5. Kesimpulan dan Saran

Penerapan autentikasi *One Time Password* (OTP) berbasis blockchain pada protokol MQTT telah diterapkan pada penelitian ini. Perangkat IoT sebagai *publisher* dapat mengirimkan data sensor suhu dan kelembapan kepada *subscriber* dengan melalui mekanisme autentikasi antar *client*. Semua informasi seperti OTP, device id, nilai suhu dan kelembapan akan terenkripsi dan tersimpan di dalam blockchain guna untuk menjaga keintegritasan data yang diterima oleh *subscriber*. Kemudian, untuk pembuktian integritas data yang diterima oleh *subscriber*, dilakukan pengujian serangan *Man in The Middle* (MITM) terhadap sistem dengan mengirimkan data palsu ke *subscriber* melalui broker. Dari hasil pengujian, sistem dengan menerapkan skema autentikasi dapat mencegah dan mengidentifikasi jika terjadi serangan MITM. Dengan menerapkan skema ini kepada perangkat IoT berbasis protokol MQTT akan menjaga keintegritasan data, khususnya data yang akan diterima oleh perangkat *subscriber*. Seperti pada pengujian sistem yang telah dilakukan, data yang diterima oleh perangkat *subscriber* berupa data suhu dan kelembapan akan terjamin dan dapat terhindar dari penerimaan nilai data palsu atau penyusupan data oleh *attacker*.

Selain itu, pengujian perfomansi sistem juga telah dilakukan. Hasil menunjukkan bahwa penggunaan *memory* pada penerapan skema autentikasi OTP pada protokol MQTT tidak jauh berbeda dengan penggunaan protokol MQTT normal (tanpa skema autentikasi). Penggunaan ruang *memory* diukur dari total waktu saat sistem dijalankan, yaitu lima menit, 10 menit, 15 menit, dan 20 menit. Rata-rata penggunaan *memory* pada penerapan skema autentikasi sebesar 3,7910155 MB dan rata-rata penggunaan *memory* tanpa penerapan skema sebesar 3,790039 MB.

Untuk penelitian di masa yang akan datang, penelitian ini masih perlu menambahkan kekurangan yang dimiliki. Seperti, dalam penelitian ini server broker tidak dijalankan melalui perangkat keras melainkan hanya melalui aplikasi *virtual machine*. Perangkat keras yang dapat digunakan untuk menjalankan broker salah satunya yaitu menggunakan Raspberry Pi. Sehingga, jika diaplikasikan di dunia nyata, sistem yang dijalankan bisa menjadi lebih layak atau *feasible*. Maka dari itu, diharapkan adanya penerapan dengan menjalankan server broker yang menggunakan perangkat keras seperti Raspberry Pi. Selain itu, kekurangan lain yang dapat ditambahkan untuk pengembangan yaitu dalam hal pengujian sistem dengan metode serangan lain, melakukan autentikasi dengan banyak *client*, dan mengembangkan aspek keamanan yang lain dengan pemanfaatan teknologi blockchain.

Daftar Pustaka

[1] G. Fortino, L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, “Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges,” *IEEE Access*, vol. 8, pp. 60117–60125, 2020, doi: 10.1109/ACCESS.2020.2982318.

[2] S. N. Firdous, Z. Baig, C. Valli, and A. Ibrahim, “Modelling and evaluation of malicious attacks against the IoT MQTT protocol,” *Proc. - 2017 IEEE Int. Conf. Internet Things, IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, vol. 2018-Janua, pp. 748–755, 2018, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115.

[3] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, and S. Karuppayah, “MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet of Things (IoT),” *IETE J. Res.*, vol. 69, no. 6, pp. 3368–3397, 2023, doi: 10.1080/03772063.2021.1912651.

[4] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, “Man-in-the-middle-attack: Understanding in simple words,” *Int. J. Data Netw. Sci.*, vol. 3, no. 2, pp. 77–92, 2019, doi: 10.5267/j.ijdns.2019.1.001.

[5] B. H. C, S. T. Jain J, and S. D. S, “Diverse Malicious Attacks and security Analysis on MQTT protocol in IoT,” vol. XII, no. Iv, pp. 440–449, 2020.

[6] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[7] T. Hsu and H. Lu, “Designing a secure and scalable service model using blockchain and MQTT for IoT devices,” *Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis. Work. 2024, pp. 645-653*, pp. 645–653, 2024.

[8] A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, and A. Takacs, “Blockchain mechanism and symmetric encryption in a wireless sensor network,” *Sensors (Switzerland)*, vol. 20, no. 10, 2020, doi: 10.3390/s20102798.

[9] M. Ataei, A. Eghmazi, A. Shakerian, R. Landry, and G. Chevrette, “*Publish* / *Subscribe* Method for Real-Time Data Processing in Massive IoT Leveraging Blockchain for Secured Storage,” 2023.

[10] D. Fakhri and K. Mutijarsa, “Secure IoT Communication using Blockchain Technology,” *ISESD 2018* -

Int. Symp. Electron. Smart Devices Smart Devices Big Data Anal. Mach. Learn., 2019, doi: 10.1109/ISESD.2018.8605485.
[11] F. Buccafurri and C. Romolo, "A Blockchain-Based OTP-Authentication Scheme for Constrainded IoT Devices Using MQTT," *ACM Int. Conf. Proceeding Ser.*, 2019, doi: 10.1145/3386164.3389095.
[12] M. ABDELRAZIG ABUBAKAR, Z. JAROUCHEH, A. AL-DUBAI, and X. LIU, "Blockchain-based identity and authentication scheme for MQTT protocol," pp. 73–81, 2021, doi: 10.1145/3460537.3460549.
[13] B. Mishra and A. Kertesz, "The use of MQTT in M2M and IoT systems: A survey," *IEEE Access*, vol. 8, pp. 201071–201086, 2020, doi: 10.1109/ACCESS.2020.3035849.
[14] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for Internet of Things," *Digit. Commun. Networks*, vol. 8, no. 6, pp. 1094–1104, 2022, doi: 10.1016/j.dcan.2022.03.013.
[15] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[16] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and op*port*unities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.
[17] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.
[18] H. Fereidouni, O. Fadeitcheva, and M. Zalai, "IoT and Man-in-the-Middle Attacks," 2023, [Online]. Available: http://arxiv.org/abs/2308.02479.
[19] M. Yano, C. Dai, K. Masuda, and Y. Kishimoto, *Blockchain and Crypt Currency: Building a High Quality Marketplace for Crypt Data*. 2020.
[20] B. Hu *et al.*, "A comprehensive survey on *smart contract* construction and execution: paradigms, tools, and systems," *Patterns*, vol. 2, no. 2, p. 100179, 2021, doi: 10.1016/j.patter.2020.100179.
[21] J. Shailak, "*Smart contract*s: Building Blocks for Digital Transformation," 2020, doi: 10.13140/RG.2.2.33316.83847.
[22] P. Tolmach, Y. Li, S. W. Lin, Y. Liu, and Z. Li, "A Survey of *Smart contract* Formal Specification and Verification," *ACM Comput. Surv.*, vol. 54, no. 7, 2022, doi: 10.1145/3464421.
[23] F. Buccafurri, V. De Angelis, and R. Nardone, "Securing MQTT by blockchain-based otp authentication," *Sensors (Switzerland)*, vol. 20, no. 7, 2020, doi: 10.3390/s20072002.
[24] J. Heikka and M. Siponen, "Abuse cases revised: An action research experience," *PACIS 2006 - 10th Pacific Asia Conf. Inf. Syst. ICT Innov. Econ.*, no. April, pp. 673–684, 2006.
[25] J. McDermott and C. Fox, "Using abuse case models for security requirements analysis," *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, vol. Part F133431, pp. 55–64, 1999, doi: 10.1109/CSAC.1999.816013.

Lampiran

….