BIBLIOGRAPHY

[1] S. Li and L. D. Xu, *Securing the Internet of Things*, 1st ed. Massachusetts, USA: Syngress Publishing, 2017.

[2] Statista. (2019) Internet of things (iot) connected devices installed base worldwide from 2015 to 2025 (in billions). https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed : 2019-07-11.

[3] M. Hung. (2017) Leading the iot : Gartner insights on how to lead in a connected world. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. Accessed : 2019-07-11.

[4] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, pp. 1–11, 2011.

[5] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, April 2015.

[6] A. F. A. Rahman, M. Daud, and M. Z. Mohamad, "Securing sensor to cloud ecosystem using internet of things (iot) security framework," in *Proceedings of the International Conference on Internet of Things and Cloud Computing*, ser. ICC '16. New York, NY, USA: ACM, 2016, pp. 79:1–79:5. [Online]. Available: http://doi.acm.org/10.1145/2896387.2906198

[7] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10 – 28, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517301455

[8] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack scenarios and security analysis of mqtt communication protocol in iot system," in *Electrical Engineering, Computer Science and Informatics (EECSI), 2017 4th International Conference on*. IEEE, 2017, pp. 1–6.

[9] S. N. Firdous, Z. Baig, C. Valli, and A. Ibrahim, "Modelling and evaluation of malicious attacks against the iot mqtt protocol," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and*

Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), June 2017, pp. 748–755.

[10] N. Naik, "Choice of effective messaging protocols for iot systems: Mqtt, coap, amqp and http," in *2017 IEEE International Systems Engineering Symposium (ISSE)*, Oct 2017, pp. 1–7.

[11] P. Waher, *Learning Internet of Things*, ser. Community experience distilled. Birmingham B3 2PB, UK: Packt Publishing Ltd., 2015.

[12] B. Russell and D. Van Duren, *Practical Internet of Things Security.* Livery place 35, Birmingham b3 2pb, UK: Packt Publishing, 2016.

[13] E. Alsaadi and A. Tubaishat, "Internet of things: features, challenges, and vulnerabilities," *International Journal of Advanced Computer Science and Information Technology*, vol. 4, no. 1, pp. 1–13, 2015.

[14] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (iot): Taxonomy of security attacks," in *2016 3rd International Conference on Electronic Design (ICED)*, Aug 2016, pp. 321–326.

[15] S. Nolan, "Authenticated payload encryption scheme for internet of things systems over the mqtt protocol," Master's thesis, Trinity Collage Dublin, The University of Dublin, Dublin, Ireland, 5 2018.

[16] G. Reiter. (2015) Securing all devices in the internet of things. https://www.ecnmag.com/article/2015/06/securing-all-devices-internet-things. Accessed :2019-07-11.

[17] J. Hee Chung, "Adaptive energy-efficient ssl/tls method using fuzzy logic for the mqtt-based internet of things," *International Journal of Engineering and Computer Science*, vol. 5, no. 12, Nov. 2016. [Online]. Available: http://www.ijecs.in/index.php/ijecs/article/view/3229

[18] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199 – 221, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618301208

[19] M. Dabbagh and A. Rayes, *Internet of Things Security and Privacy.* Cham: Springer International Publishing, 2017, pp. 195–223. [Online]. Available: https://doi.org/10.1007/978-3-319-44860-2_8

[20] D. Ding, Z. Wang, G. Wei, and F. E. Alsaadi, "Event-based security control for discrete-time stochastic systems," *IET Control Theory Applications*, vol. 10, no. 15, pp. 1808–1815, 2016.

[21] Tamarin, *Tamarin-Prover Manual : Security Protocol Analysis in the Symbolic Model*, Tamarin, 4 2019.

[22] D. Basin, C. Cremers, J. Dreier, and R. Sasse, *Symbolically Analyzing Security Protocols Using Tamarin.* New York, NY, USA: ACM, nov 2017, vol. 4, no. 4.

[23] L. Nastase, "Security in the internet of things: A survey on application layer protocols," in *Control Systems and Computer Science (CSCS), 2017 21st International Conference on.* IEEE, 2017, pp. 659–666.

[24] R. S. Bali, F. Jaafar, and P. Zavarasky, "Lightweight authentication for mqtt to improve the security of iot communication," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, ser. ICCSP '19. New York, NY, USA: ACM, 2019, pp. 6–12. [Online]. Available: http://doi.acm.org/10.1145/3309074.3309081

[25] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, "Secure mqtt for internet of things (iot)," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, April 2015, pp. 746–751.

[26] M. S. Harsha, B. M. Bhavani, and K. R. Kundhavai, "Analysis of vulnerabilities in mqtt security using shodan api and implementation of its countermeasures via authentication and acls," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sep. 2018, pp. 2244–2250.

[27] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, July 2015, pp. 180–187.

[28] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544 – 546, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17316667

[29] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, Apr 2015. [Online]. Available: https://doi.org/10.1007/s10796-014-9492-7

[30] H. Ning, *Unit and Ubiquitous Internet of Things.* Boca Raton, FL, USA: CRC Press, Inc., 2013.

[31] A. Banks and R. Gupta, *MQTT Version 3.1.1*, OASIS Standart, 10 2014.

[32] H. C. Hwang, J. Park, and J. G. Shon, "Design and implementation of a reliable message transmission system based on mqtt protocol in iot," *Wireless Personal Communications*, vol. 91, no. 4, pp. 1765–1777, Dec 2016. [Online]. Available: https://doi.org/10.1007/s11277-016-3398-2

[33] M. Kirsche and R. Klauck, "Unify to bridge gaps: Bringing xmpp into the internet of things," in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, March 2012, pp. 455–458.

[34] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[35] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, "Internet of things security: Layered classification of attacks and possible countermeasures," *Electronic Journal of Information Technology*, no. 9, 2016.

[36] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *International Journal of Advanced Networking Applications*, vol. 6, pp. 2372–2378, 01 2015.

[37] C. Bormann, M. Ersue, and A. Kernen, "Terminology for Constrained-Node Networks," RFC 7228, May 2014. [Online]. Available: https://rfc-editor.org/rfc/rfc7228.txt

[38] V. Vasyutynskyy and K. Kabitzsch, "Event-based control: Overview and generic model," in *2010 IEEE International Workshop on Factory Communication Systems Proceedings*, May 2010, pp. 271–279.

[39] F. Y. Sir Ronald A. Fisher, *Statistical tables for biological, agricultural and medical research, edited by R.A. Fisher and F. Yates. 6th ed.* Edinburgh, Scotland: Oliver and Boyd, 1963, no. Ed. 6.

[40] Z. Nasim, Z. Bano, and M. Ahmad, "Analysis of efficient random permutations generation for security applications," in *2015 International Conference on Advances in Computer Engineering and Applications*, March 2015, pp. 337–341.

[41] T. K. Hazra, R. Ghosh, S. Kumar, S. Dutta, and A. K. Chakraborty, "File encryption using fisher-yates shuffle," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, Oct 2015, pp. 1–7.

[42] T. Shah and S. Venkatesan, "Authentication of iot device and iot server using secure vaults," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug 2018, pp. 819–824.

[43] T. K. Hazra, R. Ghosh, S. Kumar, S. Dutta, and A. K. Chakraborty, "File encryption using fisher-yates shuffle," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, Oct 2015, pp. 1–7.

[44] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2014.

[45] P. Miranda, M. Siekkinen, and H. Waris, "Tls and energy consumption on a mobile device: A measurement study," in *2011 IEEE Symposium on Computers and Communications (ISCC)*, June 2011, pp. 983–989.

[46] M. Calabretta, R. Pecori, M. Vecchio, and L. Veltri, "Mqtt-auth: a token-based solution to endow mqtt with authentication and authorization capabilities," *Journal of Communications Software and Systems*, vol. 14, 12 2018.

[47] C. Xu and Y. Ge, "The public key encryption to improve the security on wireless sensor networks," in *2009 Second International Conference on Information and Computing Science*, vol. 1, May 2009, pp. 11–14.

[48] A. R. Ganesh, P. N. Manikandan, S. P. Sethu, R. Sundararajan, and K. Pargunarajan, "An improved aes-ecc hybrid encryption scheme for secure communication in cooperative diversity based wireless sensor networks," in *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, June 2011, pp. 1209–1214.

[49] S. B. Othman, A. Trad, H. Alzaid, and H. Youssef, “Performance evaluation of ec-elgamal encryption algorithm for wireless sensor networks,” in *Wireless Mobile Communication and Healthcare*, B. Godara and K. S. Nikita, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 271–285.