Peertechz

Trends in Computer Science and Information Technology
submitpaper@peertechz.com

ENGINEERING GROUP

TRENDS IN Computer Science and Information Technology

OPEN ACCESS JOURNAL

ISSN: 2641-3086 DOI: https://dx.doi.org/10.17352/tcsit

Mini Review

Internet of Things (IoT) and cyber security in the control of electrical energy systems: A review

Yusuf Kocak and Nurettin Abut*

Electrical Engineering Department, Kocaeli University, Kocaeli, Turkey

Received: 13 February, 2024
Accepted: 23 February, 2024
Published: 24 February, 2024

***Corresponding author:** Nurettin Abut, Electrical Engineering Department, Kocaeli University, Kocaeli, Turkey, E-mail: abut@kocaeli.edu.tr

ORCiD: https://orcid.org/0000-0001-6732-7575

Keywords: Internet of Things; IoT; Cyber security; Energy power system control

Summary

This article provides an assessment of the use of Internet of Things (IoT) technology in the control of electrical energy power systems and its cybersecurity risks. Electrical energy systems are complex and critical infrastructures today, and effective management and control of these systems are of great importance. The use of IoT technology in electrical energy systems allows these systems to become more efficient, flexible, and intelligent. However, the use of this technology also brings various cyber security risks. While this article examines the applications of IoT in power systems, it also focuses on how these systems can be protected against cybersecurity vulnerabilities.

Introduction

Power systems are one of the infrastructures used to meet the most basic needs of today's modern societies. These systems function in a wide range from energy production to distribution and consumption. As shown in Figure 1 they are effective in many stages of life. However, traditional energy systems have changed over time. Production, distribution, and consumption stages have become more complex. Technology has a great role in this change. Especially the use of innovative technologies such as the IoT is transforming power systems. In addition to making energy production and consumption smarter and more efficient, IoT also facilitates system management and maintenance.

Use of IoT in power systems

The use of IoT technology in power systems is seen in various areas. For example, thanks to smart meters, it is possible to monitor and analyze consumption data in real-time. This allows energy companies to better understand consumption patterns and manage resources more effectively. Additionally, through IoT sensors and smart devices, the status of energy systems can be constantly monitored and maintenance needs can be detected in advance [1-3].

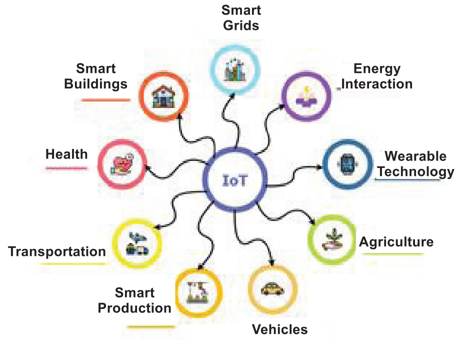

Figure 1: Areas where IoT devices are commonly used.

Cyber security risks

However, the widespread use of IoT in power systems also brings cyber security risks. Because IoT devices often have

Citation: Kocak Y, Abut N (2024) Internet of Things (IoT) and cyber security in the control of electrical energy systems: A review. Trends Comput Sci Inf Technol 9(1): 023-025. DOI: https://dx.doi.org/10.17352/tcsit.000076

limited resources and are constantly connected to the internet, they can be vulnerable to malicious attackers. Cyber attacks can cause disruption of energy systems, data manipulation, or even physical damage. This can lead to substantial human, economic and social consequences [4-7].

Cyber security strategies

Therefore, it is important to effectively protect power systems against cyber security vulnerabilities and insecure connection methods in the use of IoT. Security must be considered at every level, starting from the design of IoT devices to the network infrastructure. Precautions such as strong encryption, secure software updates, and secure network configurations should be taken. Additionally, a continuous security monitoring system should be established for monitoring and rapid response to cyber threats.

Manipulation of IoT devices

Sometimes, systems developed to be beneficial may have unintended adverse effects due to their increasing number and impact. In history, there are many examples of discoveries where the intended purpose was completely opposite to the actual usage, resulting in numerous destructive effects alongside the benefits they provided [8,9]. Naturally, it is estimated that the number of IoT devices to be added to the systems within "Electric Power Systems" will exceed 50 billion by 2025 and surpass 100 billion after 2050. However, even if these numbers are not currently considered significant, it is foreseen that without preventive measures over time, they will have a destructive impact.

For example, IoT devices in the real environment, whose input and output frequency values are given in Figure 2 and Figure 3, were designed in the virtual environment with their equivalents and function features in MathLab and Simulink libraries [10-12]. A total of 100 IoT devices using inverters were implemented in the same energy distribution environment [13]. After exposing 100 IoT current, voltage, and frequency harmonics to a seized IoT device, the behavior of the system was monitored. The observed situation appeared to indicate exposure to physical sabotage or serious system errors. This sampling, obtained from a narrow field and a single type of inverter through the Simulink test environment, can be anticipated to become even more complex with the diversity and distribution encountered in real life [7].

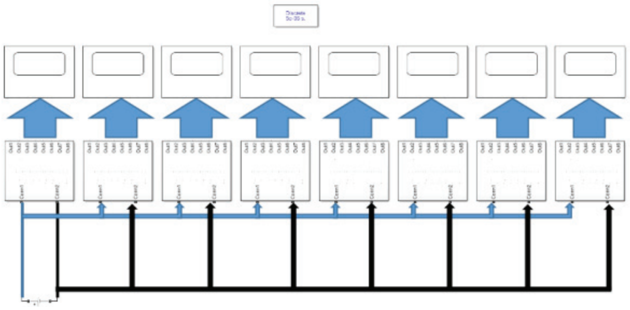

Figure 2: Simulink design of IoT devices using multiple inverters.

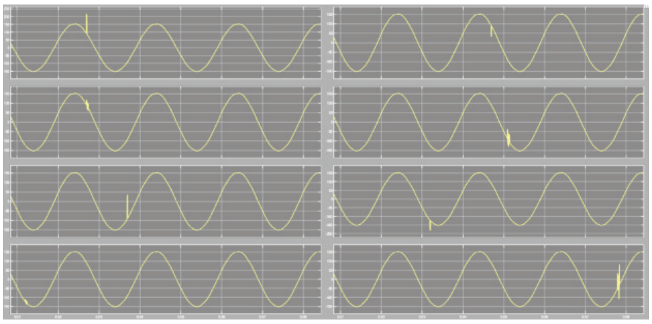

Figure 3: Harmonic effect applied to IoT devices using inverters.

Preventive measures

Preventive measures can be broadly examined under three categories: General compliance policies to national standards, managerial solutions, and technical solutions. Recommendations for the more efficient and secure use of the entire system have been provided through regulations to be managed by authorities in each category [14,15].

General compliance policies are to ensure the production and use of the systems to be added to IoT in accordance with the standards set by widespread and valid organizations such as the International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE), and National Institute of Standards and Technology (NIST) [6].

Managerial solutions are to take risk and hazard preventive work and integration measures for the products and systems to be used and to produce new policies for newly emerging situations [16].

Technical solutions are network-based controls, and third-party solutions integrated with IoT devices. IoT device identity and feature recognition, and anomaly detection in IoT devices [7].

Therefore, it is important to securely integrate IoT and implement cybersecurity strategies. In the future, the use of IoT technology in power systems is expected to increase further, which will make cyber security even more important [17-20].

Conclusion

In this article, an evaluation has been conducted on the widespread utilization of IoT technology in controlling power systems, as well as an assessment of the cybersecurity risks that may arise following its manipulation or compromise. The use and number of IoT in power systems have a great potential to increase day by day, but it also brings serious security concerns. Therefore, it is important to securely integrate IoT and implement cybersecurity strategies. In the future, the use of IoT technology in power systems is expected to increase further, which will make cyber security even more important.

Humanitarian approach: Even if we try to eliminate the problems with all precautions and technical solutions, it will not be more effective than predicting how much harm other people will suffer from a small mistake they make.

References

1. Taskesen E, Uren R, Uren S. IoT and Smart Grid: Using IoT Equipment for Smart Grid. International Journal of Advanced Natural Sciences and Engineering Researches. 2023; 7(4):43-49.

2. Yuksel O. Assessment at Power Quality of Low Voltage Power Distribution Lines of Konya Province in Different Inverters Topologies. MSc Thesis. Konya Technical University. 2022.

3. Dincer F, Karadag F. Self Energy Consumption Model and Power Quality Analysis in PV Power Plant". Journal of the Institute of Science and Technology. 2022; 12(2):704-714.

4. Avcı I. Akıllı evlerde IoT Technologies and Syber Security Problems in Smart Houses. Journal of European Science and Technology. 2022; (34):226-233.

5. Yilmaz EN, Gonen S, Sanoglu S, Karacayilmaz G, Ozbirinci O. Forgotten Factor at the Developing of Industry 4; Cyber Security. Duzce University, Journal of Science and Technology. 2021; 9(4):1142-1158.

6. Tulgar M, Zaim AH, Aydin MA. Guide of National Knowledge and Communications, An Application of IoT Security." Istanbul Commerce University, Journal of Sciences. 2022; 21(42):353-382.

7. Ozdemir IH, okrem L. Attact and Precaution of Syber Security for LoRaWAN DLOS8 Net Gateway. Gaziosmanpasa Journal of Science and Research. 2023; 12(2):42-56.

8. Keles A, Keles A. Innovations and Problems because of IoT. Electronic Turkish Studies. 2018; 13(13).

9. Ercan T, Kutay M. Endüstride nesnelerin interneti "IoT Applications in Industry. Afyon Kocatepe University, Journal of Science and Engineering. 2016; 16(3):599-607.

10. Abut N. Power Electronics, Semiconductors, and Converters. Istanbul, Turkey. Birsen Publ. 2004.

11. Asadi F, Abut N. Programing ST Microcontroller by using Waijung Block Set. Kocaeli, Turkey. Umuttepe Publ. 2018.

12. Asadi F, Abut N. Simulations of Power Electronics Circuits by using Matlab/Simulink. Kocaeli, Turkey. Umuttepe Publ. 2018.

13. Top IoT Security Solutions. eSecurity Planet. October 21, 2023. https://www.esecurityplanet.com/products/iot-security-solutions/

14. Hologram. 20 IoT security solutions for 2022 and beyond. October 23, 2023. https://www.hologram.io/blog/iot-security-solutions/

15. Altıntas AB. Viewing the Data of Medical Equipment by using IoT." MSc thesis, Kocaeli University, Institute of Science. 2018.

16. Elmas B, Alagoz I. High Frequency Switched Phase Controlled DC-AC Inverter." Erzincan University Journal of Science & Technology. 2022; 15(1).

17. Uysal E, Elewi A, Avaroglu E. Investigation of Smart Park System by using IoT Base. Euro J. Sci. Technol. 2020; 20:360-366.

18. Tariq A, Rehman RA, Kim BS. Epf an Efficient Forwarding Mechanism in SDN Controller Enabled Named Data IoTs. Applied Sciences. 2020; 10(21):7675.

19. Kurt C, Yılmazturk I, Okur F, Menemen A, Bahtiyar B, Iplikci S. Designing of an Irrigation Automation Syastem by IoT.

20. Aktas F, Çeken C, Erdemli YE. Data Collect and Analysis of Biomedical Applications by IoT. Medical Technologies Congress. 2014; 25-27.

Citation: Kocak Y, Abut N (2024) Internet of Things (IoT) and cyber security in the control of electrical energy systems: A review. Trends Comput Sci Inf Technol 9(1): 023-025. DOI: https://dx.doi.org/10.17352/tcsit.000076