IJARSCT

ISSN (Online) 2581-9429

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

Impact Factor: 6.252

Volume 2, Issue 1, June 2022

The Web Attack Detection System for Internet of Things via Ensemble Classification

Mr. P. Manikanda Prabhu[1], Ambrish. T[2], Jagadeesh. M. N[3], Abishek. M[4]

Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *Internet of Things (IoT) networks contain millions of devices with the function of interacting with each other and providing useful things that were never available to us before. However, the diversity in types of IoT devices makes the IoT networks' environments more complex and more vulnerable to various web attacks compared to traditional computer networks. We propose a novel machine learning based Web Attack Detection System (WADS) to alleviate the serious issues that IoT networks faces. Specifically, we have used two machine learning classifier to detect web attacks separately. We then use an MLP classifier to make the final decision according to the results obtained from the Dataset. In order to evaluate the proposed system, we have performed experiments on a public dataset as well as a real-word dataset running in a distributed environment. Experimental results show that the proposed system can detect web attacks accurately with low false positive and negative rates.*

Keywords: Machine learning, MLP classifier, Internet of Things (IoT), web attack detection

REFERENCES

[1]. M. Lin, C. Chiu, Y. Lee, and H. Pao, "Malicious URL filtering—A big data application," in Proc. IEEE Int. Conf. Big Data, 2013, pp. 589–596.

[2]. D. Kar, S. Panigrahi, and S. Sundararajan, "SQLiDDS: SQL injection detection using query transformation and document similarity," in Proc. Int. Conf. Distrib. Comput. Internet Technol., 2015, pp. 377–390.

[3]. A. Le, A. Markopoulou, and M. Faloutsos, "PhishDef: URL names say it all," in Proc. IEEE INFOCOM, 2011, pp. 191–195.

[4]. J. Qiu, L. Du, D. Zhang, S. Su, and Z. Tian, "Nei-TTE: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city," IEEE Trans. Ind. Informat., vol. 16, no. 4, pp. 2659–2666, Apr. 2020.

[5]. P. Bisht, P. Madhusudan, and V. N. Venkatakrishnan, "Dynamic candidate evaluations for automatic prevention of SQL injection attacks," ACM Trans. Inf. Syst. Secur., vol. 13, no. 2, pp. 398–404, 2010.

[6]. C. Luo, S. Su, and Y. Sun, "A convolution-based system for malicious URL requests detection," Comput. Mater. Continua, vol. 61, no. 3, pp. 399–411, 2019.

[7]. M. Li, Y. Sun, H. Lu, S. Maharjan, and Z. Tian, "Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems," IEEE Internet Things J., vol. 7, no. 7, pp. 6266–6278, Jul. 2020.

[8]. Y. H. Hwang, "IoT security & privacy: Threats and challenges," in Proc. 1st Acm Workshop on Iot Privacy Trust and Security, 2015.

[9]. A. Jamdagni, Z. Tan, and X. He, "RePIDS: A multi-tier real-time payload-based intrusion detection system," Comput. Netw., vol. 57, no. 3, pp. 811–824, 2013.

[10]. Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denialof-service attack detection based on multivariate correlation analysis," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 447–456, Feb. 2014.

[11]. C. Torrano-Gimenez, H. T. Nguyen, G. Alvarez, S. Petrovi´c, and K. Franke, "Applying feature selection to payload-based web application firewalls," in Proc. 3rd Int. Workshop Secur. Commun. Netw., 2011, pp. 75–81.

[12]. J. Macqueen, "Some methods for classification and analysis of multivariate observations," inProc. 5th Berkeley

DOI: 10.48175/IJARSCT-4638

Symp. Math. Statist. Probability, 1965, vol. 1, no. 14, pp. 281–297.

[13]. D. Kar, S. Panigrahi, and S. Sundararajan, “SQLiGoT: Detecting SQL injection attacks using graph of tokens and SVM,” Comput. Secur., vol. 60, pp. 206–225, 2016.

[14]. J. Saxe and K. Berlin, “eXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys,” 2017, arXiv:1702.08568.

[15]. M. Ito and H. Iyatomi, “Web application firewall using character-level convolutional neural network,” in Proc. IEEE 14th Int. Colloq. Signal Process. Its Appl., 2018, pp. 103–106.

[16]. J. Liang, W. Zhao, and W. Ye, “Anomaly-based web attack detection: A deep learning approach,” in Proc. VI Int. Conf. Netw., Commun. Comput., 2017, pp. 80–85.

[17]. J. Qiu, Z. Tian, and C. Du, “A survey on access control in the age of Internet of things,” IEEE Internet Things J., vol. 7, no. 6, pp. 4682–4696, Jun. 2020.

[18]. J. Ma, L. K. Saul, and S. Savage, “Beyond blacklists: Learning to detect malicious web sites from suspicious URLs,” in Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2009, pp. 1245–1254.

[19]. I. Lee, S. Jeong, and S. Yeo, “A novel method for SQL injection attack detection based on removing SQL query attribute values,” Math. Comput. Modelling, vol. 55, no. 1-2, pp. 58–68, 2012.

[20]. F. Yong, P. Jiayi, L. Liang, and H. Cheng, “WOVSQLI: Detection of SQL injection behaviors using word vector and LSTM,” in Proc. 2nd Int. Conf. Cryptography, Secur. Privacy, 2018, pp. 170–174.

[21]. T. Liu, Y. Qi, L. Shi, and J. Yan, “Locate-then-detect: real-time web attack detection via attention-based deep neural networks,” in Proc. Joint Conf. Artif. Intell., 2019, pp. 4725–4731.

[22]. Y. Zhou and G. Cheng, “An efficient intrusion detection system based on feature selection ensemble classifier,” Computer Networks., vol. 174, 2020, Art. no. 107247.

[23]. R. Vinayakumar, K. P. Soman, and P. Poornachandran, “Detecting malicious domain names using deep learning approaches at scale,” J. Intell. Fuzzy Syst., vol. 34, no. 3, pp. 1355–1367, 2018. [24] M. E. Ahmed and K. Hyoungshick, “Poster: Adversarial examples for classifiers in high-dimensional network data,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2017, pp. 2467–2469.

[24]. N. Papernot, P. Mcdaniel, and I. Goodfellow, “Practical black-box attacks against machine learning,” in Proc. ACM Asia Conf. Comput. Commun. Secur., 2017, pp. 506–519.

[25]. Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, “A distributed deep learning system for web attack detection on edge devices,” IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 1963–1971, Mar. 2020.

[26]. M. Zhang, B. Xu, and S. Bai, “A deep learning method to detect web attacks using a specially designed CNN,” in Proc. Int. Conf. Neural Inf. Process., 2017, pp. 828–836.

[27]. HTTP DATASETCSIC 2010. [Online]. Available: https://www.isi.csic.es/ dataset/

DOI: 10.48175/IJARSCT-4638