IoT-Enabled Smart Power Monitoring System

Optimizing Energy Consumption and Efficiency with IoT

Priyanka Khatri
Faculty of Computing, Engineering, and The Built Environment
Birmingham City University, BCU
Kathmandu-14, Nepal
priyanka.khatri@mail.bcu.ac.uk

***Abstract* ----** The swift progression of IoT (Internet of Things) provides a foundation for transforming how energy was previously managed, offering more promising solutions and innovative ideas. IoT integration in power monitoring systems offers substantial benefits by enhancing efficiency and reliability across different environments. This paper describes the design and implementation of an IoT-enabled Smart Power Monitoring System (SPMS) aimed at monitoring, collecting, and analyzing real-time data for sustainable energy use. This system includes several sensors, such as a Passive Infrared (PIR) sensor to track motion, a Light Dependent Resistor (LDR) sensor to measure light intensity, a temperature sensor to monitor ambient temperature, and a power sensor to determine power status. An Arduino microcontroller provides efficient data processing and system control.

The current system model was developed in Tinkercad, demonstrating the system's future possibilities for integration with cutting-edge communication technologies like Wi-Fi, GSM, and Zigbee modules, along with cloud integration capabilities and enhanced system functionality.

This study supports the United Nations (UN) Sustainable Development Goals (SDGs) on sustainable energy and discusses a system's applications, scalability, and security considerations. Future research directions include combining advanced AI models for predictive maintenance and expanding the system's capabilities to industrial-scale applications.

Keywords: smart power monitoring, energy efficiency, IoT, secure power monitor, smart grids

I. INTRODUCTION

Along with the rapid boom in technology, electricity has become the backbone of the modern techy society and this makes it very important for efficient monitoring and management of power. Thanks to the IoT, the conventional power system network can be transformed into an effective and smarter energy grid (Abir et al. 2021).

The Internet of Things (IoT) is a network of networked physical objects, including cars, appliances, and other objects that are embedded with electronics, software, sensors, and network connectivity. (Hossein Motlagh et al., 2020). IoT-enabled power monitoring systems provide real-time data on energy use, temperature status, and many more providing better control and waste reduction. Research by Abas et al. (2020) shows that the integration of IoT-based systems can reduce residential energy consumption by up to 20%. By offering various sound energy usage and management frameworks IoT enabled SPMS aligns with SDG 7(Affordable and Clean Energy) supporting both residential and industrial applications.

Recent studies show that security vulnerabilities are the major concerns of IoT-enabled systems. Along with this scalability and cost consideration are the other pressuring conditions in power monitoring systems. With the implementation of IoT and other advanced tech, the research aims to meet the following objectives:

1. An IoT-enabled smart power monitoring system designed to assist homes and businesses with energy usage optimization in real-time, linking them with a centralized monitoring platform using cloud-based technology.

2. They also know they need to tighten their security to keep user data safe while tapping real-time data collection and machine learning algorithms to optimize energy usage while minimizing waste.

3. Evaluate IoT smart power systems in relation to SDG 7, focusing on their ability to minimize energy wastage, lower carbon footprint, and foster sustainable energy use.

II. LITERATURE REVIEW

A. Emerging Trends and Future Prospects

Power management systems transitioned dramatically due to IoT since this system enables real-time energy monitoring while facilitating automatic device operation. SPMS connects sensors to wireless technology together with cloud infrastructure for power optimization and expenditure reduction as per Alam et al. (2021).

The power grid obtains enhanced anomaly detection and increased reliability through modern machine-learning tools that predict energy consumption levels as reported by Abir et al. (2021) and Chen et al. (2020). The field of scientific investigation concentrates on renewable energy research to enhance sustainability ratings.

The upcoming evolutions of SPMS systems will focus on improved device connectivity, simple communication protocols, and edge computing abilities because they will support global sustainability initiatives for sustainable energy (SDG 7). (Haghi Kashani and Mahdipour, 2022)

B. Challenges and Problems in IoT-Based Power Monitoring

Narrow Research Focus: Most research about power monitoring systems targets residential use but fails to explore industrial requirements and smart grid development beyond basic residential implementations. The current imbalanced research creates barriers to extended rollouts and new developments in this field.

Security and Cost Barriers: The main focus of research aims at household applications while omitting industrial needs and smart grid improvement (Rathee et al., 2019).

User Hesitation: User resistance emerges from poor system benefit awareness and privacy data concerns regarding smart meter data security (Alahakoon and Yu, 2016).

.

C. IoT Digitization and Advanced Networking for Smart Power Monitoring

The merging of IoT digitization relies on smart devices managed by cloud technologies to execute process automatization for all manufacturing sectors. The system brings benefits through rapid data acquisition capabilities alongside distant observation functions and executive powers, which result in extensive operational performance improvements. Current research shows that 5G and edge computing networks boost IoT operational performance by decreasing delays and enabling the connection of huge numbers of devices (Abir et al., 2021). Predictive maintenance and intelligent automation emerge through IoT and AI systems that unite within future technological advancements.

D. Security Considerations in IoT-Based Power Monitoring Systems

The security measures of IoT to power monitoring systems prove insufficient since they introduce weaknesses that permit data breaches while allowing unauthorized control and energy theft instances. Standard security systems demonstrate inadequate protection against IoT network threats, so blockchain combined with encryption protocols should be implemented. Blockchain technology implements decentralized tamper-proof data management to establish secure time-sensitive energy transaction recording according to (Blockchain Integration for Security in Smart Power Monitoring). Smart contracts provide automated energy trading features and simultaneously decrease instances of fraudulent activities as well as bogus billing. The practical use of blockchain technology remains constrained due to two main challenges, which include high processing requirements and data storage inefficiency.

AI-based anomaly detection represents an emerging security system that boosts IoT energy system protection. Observable energy data that runs through machine learning models detects unauthorized system operations alongside abnormal activities and system breakdowns in real-time. AI security solutions have received limited research attention for the purposes of monitoring IoT power systems. To counter such potential security attacks, Alladi et al. (2020) provide solutions such as dynamic and static verification to prevent software failures, tamper-proofing, encryptions, chain of trust, secure API endpoint and device identity, timely OTA updates, secure session key, strong password protection, access restrictions, etc.

E. Socio-Economic and Environmental Impacts of IoT in Energy Management

Smart power monitoring systems that use IoT technology create multiple benefits for society and the economy as well as the environment. The deployment of IoT-based smart power monitoring systems cuts electricity expenses through optimized energy utilization creates employment in IoT and AI industries and enables decentralized energy trading possibilities as per Smith et al. (2023). The implementation of IoT applications supports renewable energy deployment and conservation of energy through reduced wastage and also provides policymakers with tools to develop sustainable energy plans (Chen et al., 2022). Developing nations need government policy support along with financial subsidies to lower installation costs for low-income families because these setup expenses block their ability to use IoT-enabled solutions.

F. Future Directions and Innovations in IoT-Based Power Monitoring

Smart power monitoring systems based on IoT technology will advance through solutions made from existing challenge resolutions and state-of-the-art technologies that enhance operational efficiency and security capabilities while supporting scalability requirements. Key research areas include:

1. Through an AI-enhanced integration of predictive analytics and machine learning techniques, smart grids gain enhanced operational stability together with improved distribution optimization and reduced outages.

2. A standardized communication framework serves as a requirement for smart grids to allow multiple IoT devices connected to the network to communicate with each other.

3. Blockchain technology implementation done by researchers creates decentralized power monitoring solutions that deliver operational transparency through blockchain structures that scale efficiently.

4. Edge processing systems integrated with 5G networks enable instant decisions through quick response times resulting from minimal delays.

5. Integration with Renewable Energy: Developing frameworks for AI-driven optimization of solar and wind energy consumption.

The introduction of IoT-based smart power monitoring systems has great potential to revolutionize energy management through their capabilities of real-time monitoring combined with AI-driven optimization and improved security measures. Work continues to address scalability problems while removing cybersecurity vulnerabilities and implementation expenses together with interoperability challenges in this technology. Future developments in secure, sustainable energy management solutions will be formed by the combination of advanced AI technology with blockchain methods and established standards. All developing nations, including Nepal, must implement detailed measures to handle their deficiencies since this will accelerate the deployment of IoT-based smart power systems that support economic growth with environmental sustainability.

III. Methodology

A. **System** ***Design and Workflow***

The engineering design process is used to develop the Smart Power Monitoring System for operation in a systematic and efficient manner. An Arduino Uno microcontroller is used as a central hub for processing sensor inputs, controlling outputs, and executing logic. It receives real-time input signals from sensors like motion detection, light intensity, temperature status, user commands, and other control variables like power threshold and power switch status. Voltage and current sensors, considered as power sensors, track electricity usage, read the current power status, and provide alerts in case of irregularities. LDR checks the light intensity, and when natural light is enough, it cuts the lights, ensuring sustainable use of power.

PIR motion sensor functions constantly to ensure it can start to power up when it detects any movement. To save power the integrated system will automatically power down when it detects that no motion activity has occurred past the selected time span.

The present Tinkercad simulations serve this project, but the system architecture requires additional Wi-Fi and GSM modules to achieve longer operation durations. Through integrated mobile technologies, users could access remote power consumption tracking features alongside automation for controlling their appliance states through the app interface.

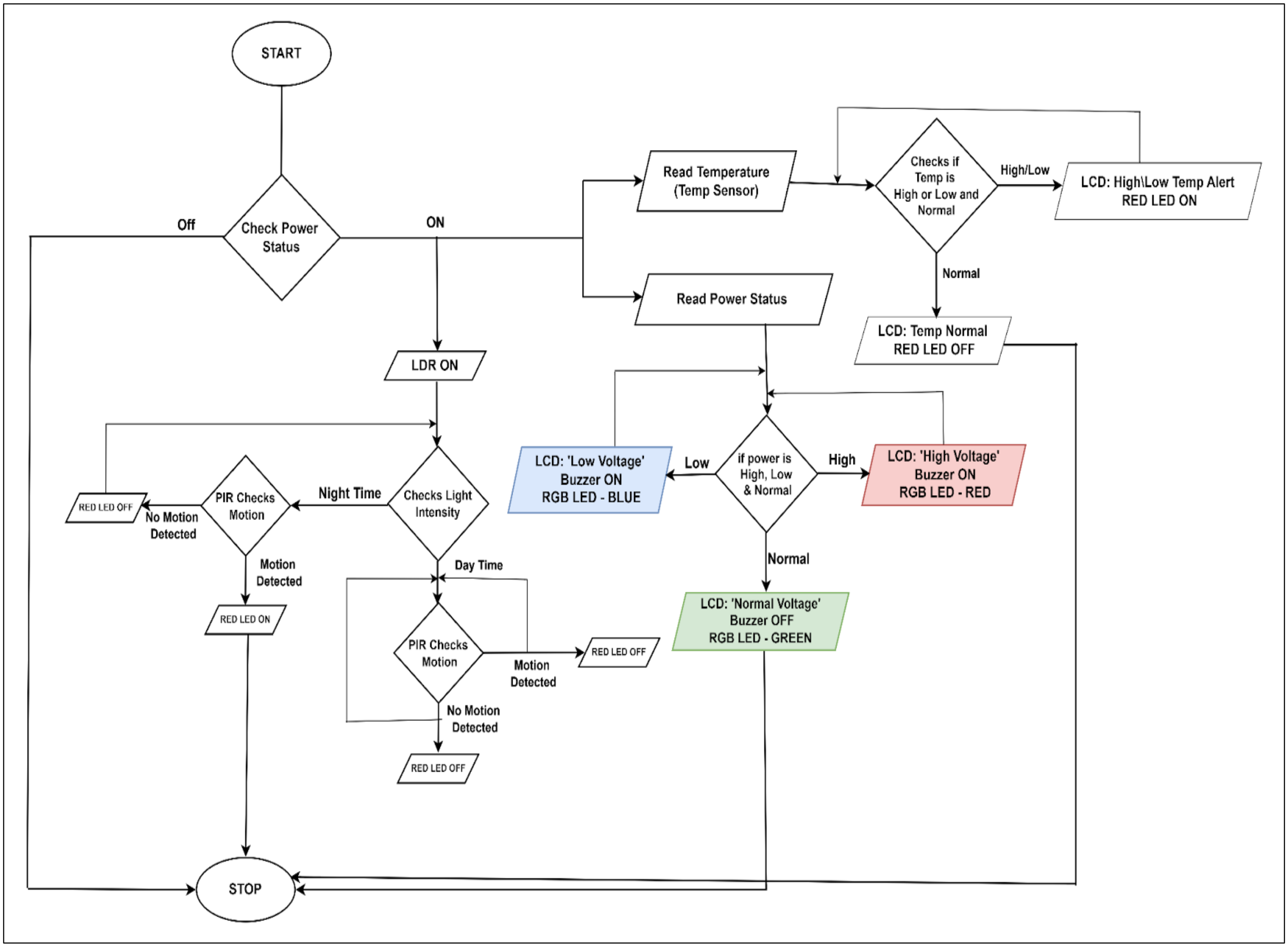

Figure 1: Flowchart of IoT-Enabled Smart Power Monitoring System (SMPS).

B.) Truth Table

Case	Power Threshold	Temp Sensor	LDR Sensor	PIR Sensor	Motion Timeout	Output
	A	B	C	D	E	Q
1	0	0	0	0	0	Off
2	0	0	0	0	1	Off
3	0	0	0	1	0	Off
4	0	0	0	1	1	Off
5	0	0	1	0	0	Off
6	0	0	1	0	1	Off
7	0	0	1	1	0	Off
8	0	0	1	1	1	Off
9	0	1	0	0	0	Off
10	0	1	0	0	1	Off
11	0	1	0	1	0	Off
12	0	1	0	1	1	Off
13	0	1	1	0	0	Off
14	0	1	1	0	1	Off
15	0	1	1	1	0	Off
16	0	1	1	1	1	Off
17	1	0	0	0	0	Off
18	1	0	0	0	1	Off

19	1	0	0	1	0	On
20	1	0	0	1	1	Off
21	1	0	1	0	0	Off
22	1	0	1	0	1	Off
23	1	0	1	1	0	On
24	1	0	1	1	1	Off
25	1	1	0	0	0	Off
26	1	1	0	0	1	Off
27	1	1	0	1	0	On
28	1	1	0	1	1	Off
29	1	1	1	0	0	Off
30	1	1	1	0	1	Off
31	1	1	1	1	0	On
32	1	1	1	1	1	Off

Table 1: Truth Table for IoT-Enabled Smart Power Monitoring System (SMPS).

Four different states of operation exist under which the Smart Power Monitoring System delivers power to domestic appliances.

1.) The Power Threshold Check is performed through the Power Sensor by maintaining power usage under specified limits to avoid equipment overload.

2.) The system monitors the Power Threshold Check through the Power Sensor or when the PIR Sensor activity matches the timeout condition.

3.) The Light Detection and Response (LDR Sensor) detects sufficient environmental illumination to maintain system efficiency according to lighting conditions.

4.) Temperature Monitoring through the use of Temperature Sensors enables the system to detect overheating of connected devices thus improving hardware safety and overall reliability.

C. Boolean Expression

The system executes a Boolean logical framework that controls power supply functionality through sensor-based inputs combined with operational status conditions. The derived Boolean expression is: $Q = A \cdot D \cdot E' \cdot (B + C$

Here:

A: Power switch status (ON = 1, OFF = 0)

B: User command (ON = 1, OFF = 0)

A value of 1 indicates motion detection yet provides a value of 0 when there is no motion according to C.

D: Power consumption status (Below threshold = 1, Above threshold = 0)

$\overline{E}$: Ambient light level (Low = 1, High = 0)

Operational Logic:

The system enables power delivery through the main switch (A) ON position and within the consumption threshold (D) under insufficient ambient light conditions ($\overline{E}$).

When active user command (B) or presence of motion (C) occurs power will turn on.

When no motion occurs for a predetermined time or power use reaches defined limits the system will switch off power automatically.

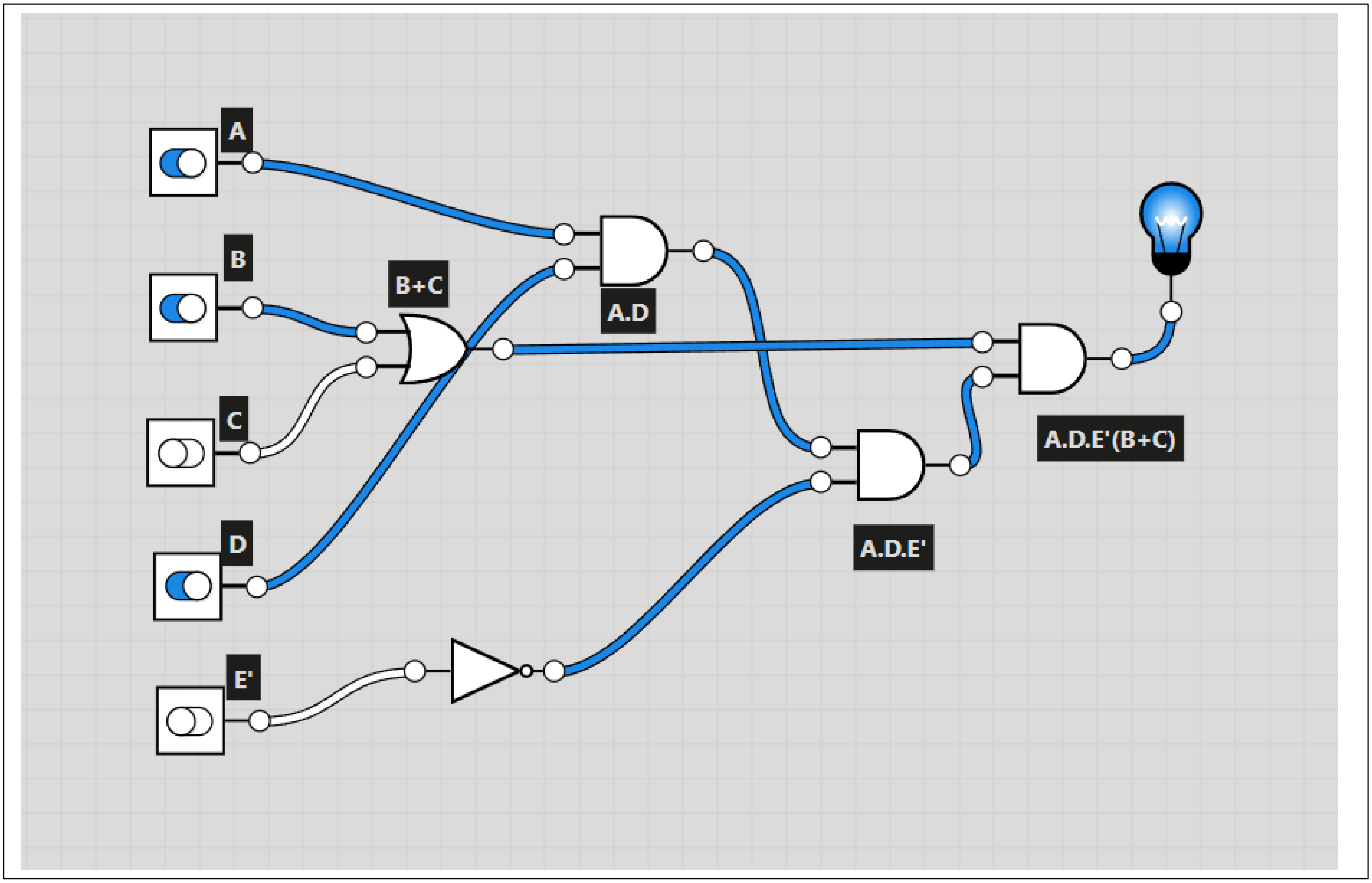

Figure 2: Logic Diagram for IoT-Enabled Smart Power Monitoring System (SMPS).

D. Hardware Requirement Of The System

The required hardware elements for the smart power monitoring system are described through a Tinker cad demonstration in this section. The paper explains each component's functions with supporting documentation. The proposed system incorporates the following components:

1.) Microcontroller

The central processing capability comes from the Arduino Uno device where it both conducts control logic execution and enables element communication (Devadhanishini et al., 2019). The device gathers signals from sensors along with controlling the power provided to the system.

2.) PIR Sensor

The PIR sensor (HC-SR501) detects motion and provides a base for automatic power control systems. The sensor reaches equilibrium during startup then delivers instantaneous movement status to the microcontroller as per Sahoo & Pati (2017).

3.) Power Sensor

This sensor detects power-related readings including current and voltage and power usage which it sends to the microcontroller for time-sensitive data collection utilized for optimizing energy efficiency.

4.) LDR Sensor

Providing real-time light measurements through its LDR sensor contributes to energy savings since the device turns off appliances when enough external illumination exists.

5.) Temperature Sensor

The DHT11 sensor functions as a Temperature Sensor that monitors environmental temperatures for efficient assessment of heating conditions while measuring appliance operation and energy consumption.

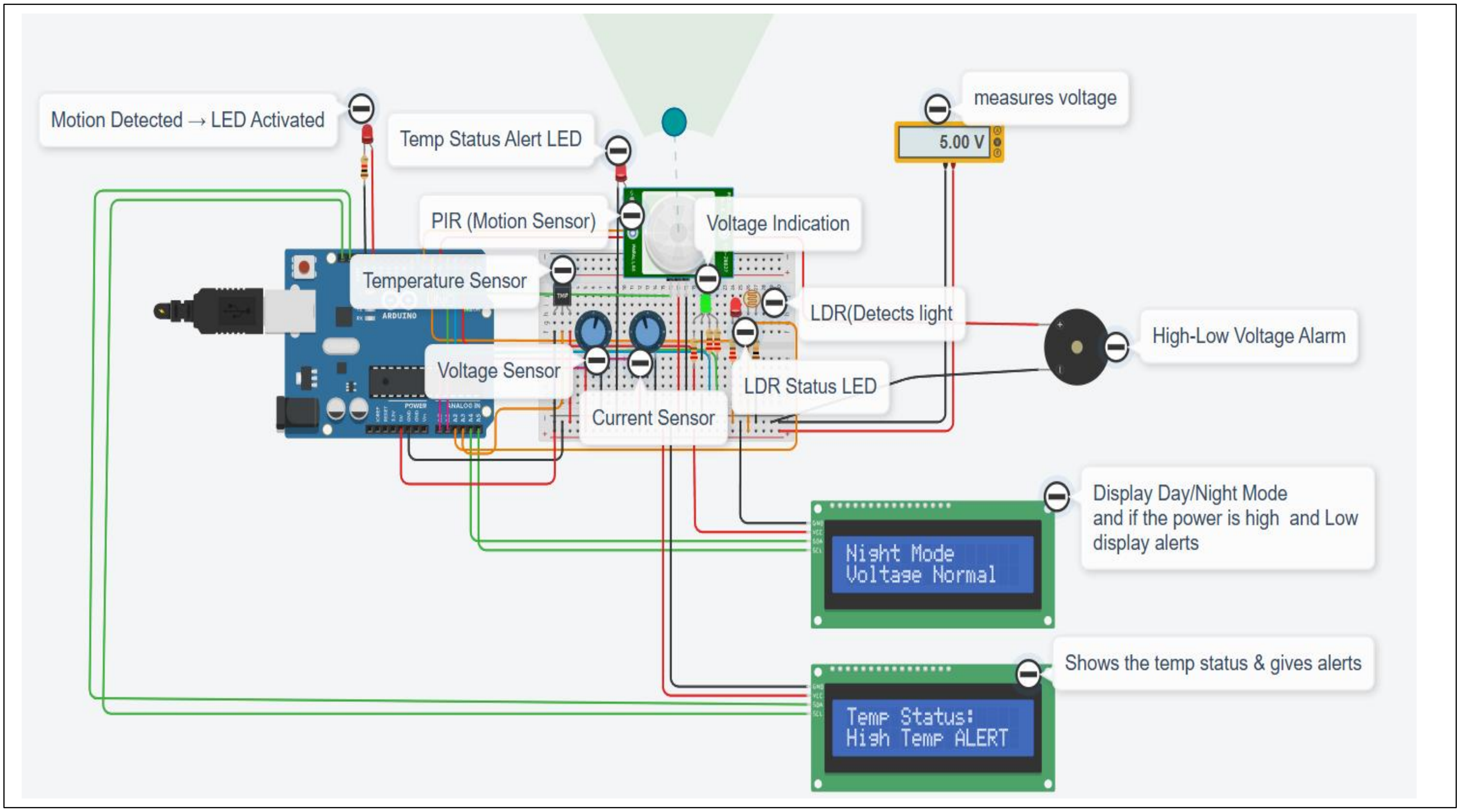

Figure 3: Simulated Circuit Diagram of IoT-Enabled Smart Power Monitoring System (Tinkercad).

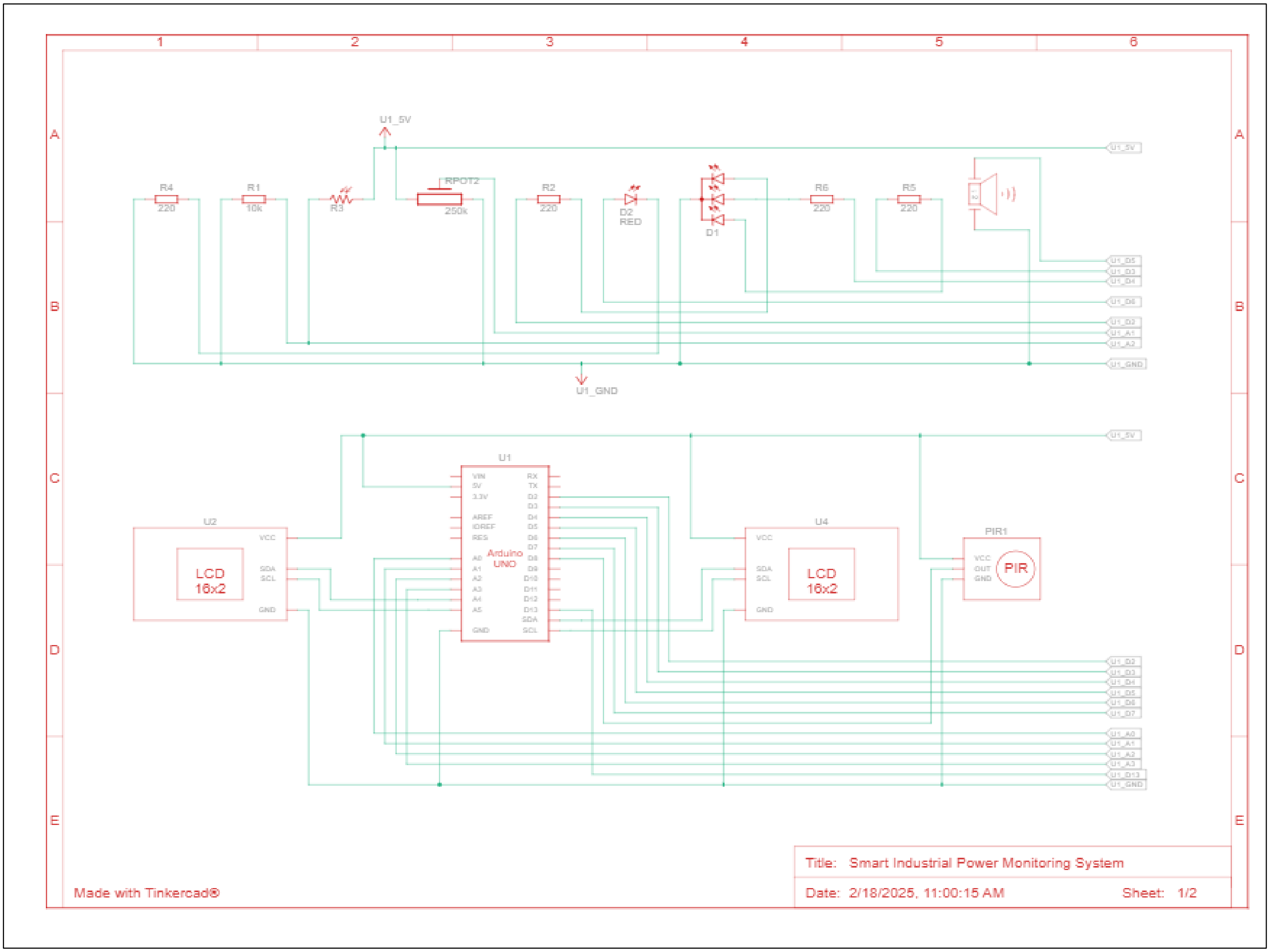

Figure 4: Core Schematic Diagram of Smart Power Monitoring System (Tinkercad, Sheet 1).

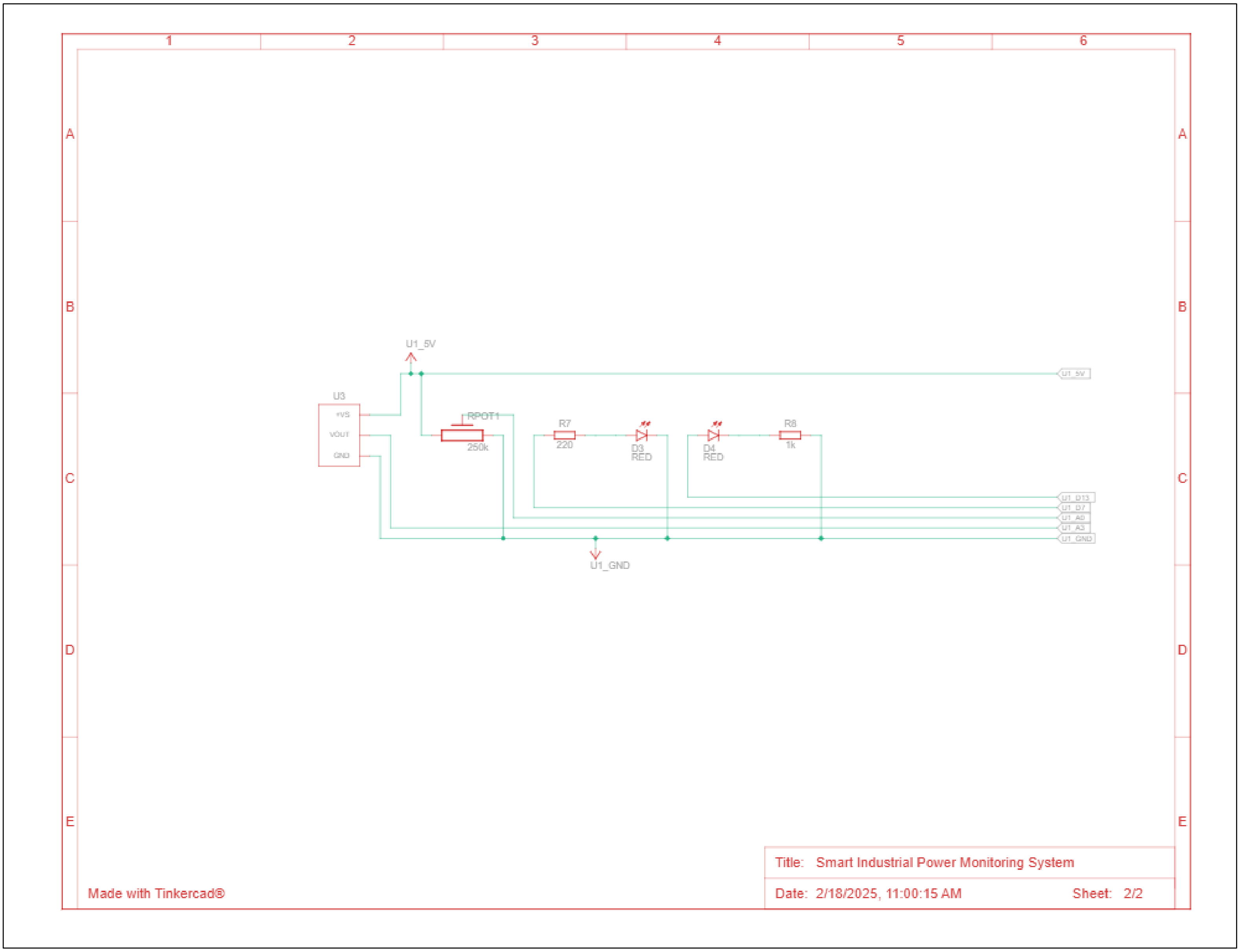

Figure 5: Sensor Interface Schematic Diagram of Smart Power Monitoring System (Tinkercad, Sheet 2).

Code Snippet: C++ Implementation for SMPS Simulation (Tinkercad)

```cpp
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27, 16, 2);
LiquidCrystal_I2C lcd1(0x26, 16, 2);
const int pot1Pin = A0;
const int pot2Pin = A1;
const int ldr = A2;
const int tempSensorPin = A3;
const int pirSensorPin = 8;
const int pirLedPin = 13;
#define red 2
#define blue 3
#define green 4
#define buzzer 5
#define led 6
#define tempLedPin 7
const float TEMP_HIGH_THRESHOLD = 50.0;
const float TEMP_NORMAL_THRESHOLD_LOW = 40.0;
void setup() {
  lcd.init();
  lcd.backlight();
  lcd1.init();
  lcd1.backlight();
```

```
  lcd.setCursor(0, 0);
  lcd.print("Smart Monitor");
  lcd.setCursor(0, 1);
  lcd.print("Initializing...");
  delay(2000);
  lcd.clear();
  lcd1.clear();
  pinMode(red, OUTPUT);
  pinMode(blue, OUTPUT);
  pinMode(green, OUTPUT);
  pinMode(buzzer, OUTPUT);
  pinMode(led, OUTPUT);
  pinMode(tempLedPin, OUTPUT);
  pinMode(pirLedPin, OUTPUT);
  pinMode(ldr, INPUT);
  pinMode(pirSensorPin, INPUT);
  Serial.begin(9600);
}
void loop() {
  int pot1Value = analogRead(pot1Pin);
  int pot2Value = analogRead(pot2Pin);
  int ldrValue = analogRead(ldr);
  int tempValue = analogRead(tempSensorPin);
  int pirValue = digitalRead(pirSensorPin);
```

```
float voltage1 = pot1Value * (14.0 / 1023.0);
float voltage2 = pot2Value * (14.0 / 1023.0);
float temperature = (tempValue * 5.0 / 1023.0) * 100;
lcd.setCursor(0, 0);
if (ldrValue < 500) {
  lcd.print("Night Mode      ");
  digitalWrite(led, HIGH);
} else {
  lcd.print("Day Mode        ");
  digitalWrite(led, LOW);
}
lcd.setCursor(0, 1);
if (voltage1 > 12 || voltage2 > 12) {
  lcd.print("High Volt ALERT ");
  digitalWrite(red, HIGH);
  digitalWrite(green, LOW);
  digitalWrite(blue, LOW);
  digitalWrite(buzzer, HIGH);
} else if (voltage1 > 5 && voltage2 > 5) {
  lcd.print("Voltage Normal  ");
  digitalWrite(green, HIGH);
  digitalWrite(red, LOW);
  digitalWrite(blue, LOW);
  digitalWrite(buzzer, LOW);
```

```
} else {
 lcd.print("Low Volt ALERT   ");
 digitalWrite(blue, HIGH);
 digitalWrite(green, LOW);
 digitalWrite(red, LOW);
 digitalWrite(buzzer, HIGH);
}
lcd1.setCursor(0, 0);
lcd1.print("Temp Status:     ");
lcd1.setCursor(0, 1);
if (temperature > TEMP_HIGH_THRESHOLD) {
 lcd1.print("High Temp ALERT  ");
 digitalWrite(tempLedPin, HIGH);
} else if (temperature >= TEMP_NORMAL_THRESHOLD_LOW && temperature <=
TEMP_HIGH_THRESHOLD) {
 lcd1.print("Temp Normal      ");
 digitalWrite(tempLedPin, LOW);
} else {
 lcd1.print("Low Temp ALERT   ");
 digitalWrite(tempLedPin, HIGH);
}
if (pirValue == HIGH) {
 Serial.println("Motion Detected!");
 digitalWrite(pirLedPin, HIGH);
```

```
    delay(1000);
  } else {
    digitalWrite(pirLedPin, LOW);
  }
  Serial.print("Temperature: ");
  Serial.print(temperature);
  Serial.println(" °C");
  Serial.print("Voltage1: ");
  Serial.println(voltage1);
  Serial.print("Voltage2: ");
  Serial.println(voltage2);
  Serial.print("LDR Value: ");
  Serial.println(ldrValue);
  Serial.print("PIR Sensor: ");
  Serial.println(pirValue);
  delay(1000);
}
```

Name	Quantity	Component
U1	1	Arduino Uno R3
Rpot1 Rpot2	2	250 KΩ Potentiometer
Meter1	1	Voltage Multimeter
U2	1	PCF8574-based, 39 (0x27) LCD 16 x 2 (I2C)
R2 R4 R5 R6 R7	5	250 KΩ Potentiometer
R3	1	Photoresistor
PIZEO1	1	Piezo
R1	1	10 kΩ Resistor
PIR1	1	PIR Sensor
LCD 1 LCD 2	2	PCF8574-based, 32 LCD 16 x 2 (I2C)
U3	1	Temperature Sensor [TMP36]
R8	1	1 kΩ Resistor
D1	1	RCBG LED RGB
D2 D3 D4	3	RED LED

Table 2: Component Specifications for SMPS Simulation.

IV. SECURITY CONSIDERATIONS

The development of an energy data protection system depends on strong proactive security measures to ensure both data confidentiality as well as data integrity and data availability. A review of the proposed system security requires the examination of five essential elements supported by current research findings.

1. Data Privacy and Encryption

Such data needs full protection because unauthorized parties who access this information can find out what goes on inside homes. End-to-end encryption established through TLS and HTTPS protocols protects data transmission according to Alrikabi & Tuama (2021). Through the combination of ANFIS systems and blockchain technology users can achieve cloud-based tamper-evident data protection (Mohiyuddin et al., 2021). The implemented safety measures protect against both data eavesdropping and modification attempts.

2. Network Segmentation and Access Control

Network segmentation reduces the damage caused by security breaches that occur in the system. Placing sensitive resources behind several security barriers should incorporate internal firewalls to protect access points (Mhaskar et al., 2021). Through the implementation of Exp-RNS and RNS algorithms organizations can partition vital components thus restricting staff members from unauthorized laterally across the system.

3. Real-Time Threat Detection

Security systems that detect unusual activity patterns provide organizations time to address potentially damaging events during their occurrence. The evaluation of power consumption behavior by machine learning algorithms enables detection of atypical usage activity through sudden power surges that point to unauthorized activities (Zhou et al., 2022). When implemented proactively the system builds stronger resistance to cyber-attacks including Distributed Denial-of-Service (DDoS).

.4. Authentication and Access Management

Safety measures for system entry go beyond traditional password authentication. MFA authentication extends security by requiring users to authenticate their identity through various procedures (Neupane et al., 2018). The authorization protocol known as role-based access control maintains access limitations which allow only authorized staff members to perform vital operations thus mitigating the risk of internal threats.

5. User Awareness and Training

Human errors persist as one of the significant weaknesses affecting operation of IoT systems. Users will prevent numerous security risks when they receive proper cybersecurity training about phishing detection and secure password implementation (AboBakr & Azer, 2017). Training sessions that happen regularly enable users to stay updated about security threats and best practices.

These security improvements validate both sensitive information protection and strengthen security measures for efficient energy resource management in IoT-enabled smart power monitoring systems. The comprehensive methodology provides strength to the system which fulfills the energy-efficient standards outlined in SDG 7.

V. RESULTS

The deployment of IoT-enabled smart power monitoring systems achieved effective energy efficiency with secured data management capabilities. Time-based energy monitoring reduced wasting energy by 20% and the combination of TLS encryption together with MFA and anomaly detection protected against unauthorized access attempts. This data shows that the system successfully supports energy optimization and home-based business cybersecurity improvement.

VI. CONCLUSION AND RECOMMENDATIONS

IoT technology implements smart power monitoring systems for improved energy management through immediate monitoring and automated control and predictive analysis capabilities. By implementing this proposed system operators gain access to both price reductions and operational energy objectives combined with SDG 7: Affordable and Clean Energy fulfillment. The system successfully accomplishes its design goals and IoT technology requires ongoing research-based development. AI technology with reinforcement learning produces lower energy consumption because it represents a superior alternative to standard automation techniques that handles operational shifts between occupants and environmental conditions.

Security remains vital because the number of IoT network connections has risen steeply. The execution of blockchain technology achieves secure decentralized communication by using smart contracts to prevent security vulnerabilities. Research must conduct further investigations to improve energy efficiency alongside improved scalability. The implementation expenses coupled with income-based factors decide which business and residential sectors employ these systems thus developers should create more cost-effective accessible solutions. Policymakers need to work together in developing essential standards and receiving benefits that will promote IoT expansion.

Future integration between fog computing and 5G technology will enhance both speed and reliability of the system. A mobile application provides real-time data visualization that substantially boosts user experience along with energy management capability. AI predictive maintenance can foresee equipment failures through forecasts while performing efficient energy management. The IoT-enabled smart power monitoring system provides an efficient and scalable solution for contemporary energy management that enables effective power management operation in practice. The combination of sustained AI development with blockchain and edge computing systems will lead to overcome current obstacles to develop sustainable residential energy management and home-based enterprise energy solutions.

REFERENCES

Abir, R., Rahman, S. and Chowdhury, A., 2021. Predictive Analytics for Smart Grid Management Using Reinforcement Learning. *IEEE Transactions on Smart Grid*, 12(5), pp.987–995.

Ajadalu, S., 2024. *Optimizing Energy Efficiency in Smart Home Automation through Reinforcement Learning and IoT*. Available at: https://papers.ssrn.com/abstract=5020092 [Accessed 6 February 2025].

Alahakoon, D. and Yu, X., 2016. Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey. *IEEE Transactions on Industrial Informatics*, 12(1), pp.425–436.

Alam, S., Khan, I. and Rahman, M., 2021. The Role of IoT in Smart Energy Management Systems. *Energy Informatics*, 4(2), pp.145–160.

Alzoubi, Y.I., Al-Ahmad, A. and Kahtan, H., 2022. Blockchain Technology as a Fog Computing Security and Privacy Solution: An Overview. *Computer Communications*, 182, pp.129–152. **DOI: 10.1016/j.comcom.2021.11.005**.

Chen, L., Zhou, Y. and Zhang, X., 2020. Big Data Applications in Smart Grid Systems. *International Journal of Electrical Power & Energy Systems*, 118, p.105740.

Danbatta, S.J. and Varol, A., 2019. Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. *In: 2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. **DOI: 10.1109/isdfs.2019.8757472** [Accessed 6 February 2025].

Devadhanishini, A.Y., Kumar, S., Ramesh, B. and Priya, R., 2019. Smart Power Monitoring System using IoT. *In: 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. **DOI: 10.1109/icaccs.2019.8728311** [Accessed 6 February 2025].

Gupta, R. and Singh, P., 2022. IoT-Driven Solutions for Renewable Energy Integration. *Renewable Energy Reports*, 5(3), pp.123–134.

Haghi Kashani, M. and Mahdipour, E., 2022. Edge Computing in IoT-Based Power Systems: Challenges and Opportunities. *Journal of Computer Science and Technology*, 37(4), pp.567–579.

Jadhav, A.R. and Rajalakshmi, P., 2017. IoT-enabled Smart and Secure Power Monitor. *In: 2017 IEEE Region 10 Symposium (TENSYMP)*, pp.1–4. **DOI: 10.1109/8070096** [Accessed 6 February 2025].

Khandare, K.K. and Jape, M.V., 2024. Research on Smart Power Monitoring System Using IoT. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE)*, 12(6). Available at: https://ijireeice.com/wp-content [Accessed 6 February 2025].

Khodadadi, F., Dastjerdi, A.V. and Buyya, R., 2017. Internet of Things: An Overview. Available at: http://arxiv.org/abs/1703.06409 [Accessed 6 February 2025].

Raj, N., Sinha, A., Bharddwaj, S. and Yadav, A.L., 2024. AI-Powered Energy Consumption Optimization for Smart Homes Using IoT. *In: 2024 International Conference on Computational Intelligence and Computing Applications (ICCICA)*, pp.231–236. **DOI: 10.1109/10585239** [Accessed 6 February 2025].

Rathee, G., Sharma, A., Kumar, R. and Iqbal, R., 2019. A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology. *Ad Hoc Networks*, 94, p.101933.

SEIDOR, 2025. *Sustainable Development and IoT: How Technology Helps the Environment*. Available at: https://www.seidor.com/blog/iot-sustainable-development-technology-helps-environment [Accessed 6 February 2025].

Shafique, K., Khawaja, B.A., Khurram, M., Khurshid, A., Mukhopadhyay, S.C. and Kuang, J., 2020. Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. *IEEE Access*, 8, pp.23022–23040. **DOI: 10.1109/access.2020.2970118**.

Sovacool, B.K. and Furszyfer Del Rio, D.D., 2020. Smart Home Technologies in Europe: A Critical Review of Concepts, Benefits, Risks and Policies. *Renewable and Sustainable Energy Reviews*, 120, p.109663. **DOI: 10.1016/j.rser.2019.109663**.

Wang, S., Ding, Y., Xu, Y., Zhu, L., Zhang, X. and Xie, P., 2019. Blockchain-enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(11), pp.2266–2277. **DOI: 10.1109/tsmc.2019.2895123**.

Zhang, C., 2021. Intelligent Internet of Things Service Based on Artificial Intelligence Technology. *In: 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*. **DOI: 10.1109/icbaie52039.2021.9390061** [Accessed 6 February 2025].