LITERATURE SURVEY

Batch Number: B2-2M4E

Team Members: 1. BAIDEHI SHARAN YADAV

2. AJAY KUMAR CHAUDHARY

3. KAMALI S

4. INDHU S

S.NO	PAPER TITLE	PAPER CONCEPT	ADVANTAGE	DISADVANTAGE
1	LongfeiWu etal..., "Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms, " IEEE 2016, pp.6678-6691.	In this paper, author did a comprehensive study on the security vulnerabilities caused by mobile phishing attacks, including the web page phishing attacks.	Author propose MobiFish, a novel automated lightweight anti-phishing scheme for mobile platforms. MobiFish verifies the validity of web pages, applications, and persistent accounts by comparing thee actual Identity to the claimed identity	Existing schemes designed for web phishing attacks on PCs cannot effectively address the various phishing attacks on mobile devices.

2	Surbhi Gupta etal., "A Literature Survey on Social Engineering Attacks: Phishing Attacks," in International Conference on Computing, Communication and Automation(ICCCA2016),2016, pp. 537-540.	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.	The paper discusses various types of Phishing attacks such as Tab-napping, spoofing emails, Trojan horse, hacking and how to prevent them.	Every organization has security issues that have been of great concern to u sets, site developers, and specialists, in order to defend the confidential data from this type of social engineering attack.
3	Guardian Analytics, "A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security". [Accessed : 08 Jan 2015]	Commercial and retail account holders at financial institutions of all sizes are under attacks by sophisticated, Organized, Well-funded cyber criminals.	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.	Implementing anomaly detection will not only meet FFIEC Expectations, it will decrease the total cost of fraud, and will increase customer loyalty and trust.
4	SANS Institute, "Phishing : An Analysis of a Growing Problem",2007. 1417[Accessed : 23 May 2017]	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.	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	Unfortunately, a growing number of cyber-thieves Are using these same systems to manipulate us and steal our private information.

			these scams to make a great deal of money.	
5	J. Phys.: Conf. Ser. "A literature survey on Retraction: Phishing website detection using machine learning and deep learning techniques" 1916 (2021) 012407.	Nowadays, website phishing is more damaging. It is becoming a big threat to people's daily life and networking environment. In these 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 we discovered is a powerful technique to detect the phished websites and can provide more effective defenses for phishing attacks of the future.	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.	The ANN's are not suitable for infrequent or utmost events where data is inadequate in order to train it. ANNs do not permit the embodiment of human mastery to be substitutive for perceptible proof.

6	"Phishing Website Detection Based on Deep Convolutional Neural Network and Random Forest Ensemble Learning" ,This research was funded by the National Key R & D Program of China Grant Numbers 2017YFB0802800 and Beijing Natural Science Foundation (4202002)	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	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.	It takes longer to train. However, the trained model is better than the others in terms of accuracy of phishing website detection. Another disadvantage is that the model cannot determine whether the URL is active or not, so it is necessary to test whether the URL is active or not before detection to ensure the effectiveness of detection. In addition, some attackers use URLs that are not imitations of
		using CNN models, classify multi-level features using multiple RF classifiers, and, finally, output prediction results using a winner-take-all approach.		other websites, and such URLs will not be detected.