credulous people by making them to disclose their unique information using counterfeit websites. The objective of phishing website URLs is to purloin the personal information like user name, passwords and online banking transactions. Phishers use the websites which are visually and semantically similar to those real websites. As technology continues to grow, phishing techniques started to progress rapidly and this needs to be prevented by using anti-phishing mechanisms to detect phishing. Machine learning is a powerful tool used to strive against phishing attacks. This paper surveys the features used for detection and detection techniques using machine learning.

**EXISTING SYSTEM:**

Where as in the case of the existing system means that what is previous system says a Manual human intervention is not that much applicable and error-prone. Legacy and Conventional Data Mining Algorithms can’t deal with huge volumes of data, slower and inaccurate.

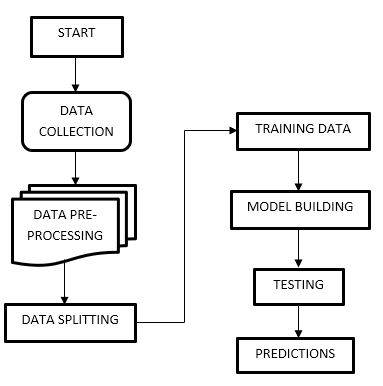
**DISADVANTAGES:**

1. Late process
2. Its more time
3. No accurate result

**PROPOSED SYSTEM:**

Machine Learning is cutting edge and trending for different kinds of diverse application in the society where it can deal with tons of data, refined and revised algorithms, and available heavy processing power in terms of GPU.

**FLOW CHART:**



**ADVANTAGES:**

* High accuracy.
* Low complexities.
* High reliability.

**SYSTEM SPECIFICATIONS:**

# H/W SPECIFICATIONS:

# Processor : I3/Intel Processor

* RAM : 4GB (min)
* Hard Disk : 128 GB
* Key Board : Standard Windows Keyboard
* Mouse : Two or Three Button Mouse
* Monitor : Any

**S/W SPECIFICATIONS:**

* Operating System : Windows 7+
* Server-side Script : Python 3.6+
* IDE : PyCharm.
* Libraries Used : Pandas, Numpy, Matplotlib, OS.