IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 1, June 2022

Browser Based Malicious Domain Detection through Extreme Learning Machine

Dr. G. Nanthakumar[1], Arunprakash. R[2], Balamurugan. G[3], Karthick. S[4]

Professor, Department of Computer Science Engineering[1]

Final Year Students, Department of Computer Science Engineering[2,3,4]

Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *The main aim of the project is to detect the malicious domains in the internet through Machine learning approaches and is helpful in preventing the cybercrime. For that Extreme Learning Machine(ELM) approach is used to find the malicious domains in the web. The Terms used for the project are Browser application, extreme learning machine, feature selection, malicious domain detection, machine learning, Real-time training. This approach will be helpful in reducing the cybercrime such as harmful websites, fake websites that stores the user information, malicious attack website domains.*

Keywords: DNS- Domain Name System, URL- Uniform Resource Locator, ELM –Extreme learning Machine .

REFERENCES

[1]. Y. Zhauniarovich, I. Khalil, T. Yu, and M. Dacier, ''A survey on malicious domains detection through DNS data analysis,'' ACM Comput. Surv., vol. 51, no. 4, pp. 1–36, Sep. 2018.

[2]. J. Woodbridge, H. S. Anderson, A. Ahuja, and D. Grant, ''Predicting domain generation algorithms with long short-term memory networks,'' 2016, arXiv:1611.00791.

[3]. S. Vosoughi, P. Vijayaraghavan, and D. Roy, ''Tweet2Vec: Learning tweet embeddings using character-level CNN-LSTM encoder-decoder,'' in Proc. 39th Int. ACM SIGIR Conf., 2016, pp. 1041–1044.

[4]. D. S. Berman, ''DGA CapsNet: 1D application of capsule networks to DGA detection,'' Information, vol. 10, no. 5, p. 157, Apr. 2019.

[5]. Y. Qiao, B. Zhang, W. Zhang, A. K. Sangaiah, and H. Wu, ''DGA domain name classification method based on long short-term memory with attention mechanism,'' Appl. Sci., vol. 9, no. 20, p. 4205, Oct. 2019.

[6]. L. Yang, G. Liu, Y. Dai, J. Wang, and J. Zhai, ''Detecting stealthy domain generation algorithms using heterogeneous deep neural network framework,'' IEEE Access, vol. 8, pp. 82876–82889, 2020.

[7]. F. Pendlebury, F. Pierazzi, R. Jordaney, J. Kinder, and L. Cavallaro, ''Tesseract: Eliminating experimental bias in malware classification across space and time,'' in Proc. USENIX Secur., 2019, pp. 729–746.

[8]. Y. Shi, G. Chen, and J. Li, ''Malicious domain name detection based on extreme machine learning,'' Neural Process. Lett., vol. 48, no. 3, pp. 1347–1357, Dec. 2018.

[9]. G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, ''Extreme learning machine: Theory and applications,'' Neurocomputing, vol. 70, nos. 1–3, pp. 489–501, Dec. 2006.

[10]. W. Cao, X. Wang, Z. Ming, and J. Gao, ''A review on neural networks with random weights,'' Neurocomputing, vol. 275, pp. 278–287, Jan. 2018.

[11]. C.-J. Chien, N. Yanai, and S. Okamura. (2021). Design of Malicious Domain Detection Dataset for Network Security. [Online]. Available: http://www-infosec.ist.osaka-u.ac.jp/~yanai/dataset.

DOI: 10.48175/IJARSCT-4754