[20] M. Humayun, M. Niazi, M. Assiri, and M. Haoues, "Secure Global Software Development: A Practitioners' Perspective," *Applied Sciences,* vol. 13, no. 4, 2023, doi: 10.3390/app13042465.

[21] M. R. Shaikh, R. Ullah, R. Akbar, K. Savita, and S. Mandala, "Fortifying Against Ransomware: Navigating Cybersecurity Risk Management with a Focus on Ransomware Insurance Strategies," *Int. J. Acad. Res. Bus. Soc. Sci,* vol. 14, no. 1, pp. 1415-1430, 2024. doi:10.6007/ijarbss/v14-i1/20566.

[22] F. F. S. Flores and S. R. d. L. Meira, "(UN)Ethical Software Engineering : A critical review about Software Engineering in face of Security Requirements in the IoT/ IoE Society," presented at the 2021 IEEE International Systems Conference (SysCon), 2021. doi:10.1109/SysCon48628.2021.9447113.

[23] M. F. Hassan, R. Akbar, K. Savita, R. Ullah, and S. Mandala, "Ransomware Classification with Deep Neural Network and Bi-LSTM," *Journal of Advanced Research in Applied Sciences and Engineering Technology,* vol. 47, no. 2, pp. 266-280, 2024. doi:10.37934/araset.47.2.266280.

[24] M. u. Rehman, R. Akbar, M. Omar, and A. R. Gilal, "A Systematic Literature Review of Ransomware Detection Methods and Tools for Mitigating Potential Attacks," in *International Conference on Computing and Informatics*, 2023: Springer, pp. 80-95. doi:10.1007/978-981-99-9589-9_7.

[25] A. A. Janisar, K. S. Kalid, A. Sarlan, and A. A. Mohammad Salameh, "Comprehensive Analysis of Security Requirements Engineering Approaches with Assurance Perspective," *Journal of Advanced Research in Applied Sciences and Engineering Technology,* pp. 104-119, 2024, doi: 10.37934/araset.54.2.104119.

[26] N. Qadir and R. Ahmad, "SecRS template to aid novice developers in security requirements identification and documentation," *International Journal of Software Engineering and Computer Systems,* vol. 8, no. 1, pp. 45-52, 2022. doi: 10.15282/ijsecs.8.1.2022.5.0095.

[27] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports,* vol. 7, pp. 8176-8186, 2021. doi: 10.1016/j.egyr.2021.08.126.

[28] R. Nath N and H. V Nath, "Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges," *Computers and Electrical Engineering,* vol. 100, 2022, doi: 10.1016/j.compeleceng.2022.107997.

[29] A. L. Mujeeb-ur-Rehman, Z. Hussain, F. H. Khoso, and A. A. Arain, "Cyber security intelligence and ethereum blockchain technology for e-commerce," *International Journal,* vol. 9, no. 7, 2021. doi:10.30534/ijeter/2021/21972021.

[30] A. Anjum, A. Siddiqua, S. Sabeer, S. Kondapalli, C. Kaur, and K. Rafi, "Analysis Of Security Threats, Attacks In The Internet Of Things," *Int. J. Mech. Eng,* vol. 6, pp. 2943-2946, 2021.

[31] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: a survey on attacks and countermeasures," *IoT,* vol. 2, no. 1, pp. 163-186, 2021. doi:10.3390/iot2010009

[32] A. Mukalazi and A. Boyaci, "The Internet of Things: a domain-specific security requirement classification," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2022: IEEE, pp. 1-8. doi:10.1109/hora55278.2022.9800035.

[33] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A review of security standards and frameworks for IoT-based smart environments," *IEEE Access,* vol. 9, pp. 121975-121995, 2021. doi:10.1109/access.2021.3109886.

[34] H. Alqarni, W. Alnahari, and M. T. Quasim, "Internet of things (IoT) security requirements: Issues related to sensors," in *2021 National Computing Colleges Conference (NCCC)*, 2021: IEEE, pp. 1-6. doi:10.1109/NCCC49330.2021.9428857.

[35] E. Klotins *et al.*, "SIoT framework: Towards an approach for early identification of security requirements for Internet-of-Things applications," *e-Informatica Software Engineering Journal,* 2021. doi:10.37190/e-Inf210103.