Monitoring and Analysis of Real-time Energy Data in IoT based Global and Secure Networking System

Raihan Bin Mofidul*, Md Morshed Alam*, ByungDeok Chung** and Yeong Min Jang*
*Dept. of Electronics Engineering, Kookmin University, Seoul, South Korea
**ENS. Co. Ltd, Ansan, South Korea
Email: raihanbinmofidul@gmail.com; mmorshed@ieee.org; bdchung@ens-km.co.kr; yjang@kookmin.ac.kr

***Abstract*—Over the past few decades, the Internet of Things (IoT) has gained enormous popularity. Combining Artificial Intelligence (AI) with the IoT offers us plenty of benefits in daily life. Nevertheless, big data analysis and secure connectivity with various IoT devices have inherent limits. This article has described how to store large amounts of data by automatically classifying it into several tables in a SQL database and how to use an easy-to-use authentication mechanism for online communication. In our proposed system, IoT devices can send data every second after connecting to the server with appropriate authentication, and the database can store massive amounts of data from multiple IoT devices in five seconds. After ensuring proper credentials, this database can be accessed by any AI or Machine Learning (ML) model through the Internet from anywhere at anytime. Therefore, our proposed system is very beneficial for configuring Artificial Intelligence of Things (AIoT).**

***Index Terms*—Energy Management Device, Big Data, Artificial Intelligence of Things, Internet of Things, Secure Connection**

I. Introduction

The Internet of Things, or IoT, is a network of connected computing devices, mechanical and digital devices, objects, creatures, or humans that may exchange data across a network without requiring human-to-human or human-to-computer interaction. According to the [1], the Fourth Industrial Revolution refers to the digital revolution that is occurring as a result of developing technologies such as robotics, IoT, and Artificial Intelligence (AI). Furthermore, COVID-19 has accelerated the usage of these technologies [2]. There are some innovative technology like LoRa for data exchange [3]. But deploying LoRa globally is kind of costly and complex. In [4], [5], Message Queuing Telemetry Transport (MQTT) has emerged as one of the leading protocols for IoT solutions in recent years because of lightweight protocols, flexibility, scalability, and security mechanisms such as Transport Layer Security (TLS) encryption. To make AI and ML models more effective in each section of our life, an online and secure data streaming system is necessary [6].

To expedite up the adoption of this concept in our daily life, we have introduced a secure communication method including login credentials for IoT devices, servers, and live streaming databases. Furthermore, real-time data is visible and accessible from anywhere at any time. As a result, AI and ML models can be trained in any computer or smart devices. Following that, these trained models can be used directly in the AIoT system, such as the Virtual Power Plant (VPP), Home Energy Management (HEM), Personal Medical Assistant (PMA), etc.

The contributions of this work include:

- Implementation of an integrated AIoT system with Node-RED [7].
- Development of a website dashboard for real-time monitoring [8]
- Implementation of a global streaming database with authentication protocol for AI and ML models

This paper is organized as follows. Our proposed Methodology is introduced in section II. Experiments in section III and section IV is the Conclusion and Future work.

II. Proposed System

A. Develop a Secure Global Broker

1) Mosquitto Broker: The MQTT protocol, which offers a simple way to carry out messaging using a publish/subscribe architecture, is implemented by Eclipse Mosquitto, an open source message broker. This qualifies it for Internet of Things messaging applications using low power sensors or mobile devices like smartphones, embedded computers, or microcontrollers [9]. We deployed a public IP. So long as we have the right credentials, we can view our broker information from anywhere.

2) Secure Connection: Our broker system needs to be configured with authentication to prevent connections from unauthorized IoT clients. As in [10], there are three options for authentication: unauthorised/anonymous access, authentication plugins, and password files. Each of the three options can be used separately or in combination. To establish a secure connection among the broker and the clients, a user name and encrypted password are stored in a password file that we have applied here. Moreover, anonymous access is disabled to prevent undesirable clients.

B. Develop "Energy Management Device" as Client

1) ESP: The official IoT Development Framework for the ESP8266, ESP32, ESP32-S, and ESP32-C line of SoCs is called ESP-IDF. Millions of devices are currently powered by ESP-IDF, which also makes it possible to develop a wide range of network-connected items, from basic light bulbs and toys to large appliances and industrial equipment [11]. In this system, ESP8266 and ESP32-S were applied due to its affordability, compact design, and compatibility with embedded devices.

2) Voltage and Current Measurement: For measuring voltage, current-type voltage transformers are employed because of their small size, high precision, and good consistency [12]. Additionally, 20A current sensors which operate based on the "Hall Current Sensing Principle" are utilized for AC current measurement because of their wide voltage range, small footprint, no soldering requirements, and a high level of precision.

C. Online Dashboard

The dashboard layout should be considered as a grid. Each group element has a width - by default 6 'units' (a unit is 48px wide by default with a 6px gap). Each widget in the group also has a width - by default, 'auto' which means it will fill the width of the group it is in, but you can set it to a fixed number of units. The layout algorithm of the dashboard always tries to place items as high and to the left as they can within their container - this applies to how groups are positioned on the page, as well as how widgets are positioned in a group.

III. Experiments

A. Secure and Live Monitoring System

An individual can view power curves of various appliances, including current meters, via any web browser after completing the necessary authorization through user name and password. In Fig. 1 and Fig. 2, the proposed secure and live monitoring system is displayed.

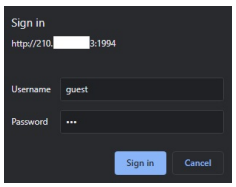

Fig. 1. Dashboard Login Credentials

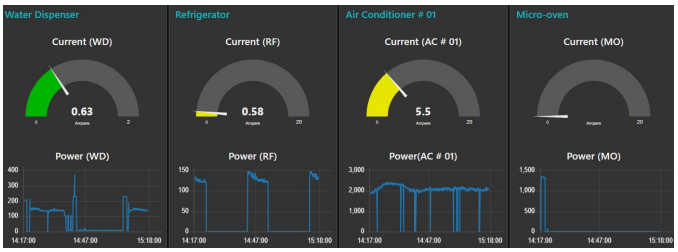

Fig. 2. Live Monitoring System

B. Analysis with AIoT

After building a "engine" with the Username, Password, IP or Web address of the Server, Port number, and Name of the Database, our AI device can access the Big Data. Data from any month can be retrieved thereafter. As a result, it is capable of train and develop AI and ML models. In Fig. 3, Big data is being accessed in remote AIoT device.

```
engine = create_engine("SQL-Name://User-Name:Password@IP-Address:Port/Database-Name")
```

```
df1 = pd.read_sql_table("wicomai_power_consumption_2022_07", engine)
df1
```

✓ 6.1s

	dt	pa_v	pb_v	pc_v	wd_a	wd_p	rf_a	rf_p	ac_01_a	ac_01_p	rh_01_a	rh_01_p	mo_a	mo_p	ac_02_a	ac_02_p	rh_02_a	rh_02_p
0	2022-07-19 15:24:21	0.0	214.9	0.0	0.38	83.6	0.00	0.0	5.81	2207.8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1	2022-07-19 15:24:23	0.0	0.0	0.0	0.38	83.6	0.00	0.0	5.74	2181.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
2	2022-07-19 15:24:24	0.0	213.8	0.0	0.38	83.6	0.00	0.0	0.00	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Fig. 3. Analysis Big Data in AIoT System

IV. Conclusion and Future Work

In this article, we've covered both conventional and newly developed technologies for the Internet of Things and Big Data analysis. Because the current method has various funding, privacy, sturdiness, and performance issues, we have introduced our integrated and secure web application. This may then be used remotely with AIoT devices. The system has evolved, and the findings are displayed under the experiments section. However, our future plan is to adopt block-chain for more secure commnunication environment.

Acknowledgment

This work was supported by the Technology development Program (S3098815) funded by the Ministry of SMEs and Startups(MSS, Korea).

References

[1] K. Schwab and World Economic Forum, "The fourth industrial revolution: what it means and how to respond," https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/, Jan. 2016, accessed: 2022-8-10.

[2] M. Z. Chowdhury, M. T. Hossan, M. Shahjalal, M. K. Hasan, and Y. M. Jang, "A new 5G ehealth architecture based on optical camera communication: An overview, prospects, and applications," *IEEE consum. electron. mag.*, vol. 9, no. 6, pp. 23–33, 2020.

[3] M. Shahjalal, M. K. Hasan, M. M. Islam, M. M. Alam, M. F. Ahmed, and Y. M. Jang, "An overview of AI-enabled remote smart- home monitoring system using LoRa," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2020, pp. 510–513.

[4] "What is MQTT and why it is important for the internet of things," https://akenza.io/blog/what-is-mqtt, Nov. 2021, accessed: 2022-8-10.

[5] F. Chen, Y. Huo, K. Liu, W. Tang, J. Zhu, and Z. Sui, "A study on MQTT node selection," in *2020 16th International Conference on Mobility, Sensing and Networking (MSN)*. IEEE, 2020, pp. 622–623.

[6] P. Ferrari, E. Sisinni, A. Depari, A. Flammini, S. Rinaldi, P. Bellagente, and M. Pasetti, "Evaluation of the impact of cloud database services on industrial IoT applications," in *2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. IEEE, 2020, pp. 1–6.

[7] C. OpenJS Foundation, "Node-red," https://nodered.org, accessed: 2022-8-11.

[8] ——, "Node-red-dashboard," https://flows.nodered.org/node/node-red-dashboard, accessed: 2022-8-11.

[9] "Eclipse mosquitto," https://mosquitto.org, Jan. 2018, accessed: 2022-8-12.

[10] "Authentication methods," https://mosquitto.org/documentation/authentication-methods/, Feb. 2021, accessed: 2022-8-12.

[11] "IoT development framework I espressif systems," https://www.espressif.com/en/products/sdks/esp-idf, accessed: 2022-8-13.

[12] M. M. Alam, M. Shahjalal, M. M. Islam, M. K. Hasan, M. F. Ahmed, and Y. M. Jang, "Power flow management with demand response profiles based on user-defined area, load, and phase classification," *IEEE Access*, vol. 8, pp. 218 813–218 827, 2020.