IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

A Review on Machine Learning Techniques for Cyber Security in the Last Decade

Ishita Bhadekar[1], Aarya S Dawre[2], Tanmay Chavhan[3], Vishakha N. Pawar[4]
MKSSS's College of Engineering for Women, Pune[1]
Guru Gobind Singh College Of Engineering And Research Centre, Nashik, Maharashtra, India[2,3]
Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India[4]

Abstract: *Universal growth and usage of the Internet and mobile applications have elongated cyberspace. The cyberspace has become more exposed to automated and protracted cyberattacks. Cyber security approaches provide enrichments in security processes to detect and react against cyberattacks. The formerly used security systems are no longer enough since cybercriminals are sharp enough to avoid conventional security systems. Conventional security systems privation efficiency in perceiving formerly unseen and polymorphic security attacks. Machine learning (ML) techniques are playing a vigorous role in several applications of cyber security. However, regardless of the ongoing achievement, there are substantial challenges in safeguarding the honesty of Machine Learning systems. There are incentivized nasty opponents present in the cyberspace that are eager to game and adventure such Machine Learning vulnerabilities. This paper aims to afford a complete outline of the challenges that Machine Learning techniques expression in shielding cyberspace against attacks, by bestowing a literature on Machine Learning techniques for cyber security inclusive of intrusion detection, spam detection, and malware detection on computer networks and mobile networks in the last decade. It also provides brief descriptions of each ML method, frequently used security datasets, essential ML tools, and evaluation metrics to evaluate a classification model. It finally discusses the challenges of using ML techniques in cyber security. This paper provides the latest extensive bibliography and the current trends of ML in cyber security.*

Keywords: Deep Learning, Cyber Security, Malware, Intrusion Detection, Spam, Machine Learning

REFERENCES

[1] ICT Fact and Figures 2017. Accessed: Jun. 1, 2020. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
[2] ICT Facts and Figures, International Telecommunication Union. (2017). Telecommunication Development Bureau. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (accessed Oct. 09, 2019).
[3] D. K. Bhattacharyya and J. K. Kalita, Network Anomaly Detection: A Machine Learning Perspective. London, U.K.: Chapman & Hall, 2013.
[4] V. Ambalavanan, ``Cyber threats detection and mitigation using machine learning," in Handbook of Research on Machine and Deep Learning Applications for Cyber Security. Hershey, PA, USA: IGI Global, 2020, pp. 132149.
[5] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, ``Machine learning and cybersecurity," in Machine Learning Approaches in Cyber Security Analytics. Singapore: Springer, 2020, pp. 3747. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-1706-8_3
[6] The Comprehensive National Cybersecurity Initiative. Accessed: Jun. 1, 2020. [Online]. Available: https://obamawhitehouse. archives.gov/issues/foreign-policy/cybersecurity/national-initiative
[7] The White House, Remarks by APHSCT Lisa O. Monaco at the International Conference on Cyber Security. Accessed: Oct. 17, 2019. [Online]. Available: https://obamawhitehouse.archives.gov/thepress-office/2016/07/26/remarks-aphsct-lisa-o-monaco-internationalconference-cyber-security

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

[8] 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? Accessed: Jun. 1, 2020. [Online]. Available: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmarkattack-on-estonia-is-the-world-better-prepared-for-cyber-threats/
[9] North Atlantic Treaty Organization. (Apr. 3, 2008). Bucharest Sum-mit Declaration. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Bucharest. Accessed: Oct. 9, 2019. [Online]. Available: https://www.nato.int/cps/en/natolive/official_texts_8443.htm
[10] F. Farahmand, S. B. Navathe, P. H. Enslow, and G. P. Sharp, ``Managing vulnerabilities of information systems to security incidents," in Proc. 5thInt. Conf. Electron. Commerce (ICEC), 2003, pp. 348354.
[11] D. Craigen, N. Diakun-Thibault, and R. Purse, ``Defining cybersecurity," Technol. Innov. Manage. Rev., vol. 4, no. 10, pp. 1321, Oct. 2014.
[12] P. Szor, The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE_p1. London, U.K.: Pearson, 2005.
[13] I. Firdausi, C. Lim, A. Erwin, and A. S. Nugroho, ``Analysis of machine learning techniques used in behavior-based malware detection," in Proc. 2nd Int. Conf. Adv. Comput., Control, Telecommun. Technol., Dec. 2010, pp. 201203.
[14] S. Gu, B. T. Kelly, and D. Xiu, ``Empirical asset pricing via machine learning," in Proc. 31st Australas. Finance Banking Conf., Chicago Booth Res. Paper 18-04, Yale ICFWorking Paper 2018-09, Sep. 2019. [Online]. Available: https://ssrn.com/abstract=3159577
[15] P. Mathur, ``Overview of machine learning in finance," in Machine Learning Applications Using Python. Berkeley, CA, USA: Apress, 2019, pp. 259270. [Online]. Available: https://link.springer.com/chapter/10.1007/978-1-4842-3787-8_13
[16] S. Emerson, R.Kennedy, L. O'Shea, and J. O'Brien, ``Trends and applications of machine learning in quantitative finance," in Proc. 8th Int. Conf. Econ. Finance Res. (ICEFR), 2019, pp. 19.
[17] K. Shaukat et al., ``Student's performance in the context of data mining," in Proc. 19th Int. Multi-Topic Conf. (INMIC), 2016.
[18] S. Jha and E. J. Topol, ``Adapting to artificial intelligence: Radiologists and pathologists as information specialists," Jama, vol. 316, no. 22, pp. 23532354, 2016.
[19] A. I. Tekkesin, ``Articial intelligence in healthcare: Past, present and future," Anatolian J. Cardiol., vol. 2, no. 4, pp. 230243, 2019.
[20] K. Shaukat, N. Masood, A. Bin Shafaat, K. Jabbar, H. Shabbir, and S. Shabbir, ``Dengue fever in perspective of clustering algorithms," 2015, arXiv:1511.07353. [Online]. Available: http://arxiv.org/abs/1511.07353
[21] K. S. Dar and S. M. U. Azmeen, ``Dengue fever prediction: A data mining problem," J. Data Mining Genomics Proteomics, vol. 6, no. 3, pp. 15, 2015.
[22] B.-H. Li, B.-C. Hou,W.-T. Yu, X.-B. Lu, and C.-W. Yang, ``Applications of artificial intelligence in intelligent manufacturing:Areview," Frontiers Inf. Technol. Electron. Eng., vol. 18, no. 1, pp. 8696, 2017.
[23] C. Virmani, T. Choudhary, A. Pillai, and M. Rani, ``Applications of machine learning in cyber security," in Handbook of Research on Machine and Deep Learning Applications for Cyber Security. Hershey, PA, USA: IGI Global, 2020, pp. 83103.
[24] R. Calderon, ``The benets of artificial intelligence in cybersecurity," La Salle Univ., Philadelphia, PA, USA, Tech. Rep. Winter 1-15-2019, 2019.