Journal of Electrical Engineering, Electronics, Control and Computer Science – JEEECCS, Volume 9, Issue 33, pages 1-8, 2023

Internet of Things for Enhancing Stability and Reliability in Power Systems

Anshu Prakash Murdan
Department of Electrical and Electronic Engineering
University of Mauritius
Reduit, Mauritius
a.murdan@uom.ac.mu

***Abstract* – This paper presents an overview of IoT-based approaches for enhancing power system stability with the objective to explore real-time monitoring, control of system components, predictive maintenance, optimization of energy usage, and to evaluate the communication infrastructure required for IoT-enabled power systems. It also includes real-world case studies to illustrate the potential benefits and challenges of implementing IoT in power systems. We discuss the communication infrastructure required for IoT-enabled power systems, including the types of sensors and devices needed, as well as the protocols for data transmission and storage. The role of data analytics is also explored, including the use of machine learning algorithms to predict system behavior and identify potential faults. The paper further addresses security concerns associated with IoT-enabled power systems, including the need for encryption, authentication, and access control measures. Finally, potential future developments in IoT-enabled power systems are discussed, including the integration of renewable energy sources, the use of blockchain technology for data management, and the development of autonomous control systems. Overall, this paper highlights the significance of IoT in enhancing power system's stability and reliability. A roadmap for future research and development in this field is also presented.**

Keywords-component; Internet of Things (IoT); Power systems; Stability enhancement; Data analytics; Security concerns

I. INTRODUCTION

Power systems are critical infrastructure that form the backbone of modern society. These systems are responsible for generating, transmitting, and distributing electricity to various end-users such as homes, businesses, and industries. The power grid is a complex network of power plants, transmission lines, distribution substations, and transformers that work together to provide a continuous supply of electricity. Stability in power systems is of utmost importance as it ensures the system can maintain a steady and reliable supply of power despite disturbances. The stability of a power system is determined by the balance between power generation and consumption, and any deviation from this balance can lead to instability [1]. A stable power system can withstand disturbances such as sudden changes in demand or the failure of a power plant without causing power outages or damage to equipment. A power system that lacks stability can experience a variety of issues, such as voltage fluctuations, frequency instability, and power outages [2]. These problems can cause significant economic and social costs, including lost productivity, equipment damage, and potential safety hazards. Additionally, unstable power systems can lead to a decrease in the quality of power supply, which can negatively impact the performance of electronic devices and machinery [3]. The importance of stability in power systems is further amplified by the increasing complexity of power grids, which are becoming more interconnected and incorporating more renewable energy sources [4]. Renewable energy sources such as wind and solar power are variable and intermittent, which can make it challenging to maintain power system stability. Therefore, it is imperative to develop effective strategies to enhance power system stability to ensure that power grids can operate efficiently and sustainably.

Achieving stability in power systems can be challenging due to several factors. One of the main challenges is the complexity of the power system, which comprises a large number of interconnected components such as generators, transformers, and transmission lines. As a result, even small disturbances in one part of the system can have a significant impact on the overall stability of the system. Another challenge is the dynamic nature of power demand, which can fluctuate rapidly and unpredictably. This makes it difficult to maintain a balance between power generation and consumption and can lead to instability. Additionally, power systems often suffer from aging infrastructure, which can result in equipment failures, leading to instability. To address these challenges, several existing techniques are used for stability enhancement in power systems. One technique is load shedding [5], which involves disconnecting specific loads from the power system to restore balance and prevent power outages. Another technique is frequency control, which adjusts the power output of generators to maintain a constant frequency in the system [6]. Similarly, voltage regulation is used to maintain a constant voltage level in the system by adjusting the output of transformers [7].

This paper focuses on how the Internet of Things (IoT) can be employed to enhance power system stability by offering real-time monitoring and control of system components, predictive maintenance, optimization of energy usage, and evaluating the communication infrastructure required for IoT-enabled power systems.

II. IoT in Power Systems

In addition to the traditional techniques, new technologies such as the Internet of Things (IoT) are being explored for their potential to enhance power system stability. The Internet of Things (IoT) is a concept that refers to the interconnectivity of devices and sensors that can communicate with each other over the internet [8]. These devices and sensors collect and analyse data in real-time, enabling better control and optimization of systems.

A. Real-time monitoring and control of system components

IoT technologies enable real-time monitoring and control of power system components [9], allowing for rapid response to disturbances and optimization of power usage. Real-time monitoring and control of system components involves the installation of IoT-enabled sensors and devices throughout the power system to collect and transmit data on system performance in real-time. These sensors and devices can be installed in various components of the power system, including power plants, transmission lines, and distribution substations. IoT-enabled sensors measure and transmit data on various parameters, such as voltage, frequency, power factor, and temperature. These sensors are typically connected to a central monitoring system that collects and analyses the data, providing real-time information on the performance of the power system. This information is used to detect and respond to disturbances quickly, improving the stability of the power system. For example, PMUs can be installed at various points in the power system, including transmission lines and substations, to measure and transmit data on the voltage and frequency of the system. This data can be used to detect disturbances such as voltage and frequency fluctuations, allowing power system operators to take corrective action before the system becomes unstable.

Similarly, IoT-enabled sensors can be installed in individual components such as transformers and generators to monitor their performance in real-time. For example, temperature sensors installed in transformers monitor their temperature to ensure that they operate within safe limits. In addition to monitoring the performance of individual components, IoT technology can be used to monitor the performance of the power system as a whole. By collecting and analysing data on various parameters such as power consumption and energy usage, power system operators are empowered to identify areas where energy efficiency can be improved and take corrective action to improve overall system performance.

B. Predictive maintenance

Predictive maintenance is a technique that uses IoT technology, and advanced analytics techniques to predict potential equipment failures before they occur [10], [11]. As mentioned earlier, this also involves the installation of sensors in individual components of the power system to monitor their performance in real-time. The data collected by these sensors are then analysed using machine learning algorithms to identify patterns and anomalies in the data. This technique has several advantages over traditional maintenance methods. First, it enables power system operators to detect potential faults before they occur, thus reducing downtime and preventing equipment failures that could impact the stability of the power system. Second, predictive maintenance reduces maintenance costs by optimizing the timing of maintenance activities, minimizing the number of unnecessary maintenance activities [12].

C. Optimization of energy usage

Optimization of energy usage is a technique that uses IoT technology to improve the efficiency of the power system. In this case as well, sensors and devices are installed throughout the power system to collect data on energy consumption patterns in real-time. By analysing this data, power system operators identify areas of high energy usage and develop strategies to reduce energy consumption [13]. IoT-enabled sensors measure and transmit data on various parameters such as energy consumption, power factor, and load demand. Optimization of energy usage has several benefits for power systems. By reducing energy consumption, power systems improve their overall efficiency, reduce costs and minimize the environmental impact of energy generation. Additionally, optimizing energy usage leads to a more stable and reliable power system.

III. Communication Infrastructure

IoT-enabled power systems typically require a communication infrastructure that enables the collection and transmission of data from sensors and devices throughout the power system. The communication infrastructure is generally capable of transmitting data in real-time, enabling power system operators to monitor the system's health and respond to disturbances almost instantaneously [14]. The sensors and devices required for an IoT-enabled power system may include a variety of different types, such as phasor measurement units (PMUs) for measuring voltage and frequency [15], temperature sensors for monitoring the performance of transformers and generators [16], and smart meters for measuring energy consumption patterns [17]. These sensors and devices are generally designed to operate in the harsh environments typically found in power systems, such as high temperatures, humidity, and electromagnetic interference.

The communication protocols used in IoT-enabled power systems are able to transmit data in real-time and ensure the security and reliability of the data transmission. The protocols used for data transmission and storage may include various communication standards such as the IEEE 802.15.4 for wireless sensor networks [18] or TCP/IP for wired networks. These protocols ensure that the data collected by the sensors and devices is transmitted securely and reliably to the central monitoring system for analysis.

On the other hand, for wireless data transmission, IoT-enabled power systems make use of communication technologies such as Wi-Fi [19], Zigbee[20], or cellular networks [21]. The choice of communication technology depends on factors such as the distance between sensors and the central monitoring system, the required data rate, and the level of security required [22]. The data collected by the sensors and devices is stored and analysed in a central monitoring system. This system is designed to handle large volumes of data in real-time and provides insights into the performance of the power system.

IV. Data Analytics

Data analytics plays a critical role in power systems by providing insights into the performance of the power system [23] and enabling power system operators to make informed decisions. The following section briefly highlights a few applications of machine learning algorithms in IoT-enabled power systems.

A. Fault detection and diagnosis

One key application of data analytics in power systems is the use of machine learning algorithms to predict system behaviour and identify potential faults before they occur [24]. This involves the use of historical data collected by sensors and devices to train machine learning algorithms to identify patterns and anomalies in the data that may indicate potential issues with the power system.

B. Load forecasting

Machine learning algorithms can also be used to predict future load demand in the power system [25], enabling power system operators to optimize the use of resources and minimize waste. For example, the algorithms can analyse historical load data and weather patterns to predict future load demand, helping power system operators to optimize the generation and distribution of power to meet future demand. For instance, authors of [26] proposed a point-interval mid-term electricity demand forecasting model, taking into account socio-economic as well as meteorological factors.

C. Asset management

Furthermore, nowadays machine learning algorithms can be applied to optimize asset management in the power system, enabling power system operators to prioritize maintenance activities and extend the lifespan of equipment. In essence, the algorithms analyse data from sensors and devices to predict the remaining lifespan of equipment such as transformers and generators, helping power system operators to schedule maintenance activities and replacement before equipment failures occur [27].

Overall, the application of machine learning algorithms in IoT-enabled power systems has the potential to improve the efficiency, reliability, and resilience of the power system.

D. Identification of opportunities for optimization

By analysing energy consumption patterns and other data collected from IoT-enabled sensors and devices, power system operators can identify areas of high energy usage and develop strategies to reduce energy consumption [28]. This could involve adjusting system parameters, replacing inefficient components, or changing energy usage practices. One key strategy for reducing energy consumption in IoT-enabled power systems is load shifting [29], which involves shifting energy consumption to off-peak hours when energy is cheaper and more abundant. By analysing energy consumption patterns, power system operators can identify opportunities for load shifting and develop strategies to encourage consumers to shift their energy consumption to off-peak hours. Another strategy for reducing energy consumption is demand response [30], which involves adjusting energy usage in response to changes in the supply of energy. For example, if the supply of energy is low, power system operators can send signals to IoT-enabled devices, such as smart thermostats, to reduce energy consumption until the supply of energy is restored.

V. Case Studies

There are several real-world applications of IoT in power systems, which have demonstrated significant benefits, but also encountered challenges during implementation. Two examples are elaborated below:

A. Duke Energy

Duke Energy, one of America’s largest energy holding companies, implemented an IoT-enabled power system to optimize the use of renewable energy sources such as solar and wind [31]. The system uses advanced analytics to predict energy demand and optimize the use of renewable energy sources. This has enabled Duke Energy to reduce the use of fossil fuels, increase the use of renewable energy, and improve the efficiency of the power system. This has helped Duke Energy to meet its sustainability goals and reduce its impact on the environment.

Duke Energy, one of the major energy holding companies in America, undertook a strategic initiative to harness the power of the Internet of Things (IoT) to refine its energy production and distribution, particularly emphasizing on renewable sources like solar and wind power [31]. This compelling case study is characterized by several stages of implementation and sophisticated methodologies.

The initial phase involved a comprehensive evaluation of the existing power system, identifying areas that could benefit from IoT-enabled solutions, and building a strategic roadmap for deployment. Key operational areas that were identified included demand prediction, renewable energy utilization, and system efficiency enhancement. To address these, the company decided to invest in IoT sensors and devices, advanced analytics solutions, and communication infrastructure that could facilitate real-time data transmission and analysis.

The next stage was the design and deployment of these IoT-enabled systems. A network of sensors was established across their renewable energy infrastructures, including wind turbines and solar panels. These sensors were equipped to capture various data points like wind speed, solar radiation, energy generated, and any potential equipment malfunction.

IoT devices, deployed strategically in their grid, were used to monitor and control energy distribution based on real-time data.

Subsequently, the company implemented advanced analytics to harness the data gathered. Predictive models were developed to forecast energy demand accurately, enabling Duke Energy to optimize the allocation of energy produced from renewable sources. By predicting periods of high and low demand, they were able to balance their supply more efficiently and reduce reliance on fossil fuels.

This IoT-driven approach not only led to increased utilization of renewable energy but also markedly improved the overall efficiency of their power system. The real-time monitoring facilitated by IoT reduced instances of unplanned downtime, as potential faults could be detected and rectified in a timely manner. In addition, the use of predictive analytics enabled proactive maintenance of equipment, further enhancing system reliability and efficiency.

Ultimately, this IoT-enhanced approach helped Duke Energy to meet its sustainability objectives and diminish its environmental footprint. By integrating IoT with advanced analytics, Duke Energy transformed its energy management, leading to substantial reductions in fossil fuel usage, while significantly increasing renewable energy deployment. The success of this initiative serves as an encouraging testament to the transformative potential of IoT technology in the power industry.

B. Tokyo Electric Power Company

The Tokyo Electric Power Company (TEPCO), a significant player in Japan's energy industry, launched an IoT-driven initiative aimed at enhancing the stability and reliability of their power systems [32]. This was especially critical in the aftermath of the Fukushima nuclear disaster in 2011, which had underscored the necessity of robust power systems that could withstand severe disturbances. The deployment of this IoT-enabled power system involved several strategic stages and methodological choices.

At the onset, TEPCO identified key areas of their power system that were crucial for system stability and could benefit from IoT integration. This included components such as transformers and generators, which were pivotal in energy transmission and generation. Recognizing that early detection of faults in these components could prevent system-wide failures, they decided to implement a real-time monitoring system enabled by IoT devices and sensors.

In the second stage, TEPCO proceeded to design and install an array of sensors and IoT devices across these identified components. These devices were configured to monitor a wide array of parameters, such as voltage levels, current flow, temperature, and vibrational data. All these data points were valuable indicators of the health of these components and could pre-emptively flag potential issues.

Once the sensor network was established, the third stage involved setting up a robust communication and data infrastructure. This infrastructure facilitated real-time data transmission from the sensors to a centralized control centre. By doing so, it ensured that power system operators were kept constantly informed of the status of the system components.

With the influx of real-time data, the fourth stage involved leveraging this information to optimize operations. Advanced analytics was employed to interpret the data, enabling TEPCO to detect potential issues before they escalated into full-blown faults. Upon detection of any anomalies, operators could promptly respond, adjust system parameters, or deploy maintenance teams, if necessary, thereby improving the stability and reliability of the power system.

Furthermore, this IoT-driven approach significantly reduced system downtime. The combination of real-time monitoring and prompt responses to disturbances allowed TEPCO to minimize disruptions, a benefit that rippled out to businesses and consumers dependent on their power supply. Consequently, this had a positive impact on the Japanese economy, demonstrating the far-reaching implications of efficient and reliable power system management.

Essentially, TEPCO's successful implementation of an IoT-enabled power system underscores the potential of IoT technology to transform the reliability and stability of power systems while minimizing system downtime. This case study serves as a valuable example of how IoT can be applied strategically to address challenges and improve outcomes in the power industry.

VI. Results and Discussion

The integration of Internet of Things (IoT) technology with power systems has become a key research area due to its potential to enhance the stability, reliability, and efficiency of these systems. The unique aspect of our research lies in the detailed examination of this integration and its implications, as evidenced through the case studies of Duke Energy and the Tokyo Electric Power Company (TEPCO). By juxtaposing these real-world implementations with existing studies in the field, we present a comparative analysis that accentuates the improvements brought about by the application of IoT in power systems.

A. Results

The case study of Duke Energy demonstrates the power of IoT to foster the optimization of renewable energy resources. Through an advanced, IoT-driven analytics system, Duke Energy accurately forecasts energy demand, effectively managing their energy supply. Consequently, they've witnessed a decline in fossil fuel dependence, an increase in renewable energy use, and a surge in the overall system's efficiency. These strides towards sustainability highlight the potential of IoT in driving the renewable energy transition. In contrast, the case of Tokyo Electric Power Company (TEPCO) showcases how IoT can bolster system stability and reliability. Following the Fukushima nuclear disaster, TEPCO introduced an IoT-based monitoring framework that enabled real-time fault detection and rapid disturbance response. The implementation has significantly minimized system downtime, leading to less business disruption and a more resilient economy in Japan.

B. Discussion

The outcomes of the case studies provide compelling evidence that integrating IoT within power systems leads to multiple benefits. Duke Energy's strides towards sustainability and TEPCO's enhanced system reliability present a broader picture of the socio-economic implications of IoT-enabled power systems. Our research outcomes resonate with existing studies in the field, further cementing the benefits of IoT-based approaches. What distinguishes our work is the real-world application scenarios providing a more holistic view of the implications of IoT implementation in power systems.

VII. Security concerns associated with IoT-enabled power systems

Security is a critical concern when it comes to IoT-enabled power systems. The deployment of IoT devices and sensors throughout the power system creates new opportunities for cyberattacks, which could result in power outages, equipment damage, or even physical harm to individuals [33]. To address the security concerns associated with IoT-enabled power systems, several measures need to be implemented, including encryption, authentication, and access control measures.

Encryption is essential for securing data transmitted between IoT devices and sensors in the power system. Encryption ensures that data is only accessible to authorized parties and prevents unauthorized access or tampering [34]. Encryption mechanisms such as AES (Advanced Encryption Standard) can be used to protect data transmitted between IoT devices and sensors. Authentication is another important security measure for IoT-enabled power systems. Authentication mechanisms, such as digital certificates or biometric authentication, are typically used to ensure that only authorized personnel have access to the IoT-enabled power system. Authentication ensures that IoT devices and sensors are only accessible by authorized parties and helps prevent unauthorized access [35]. Access control measures are implemented to ensure that only authorized personnel can access the IoT-enabled power system. Access control measures such as firewalls, intrusion detection systems, and role-based access control can be used to ensure that only authorized personnel can access the IoT-enabled power system [36]. This helps to prevent unauthorized access and helps to ensure that the IoT-enabled power system remains secure.

In addition to encryption, authentication, and access control measures, there are other security measures that can be implemented to enhance the security of IoT-enabled power systems. Here are some additional security measures that can be implemented:

Vulnerability assessments: Regular vulnerability assessments can be conducted to identify potential security weaknesses in the IoT-enabled power system [37]. This can help power system operators to identify potential vulnerabilities before they are exploited by attackers.

Intrusion detection systems: Intrusion detection systems can be used to detect potential cyberattacks in real-time. Intrusion detection systems can detect unusual activity within the IoT-enabled power system and alert power system operators to potential security threats [38].

Physical security measures: Physical security measures, such as access control systems and video surveillance, can be implemented to secure the physical components of the IoT-enabled power system [39]. This can help prevent physical attacks on the power system, such as sabotage or theft.

Disaster recovery plans: Disaster recovery plans can be developed to ensure that the power system can be quickly restored in the event of a cyberattack or other security breach. Disaster recovery plans should include procedures for backing up data and restoring system functionality [40].

Overall, addressing security concerns in IoT-enabled power systems is critical to ensuring the stability and reliability of the power system. A comprehensive security strategy that includes encryption, authentication, access control measures, vulnerability assessments, intrusion detection systems, physical security measures, and disaster recovery plans can help to ensure that IoT-enabled power systems are secure and can withstand potential cyberattacks or other security breaches.

VIII. Potential Future Developments in IoT-Enabled Power Systems

IoT-enabled power systems have already shown significant benefits in terms of stability, efficiency, and reliability. However, there are several potential future developments that could further improve the capabilities of IoT-enabled power systems.

One of the most significant potential future developments in IoT-enabled power systems is the integration of renewable energy sources. The integration of renewable energy sources such as solar and wind is critical for reducing greenhouse gas emissions and improving the sustainability of the power system [41]. However, renewable energy sources are variable and intermittent, which can pose challenges for power system stability and reliability. IoT-enabled power systems can help to manage the variability and intermittency of renewable energy sources by predicting energy demand and adjusting power output accordingly [42]. By optimizing the use of renewable energy sources, IoT-enabled power systems can help to improve the sustainability of the power system while maintaining stability and reliability.

Another potential future development is the use of blockchain technology for data management in IoT-enabled power systems. Blockchain technology has the potential to revolutionize data management in IoT-enabled power systems [43]. Blockchain technology can be used to securely manage data from IoT devices and sensors, ensuring that data is accurate, transparent, and tamper-proof. This can help to increase trust and reliability in IoT-enabled power systems, which is critical for the adoption of new technologies and business models. Blockchain technology can also enable new business models such as peer-to-peer energy trading, where individuals can buy and sell energy from each other directly, without the need for intermediaries.

Furthermore, the development of autonomous control systems is another potential future development in IoT-enabled power systems. Autonomous control systems have the potential to revolutionize the management and optimization of the power system. Autonomous control systems can be used to manage and optimize the power system in real-time, without human intervention. This can help to improve the efficiency and reliability of the power system and reduce the risk of human error. For example, autonomous control systems can be used to optimize the use of energy resources, predict energy demand, and respond to disturbances in real-time.

IX. Conclusion

In this paper, we delved into the potential of Internet of Things (IoT) in enhancing the stability of power systems, pivotal infrastructure that provides indispensable services like electricity to residences, commercial establishments, and industries. The crux of a reliable power system lies in its ability to maintain a consistent supply of power despite potential disturbances. IoT technology, when integrated with power systems, offers a multifaceted approach towards augmenting stability. It provides real-time monitoring and control of system components, facilitates predictive maintenance, and allows optimization of energy usage. IoT in power systems is a comprehensive solution to several persistent challenges in the power industry. It is capable of monitoring and responding to changes in demand and supply, and identifying potential faults proactively, thereby permitting pre-emptive actions to avoid power outages and maintain system stability. Furthermore, IoT-enabled power systems can detect disturbances such as voltage fluctuations or equipment failures in real-time, and automatically respond by rerouting power or adjusting system parameters. By deploying IoT-enabled sensors and devices throughout the system, operators can gather real-time data on the performance of the system and its components, facilitating optimal functioning of the power system.

While we recognize the significance of addressing security concerns in IoT-enabled power systems, measures such as encryption, authentication, and access control are typically employed to ensure robust security. The future scope of IoT-enabled power systems promises further advancement, with potential developments including the integration of renewable energy sources, utilization of blockchain technology for data management, and the inception of autonomous control systems. IoT technology offers considerable value in improving the stability, reliability, and efficiency of power systems, while also reducing costs and enhancing sustainability. This transformative application of IoT offers a powerful solution to long-standing challenges and opens the gateway to a sustainable future in the power industry.

References

[1] S. U. Khan, N. Khan, F. U. M. Ullah, M. J. Kim, M. Y. Lee, and S. W. Baik, “Towards intelligent building energy management: AI-based framework for power consumption and generation forecasting,” *Energy Build*, vol. 279, p. 112705, Jan. 2023, doi: 10.1016/J.ENBUILD.2022.112705.

[2] M. Z. Zakariya and J. Teh, “A Systematic Review on Cascading Failures Models in Renewable Power Systems with Dynamics Perspective and Protections Modeling,” *Electric Power Systems Research*, vol. 214, p. 108928, Jan. 2023, doi: 10.1016/J.EPSR.2022.108928.

[3] S. Perera and S. Elphick, “Implications of equipment behaviour on power quality,” *Applied Power Quality*, pp. 185–258, Jan. 2023, doi: 10.1016/B978-0-323-85467-2.00002-0.

[4] P. Makolo, R. Zamora, and T. T. Lie, “The role of inertia for grid flexibility under high penetration of variable renewables - A review of challenges and solutions,” *Renewable and Sustainable Energy Reviews*, vol. 147, p. 111223, Sep. 2021, doi: 10.1016/J.RSER.2021.111223.

[5] M. Ghotbi-Maleki, R. M. Chabanloo, and H. Javadi, “Load shedding strategy using online voltage estimation process for mitigating fault-induced delayed voltage recovery in smart networks,” *Electric Power Systems Research*, vol. 214, p. 108899, Jan. 2023, doi: 10.1016/J.EPSR.2022.108899.

[6] M. N. H. Shazon, Nahid-Al-Masood, and A. Jawad, “Frequency control challenges and potential countermeasures in future low-inertia power systems: A review,” *Energy Reports*, vol. 8, pp. 6191–6219, Nov. 2022, doi: 10.1016/J.EGYR.2022.04.063.

[7] K. D. Pippi, G. C. Kryonidis, A. I. Nousdilis, and T. A. Papadopoulos, “A unified control strategy for voltage regulation and congestion management in active distribution networks,” *Electric Power Systems Research*, vol. 212, p. 108648, Nov. 2022, doi: 10.1016/J.EPSR.2022.108648.

[8] A. Das, S. C. M. Sharma, and B. K. Ratha, “The New Era of Smart Cities, From the Perspective of the Internet of Things,” *Smart Cities Cybersecurity and Privacy*, pp. 1–9, Jan. 2019, doi: 10.1016/B978-0-12-815032-0.00001-9.

[9] C. Brosinsky, M. Karaçelebi, and J. L. Cremer, “Machine learning and digital twins: monitoring and control for dynamic security in power systems,” *Monitoring and Control of Electrical Power Systems Using Machine Learning Techniques*, pp. 79–106, Jan. 2023, doi: 10.1016/B978-0-32-399904-5.00010-7.

[10] S. Ayvaz and K. Alpay, “Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time,” *Expert Syst Appl*, vol. 173, p. 114598, Jul. 2021, doi: 10.1016/J.ESWA.2021.114598.

[11] P. Nunes, J. Santos, and E. Rocha, “Challenges in predictive maintenance – A review,” *CIRP J Manuf Sci Technol*, vol. 40, pp. 53–67, Feb. 2023, doi: 10.1016/J.CIRPJ.2022.11.004.

[12] “Predictive maintenance for critical infrastructure,” *Expert Syst Appl*, vol. 210, p. 118413, Dec. 2022, doi: 10.1016/J.ESWA.2022.118413.

[13] A. Balali, A. Yunusa-Kaltungo, and R. Edwards, “A systematic review of passive energy consumption optimisation strategy selection for buildings through multiple criteria decision-making techniques,” *Renewable and Sustainable Energy Reviews*, vol. 171, p. 113013, Jan. 2023, doi: 10.1016/J.RSER.2022.113013.

[14] “Faults in smart grid systems: Monitoring, detection and classification,” *Electric Power Systems Research*, vol. 189, p. 106602, Dec. 2020, doi: 10.1016/J.EPSR.2020.106602.

[15] “A review on optimal placement of phasor measurement unit (PMU),” pp. 513–530, Jan. 2022, doi: 10.1016/B978-0-323-90240-3.00028-X.

[16] “New-age condition monitoring of on-load tap changing transformers in distributed energy systems for Industry 4.0,” *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 2, p. 100087, Jan. 2022, doi: 10.1016/J.PRIME.2022.100087.

[17] E. Viciana, F. M. Arrabal-Campos, A. Alcayde, R. Baños, and F. G. Montoya, "All-in-one three-phase smart meter and power quality analyzer with extended IoT capabilities," *Measurement*, vol. 206, p. 112309, Jan. 2023, doi: 10.1016/J.MEASUREMENT.2022.112309.

[18] A. Viloria, N. A. L. Zelaya, and N. Mercado-Caruzo, "Design of a Network with wireless sensor applied to data transmission based on IEEE 802.15.4 standard," *Procedia Comput Sci*, vol. 175, pp. 665–670, Jan. 2020, doi: 10.1016/J.PROCS.2020.07.097.

[19] J. Epstein, "Introduction to Wi-Fi," *Scalable VoIP Mobility*, pp. 101–202, Jan. 2009, doi: 10.1016/B978-1-85617-508-1.00005-0.

[20] "ZigBee Applications," *Zigbee Wireless Networking*, pp. 111–206, Jan. 2008, doi: 10.1016/B978-0-7506-8597-9.00004-5.

[21] J. Bair, "The Cellular Network," *Seeking the Truth from Mobile Evidence*, pp. 55–70, Jan. 2018, doi: 10.1016/B978-0-12-811056-0.00005-4.

[22] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1–13, Jan. 2023, doi: 10.1016/J.IOTCPS.2022.12.003.

[23] R. Soni and B. Mehta, "Evaluation of power transformer health analysis by internal fault criticalities to prevent premature failure using statistical data analytics approach," *Eng Fail Anal*, vol. 136, p. 106213, Jun. 2022, doi: 10.1016/J.ENGFAILANAL.2022.106213.

[24] M. Nikfar, J. Bitencourt, and K. Mykoniatis, "A Two-Phase Machine Learning Approach for Predictive Maintenance of Low Voltage Industrial Motors," *Procedia Comput Sci*, vol. 200, pp. 111–120, Jan. 2022, doi: 10.1016/J.PROCS.2022.01.210.

[25] P. Tejaswi and O. V. Gnana Swathika, "Machine learning algorithms-based solar power forecasting in smart cities," *Artificial Intelligence and Machine Learning in Smart City Planning*, pp. 171–179, Jan. 2023, doi: 10.1016/B978-0-323-99503-0.00001-6.

[26] T. Gao, D. Niu, Z. Ji, and L. Sun, "Mid-term electricity demand forecasting using improved variational mode decomposition and extreme learning machine optimized by sparrow search algorithm," *Energy*, vol. 261, p. 125328, Dec. 2022, doi: 10.1016/J.ENERGY.2022.125328.

[27] H. Ghasemi, E. Shahrabi Farahani, M. Fotuhi-Firuzabad, P. Dehghanian, A. Ghasemi, and F. Wang, "Equipment failure rate in electric power distribution networks: An overview of concepts, estimation, and modeling methods," *Eng Fail Anal*, vol. 145, p. 107034, Mar. 2023, doi: 10.1016/J.ENGFAILANAL.2022.107034.

[28] P. He, N. Almasifar, A. Mehbodniya, D. Javaheri, and J. L. Webber, "Towards green smart cities using Internet of Things and optimization algorithms: A systematic and bibliometric review," *Sustainable Computing: Informatics and Systems*, vol. 36, p. 100822, Dec. 2022, doi: 10.1016/J.SUSCOM.2022.100822.

[29] M. Ghahramani, S. Nojavan, K. Zare, and B. Mohammadi-ivatloo, "Application of Load Shifting Programs in Next Day Operation of Distribution Networks," *Operation of Distributed Energy Resources in Smart Distribution Networks*, pp. 161–177, Jan. 2018, doi: 10.1016/B978-0-12-814891-4.00007-2.

[30] B. Khan and I. G. Hagos, "Demand response aggregation," *Active Electrical Distribution Network: Issues, Solution Techniques, and Applications*, pp. 345–358, Jan. 2022, doi: 10.1016/B978-0-323-85169-5.00008-3.

[31] ERP TODAY, "Duke Energy drives clean energy transition with AWS ," 2022. https://erp.today/duke-energy-drives-clean-energy-transition-with-aws/ (accessed Mar. 03, 2023).

[32] T. E. P. C. H. TEPCO, "TEPCO BEGINS REMOTE USE OF 'INTERNET OF THINGS'TO IMPROVE PERFORMANCE OF THERMAL POWER STATIONS," 2018. https://www.tepco.co.jp/en/press/corp-com/release/2018/1476022_15409.html (accessed Mar. 03, 2023).

[33] A. Rahiminejad *et al.*, "A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations," *International Journal of Electrical Power & Energy Systems*, vol. 145, p. 108610, Feb. 2023, doi: 10.1016/J.IJEPES.2022.108610.

[34] V. Shaik and D. N. K, "Flexible and cost-effective cryptographic encryption algorithm for securing unencrypted database files at rest and in transit," *MethodsX*, vol. 9, p. 101924, Jan. 2022, doi: 10.1016/J.MEX.2022.101924.

[35] S. Li, "IoT Node Authentication," *Securing the Internet of Things*, pp. 69–95, Jan. 2017, doi: 10.1016/B978-0-12-804458-2.00004-4.

[36] C. Best and J. Nelson, "Access Control," *The Professional Protection Officer: Practical Security Strategies and Emerging Trends*, pp. 165–173, Jan. 2020, doi: 10.1016/B978-0-12-817748-8.00015-8.

[37] F. Hashmat, S. G. Abbas, S. Hina, G. A. Shah, T. Bakhshi, and W. Abbas, "An automated context-aware IoT vulnerability assessment rule-set generator," *Comput Commun*, vol. 186, pp. 133–152, Mar. 2022, doi: 10.1016/J.COMCOM.2022.01.022.

[38] A. Gumaei *et al.*, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids," *Appl Soft Comput*, vol. 96, p. 106658, Nov. 2020, doi: 10.1016/J.ASOC.2020.106658.

[39] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1–13, Jan. 2023, doi: 10.1016/J.IOTCPS.2022.12.003.

[40] A. Inanlouganji, G. Pedrielli, T. A. Reddy, and F. Tormos Aponte, "A computational approach for real-time stochastic recovery of electric power networks during a disaster," *Transp Res E Logist Transp Rev*, vol. 163, p. 102752, Jul. 2022, doi: 10.1016/J.TRE.2022.102752.

[41] A. Panda, A. K. Dauda, H. Chua, R. R. Tan, and K. B. Aviso, "Recent advances in the integration of renewable energy sources and storage facilities with hybrid power systems," *Clean Eng Technol*, vol. 12, p. 100598, Feb. 2023, doi: 10.1016/J.CLET.2023.100598.

[42] N. Mostafa, H. S. M. Ramadan, and O. Elfarouk, "Renewable energy management in smart grids by using big data analytics and machine learning," *Machine Learning with Applications*, vol. 9, p. 100363, Sep. 2022, doi: 10.1016/J.MLWA.2022.100363.

[43] A. Zahoor *et al.*, "An access control scheme in IoT-enabled Smart-Grid systems using blockchain and PUF," *Internet of Things*, p. 100708, Feb. 2023, doi: 10.1016/J.IOT.2023.100708.