New Research and Development Ideas

Authors: Anti E., Vartiainen T.

Organizations: UVA,

Project: CR-DES

Submission Date: Vaasa June .2023

Vipuvoimaa EU:lta 2014–2020

New Research and Development Ideas

Smart Grids are among today's critical infrastructure services, offering electrical power to consumers via two-way digital communications. As cyber threats and attacks become increasingly complex, there are various research and development areas available through cyber security virtual laboratories to assist organizations, academics, and security professionals in improving their cyber security capabilities. Some research and development ideas are as follows:

1. Blockchain Security: A virtual laboratory must evaluate blockchain security measures as blockchain technology spreads. Smart Grid cybersecurity threats can arise from various sources, including cybercrime, hacking, cyberwarfare, etc. Utility companies will need to communicate and coordinate the flow of cybersecurity information, such as intelligence and vulnerabilities, with governmental agencies and, most likely, other public and private sector cyber research institutes to reduce cybersecurity threats. Applying blockchain has the potential to be a dominant tool in cybersecurity since it provides better methods of protection and greater flexibility. Although blockchain may aid in defense against many attacks, the Smart Grid design is complex, and no single technology will protect against all potential dangers. As a result, cyber security in general, and intelligent metering in particular, are significant research issues and highly productive research subjects for the future.
2. Incorporating artificial intelligence and machine learning algorithms into a virtual laboratory can increase danger identification, response accuracy, and speed. Organizations can improve their threat detection and response capabilities by training machine learning models on massive datasets of cyber threat data. Future studies in Smart Grid cybersecurity could include a look at deploying a machine learning-based malware detection system. Specifically, how to mix machine learning with malware intrusion detection systems (IDS) designed specifically for Smart Grids.
3. The convergence of IoT with Smart Grids allows real-time data collection from all network locations. The smart grid is an electricity transport and distribution network that has been improved with digital control, surveillance, and telecommunications capabilities. The energy shift and new smart grids provide numerous difficulties for industrial cybersecurity. Smart grid cybersecurity is becoming a critical component in safeguarding the worldwide security of our global energy system. With the expansion of IoT devices, a virtual laboratory that can simulate IoT-based threats and evaluate IoT security measures is required. This can assist enterprises in ensuring the security of their IoT devices and networks.

References

Guo, Y., Wan, Z., & Cheng, X. (2022). When blockchain meets smart grids: A comprehensive survey. *High-Confidence Computing*, 100059.

Hasan, M. K., Alkhalifah, A., Islam, S., Babiker, N. B., Habib, A. A., Aman, A. H. M., & Hossain, M. A. (2022). Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations. *Wireless Communications and Mobile Computing*, *2022*, 1–26.

Mendel, J. (2019). *Blockchain as a Solution to Cyber Threats in the Smart Grid of the Future*.

Mollah, M. B., Zhao, J., Niyato, D., Lam, K.-Y., Zhang, X., Ghias, A. M., Koh, L. H., & Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal*, *8*(1), 18–43.