# LITERATURE SURVEY

Batch Number: **B6-6M2E** Team Members:

1. **Santhosh S**
2. **Yashwanth N**
3. **Prajwel V**
4. **Nandish P**

## Web phishing detection

1. Oluwatobi Ayodeji Akanbi, ... Elahe Fazeldehkordi, in A Machine-Learning Approach to Phishing Detection and Defense, 2015

This paper presented an intelligent phishing detection and protection scheme by employing a new approach using the integrated features of images, frames and text of phishing websites. An efficient ANFIS algorithm was developed, tested and verified for phishing website detection and protection based on the schemes proposed in Aburrous et al. (2010) and Barraclough and Sexton (2015). A set of experiments was performed using 13,000 available datasets.

**Advantage:**

The approach showed an accuracy of 98.3%, which so far, is the best-integrated solutions for web-phishing detection and protection.

2. LongfeiWu etal..., "Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms, "

In this paper, author did a comprehensive study on the security vulnerabilities caused by mobile phishing attacks, including the web page phishing attacks.

**Advantage:**

Author propose MobiFish, a novel automated lightweight antiphishing scheme for mobile platforms. MobiFish verifies the validity of web pages, applications, and persistent accounts by comparing thee actual Identity to the claimed identity

3. Surbhi Gupta etal., "A Literature Survey on Social Engineering Attacks: Phishing Attacks," in International Conference on Computing, Communication and Automation(ICCCA2016)
   To fool an online user into elicit personal Information. The prime objective of this review is to do literature survey on social engineering attack:
   Phishing attacks and techniques to detect attack.
   **Advantage:**

   The paper discusses various types of Phishing attacks such as Tab-napping, spoofing emails, Trojan horse, hacking and how to prevent them.

4. **SANS Institute, "Phishing : An Analysis of a Growing Problem",2007.** This paper gives an in depth analysis of phishing : what it is, the technologies and security Weaknesses it takes advantage of the dangers it poses to end users.
   **Advantage:**

   In this analysis author explain the concepts and technology behind phishing, show how the threat is much more then just a nuisance or passing trend, and discuss how gangs of criminals are Using these scams to make a great deal of money.

5. **Guardian Analytics, "A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security"** Commercial and retail account holders at financial institutions of all sizes are under attacks by sophisticated, Organized, Well-funded cyber criminals **Advantage:**

Anomaly detection solutions are readily available, are deployed quickly and immediately and automatically protect all account holders against all types of fraud attack with minimal Disruption to legitimate online banking activity.

6. **literature survey on Retraction: Phishing website detection using machine learning and deep learning techniques" 1916**
   In phishing attacks, the intruder puts on an act as if it is a trusted organization with an intention to purloin liable and essential information. The methodology they discovered is a powerful technique to detect the phished websites and can provide more effective defenses for phishing attacks of the future
   **Advantage:**
   The association between independent variables as well as dependent variables can be formed without any presumptions about the statistical depiction of the aspect. It contributes positive gains on regression algorithm which includes its competence to act with noisy data.

7. **Phishing Website Detection Based on Deep Convolutional Neural Network and Random Forest Ensemble Learning**
   This paper proposes an integrated phishing website detection method based on convolutional neural networks (CNN) and random forest (RF). The method can predict the legitimacy of URLs without accessing the web content or using third-party services. The proposed technique uses character embedding techniques to convert URLs into fixed-size matrices, extract features at different levels
   **Advantage:**
   A 99.35% correct classification rate of phishing websites was obtained on the dataset. Experiments were conducted on the test set and training set, and the experimental results proved that the proposed method has good generalization ability and is useful in practical applications.