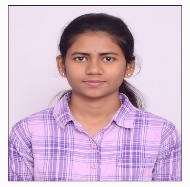
****

**16WH1A1230**

**M. Lavanya**



**16WH1A1232**

**K. Bindu Sri**



**16WH1A1251**

**V. Dharani**

**Ms. P. Sree Lakshmi**

**Assistant Professor of IT**

**sreelakshmi.p@bvrithyderabad.edu.in**





**Team**

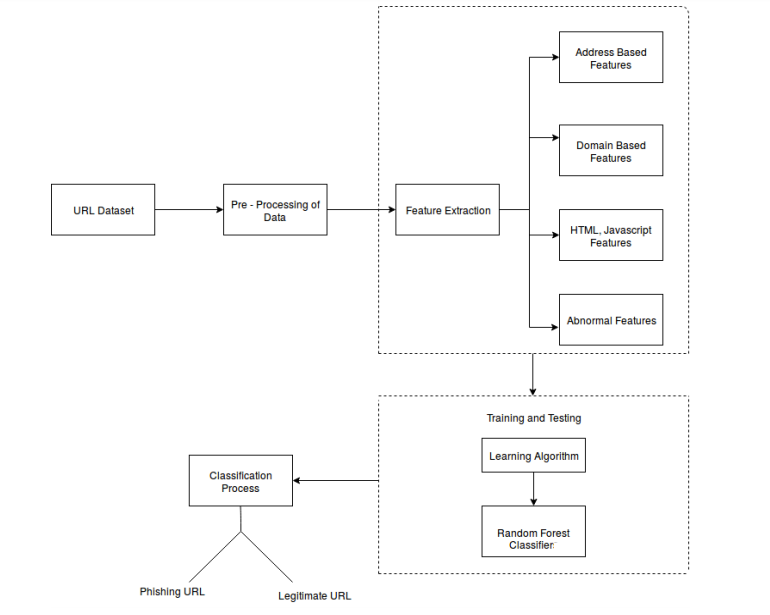
**Tools and Technologies**

* **Python 3.7**
* **Jupyter Notebook**
* **Spyder**
* **Mathplotlib**
* **Pandas**
* **Numpy**
* **SKLearn**

**Conclusion and Future Scope**

It is seen that existing system give less accuracy so we proposed a new phishing method that employs URL based features and also we generated classifiers through machine learning algorithm. We have found that our system provides us with 92.28% of accuracy for Random Forest. The proposed technique more secure as it detects new and previous phishing sites.

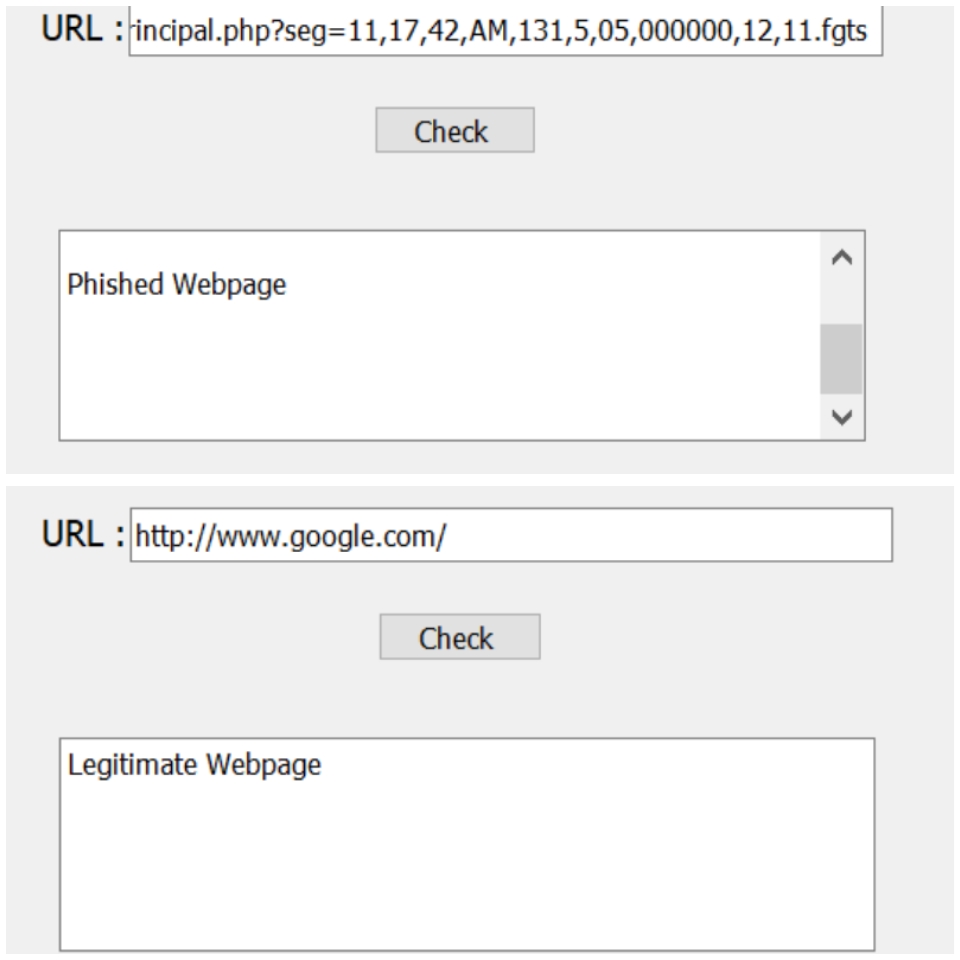
**Architecture**



**Modules**

Feature Collector

Random Forest

****

**Abstract**

Phishing is the most unsafe criminal exercises in cyber space. The objective of phishing website URLs is to track and get personal information like user name, passwords and online banking transactions. It can be described as the process of attracting online users to obtain their sensitive information. The system is based on a machine learning method, particularly supervised learning. We have selected the Random Forest technique due to its good performance in classification. Classification is done by ranking the page from 0 to 1 and the output format is according to the page rank.

**Web 2.0 technologies made users to spend more time on the Internet to search for answers about various questions.**

**TEAM**

**15**

**Web Phishing Detection Using**

**Machine Learning**

**BVRIT HYDERABAD**

**College of Engineering for Women**

**Department of Information Technology**

**Major Project - Academic Year 2019-20**

**Guide**