**LITERATURE SURVEY**

1. M. Vijayalakshmi, S. Mercy Shalinie, Ming Hour Yang and Raja Meenakshi U, “Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future directions”, IET Networks, Vol. 9, Iss. 5, pp. 235-246, 2020.

**Description:**

Phishing is the most deceiving attack, which exploits the vulnerabilities in the end-users. Phishing is often done through emails and malicious websites to lure the user by posing themselves as a trusted entity. Security experts have been proposing many anti-phishing techniques. Till today, there is no single solution that is capable of mitigating all the vulnerabilities.

1. Peng Yang, Guangzhen Zhao and Peng Zeng, “Phishing Website Detection based on Multidimensional Features driven by Deep Learning”, IEEE Access, Vol. 7, pp. 15196-15209, 2019.

**Description:**

Phishing is currently a critical threat facing the Internet, and losses are growing steadily. Feature engineering is important in phishing website detection solutions, but the accuracy of detection critically depends on prior knowledge of features. This approach can reduce the detection time for setting a threshold.

1. Jian Mao, Jingdong Bian, Wenqian Tian, Shishi Zhu, Tao Wei, Aili Li and Zhenkai Liang, “Phishing page detection via learning classifiers from page layout feature”, EURASIP Journal on Wireless Communications and Networking, pp: 1-14, 2019.

**Description:**

In phishing web site detection, comprehensively evaluating page similarity remains a great challenge. In this paper, a learning-based aggregation analysis was use mechanism to determine similarity of page layouts and detect phishing pages. Our approach can effectively enhance the performance of existing anti-phishing mechanisms.

1. Zhu, E., Chen, Y., Ye, C., et al.: ‘OFS-NN: an effective phishing websites detection model based on optimal feature selection and neural network’, IEEE Access, 2019, 7, pp. 73271–73284

**Description:**

Phishing attack is now a big threat to people’s daily life and networking environment. The selected optimal features are used to train the underlying neural network, and finally, an optimal classifier is constructed to detect the phishing websites. This algorithm could properly deal with problems of big number of phishing sensitive features and the continuous changes of features.

1. Mao, J., Tian, W., Li, P., et al.: ‘Phishing-alarm: robust and efficient phishing detection via page component similarity’, IEEE Access, 2017, 5, pp. 17020– 17030

**Description:**

Social networks have become one of the most popular platforms for users to interact with each other. Given the huge amount of sensitive data available in social network platforms, user privacy protection on social networks has become one of the most urgent research issues. We develop techniques to identify effective CSS features, as well as algorithms to efficiently evaluate page similarity.

1. Gowtham, R., Krishnamurthi, I.: ‘A comprehensive and efficacious architecture for detecting Phishing webpages’, Comput. Sec., 2014, 40, pp. 23–37

**Description:**

Phishing is a web-based criminal act. Phishing sites lure sensitive information from naive online users by camouflaging themselves as trustworthy entities. These heuristic results were fed as an input to a trained machine learning algorithm to detect phishing sites. Before applying heuristics to the webpages, we used two preliminary screening modules in this system

In phishing web site detection, comprehensively evaluating page similarity remains a great challenge. In this paper, a learning-based aggregation analysis was use mechanism to determine similarity of page layouts and detect phishing pages. Our approach can effectively enhance the performance of existing anti-phishing mechanisms.