Referensi

[1] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," *Proc. 2015 Int. Conf. Green Comput. Internet Things, ICGCIoT 2015*, pp. 1577–1581, 2016, doi: 10.1109/ICGCIoT.2015.7380718.

[2] O. P. Manual, "Orange Pi Zero User Manual."

[3] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack scenarios and security analysis of mqtt communication protocol in iot system," in *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2017, vol. 4, pp. 600–604, doi: 10.11591/eecsi.4.1064.

[4] T. H. Team, "MQTT Security Fundamentals TLS/SSL," *MQTT Security Fundamentals*, 2017. https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl/ (accessed Jul. 06, 2021).

[5] A. Gupta and N. K. Walia, "Cryptography Algorithms : A Review," *Int. J. Eng. Dev. Res.*, vol. 2, no. 2, pp. 1667–1672, 2014, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=FEF3E8340DC536679E3C83BF43F1616C?doi=10.1.1.674.7141&rep=rep1&type=pdf.

[6] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," *J. Cryptol.*, vol. 34, no. 3, pp. 1–42, 2021, doi: 10.1007/s00145-021-09398-9.

[7] O. Sadio, I. Ngom, and C. Lishou, "Lightweight Security Scheme for MQTT/MQTT-SN Protocol," *2019 6th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2019*, pp. 119–123, 2019, doi: 10.1109/IOTSMS48152.2019.8939177.

[8] H. L. Manohar and T. R. G. Asir, "Data Consumption Pattern of MQTT Protocol for IoT Applications," *Int. Conf. Intell. Inf. Technol.*, vol. 2, pp. 12–22, 2017.