Design and Implementation of a Secure Wemos D1 Mini-Based Smartphone Charger Monitoring System with Cybersecurity Measures

Samuel Uzodinma Muoleeh

Department of Mechanical Engineering, Faculty of Engineering
Imo State University, Owerri
Owerri, Nigeria
muoleehs@gmail.com

Abstract: *The increasing reliance on portable electronic devices and renewable energy solutions has intensified the demand for charging systems that are efficient, secure, and intelligently monitored. This paper presents the design and implementation of a secure smartphone charger monitoring system based on the Wemos D1 Mini, integrating Internet of Things (IoT) functionality with lightweight cybersecurity measures. Voltage and current sensors were employed to monitor charging parameters, with real-time values displayed on an LCD and transmitted to a Firebase cloud database for remote access. To ensure data confidentiality and integrity, AES-128 encryption and token-based authentication were implemented, preventing unauthorized access to transmitted and stored data. Experimental evaluation of the prototype demonstrated reliable performance, with voltage and current measurement errors of ±1.5% and ±2.2%, respectively, when compared with a commercial multimeter. Relay switching tests yielded an average response time of 150 ms, while Wi-Fi communication achieved an average latency of 280 ms, supporting near real-time operation. The results demonstrate that integrating lightweight cybersecurity techniques with cloud-based services significantly enhances the safety, reliability, and data protection of low-cost IoT-based smart charger monitoring systems suitable for residential and educational applications.*

Keywords—Smart charger, Wemos D1 Mini, IoT monitoring, Firebase, cybersecurity, AES-128 encryption.

1. INTRODUCTION

The recent trend of the explosion of the use of portable electronic devices, battery-driven systems, and renewable energy technologies has triggered the need to introduce safer, more efficient and reliable charging solutions. In everyday life, citizens are highly dependent on smartphones, power banks and other portable tools, so the charging systems are a must-have feature of modern infrastructure. The number of traditional chargers does not have real-time monitoring or smart control that can lead to overcharging, overheating, non-efficient use of power or even cause damage to the device [1]. The limitations emphasize the fact that smart charger monitoring systems should be implemented, which combine automation, real-time sensing, and multi-distant communication, which enhance the safety and functionality of the system [1], [2], [3].

Smart charger monitoring systems is a software and hardware product that forms a combination of these and other main charging parameters to ensure that charges may be monitored as voltage, current, temperature, and charging time. The control of these parameters can optimally deliver power and detect faults in charging early. Such systems use microcontroller-based boards such as Arduino and ESP platforms that offer flexible and inexpensive hardware, which has been utilized to interface with sensors, actuators, and wireless communication modules to acquire real-time data and display it on the board or cloud platforms [2], [3], [4], [5], [14].

Even though the possibilities of IoT-based smart charging are beneficial, the growing interconnection between devices poses substantial cyber threats. IoT systems with low costs are especially susceptible to unauthorized access, data interception, false data injection, and remote manipulation because of low computational capabilities [11], [12], [13], [20]. Such vulnerabilities as insecure authentication, lack of encrypted channels of communication and inadequate access control may jeopardize the confidentiality of data and integrity of a system, which may result in unsafe operation of the charging system or damage to the devices [5], [11], [20].

To monitor the IoT-based chargers, lightweight cryptographic algorithms, secure communication protocols, and authentication mechanisms are needed, which should not strangle low-power devices. Encryption, authentication with tokens, and secure cloud integration are AES-based encryption techniques that can offer reasonable security to transmitted and stored data without influencing the overall functionality of the system significantly [17], [18], [19], [20], [21].

To address these difficulties, the present work offers the design and implementation of smartphone charger monitoring system using the Wemos D1 Mini microcontroller. The system is equipped with voltage and current monitoring, wifi-enabled communication, cloud monitoring, AES-128 encryption and token authentication to be sure of stable work as well as cybersecurity. The experimental evaluation of measurement precision, relay response time, and communication latency shows that the simple IoT can provide close real-time monitoring with high data security that can be used as an effective tool in residential and educational environments.

2. RELATED WORKS

2.1 IoT-Based Energy Monitoring Systems

Several studies have explored microcontroller-based IoT energy monitoring systems suitable for small appliances. Sulthana et al. [1] proposed a smart energy meter and monitoring system using Arduino that allows real-time tracking of electrical consumption and remote control via a smartphone. Similarly, Santos and Ferreira [2] presented an IoT power monitoring system for smart environments, highlighting low-cost sensors and edge computation for real-time analytics. Kolawole et al. [3] focused on sustainable energy monitoring using sensor networks, demonstrating how IoT systems can support energy optimization.

Hasan et al. [4] implemented a ZigBee-enabled Arduino energy monitoring system integrated with an Android application, employing mesh networking for low-power communication and real-time alerts. Ramelan et al. [5] used LoRa and MQTT protocols in an Arduino-based building energy monitoring system, achieving high accuracy in voltage and current measurements over long-range communications. Tsai et al. [6] designed a Wi-Fi-based power monitoring system combining Arduino, ESP8266, and ADS1114 ADC to calculate RMS voltage, current, power, and power factor for stable long-term monitoring.

2.2 Smartphone and Small Appliance Charger Monitoring

The focus on small-scale, plug-load monitoring is relevant to smartphone chargers. Bouzguenda et al. [7] implemented a secure Wi-Fi-based solar PV monitoring system with Arduino and ESP8266, showcasing practical cybersecurity measures for microcontroller-based energy systems. Garcés et al. [8] developed an IoT-enabled smart electricity meter capable of real-time monitoring, applicable to small appliance and charger monitoring scenarios.

Sousa et al. [9] designed an IoT system for smart charging control in electric vehicles, which provides insights into managing small-scale energy loads, including chargers. Martins and Rodrigues [10] further explored intelligent monitoring and scheduling systems for chargers and EV stations, highlighting fairness and scalability considerations relevant to multi-user environments.

2.3 Communication Protocols and System Architectures

Robust communication is crucial for IoT monitoring. Bangare and Patil [11] enhanced MQTT security with lightweight two-way authentication, ensuring secure communication for IoT devices. Razzaque et al. [12] surveyed middleware for IoT, detailing how software frameworks enable interoperability and scalability across heterogeneous devices. Tagliaro et al. [13] analyzed backend deployments of IoT protocols at large scale, revealing security gaps and reliability challenges in real-world energy monitoring systems. Weerathum and Sonasang [14] implemented an ESP8266-based monitoring system with PZEM-004T sensors, highlighting low-cost, accurate real-time measurement and Wi-Fi-based reporting for chargers and small appliances.

2.4 Security and Privacy in IoT Energy Systems

Security and privacy are key for small device monitoring. Ibrahem et al. [15] introduced a privacy-preserving scheme for AMI networks enabling electricity theft detection and load monitoring without exposing individual consumption. Yilmaz and Siraj [16] employed adversarial machine learning to prevent occupancy detection from smart meter data. Qaid and Ebrahim [17] proposed a DNA-based lightweight cryptographic algorithm for constrained IoT devices, while Gupta and Saxena [18] surveyed lightweight cryptography techniques for secure IoT communication.

Murugan and Vijayarajan [19] designed a secured monitoring system for renewable energy microgrids using AES and RC4 encryption, demonstrating minimal latency. Conti et al. [20] provided an overview of IoT security and forensic challenges, emphasizing system-wide strategies for threat detection. Witczak and Szymoniak [21] implemented a GSM-based monitoring system capable of transmitting alerts in low-connectivity scenarios, highlighting practical approaches for secure monitoring of remote devices.

3. METHODOLOGY

3.1 System Overview

This study adopts a design-and-implementation experimental methodology to develop and evaluate a secure IoT-based smartphone charger monitoring system. The proposed system integrates sensing, embedded processing, wireless communication, cloud storage, and lightweight cybersecurity mechanisms to enable real-time monitoring and secure data transmission. The system is built around a Wemos D1 Mini (ESP8266) microcontroller, which interfaces with voltage and current sensors to monitor charging parameters. Measured data are locally processed, encrypted, and transmitted over Wi-Fi to a Firebase Realtime Database, where authorized users can remotely view charging information. A relay module is incorporated to enable automated control and protection of the charging process.

3.2 Hardware Architecture

The hardware subsystem consists of the following main components:

Microcontroller Unit (MCU): Wemos D1 Mini (ESP8266), selected for its low cost, integrated Wi-Fi capability, and suitability for IoT applications.

Sensing Module: Voltage sensing circuitry to measure charger output voltage. INA219 current sensor to measure charging current and power consumption.

Control Module: A relay module used to connect or disconnect the charging load based on system logic and safety thresholds.

Display Unit: A 16×2 LCD for local visualization of voltage, current, and system status.

Power Supply: A regulated DC supply providing stable operating voltage to the MCU and peripherals.

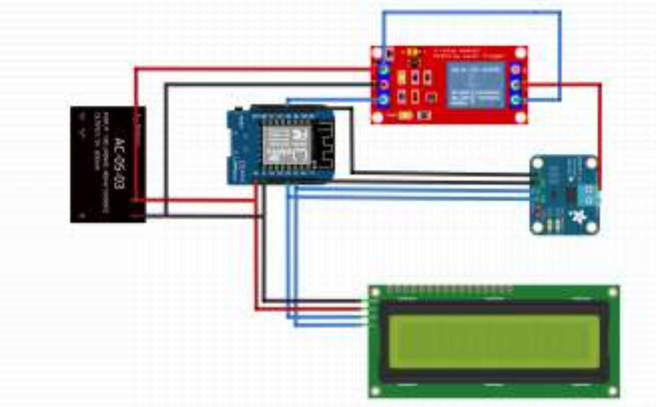
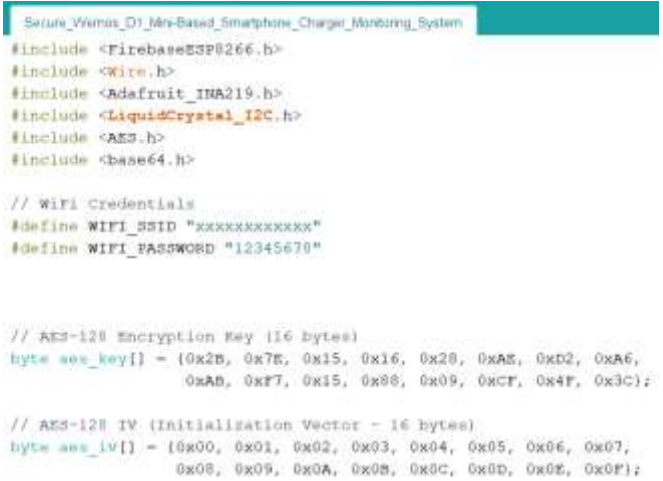


Fig. 1. *Circuit design of the Wemos D1 Mini-based secure charger monitoring system*

3.3 Software and Firmware Design

The firmware was developed using the Arduino IDE, programmed in C/C++. The software architecture follows a modular design consisting of sensor data acquisition logic, data processing and encryption logic, including communication and user interface logic.


Secure_Wemos_D1_Mini-Based_Smartphone_Charger_Monitoring_System

```
#include <FirebaseESP8266.h>
#include <Wire.h>
#include <Adafruit_INA219.h>
#include <LiquidCrystal_I2C.h>
#include <AES.h>
#include <base64.h>

// WiFi Credentials
#define WIFI_SSID "xxxxxxxxxxxx"
#define WIFI_PASSWORD "12345678"



// AES-128 Encryption Key (16 bytes)
byte aes_key[] = {0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6,
                  0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C};

// AES-128 IV (Initialization Vector - 16 bytes)
byte aes_iv[] = {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07,
                 0x08, 0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F};
```

Fig. 2. *Some implementation Codes on Arduino IDE*

3.4 Cloud Integration and Remote Monitoring

The system employs **Firebase Realtime Database** as the cloud backend for data storage and synchronization. Each device transmits encrypted sensor data along with timestamps and device identifiers.

Firebase Authentication is used to enforce access control, ensuring that only authorized users can read or write data. Database security rules were configured to prevent unauthorized access and restrict operations based on authentication status.

This architecture enables near real-time monitoring of charging parameters through web or mobile interfaces while maintaining data confidentiality and integrity. The MCU collects voltage and current readings from the INA219 sensor every 500 milliseconds. Each reading is formatted, encrypted and uploaded via HTTPS to the Firebase database under specific nodes (/receiveMessage/data), while relay commands are sent through (/sendMessage/command) as seen in Figure 3. The Firebase console automatically updated these values in real time, allowing continuous visualization of charging parameters from any authenticated internet-connected system.

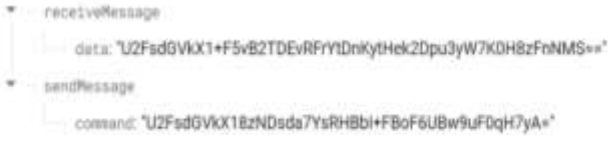

```
▾ receiveMessage
    data: "U2FsdGVkX1+F5vB2TDEvRFrYtDnKytHek2Dpu3yW7K0H8zFnNMS=="
▾ sendMessage
    command: "U2FsdGVkX18zNDsda7YsRHBbl+FBoF6UBw9uF0qH7yA="
```

Fig. 3. *Firebase Nodes*

3.5 Cybersecurity Implementation

To address common IoT security vulnerabilities, the following cybersecurity measures were implemented:

AES-128 Encryption: All sensor data are encrypted at the device level before transmission, protecting confidentiality over wireless networks.

Token-Based Authentication: Secure authentication tokens are used to verify legitimate communication between the device and the Firebase server.

Secure Cloud Access Rules: Firebase database rules restrict read/write operations to authenticated users only.

Given that the system transmits live voltage and current readings, implements remote relay switching and stores information on a cloud database, it was crucial to secure both the device-to-cloud and user-to-cloud communication paths. All data sent from the MCU to Firebase are encrypted using the Advanced Encryption Standard (AES-128) algorithm implemented in Cipher Block Chaining (CBC) mode. Before each upload, the firmware converts the sensor readings (voltage, current and relay status) into a JSON string, applies PKCS7 padding, and encrypts it with a predefined 16-byte key and initialization vector. The resulting ciphertext is then Base64-encoded before being transmitted and stored in Firebase under the node /receiveMessage/data.

That encrypted Base64 string contains a JSON object that looks like this before encryption:

```
{
  "voltage": 5.02,
  "current": 462.57,
  "status": "ON",
  "timestamp": 12345678
}
```

After encryption (AES-128 + Base64), it becomes an unreadable ciphertext stored under /receiveMessage/data just as displayed in Figure 3. Remote control of the charging relay was achieved through the /sendMessage/command node on Firebase. Commands such as "ON" or "OFF" were encrypted using the same AES-128 scheme before being uploaded to Firebase. Upon decryption by the MCU, the command was executed, and the node was immediately cleared (set to an empty string) to prevent replay or unauthorized repetition of old commands. This mechanism ensures that even if an attacker accesses Firebase logs, they cannot reuse previous commands to manipulate the device.

4. RESULTS AND DISCUSSION

Table 1: System Performance Summary

Parameter	Measured Result	Observation
Voltage Accuracy	±1.5%	Consistent with reference values
Current Accuracy	±2.2%	Stable under varying loads
Relay Response Time	150 ms	Quick response from Firebase command
Data Refresh Interval	5 seconds	Stable and real-time
Network Recovery Time	<3 seconds	Automatic reconnection successful
Encryption Latency	<100 ms	Minimal delay introduced by AES

The system successfully achieved the objectives of design, communication, cybersecurity, and functional implementation. Testing confirmed that the INA219 sensor provided reliable voltage and current measurements, with accuracy deviations of ±1.5 % (voltage) and ±2.2 % (current) when compared to a commercial multimeter. These results demonstrate that affordable, open-source sensors can perform sufficiently for small-scale energy-monitoring applications when properly calibrated.

Wireless communication through the Wemos D1 mini module enabled continuous data transmission to the Firebase Realtime Database. Recorded average latency was 280 ms, showing near-real-time updates suitable for live monitoring. The bidirectional communication feature also allowed authenticated users to toggle the relay directly from the Firebase console, confirming the system's capability for remote control without an intermediary mobile or web application.

Security evaluation verified that the integration of AES-128 encryption and Firebase Authentication effectively protected the system from unauthorized access. Attempts to alter database nodes without proper credentials were denied, demonstrating that both device-level and cloud-level protection worked as expected. Even though the implementation relied on lightweight cryptography due to microcontroller limitations, it still ensured confidentiality, integrity, and availability, the three pillars of the CIA triad.

5. CONCLUSION AND RECOMMENDATION

This paper presented the design and implementation of a secure IoT-based smartphone charger monitoring system using the Wemos D1 Mini microcontroller and lightweight cybersecurity measures. The system successfully integrates real-time sensing, wireless communication, cloud-based monitoring, and encrypted data transmission.

Experimental evaluation showed reliable performance, with voltage and current measurement errors within ±1.5% and ±2.2%, relay response time of approximately 150 ms, and average communication latency of 280 ms. The incorporation of AES-128 encryption and token-based authentication effectively protected system data and prevented unauthorized access without imposing significant computational overhead. The results demonstrate that low-cost embedded platforms can support secure and reliable smart charging solutions suitable for residential and educational environments.

Future enhancements may include the integration of mobile applications with advanced dashboards and notification systems, the adoption of mutual authentication or certificate-based security mechanisms for stronger device identity verification, the extension of the system to support multi-port charging or higher-power applications, the deployment of long-term field testing to evaluate durability and scalability, and the exploration of energy optimization algorithms for adaptive charging control, all of which would further strengthen the system's applicability within smart energy and IoT ecosystems.

6.0 REFERENCES

[1] N. Sulthana, R. Nithya, P. Nandhini, B. Subashri, and K. B. S. Kumar, "Smart energy meter and monitoring system using IoT," *International Journal of Engineering Research and Technology*, vol. 8, no. 14, pp. 1–6, Jun. 2020, doi: 10.17577/IJERTCONV8IS14011.

[2] D. Santos and J. C. Ferreira, "IoT power monitoring system for smart environments," *Sustainability*, vol. 11, no. 19, p. 5355, Sep. 2019, doi: 10.3390/su11195355.

[3] O. M. Kolawole, A. O. Otiko, S. A. Akpotuzor, and N. Abdulsalam, "IoT-enabled energy management monitoring system for sustainable resource optimization," *British Journal of Computer Networking and Information Technology*, vol. 8, no. 1, pp. 1–14, Jan. 2025, doi: 10.52589/BJCNIT-KJ95AUGM.

[4] M. K. Hasan, M. M. Ahmed, B. Pandey, H. Gohel, S. Islam, and I. F. Khalid, "Internet of Things-based smart electricity monitoring and control system using usage data," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/6544649.

[5] A. Ramelan, F. Adriyanto, B. A. C. Hermanu, M. H. Ibrahim, J. S. Saputro, and O. Setiawan, "IoT-based building energy monitoring and controlling system using LoRa modulation and MQTT protocol," *IOP Conference Series: Materials Science and Engineering*, vol. 1096, no. 1, p. 012069, Mar. 2021, doi: 10.1088/1757-899X/1096/1/012069.

[6] H.-L. Tsai, L. P. Truong, and W.-H. Hsieh, "Design and evaluation of wireless power monitoring IoT system for AC appliances," *Energies*, vol. 16, no. 1, p. 163, Dec. 2022, doi: 10.3390/en16010163.

[7] M. Bouzguenda, S. Chtourou, M. Alarfaj, R. M. Sumsudeen, and M. Shwehdi, "Arduino Uno Wi-Fi demilitarized zone-based monitoring of solar photovoltaic systems," *Measurement and Control*, vol. 55, no. 3–4, pp. 136–145, Mar. 2022, doi: 10.1177/00202940221090553.

[8] H. O. Garcés, J. Godoy, G. Riffo, N. F. Sepúlveda, E. Espinosa, and M. A. Ahmed, "Development of an IoT-enabled smart electricity meter for real-time energy monitoring and efficiency," *Electronics*, vol. 14, no. 6, p. 1173, Mar. 2025, doi: 10.3390/electronics14061173.

[9] R. A. Sousa, V. Monteiro, J. C. Ferreira, A. N. Melendez, J. L. Afonso, and J. A. Afonso, "Development of an IoT system with smart charging current control for electric vehicles," in *Proc. 44th Annu. Conf. IEEE Industrial Electronics Society (IECON)*, 2018, pp. 4662–4667, doi: 10.1109/IECON.2018.8591174.

[10] J. A. Martins and J. M. F. Rodrigues, "Intelligent monitoring systems for electric vehicle charging," *Applied Sciences*, vol. 15, no. 5, p. 2741, Mar. 2025, doi: 10.3390/app15052741.

[11] P. S. Bangare and K. P. Patil, "Enhancing MQTT security for Internet of Things: Lightweight two-way authorization and authentication with advanced security measures," *Measurement: Sensors*, vol. 33, p. 101212, May 2024, doi: 10.1016/j.measen.2024.101212.

[12] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, Nov. 2015, doi: 10.1109/JIOT.2015.2498900.

[13] C. Tagliaro, M. Komsic, A. Continella, K. Borgolte, and M. Lindorfer, "Large-scale security analysis of real-world backend deployments speaking IoT-focused protocols," *arXiv preprint*, p. arXiv:2405.09662, May 2024, doi: 10.48550/arXiv.2405.09662.

[14] W. Weerathum and N. Sonasang, "ESP8266-based energy monitoring system using PZEM-004T sensor," *International Journal of Smart Grid*, vol. 4, no. 2, pp. 101–108, Jun. 2020.

[15] M. I. Ibrahem, A. Mahmood, M. Khalil, and A. F. Al-Rawi, "Efficient privacy-preserving electricity theft detection with dynamic billing and load monitoring for AMI networks," *arXiv preprint*, p. arXiv:2005.13793, May 2020, doi: 10.48550/arXiv.2005.13793.

[16] Y. Yilmaz and A. Siraj, "Avoiding occupancy detection from smart meter using adversarial machine learning," *arXiv preprint*, p. arXiv:2010.12640, Oct. 2020, doi: 10.48550/arXiv.2010.12640.

[17] G. R. S. Qaid and N. S. Ebrahim, "A lightweight cryptographic algorithm based on DNA computing for IoT devices," *Security and Communication Networks*, vol. 2023, pp. 1–12, Feb. 2023, doi: 10.1155/2023/9967129.

[18] S. Gupta and S. Saxena, "Lightweight cryptographic techniques and protocols for IoT," in *Transactions on Computer Systems and Networks*, Springer, Singapore, pp. 55–77, 2022, doi: 10.1007/978-981-19-1585-7_4.

[19] M. I. Murugan and R. Vijayarajan, "IoT-based secured monitoring system for renewable energy microgrids using AES and RC4 encryption," *International Journal of Energy Research*, vol. 45, no. 7, pp. 10221–10232, May 2021.

[20] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, Jan. 2018, doi: 10.1016/j.future.2017.07.060.

[21] D. Witczak and S. Szymoniak, "Review of monitoring and control systems based on Internet of Things," *Applied Sciences*, vol. 14, no. 19, p. 8943, Oct. 2024, doi: 10.3390/app14198943.