REFERENCES

[1] A. Hameed and A. Alomary, "Security issues in iot: A survey," in *2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*. IEEE, 2019, pp. 1–5.

[2] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," *Computer Communications*, vol. 153, pp. 311–335, 2020.

[3] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE communications magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[4] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for internet of things," *Digital Communications and Networks*, vol. 8, no. 6, pp. 1094–1104, 2022.

[5] C. Li, J. Wang, S. Wang, and Y. Zhang, "A review of iot applications in healthcare," *Neurocomputing*, vol. 565, p. 127017, 2024.

[6] M. M. Islam, S. Nooruddin, F. Karray, and G. Muhammad, "Internet of things: Device capabilities, architectures, protocols, and smart applications in healthcare domain," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3611–3641, 2022.

[7] S. U. A. Laghari, W. Li, S. Manickam, P. Nanda, A. K. Al-Ani, and S. Karuppayah, "Securing mqtt ecosystem: Exploring vulnerabilities, mitigations, and future trajectories," *IEEE Access*, vol. 12, pp. 139 273–139 289, 2024.

[8] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "A new approach to investigate iot threats based on a four layer model," in *2016 13th international conference on new technologies for distributed systems (NOTERE)*. IEEE, 2016, pp. 1–6.

[9] S. Elhadi, A. Marzak, N. Sael, and S. Merzouk, "Comparative study of iot protocols," *Smart Application and Data Analysis for Smart Cities (SADASC'18)*, 2018.

[10] A. Niruntasukrat, C. Issariyapat, P. Pongpaibool, K. Meesublak, P. Aiumsupucgul, and A. Panya, "Authorization mechanism for mqtt-based internet of things," in *2016 IEEE international conference on communications workshops (ICC)*. IEEE, 2016, pp. 290–295.

[11] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1. 2: Lightweight authenticated encryption and hashing," *Journal of Cryptology*, vol. 34, no. 3, p. 33, 2021.

[12] G. Cagua, V. Gauthier-Umaña, and C. Lozano-Garzon, "Implementation and performance of lightweight authentication encryption ascon on iot devices," *IEEE Access*, 2025.

[13] M. Bansal *et al.*, "Application layer protocols for internet of healthcare things (ioht)," in *2020 fourth international conference on inventive systems and control (ICISC)*. IEEE, 2020, pp. 369–376.

[14] D. Zeng, A. Badshah, S. Tu, M. Waqas, and Z. Han, "A security-enhanced ultra-lightweight and anonymous user authentication protocol for telehealthcare information systems," *IEEE Transactions on Mobile Computing*, 2025.

[15] A. Velinov, A. Mileva, S. Wendzel, and W. Mazurczyk, "Covert channels in the mqtt-based internet of things," *IEEE Access*, vol. 7, pp. 161 899–161 915, 2019.

[16] S. Kumari, M. K. Khan, and R. Kumar, "Cryptanalysis and improvement of 'a privacy enhanced scheme for telecare medical information systems'," *Journal of medical systems*, vol. 37, no. 4, p. 9952, 2013.

[17] M. K. Khan, J. Zhang, and L. Tian, "Chaotic secure content-based hidden transmission of biometric templates," *Chaos, Solitons & Fractals*, vol. 32, no. 5, pp. 1749–1759, 2007.

[18] Z. Siddiqui, J. Gao, and M. K. Khan, "An improved lightweight puf–pki digital certificate authentication scheme for the internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 19 744–19 756, 2022.

[19] M. Adil, M. K. Khan, N. Kumar, M. Attique, A. Farouk, M. Guizani, and Z. Jin, "Healthcare internet of things: Security threats, challenges, and future research directions," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19 046–19 069, 2024.

[20] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health iot threats: survey of risks and vulnerabilities," *Future Internet*, vol. 16, no. 11, p. 389, 2024.

[21] P. Shojaei, E. Vlahu-Gjorgievska, and Y.-W. Chow, "Security and privacy of technologies in health information systems: A systematic literature review," *Computers*, vol. 13, no. 2, p. 41, 2024.

[22] N. U. Kumara, I.N. and H. Dissanayake, "Enhancing data privacy of medical data through encryption and access control," *Int. J. Res. Eng. Sci. Manage.*, vol. 6, no. 11, pp. 38–43, 2023.

[23] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 2002.

[24] S. Wendzel, "Covert and side channels in buildings and the prototype of a building-aware active warden," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 6753–6758.

[25] I. Ahmad, F. Shahid, J. Islam, K. N. Haque, and E. Harjula, "Adaptive lightweight security for performance efficiency in critical healthcare monitoring," in *2024 18th International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE, 2024, pp. 78–83.

[26] N. B. Rofiatunnajah and A. M. Barmawi, "Improving anitw performance using bigrams character encoding and identity-based signature," *IEEE Access*, vol. 11, pp. 24 257–24 280, 2023.