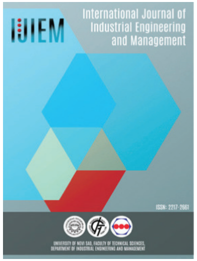

International Journal of Industrial
Engineering and Management

Cybersecurity Framework for IoT-Integrated Electric Power Information Systems

M. Orken[a] 0000-0001-8318-3794, B. D. Abdumauvlenovna[b,*] 0009-0008-3130-5356, Z. A. Tursynkanovna[c] 0000-0002-4525-5299, N. Mekebayev[d] 0000-0002-9117-4369, T. Serikov[e] 0000-0001-7026-7702, S. Zhazira[b] 0000-0003-4865-9800, K. Aizat[f] 0000-0001-5740-4100

[a] *Institute of Information and Computational Technologies, Almaty, Kazakhstan;*
[b] *AL- Farabi Kazakh National University, Almaty, Kazakhstan;*
[c] *Department of "Radio engineering, electronics and telecommunications" L.N. Gumilyov Eurasian National University, Astana, Kazakhstan;*
[d] *Kazakh National Women's Teacher Training University, Almaty, Kazakhstan;*
[e] *Electronics and Telecommunication Department, S. Seifullin Kazakh AgroTechnical Research University, Astana, Kazakhstan;*
[f] *M. Auezov South Kazakhstan University, Shymkent, Kazakhstan*

References

[1] D. Anyanwu, "Cybersecurity in the age of internet of things: A review of challenges and solutions," Fac. Nat. Appl. Sci. J. Comput. Appl., vol. 1, no. 1, pp. 1–9, 2024.

[2] E. James and F. Rabbi, "Fortifying the IoT landscape: Strategies to counter security risks in connected systems," Tensorgate J. Sustain. Technol. Infrastruct. Dev. Ctries., vol. 6, no. 1, pp. 32–46, 2023.

[3] J. Vostoupal and K. Uhlířová, "Of Hackers and Privateers: The Possible Evolution of the Problem of Cyber-Attribution," Masaryk Univ. J. Law Technol., vol. 18, no. 2, pp. 169–214, 2024, doi: 10.5817/mujlt2024-2-2.

[4] T. Johansmeyer, "How Reversibility Differentiates Cyber from Kinetic Warfare: A Case Study in the Energy Sector," Int. J. Secur. Privacy Trust Manag., vol. 12, no. 1, pp. 1–14, 2023, doi: 10.5121/ijsptm.2023.12101.

[5] S. A. Hashmi, C. F. Ali, and S. Zafar, "Internet of things and cloud computing-based energy management system for demand side management in smart grid," Int. J. Energy Res., vol. 45, no. 1, pp. 1007–1022, 2021, doi: 10.1002/er.6141.

[6] B. G. Kang and B. S. Kim, "Attachable IoT-based digital twin framework specialized for SME production lines," Int. J. Simul. Model., vol. 23, no. 3, pp. 471–482, Sep. 2024, doi: 10.2507/IJSIMM23-3-694.

[7] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," IEEE Syst. J., vol. 17, no. 4, pp. 6695–6709, 2023, doi: 10.1109/JSYST.2023.3305757.

[8] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, T. C. Bălan, E. Tuyishime, and R. Acheampong, "Cybersecurity challenges in IoT-based smart renewable energy," Int. J. Inf. Secur., vol. 23, no. 1, pp. 101–117, 2024, doi: 10.1007/s10207-023-00732-9.

[9] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," J. Supercomput, vol. 76, no. 7, pp. 5320–5363, 2020, doi: 10.1007/s11227-019-02945-z.

[10] R. Karthikeyani and E. Karthikeyan, "A Review on Distributed Denial of Service Attack," Asian J. Res. Comput. Sci., vol. 16, no. 4, pp. 133–144, 2023, doi: 10.9734/AJRCOS/2023/v16i4378.

[11] K. Vaigandla, N. Azmi, and R. Karne, "Investigation on intrusion detection systems (IDSs) in IoT," Int. J. Emerg. Trends Eng. Res., vol. 10, no. 3, 2022, doi: 10.30534/ijeter/2022/041032022.

[12] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," J. Netw. Comput. Appl., vol. 209, p. 103540, 2023, doi: 10.1016/j.jnca.2022.103540 .

[13] R. J. Rabelo, S. P. Zambiasi, and D. Romero, "Softbots 4.0: supporting cyber-physical social systems in smart production management," Int. J. Ind. Eng. Manag., vol. 14, no. 1, pp. 63–93, 2023, doi: 10.24867/IJIEM-2023-1-325.

[14] J. Basulo-Ribeiro, M. Amorim, and L. Teixeira, “How to accelerate digital transformation in companies with Lean Philosophy? Contributions based on a practical case,” Int. J. Ind. Eng. Manag., vol. 14, no. 2, pp. 94–104, 2023, doi: 10.24867/IJIEM-2023-2-326.

[15] S. Zahoor and R. N. Mir, “Resource management in pervasive Internet of Things: A survey,” J. King Saud Univ.-Comput. Inf. Sci., vol. 33, no. 8, pp. 921–935, 2021, doi: 10.1016/j.jksuci.2018.08.014.

[16] F. E. Salamh, U. Karabiyik, and M. Rogers, “A constructive direst security threat modeling for drone as a service,” J. Digit. Forensics Secur. Law, vol. 16, no. 1, p. 2, 2021, doi: 10.15394/jdfsl.2021.1695.

[17] E. Süren, F. Heiding, J. Olegård, and R. Lagerström, “PatrIoT: practical and agile threat research for IoT,” Int. J. Inf. Secur., vol. 22, no. 1, pp. 213–233, 2023, doi: 10.1007/s10207-022-00633-3.

[18] F. Thabit, S. A.-H. Alhomdy, A. Alahdal, and S. B. Jagtap, “Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques,” J. Inf. Comput. Sci., vol. 12, no. 10, pp. 17-41, 2020.

[19] H. Jahangir, S. Lakshminarayana, C. Maple, and G. Epiphaniou, "A Deep-Learning-Based Solution for Securing the Power Grid Against Load Altering Threats by IoT-Enabled Devices," IEEE Internet Things J., vol. 10, no. 12, pp. 10687-10697, 2023, doi: 10.1109/JIOT.2023.3240289.

[20] D. Mukherjee et al., “Cyber Security: Perspective of Challenges in Operational Technology Systems in Power Sector,” Power Res.-J. CPRI, pp. 35–45, 2024, doi: 10.33686/pwj.v20i1.1168.

[21] Y. Wang, T.-L. Nguyen, Y. Xu, Q.-T. Tran, and R. Caire, “Peer-to-peer control for networked microgrids: Multi-layer and multi-agent architecture design,” IEEE Trans. Smart Grid, vol. 11, no. 6, pp. 4688–4699, 2020, doi: 10.1109/TSG.2020.3006883.

[22] L. Chen, W. Hu, K. Jamieson, X. Chen, D. Fang, and J. Gummeson, “Pushing the physical limits of IoT devices with programmable metasurfaces,” in Proc. 18th USENIX Symp. Netw. Syst. Design Implement. (NSDI 21), 2021, pp. 425–438.

[23] M. Liu et al., "Enhancing Cyber-Resiliency of DER-Based Smart Grid: A Survey," IEEE Trans. Smart Grid, vol. 15, no. 5, pp. 4998-5030, 2024, doi: 10.1109/TSG.2024.3373008

[24] V. V. Vegesna, “Cybersecurity of Critical Infrastructure,” Int. Mach. Learn. J. Comput. Eng., vol. 7, no. 7, pp. 1–17, 2024.