Phishing Detection with Machine Learning Technology

Aishwarya Shahane[1], Shivam Shete[2], Manasi Nemane[3], Pravin Katkade[4], Dr. H. B. Jadhav[5]

Students, Computer Engineering[1,2,3,4]

Professor, Computer Engineering[5]

Adsul Technical Campus, Ahmednagar, Maharashtra, India

Abstract*: Today everyone is highly addicted to Internet. Everyone has done online shopping and online activities like online bank, online booking, online recharge and others on the Internet. Phishing is a type of web threat and phishing is Illegally on the original website Information such as login name, password and credit card information. This paper proposed an efficient phishing detection based on machine learning technique. Overall, the experimental results show that the proposed when integrated with the Support vector machine classifier, has the best performance in accurate discrimination 95.66% of phishing and suitable websites are used by only 22.5% innovative functionality. The proposed technique shows optimistic results when compared to a number of benchmarks "University of California Irvine (UCI)" phishing data files archives. Therefore, the proposed technique is preferred and used for machine learning-based phishing detection*

Keywords: phishing , web , machine learning , director component analysis, vector machine support.

REFERENCES

[1] Higashino, M., et al. An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage. in 2019 5th International Conference on Information Management (ICIM). 2019.

[2] H. Bleau, Global Fraud and Cybercrime Forecast,. 2017.

[3] Michel Lange, V., et al., Planning and production of grammatical and lexical verbs in multi-word messages. PloS one, 2017. 12(11): p. e0186685-e0186685.

[4] Rahman, S.S.M.M., et al. Performance Assessment of Multiple Machine Learning Classifiers for Detecting the Phishing URLs. 2020. Singapore: Springer Singapore.

[5] He, M., et al., An efficient phishing webpage detector. Expert Systems with Applications, 2011. 38(10): p. 12018-12027.

[6] Mohammad, R.M., F. Thabtah, and L. McCluskey. An assessment of features related to phishing websites using an automated technique. In 2012 International Conference for Internet Technology and Secured Transactions. 2012.

[7] Abdelhamid, N., A. Ayesh, and F. Thabtah, Phishing detection based Associative Classification data mining. Expert Systems with Applications, 2014. 41(13): p. 5948-5959.

[8] Toolan, F. and J. Carthy. Feature selection for Spam and Phishing detection. in 2010 eCrime Researchers Summit. 2010.

[9] Jain, A.K. and B.B. Gupta, Towards detection of phishing websites on client-side using machine learning based approach. Telecommunication Systems, 2018. 68(4): p. 687-700.

[10] 1PhishTank, Phishing dataset. 2018, Verified phishing URL.

[11] 1Openfish, Phishing dataset. 2018.

[12] 1Chiew, K.L., et al., Utilisation of website logo for phishing detection. Computers & Security, 2015. 54: p. 16-26.

[13] Benavides, E., et al. Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review. 2020. Singapore: Springer Singapore.

[14] Zhang, W., et al., Two-stage ELM for phishing Web pages detection using hybrid features. World Wide Web, 2017. 20(4): p. 797-813.

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-9868

242

ISSN
2581-9429
IJARSCT

[15] El-Alfy, E.-S.M., Detection of phishing websites based on probabilistic neural networks and K-medoids clustering. The Computer Journal, 2017. 60(12): p. 1745-1759.

[16] Montazer, G.A. and S. ArabYarmohammadi, Detection of phishing attacks in Iranian e-banking using a fuzzy–rough hybrid system.Applied Soft Computing, 2015. 35: p. 482-492.

[17] Wang, Y.-G., G. Zhu, and Y.-Q. Shi, Transportation spherical watermarking. IEEE Transactions on Image Processing, 2018. 27(4): p. 2063-2077.

[18] De Maio, C., et al., Time-aware adaptive tweets ranking through deep learning. Future Generation Computer Systems, 2019. 93: p. 924-932.

[19] De Maio, C., et al., Social media marketing through time aware collaborative filtering. Concurrency and Computation: Practice and Experience, 2018. 30(1): p. e4098.

[20] Peng, T., I. Harris, and Y. Sawa. Detecting Phishing Attacks Using Natural Language Processing and Machine Learning. in 2018 IEEE 12th International Conference on Semantic Computing (ICSC). 2018.

[21] Abdi, H. and L.J. Williams, Principal component analysis. WIREs Computational Statistics, 2010. 2(4): p. 433-459.

[22] Sahingoz, O.K., et al., Machine learning based phishing detection from URLs. Expert Systems with Applications, 2019. 117: p. 345-357.