IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

A Critical Review on Learning Behavior for Protection of User's Privacy using IOT

Shrikanta Kolay[1] and Dr. Tryambak Hiwarkar[2]
Research Scholar, Department of Computer Science& Engineering[1]
Professor, Department of Computer Science& Engineering[2]
Sardar Patel University, Balaghat, MP, India

Abstract: *Changes and improvements to human existence have been made possible by recent advancements in communication and information technology, notably the internet of things (IoT). The IoT system is vulnerable to cyber-physical security and privacy assaults such denial of service, spoofing, phishing, obfuscations, and jamming because of the widespread availability and rising demand for smart devices. Cyber dangers to IoT systems, such as eavesdropping, attacks, and more. The new threats to cyber-physical security cannot be effectively avoided or mitigated using the same old methods. Keeping IoT systems safe calls on security measures that are not only effective, but also flexible and up-to-date. Among the various approaches to cyber-physical system security, machine learning (ML) is widely regarded as the most cutting-edge and promising since it has spawned several new lines of inquiry into the problem (CPS). This literature study provides an overview of the structure of Internet of Things (IoT) systems, explores the many attacks that may be launched against them, and discusses the current thinking on how to best use machine learning to ensure the security and safety of IoT infrastructure. It also covers the probable future research obstacles that may arise while implementing security measures in IoT systems.*

Keywords: IoT System, Security Threats

REFERENCES

[1]. Rancesco Restuccia, Salvatore DrOro, and TommasoMelodia. 2018. Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking. *IEEE Internet of Things Journal* 1, 1 (2018), 1–14

[2]. Shaila Sharmeen, Shamsul Huda, Jemal H. Abawajy, Walaa Nagy Ismail, and Mohammad Mehedi Hassan. 2018. Malware Threats and Detection for Industrial Mobile-IoT Networks. *IEEE Access* 6 (2018), 15941–15957.

[3]. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Communications Surveys Tutorials* 21, 3 (third quarter 2019), 2671–2701.

[4]. Liang Xiao, Donghua Jiang, Dongjin Xu, and Ning An. 2018. Secure Mobile Crowd sensing with Deep Learning. *China Communications*15 (2018), 1–11. http://arxiv.org/abs/1801.07379

[5]. Elena Milosevic, MiroslawMalek, and Alberto Ferrante. 2016. A Friend or a Foe? Detecting Malware using Memoryand CPU Features. In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016)*, Vol. 4. 73–84.

[6]. Muhamad Erza Aminanto, Rakyong Choi, Harry Chandra Tanuwidjaja, Paul D. Yoo, and Kwangjo Kim. 2017. Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. IEEE Transactions on Information Forensics and Security 13, 3 (2017), 621–636.

[7]. Mandrita Banerjee, Junghee Lee, and Kim Kwang Raymond Choo. 2018. A blockchain future for internet of things security: a position paper. Digital Communications and Networks 4, 3 (2018), 149–160. https://@doi.org/10.1016/j.dcan.2017.10.006

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

[8]. I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock. 2018. Standardising a moving target: The development and evolution of IoT security standards. In Living in the Internet of Things: Cybersecurity of the IoT - 2018. 1–9

[9]. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys Tutorials 21, 3 (third quarter 2019), 2671–2701

[10]. Konstantinos Christidis and Michael Devetsikiotis. 2016. Blockchains and Smart Contracts for the Internet of Things.IEEE Access 4 (2016), 2292–2303. http://ieeexplore.ieee.org/document/7467408/

[11]. Tim Dalgleish, J. Mark G.. Williams, Ann-Marie J. Golden, Nicola Perkins, Lisa Feldman Barrett, Phillip J.Barnard, Cecilia Au Yeung, Victoria Murphy, Rachael Elward, Kate Tchanturia, and Edward Watkins. 2018. The Blockchain-enabled Intelligent IoT Economy. (2018). https://www.forbes.com/sites/cognitiveworld/2018/10/04/the-blockchain-enabled-intelligent-iot-economy/#14b65de82a59