Daftar Pustaka

[1] Nitin Naik. Choice of effective messaging protocols for iot systems: Mqtt, coap, amqp and http. In *2017 IEEE international systems engineering symposium (ISSE)*, pages 1–7. IEEE, 2017.

[2] Shancang Li and Li Da Xu. *Securing the internet of things*. Syngress, 2017.

[3] Carsten Bormann, Mehmet Ersue, and Ari Keranen. Terminology for constrained-node networks. *Internet Engineering Task Force (IETF): Fremont, CA, USA*, pages 2070–1721, 2014.

[4] James King and Ali Ismail Awad. A distributed security mechanism for resource-constrained iot devices. *Informatica*, 40(1), 2016.

[5] Hyun Cheon Hwang, JiSu Park, and Jin Gon Shon. Design and implementation of a reliable message transmission system based on mqtt protocol in iot. *Wireless Personal Communications*, 91(4):1765–1777, 2016.

[6] Javier Suarez, Jose Quevedo, Ivan Vidal, Daniel Corujo, Jaime Garcia-Reinoso, and Rui L Aguiar. A secure iot management architecture based on information-centric networking. *Journal of Network and Computer Applications*, 63:190–204, 2016.

[7] Alessandra Rizzardi, Sabrina Sicari, Daniele Miorandi, and Alberto Coen-Porisini. Aups: an open source authenticated publish/subscribe system for the internet of things. *Information Systems*, 62:29–41, 2016.

[8] Nico Ferrari, Teklay Gebremichael, Ulf Jennehag, and Mikael Gidlund. Lightweight group-key establishment protocol for iot devices: Implementation and performance analyses. In *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, pages 31–37. IEEE, 2018.

[9] Reem Abdul Rahman and Babar Shah. Security analysis of iot protocols: A focus in coap. In *2016 3rdMEC international conference on big data and smart city (ICBDSC)*, pages 1–7. IEEE, 2016.

[10] Oliver Hahm, Emmanuel Baccelli, Hauke Petersen, and Nicolas Tsiftes. Operating systems for low-end devices in the internet of things: a survey. *IEEE Internet of Things Journal*, 3(5):720–734, 2015.

[11] Shancang Li. Iot node authentication. In *Securing the Internet of Things*, pages 69–95. Syngress Boston, 2017.

[12] Securing mqtt systems - mqtt security fundamentals, Jun 2015. https://www.hivemq.com/blog/ mqtt-security-fundamentals-payload-encryption/, Terakhir diakses 07/09/2019.

[13] William Stallings. *Network Security Essentials: Applications and Standards, 4/e*. Pearson Education India, 2003.

[14] Shivendra Singh, Md Sarfaraz Iqbal, and Arunima Jaiswal. Survey on techniques developed using digital signature: Public key cryptography. *International Journal of Computer Applications*, 117(16), 2015.

[15] Pooja Yadav and Mamta Yadav. Digital signature. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, 3(6), 2018.

[16] B Sindhu and RM Noorullah. Secure elliptic curve digital signature algorithm for internet of things. *Global Journal of Computer Science and Technology*, 2016.

[17] Aleksandr Ometov, Pavel Masek, Lukas Malina, Roman Florea, Jiri Hosek, Sergey Andreev, Jan Hajny, Jussi Niutanen, and Yevgeni Koucheryavy. Feasibility characterization of cryptographic primitives for constrained (wearable) iot devices. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 1–6. IEEE, 2016.

[18] B Vinayaga Sundaram, M Ramnath, M Prasanth, and Varsha Sundaram. Encryption and hash based security in internet of things. In *2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)*, pages 1–6. IEEE, 2015.

[19] Morris J Dworkin, Elaine B Barker, James R Nechvatal, James Foti, Lawrence E Bassham, E Roback, and James F Dray Jr. Advanced encryption standard (aes). Technical report, 2001.

[20] Leandro Marin, Marcin Pawlowski, and Antonio Jara. Optimized ecc implementation for secure communication between heterogeneous iot devices. *Sensors*, 15(9):21478–21499, 2015.

[21] Mohamed Elhoseny, Hamdy Elminir, Alaa Riad, and Xiaohui Yuan. A secure data routing schema for wsn

using elliptic curve cryptography and homomorphic encryption. *Journal of King Saud University-Computer and Information Sciences*, 28(3):262–275, 2016.

[22] Douglas Stebila. Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer. RFC 5656, December 2009.

[23] Husnul Hidayat, Parman Sukarno, and Aulia Arif Wardana. Overhead analysis on the use of digital signature in mqtt protocol. In *2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, pages 87–92. IEEE, 2019.

[24] Aulia Arif Wardana and Riza Satria Perdana. Access control on internet of things based on publish/subscribe using authentication server and secure protocol. In *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pages 118–123. IEEE, 2018.

[25] Muneer Bani Yassein, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, and Yaser Khamayseh. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 international conference on engineering and technology (ICET)*, pages 1–7. IEEE, 2017.

[26] Simon Josefsson and Ilari Liusvaara. Edwards-curve digital signature algorithm (eddsa). In *Internet Research Task Force, Crypto Forum Research Group, RFC*, volume 8032, 2017.

[27] A Langley, M Hamburg, and S Turner. Rfc 7748: Elliptic curves for security. internet engineering task force (ietf), 2016.

[28] Kerry A McKay, Larry Bassham, Meltem Snmez Turan, and Nicky Mouha. Nistir 8114 report on lightweight cryptography. *National Institute of Standards and Technology (NIST), Gaithersburg*, 2017.