Smart Power Monitoring System

Prashanta Acharya
Bachelor of Science with Honours Computer Science and Artificial Intelligence
(Faculty of Computing, Engineering, and the Built Environment), Sunway College Kathmandu
Birmingham City University (BCU)
Prashanta.Acharya@mail.bcu.ac.uk

***Abstract* — The Smart Power Monitoring System also counts among the technological advancements in energy management technologies by utilizing the Internet of Things (IoT) to improve energy consumption and promote sustainable consumption habits. In this paper we will explore what the hardware needs are, the security issues, and the ongoing technological developments. Through the utilization of the Internet of Things connectivity, the designed system assembles a set of many sensors and actuators that enables real-time visualization of patterns of energy consumption thereby empowering users to make informed decisions on energy use. An Arduino Uno microcontroller board drives the device, and it provides data on voltage, current, and temperature through its user sensors. Via processing and display of this data on networked LCD screens the users can see how much energy they use and modify that if it is necessary. Like all developments, there are security challenges that arise from the growth of IoT such as the need for strong encryption, access controls, and intrusion detection systems. There is a secured data transmission across the network by using secure communication protocols like HTTPS and MQTT-TLS and the device authentication guarantees that only the genuine devices can connect to the system. Regularly updating the firmware and utilizing the integrity checks provides the opportunity to minimize the probability of tampering and unintended access. The last layers of cyberattacks defensive positions are given by physical barriers as well as intrusion detection systems. Organizations can gain the competitive edge from the smart power monitoring systems that use IoT technology, thus promoting sustainability, reliability, and integrity in the energy system, and at the same time avoid the security dangers associated with IoT adoption, if the security issues are addressed and strategic measures are taken.**

I. Introduction:

IOT is a method which connects many devices with each other with the help of internet to make control over those devices. It’s a modern technology which uses internet for networking one devices with many other devices(Khanna & Kaur, 2020).IOT helps us to connect hardware devices using different networking technologies.

The introduction of a smart power monitoring system clarifies the revolutionary potential of Internet of Things (IoT) technology by enabling device connectivity for effective online control. Energy-efficient solutions are critical since energy usage is rising and resources are becoming scarce. To meet this problem, smart power monitoring systems prove to be essential tools because they provide real-time insights into patterns of energy consumption. These solutions enable users to make informed decisions with the goal of minimizing ecological footprints by utilizing IoT capabilities. By means of ongoing observation and evaluation, opportunities for enhancement can be recognized, culminating in customized approaches for maximizing energy use. This proactive strategy promotes a sustainable culture in addition to improving energy efficiency.(Kumar et al., 2019).

IoT-based smart power monitoring solutions help close the gap between energy use and conservation. These systems give customers a thorough perspective of power usage, empowering them to manage energy resources more effectively by being proactive. They provide insights into patterns of energy usage through the integration of sensors and data analytics, enabling well-informed decision-making and encouraging sustainable habits.

II. Literature Review

A) IOT

IOT is a embedded system which connects multiple devices with each other and give the access over the devices with the help of internet. Over the past few years, IOT has been an important factor on the rise of communication technology all around the world. Basically, IOT has three level architecture. The first layer of the IOT is perception layer which is the connection of sensors and it gathers all the information collected by the sensor about the system. The second layer is the network layer which is responsible for connection the system with our network devices and servers. The last one is application layer which delivers the information from the servers to the user (Radouan Ait Mouha, 2021).

B) Innovation

Innovation has grown these days due to the growing technology of IOT where IOT has made innovations of new technologies very easier task. In recent years innovation has brought technological advancement in every sectors which has brought increasing change in the economic growth(Wang et al., 2021). As the technology is increasing day by day, the increase of digitalization in every sector has brought huge impact in every persons daily. It has brought significant improvements in the era of IOT and Innovation. Innovation is the process of introducing novel ideas, methods, or products that create value or address societal needs. This study delves into the digitalization of innovation across sectors, emphasizing its role in driving economic growth and advancement. Through the integration of emerging technologies and creative approaches, innovation serves as a catalyst for positive change, fostering competitiveness and addressing complex challenges in today's dynamic landscape(Agostini et al., 2019).

C) Security

Security and Privacy are the most complicated challenges in the modern IOT devices. Some issues that IOT devices are facing these days are user ignorance, using of unauthorized devices, inappropriate and ineffective security procedures (Tawalbeh et al., 2020) etc. While it's clear that Internet of Things (IoT) products and services offer numerous advantages, it's crucial to acknowledge the potential security threats that come with being connected to the Internet. We all know that the Internet comes with a certain level of risk, so extending its access to everyday devices only amplifies the range of potential dangers(Wheelus & Zhu, 2020) . Many securities issues related to Internet has been widely introduced in the past few years as internet is commercially used these days.

D) Current and Future Trends :

IOT has brought huge impact in every sectors these days. IOT has contributed in different field by its different impact such as AI and Machine Learning integration, IOT in healthcare, Industrial IOT(IIOT), and in every sectors of technology which is growing these days (Banerjee et al., 2020) . AI and Machine Learning technologies are being applied to different IOT devices which gives accuracy in the results by processing the data provided by IOT devices. An imminent trend in IoT future is the rise of edge computing. In contrast to the centralised data centre-based systems, edge computing involves data processing at the closest point to the edge of the network or even further down to the source. This technique proves to be highly effective for Internet of Things applications which need real time processing and low latency communication, since it reduces latency, bandwidth consumption, and dependency on cloud services. Edge computing principles, architectural design, and implementation issues, as well as their role in the Internet of Things. It outlines the fact that edge computing could be a stepping stone to overcome the problems of scalability, privacy, and security of IoT implementations and open many new use cases and applications (Mothukuri et al., 2021) .

III. Technical Development

A. Working Mechanism of the proposed system

A widespread and adaptable microcontroller board, Arduino Uno, is the mainstay of this system. Functionality can be programmed on the Arduino thus allowing integration with a variety of sensors and actuators. In this case, voltage data from the power supply is read by Arduino using analogRead() function. This information is then processed through custom code that converts it into metric measurements such as wattage and power factor. Finally, the interconnected LCD displays reveal the values, providing users with real-time insight into how much electricity their devices consume. The development approach to this system emphasizes on keeping it simple, affordable, and user-friendly for ease in its use for educational purposes, laying foundation for hobbyist projects and probably even rudimentary real world applications like home energy monitoring.

The proposed system have used current sensor to record current, potentiometer to measure voltage flowing and temperature sensor to measure temperature of the device. If the current flowing in the system is normal the system shows the amount of current, amount of voltage , Power of the system and power factor of the system. The initial current amount can be changed with the help of the button. However if the amount of current flowing is high than the system gives warning about the power and its power factor.

B. Truth Table:

The truth table provided illustrates how a device reacts to inputs from its power supply, current sensor, temperature sensor, and output, which can be in one of two states: "Off" or "On."

Based on the input data, the truth table indicates the device's ultimate state. For example, the output is "Off" if the temperature and current sensor are both "0" (i.e., off), and the power supply is "1" (i.e., on). Conversely, if every single one of the following indications is "1" (that is, on), the device state is "On": Temperature, Current Sensor, and Power Source.

Power Source	Current	Temperature	Output
0	0	0	OFF
0	0	1	OFF
0	1	0	OFF
0	1	1	OFF
1	0	0	OFF
1	0	1	ON
1	1	0	ON
1	1	1	ON

Table 1 : Truth Table

C. Booleans Algebra:

Here, P is the Power source of the system,
C is the input from current sensor and
T is the input from temperature sensor.

(P*C*T) + (P *(! C)* T) + (P * C * (! T))

D. Logic gates diagram:

Logic gates are essential components of digital circuits because they can process one or more binary inputs logically and output a single binary result. In circuit diagrams, these gates are commonly represented by symbols, with lines denoting the input and output connections.

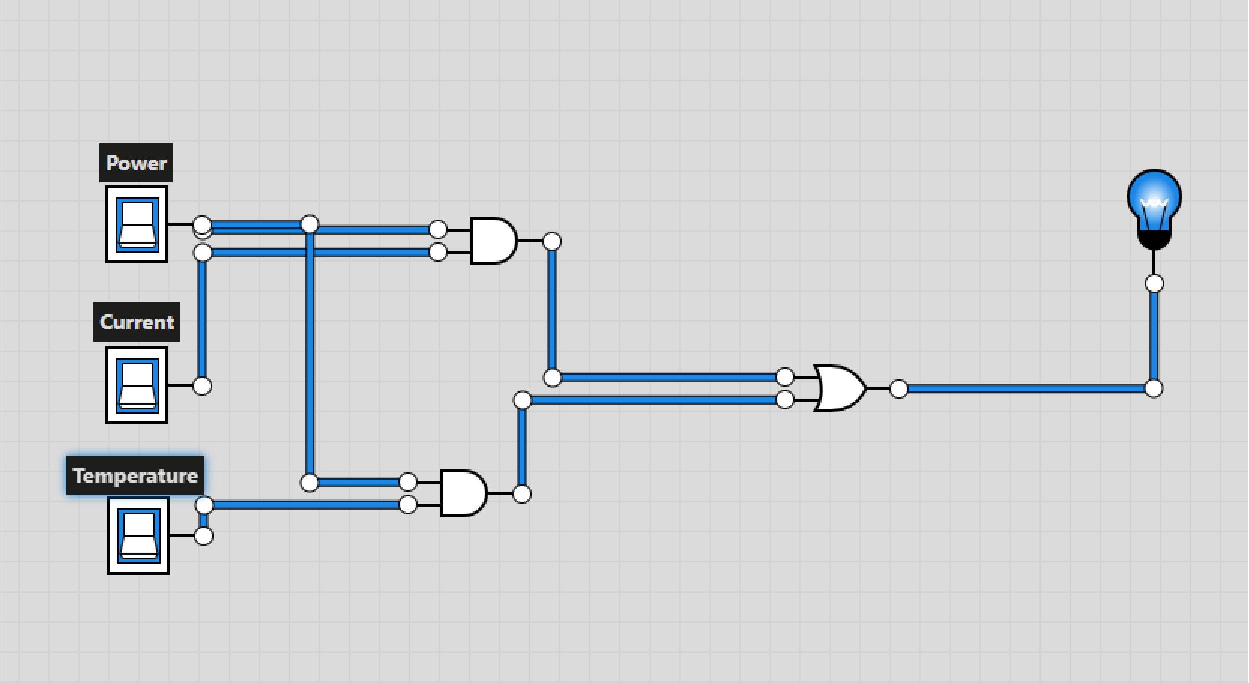

Figure 1: Logic Diagram from Logicly

IV. *Hardware Requirements and Design*

- *Hardware Components*

  a. Arduino UNO:

  Arduino is an open-source electronics platform that is built on user-friendly hardware and software. Designers, artists, amateurs, and professionals all use it to prototype and create interactive creations. In the proposed system, we have used Arduino as our microcontroller which provides electronic connection of our system. Arduino is an open-source electronic programmable board which gives us a platform to build our projects. Arduino board has wide range of applications such as robotics, home automation, Internet of Things (IOT) etc. Compared to other microcontroller boards Arduino is much cheaper and more versatile(Kim et al., 2020).

  b. Current Sensor

  Current Sensor can be defined as an electronic devices which is used to monitor the flow of current in any device which enables the safety of the devices. Moreover these sensor are necessary for power monitoring and also helps in optimizing usage of energy and also identifies inefficiencies. A main wire carrying the current to be measured is placed between a coil of wire and a ferrite ring, in the sensors. The secondary wire generates an alternating current that's proportional. Moreover CT sensors are available, in ratings each indicating the voltage or current that responds to a specific primary current (Santos & Ferreira, 2019).

  c. Temperature Sensor

  A temperature sensor is a device designed to measure the temperature of its surroundings and convert this physical parameter into an electrical signal. These sensors come in various types, each employing different principles of operation to suit specific applications. With applications ranging from environmental monitoring to industrial process control, the choice of temperature sensor depends on factors like accuracy, operating range, response time, and cost, each fulfilling specific needs across various domains (Arman Kuzubasoglu & Kursun Bahadir, 2020).

d. LCDs Display

Liquid Crystal Display (LCD) technology is widely used in electronic devices to present visual information. LCDs consist of a layer of liquid crystal material sandwiched between two transparent electrodes and two polarizing filters. The liquid crystal molecules can be aligned in different ways by applying electric current, which affects the polarization of light passing through them (Araya et al., 2021).

`

- *Hardware Requirements and Design*

We have used different switch as sensor and other components as the component that are proposed in our system were not available in Tinkercad. For measuring current and voltage potentiometer was used and to increase the flow of current switch was used.

The Tinkercad design looks to be an Arduino Uno controlled circuit for distance measurement between two LCD screens. Both LCDs are fed by the power and signals from the Arduino and each displays a different set of data. A potentiometer pin (A0) that is connected between 5 volts and GND will sense changes in voltage as it moves. The LCD of the third one can illustrate the distance that is supported by this voltage. The only inscription that can be read on the second LCD is "Power Factor = 0.8".

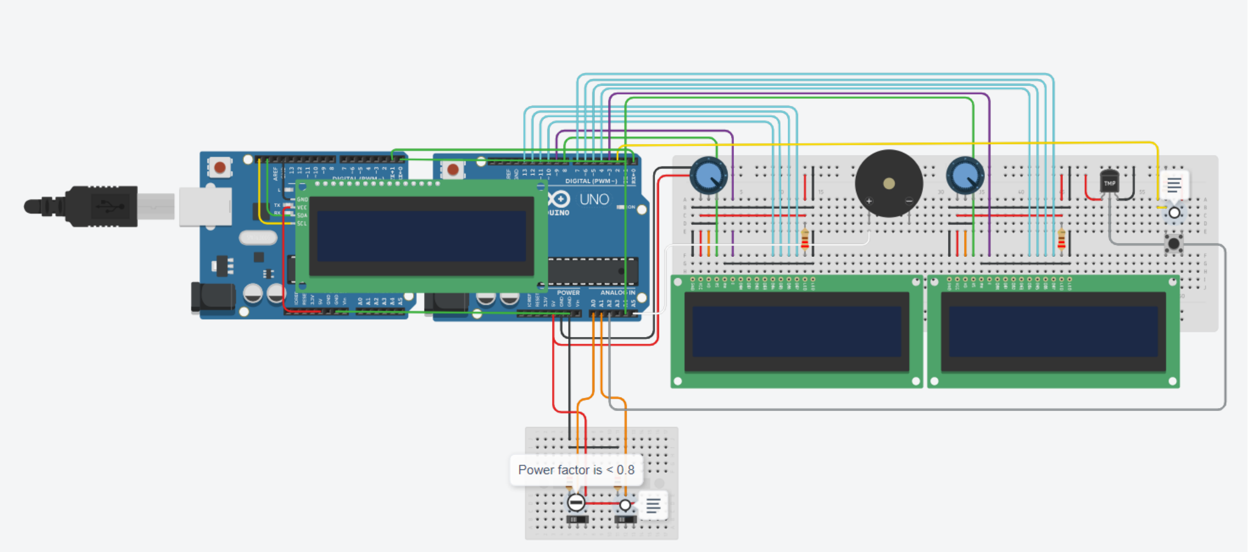

Figure 2: Tinkercad Design

Component	Quantity
Arduino UNO	3
Potentiometer	2
Temperature Sensor	1

Slide Switch	2
Button	1
Buzzer	1

Table 2 : Components used

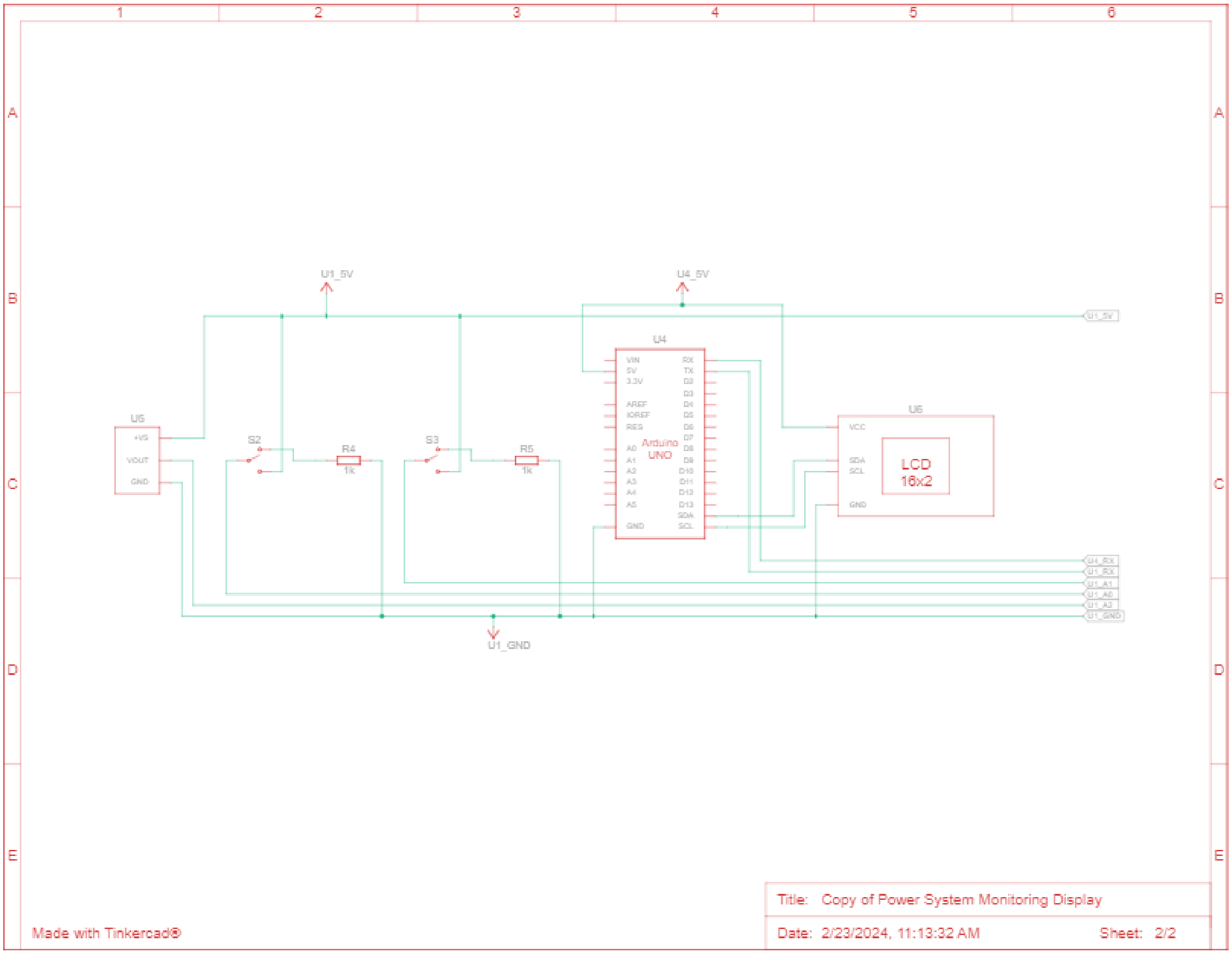

Figure 3: Schematic Diagram

V. Security Considerations:

Smart power monitoring under secure mode needs a comprehensive strategy to protect sensitive data and vital infrastructures when they are being implemented. The issue of encryption is one that is worth giving consideration to. Strong encryption algorithms are deployed by the platform to secure all data that is transmitted within the network, thus making it difficult for unauthorized access or alteration. Access controls such as multi-factor authentication to enhance the security are important in of granting the only authorized workers the access. For securing the data, while transmitting it over networks, we need to have secure communication methods such as HTTPS, MQTT-TLS. Part of these security designs should cover the authentication of devices to ensure that only trustworthy devices are able to connect to the system. To reduce risks of devastating alterations and unauthorized access, regular firmware updates and integrity checks are needed. IDS and IPS systems should be put in place as well to allow for the monitoring of network traffic to uncover abnormal activity. The aim of this is to provide impediments to illegal access or unauthorized tampering with system components and physical security must be ensured. To fulfill data availability and integrity, as backup saving and disaster recovery are critical the system's security position is also bolstered by taking privacy standards as well as configuring the system securely into consideration. In order for the implementation of proactive security measures for the detection and mitigation of security threats, penetration testing, security audits, as well as incident response plans are of paramount importance. Cyber security of intelligent power monitoring systems can be developed by using these factors, thus will ensure cyber-attack resistance, and dependability and authenticity of the intelligent power monitoring system infrastructure (Qiu et al., 2012) .

VI. Result and Conclusion:

The Smart Power Monitoring System, which leverages the Internet of Things that helps control energy efficiency and implement realistic energy-consuming, is a possible option to do so. By integrating the visualization of data on the power consumption with creative actuators, the system enables users to observe and regulate their energy consumption on-the fly, helping in to save more energy which can be achieved by precautions taken ahead of time and to make correct decision in time. Though the technologies have been put in place, they create various security issues which should be addressed properly, and this problem is solved by using these technologies not by irresponsible users.

Organizations can enhance the ability of their monitoring systems to resist potential cyber threats by adhering to privacy standards and building the system securely followed by conducting regular security audits and penetration tests. To really take the maximum benefit of IoT-enabled smart power monitoring systems and ensure substantiality, reliability and integrity, a well-defined security architecture is the focal point.

This study paper's conclusion on smart power monitoring systems highlights how IoT-enabled systems can improve energy efficiency and encourage well-informed decision-making. The conclusion, while acknowledges technical developments, emphasizes the need for proactive measures like privacy standards, security audits, and incident response plans to fully realize the benefits of such systems. In the end, it is believed that a clear security architecture is necessary to guarantee the integrity, longevity, and dependability of intelligent power monitoring systems.

References:

Khanna, A. and Kaur, S. (2020a) ‘Internet of things (IOT), applications and challenges: A comprehensive review’, *Wireless Personal Communications*, 114(2), pp. 1687–1762. doi:10.1007/s11277-020-07446-4.

Kumar, S., Tiwari, P. and Zymbler, M. (2019) ‘Internet of things is a revolutionary approach for future technology enhancement: A Review’, *Journal of Big Data*, 6(1). doi:10.1186/s40537-019-0268-2.

Radouan Ait Mouha, R.A. (2021) ‘Internet of things (IOT)’, *Journal of Data Analysis and Information Processing*, 09(02), pp. 77–101. doi:10.4236/jdaip.2021.92006.

Wang, K.-H. *et al.* (2021) ‘Is Technological Innovation Making World “greener”? an evidence from changing growth story of China’, *Technological Forecasting and Social Change*, 165, p. 120516. doi:10.1016/j.techfore.2020.120516.

Agostini, L., Galati, F. and Gastaldi, L. (2019) ‘The digitalization of the innovation process’, *European Journal of Innovation Management*, 23(1), pp. 1–12. doi:10.1108/ejim-11-2019-0330.

Tawalbeh, L. *et al.* (2020) ‘IOT privacy and security: Challenges and solutions’, *Applied Sciences*, 10(12), p. 4102. doi:10.3390/app10124102.

Wheelus, C. and Zhu, X. (2020) ‘IOT network security: Threats, risks, and a data-driven defense framework’, *IoT*, 1(2), pp. 259–285. doi:10.3390/iot1020016.

Banerjee, A. *et al.* (2020) ‘Emerging trends in IOT and Big Data Analytics for Biomedical and Health Care Technologies’, *Handbook of Data Science Approaches for Biomedical Engineering*, pp. 121–152. doi:10.1016/b978-0-12-818318-2.00005-2.

Kim, S.-M., Choi, Y. and Suh, J. (2020) ‘Applications of the open-source hardware Arduino platform in the mining industry: A Review’, Applied Sciences, 10(14), p. 5018. doi:10.3390/app10145018.

Santos and Ferreira (2019) ‘IOT Power Monitoring System for Smart Environments’, Sustainability, 11(19), p. 5355. doi:10.3390/su11195355.

Arman Kuzubasoglu, B. and Kursun Bahadir, S. (2020) ‘Flexible temperature sensors: A Review’, Sensors and Actuators A: Physical, 315, p. 112282. doi:10.1016/j.sna.2020.112282.

Araya, M., Harada, M. and Saito, K. (2021) ‘Characterization and classification of optimal LCD codes’, Designs, Codes and Cryptography, 89(4), pp. 617–640. doi:10.1007/s10623-020-00834-8.

Qiu, M. et al. (2012) ‘Balance of security strength and energy for a PMU monitoring system in smart grid’, IEEE Communications Magazine, 50(5), pp. 142–149. doi:10.1109/mcom.2012.6194395.

Mothukuri, V. et al. (2021) ‘A survey on security and privacy of Federated Learning’, Future Generation Computer Systems, 115, pp. 619–640. doi:10.1016/j.future.2020.10.007.