IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

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

Volume 2, Issue 2, February 2022

Analysis of Lightweight Security Techniques oor IoT Data and Communication

Prof. Mohan S. Khedkar[1], Prof. Sandip R. Devkate[2], Prof. Shilpa Chaudhari[3]

Department of Information Technology[1], Department of Electronics and Telecommunication[2]
Department of Computer Technology[3]
Government Polytechnic Nashik, Maharashtra, India[1]
Matoshree College of Engineering And Research Centre, Nashik, Maharashtra, India[2,3]
mohan_khedkar@hotmail.com[1], sandiprdevkate@gmail.com[2], sawaghulde@gmail.com[3]

Abstract: *The Internet of Things (IoT) aims to transform everyday physical objects into an interconnected ecosystem with digital data accessible anywhere and anytime. ''Things'' in IoT are embedded with sensing, processing, and actuating capabilities and cooperate in providing smart and innovative services autonomously. The rapid spread of IoT services arises different security vulnerabilities that need to be carefully addressed. Several emerging and promising technologies and techniques are introduced to improve the security of IoT. This paper aims to provide an up-to-date vision of the current research topics related to IoT security. Initially, we introduce common elements and protocols of IoT to demystify the origins of threats in IoT. Then, we propose a taxonomy of IoT attacks and analyse the security vulnerabilities of IoT at different layers. Subsequently, we provide a comparison of recent security schemes based on emerging solutions including fog computing, edge computing, software-defined networking (SDN), blockchain, lightweight cryptography, homomorphic and searchable encryption, and machine learning. Finally, security challenges are discussed and future directions are highlighted for future interested researchers.*

Keywords: Blockchain, edge computing, fog computing, IoT, lightweight cryptography, machine learning, SDN

References

[1]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generat. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[2]. S. Hammoudi, Z. Aliouat, and S. Harous, "Challenges and research directions for Internet of Things," Telecommun. Syst., vol. 67, no. 2,pp. 367–385, 2018.

[3]. D. Evans, "The Internet of Things: How the next evolution of the internet is changing everything," CISCO White Paper, vol. 1, pp. 1–11, Apr. 2011.

[4]. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Comput. Netw., vol. 57, no. 10, pp. 2266–2279, 2013.

[5]. J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "Unlocking the potential of the Internet of Things," McKinsey Global Inst., Tech. Rep., 2015, vol. 1.

[6]. V. Adat and B. B. Gupta, "Security in Internet of Things: Issues, chal- lenges, taxonomy, and architecture," Telecommun. Syst., vol. 67, no. 3, pp. 423–441, 2017.

[7]. D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," Comput. Netw., vol. 141, pp. 199–221, Aug. 2018.

[8]. Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," IEEE Internet Things J., vol. 6, no. 2,pp. 2103–2115, Apr. 2019.

[9]. M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," Comput. Netw., vol. 148, pp. 283– 294,Jan. 2018.

DOI: 10.48175/IJARSCT-2750

[10]. A. Tewari and B. B. Gupta, ''Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,'' Future Gener. Comput. Syst., vol. 108, pp. 909–920, Jul. 2018.

[11]. Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, ''A review of security in Internet of Things,'' Wirel. Pers. Commun., vol. 108, no. 1,pp. 325–344, Sep. 2019.

[12]. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, ''A survey on IoT security: Application areas, security threats, and solu- tion architectures,'' IEEE Access, vol. 7, pp. 82721–82743, 2019.

[13]. F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, ''IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices,'' IEEE Internet Things J., vol. 6, no. 5, pp. 8182– 8201,Oct. 2019.

[14]. N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, ''Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations,'' IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2702– 2733, 3rd Quart., 2019.

[15]. S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, ''Realizing an internet of secure things: A survey on issues and enabling technolo- gies,'' IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1372– 1391,2nd Quart., 2020.

[16]. M. Mahbub, ''Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and pre- emptive architectonics,'' J. Netw. Comput. Appl., vol. 168, Oct. 2020, Art. no. 102761.

[17]. H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, ''A survey of IoT security based on a layered architecture of sensing and data analysis,'' Sensors, vol. 20, no. 13, p. 3625, Jun. 2020.

[18]. P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, ''Internet of Things: Evolution, concerns and security chal-lenges,'' Sensors, vol. 21, no. 5, p. 1809, Mar. 2021.

[19]. V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, ''Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities,'' IEEE Access, vol. 9,pp. 28177–28193, 2021.

[20]. P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-H. Kim, ''A taxonomy of security issues in industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges,'' IEEE Access, vol. 9, pp. 25344–25359, 2021. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ''A sur- vey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,'' IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[21]. X. Jia, Q. Feng, T. Fan, and Q. Lei, ''RFID technology and its applications in Internet of Things (IoT),'' in Proc. 2nd Int. Conf. Consum. Electron., Commun. Netw. (CECNet), Apr. 2012, pp. 1282– 1285.

[22]. M. Kocakulak and I. Butun, ''An overview of wireless sensor networks towards Internet of Things,'' in Proc. IEEE 7th Annu. Comput. Commun.Workshop Conf. (CCWC), Jan. 2017, pp. 1–6.

[23]. Zigbee Document 053474r13, Z. Specification, ZgBee Standards Org., USA, 2006.

[24]. Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks, I. W. Group, IEEE Standard802.15.4, vol. 802, no. 4, 2003, p. 2003.

[25]. J. Li, X. Zhu, N. Tang, and J. Sui, ''Study on ZigBee network architecture and routing algorithm,'' in Proc. 2nd Int. Conf. Signal Process. Syst.,vol. 2, Jul. 2010, pp. V2-389–V2-393.

[26]. Bluetooth Core Specification Version 4.0, Specification Bluetooth Syst., USA, vol. 1, 2010, p. 7.

[27]. G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, ''Transmission of IPv6 packets over IEEE 802.15. 4 networks,'' Internet Proposed StandardRFC, vol. 4944, p. 130, Sep. 2007.

[28]. G. Mulligan, ''The 6LoWPAN architecture,'' in Proc. 4th Workshop Embedded Networked Sensors (EmNets), 2007, pp. 78–82.

[29]. T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. K. Alexander, RPL: IPv6 Routing Pro- tocol for Low-Power and Lossy Networks, document RFC 6550, 2012, pp. 1–157.

[30]. Lorawan 1.1 Specification, Tech. Specification, L. Alliance, USA, 2017.

DOI: 10.48175/IJARSCT-2750

[31]. Z. Shelby, K. Hartke, and C. Bormann, The Constrained Application Protocol (COAP), document RFC 7252, 2014.

[32]. T. Zillner and F. Eichelberger, "ZigBee smart homes: A hacker's open house," in Proc. CRESTCon Conf., 2016.

[33]. X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost- in-ZigBee: Energy depletion attack on ZigBee-based wireless networks," IEEE Internet Things J., vol. 3, no. 5, pp. 816–829, Oct. 2016.

[34]. L. Coppolino, V. D'Alessandro, S. D'Antonio, L. Levy, and L. Romano, "My smart home is under attack," in Proc. IEEE 18th Int. Conf. Comput.Sci. Eng., Oct. 2015, pp. 145–151.

[35]. P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, "Insecure to the touch: Attacking ZigBee 3.0 via touchlink commission- ing," in Proc. 10th ACM Conf. Secur. Privacy Wireless Mobile Netw., Jul. 2017, pp. 230–240.

[36]. M. Ryan, "Bluetooth: With low energy comes low security," in Proc. 7thUSENIX Workshop Offensive Technol. (WOOT), 2013, pp. 1–7.

[37]. A. Y. Lindell, "Attacks on the pairing protocol of Bluetooth v2. 1," BlackHat USA, Las Vegas, NV, USA, Tech. Rep., 2008.

[38]. W. K. Zegeye, "Exploiting Bluetooth low energy pairing vulnerability intelemedicine," Int. Found. Telemetering, USA, Tech. Rep., 2015.

[39]. T. Rosa, "Bypassing passkey authentication in Bluetooth low energy," IACR Cryptol. ePrint Arch., vol. 2013, p. 309, May 2013.

[40]. M. Ye, N. Jiang, H. Yang, and Q. Yan, "Security analysis of Internet- of- Things: A case study of August smart lock," in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), May 2017, pp. 499–504.

[41]. R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," in Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw., 2013, pp. 55–66.

[42]. A. Rghiout, A. Khannous, and M. Bouhorma, "Denial-of-service attacks on 6LoWPAN-RPL networks: Issues and practical solutions," J. Adv. Comput. Sci. Technol., vol. 3, no. 2, pp. 143–153, 2014.

[43]. P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in Proc. Int. Conf. Pervas. Comput. (ICPC), Jan. 2015, pp. 1– 6.

[44]. A. Mayzaud, R. Badonnel, I. Chrisment, and I. G. Est-Nancy, "A tax- onomy of attacks in RPL-based Internet of Things," Int. J. Netw. Secur.,vol. 18, no. 3, pp. 459–473, 2016.

[45]. R. Miller, "LoRa security: Building a secure LoRa solution," MWR Labs,White Paper, 2016.

[46]. X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulner- abilities in LoRaWAN," in Proc. IEEE/ACM 3rd Int. Conf. Internet-of- Things Design Implement. (IoTDI), Apr. 2018, pp. 129– 140.

[47]. J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, Aug. 2015.

DOI: 10.48175/IJARSCT-2750