

References

- [1] Baykara, M., & Gürel, Z. Z. (2018, March). Detection of phishing attacks. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-5). IEEE.
- [2] Brijain, M., Patel, R., Kushik, M. R., & Rana, K. (2014). A survey on decision tree algorithm for classification.
- [3] Cahyani, D. E., & Nuzry, K. A. P. (2019, November). Trending Topic Classification for Single-Label Using Multinomial Naive Bayes (MNB) and Multi-Label Using K-Nearest Neighbors (KNN). In *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 547-552). IEEE
- [4] Chawla, N. V. (2009). Data mining for imbalanced datasets: An overview. *Data mining and knowledge discovery handbook*, 875-886.
- [5] Chauhan, H., & Chauhan, A. (2013). Implementation of decision tree algorithm c4. 5. *International Journal of Scientific and Research Publications*, 3(10), 1-3.
- [6] Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006, June). Phishing email detection based on structural properties. In *NYS cyber security conference* (Vol. 3).
- [7] El Aassal, A., Moraes, L., Baki, S., Das, A., Verma, R., & Verma, A. D. R. (2018). Anti-phishing pilot at ACM IWSPA 2018. In *Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secur. Privacy Anal. (IWSPA)* (pp. 1-9). Tempe, AZ, USA.
- [8] Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016, August). Social engineering attack strategies and defence approaches. In *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)* (pp. 145-149). IEEE.
- [9] Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation (ICCCA)* (pp. 537-540). IEEE.
- [10] Hu, W., Hu, W., & Maybank, S. (2008). Adaboost-based algorithm for network intrusion detection. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 38(2), 577-583
- [11] Ivaturi, K., & Janczewski, L. (2011, June). A taxonomy for social engineering attacks. In *International Conference on Information Resources Management* (pp. 1-12). Centre for Information Technology, Organizations, and People.
- [12] Kibriya, A. M., Frank, E., Pfahringer, B., & Holmes, G. (2004, December). Multinomial naive bayes for text categorization revisited. In *Australasian Joint Conference on Artificial Intelligence* (pp. 488-499). Springer, Berlin, Heidelberg
- [13] Lansley, M., Mouton, F., Kapetanakis, S., & Polatidis, N. (2020). SEADer++: social engineering attack detection in online environments using machine learning. *Journal of Information and Telecommunication*, 4(3), 346-362.
- [14] Miyamoto, D., Hazeyama, H., & Kadobayashi, Y. (2008, November). An evaluation of machine learning-based methods for detection of phishing sites. In *International Conference on Neural Information Processing* (pp. 539-546). Springer, Berlin, Heidelberg.
- [15] Ni, S., Qian, Q., & Zhang, R. (2018). Malware identification using visualization images and deep learning. *Computers & Security*, 77, 871-885.
- [16] Parekh, S., Parikh, D., Kotak, S., & Sankhe, S. (2018, April). A new method for detection of phishing websites: URL detection. In *2018 Second international conference on inventive communication and computational technologies (ICICCT)* (pp. 949-952). IEEE.
- [17] Pinto, A., Gonçalo Oliveira, H., & Oliveira Alves, A. (2016). Comparing the performance of different NLP toolkits in formal and social media text. In *5th Symposium on Languages, Applications and Technologies (SLATE'16)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
- [18] Repalle, S. A., & Kolluru, V. R. (2017). Intrusion detection system using ai and machine learning algorithm. *International Research Journal of Engineering and Technology (IRJET)*, 4(12), 1709-1715.
- [19] Şahingöz, Ö. K., Buber, E., Demir, Ö., & Diri, B. (2017). Machine Learning Based Phishing Detection from URIs.
- [20] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: a survey. *Future Internet*, 11(4), 89.
- [21] Stergiou, D. (2013). Social Engineering and Influence: A Study that Examines Kevin Mitnick's Attacks through Robert Cialdini's Influence Principles
- [22] Su, J., & Zhang, H. (2006, July). A fast decision tree learning algorithm. In *AAAI* (Vol. 6, pp. 500-505).
- [23] Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, 8, 85094-85115.
- [24] Waykole, R. N., & Thakare, A. D. (2018). A Review of feature extraction methods for text classification. *Int. J. Adv. Eng. Res. Dev.*, 5(04).
- [25] Unnithan, N. A., Harikrishnan, N. B., Vinayakumar, R., Soman, K. P., & Sundarakrishna, S. (2018). Detecting phishing E-mail using machine learning techniques. In *Proc. 1st Anti-Phishing Shared Task Pilot 4th ACM IWSPA Co-Located 8th ACM Conf. Data Appl. Secur. Privacy (CODASPY)* (pp. 51-54).
- [26] Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. *Security and Privacy*, 2(4), e73.
- [27] Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4), 297-307.
- [28] Young, T., Hazarika, D., Poria, S., & Cambria, E. (2018). Recent trends in deep learning based natural language processing. *IEEE Computational Intelligence Magazine*, 13(3), 55-75.
- [29] Zoghi, Z. (2020). Ensemble Classifier Design and Performance Evaluation for Intrusion Detection Using UNSW-NB15 Dataset (Doctoral dissertation, University of Toledo).

Authors Profile

Asma A. Alsufyani, Master Cybersecurity, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia

Sabah M. Alzahrani, Assistance professor of Computer and Information systems Engineering. Vice Chair of Computer Engineering Department, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia