Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
College of Engineering

Design and Implementation of Cloud Computing System for Data Collection and Processing for Smart Operation Centre

A Thesis

Submitted to the College of Engineering of the University of Babylon in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Engineering \ Electrical Engineering \ Electronic and Communications

by

Mafaz Mohammed Abed Jafar

Supervised by

Prof. Dr. Laith Ali Abdul-Rahaim

Asst. Prof. Dr. Ahmed Abdulkadhim Hamad

2022 A.D

﴿ بِسْمِ اللّهِ الرَّحْمَنِ الرَّحِيمِ ﴾

اقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ ﴿١﴾
خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ ﴿٢﴾ اقْرَأْ
وَرَبُّكَ الْأَكْرَمُ ﴿٣﴾ الَّذِي عَلَّمَ بِالْقَلَمِ
﴿٤﴾ عَلَّمَ الْإِنْسَانَ مَا لَمْ يَعْلَمْ ﴿٥﴾

صدق الله العلي العظيم

سورة العلق الايات (١-٥)

Dedication

To

Whom are tried to get me to this stage …… My Parents

To

My buttress, love and encourage in life……My Wife

To

The eyes of future ……My sons

To

Precious people……My siblings and relatives

To

My teachers, friends, colleagues and anyone assist me

I dedicate this work

Supervisor Certification

We certify that this thesis entitled "**Design and Implementation of Cloud Computing System for Data Collection and Processing for Smart Operation Centre**" was prepared by **Mafaz Mohammed Abed Jafar Shubbar** under our supervision at the Department of Electrical Engineering, College of Engineering, University of Babylon, as a partial fulfillment of the requirement for the degree of Doctor of Philosophy in Electrical Engineering \ Electronic and Communication Engineering.

Signature:

Name: ***Prof. Dr. Laith Ali Abdul-Rahaim***

(Supervisor)

Date: / / 2022

Signature:

Name: ***Asst. Prof. Dr. Ahmed Abdulkadhim Hamad***

(Supervisor)

Date: / / 2022

In view of the above recommendation, I am forward this thesis for discussion by the Examination Committee.

Signature:

Name: ***Asst. Prof. Dr. Shamam Fadhil Alwash***

(Head of Electrical Engineering Dept.)

Date: / / 2022

Examining Committee Certificate

We certify that we have read this thesis entitled "**Design and Implementation of Cloud Computing System for Data Collection and Processing for Smart Operation Centre**", and as an examining committee, examined the student "**Mafaz Mohammed Abed Jafar Shubbar**", in its contents and that in our opinion it meets the standard of a thesis for the degree of Doctor of Philosophy in Electrical Engineering\Electronic and Communication Engineering.

Signature:
Name: ***Prof. Dr. Ahmad T. Abdulsadda*** (Member)
Date: / / 2022

Signature:
Name: ***Prof. Dr. Osama Qasim Jumah Al-Thahab*** (Member)
Date: / / 2022

Signature:
Name: ***Prof. Dr. Ibrahim A. Murdas*** (Member)
Date: / / 2022

Signature:
Name: ***Prof. Dr. Hassan Jassim Motlak*** (Member)
Date: / / 2022

Signature:
Name: ***Prof. Dr. Bayan Mahdi Sabbar*** (Chairman)
Date: / / 2022

Signature:
Name: ***Prof. Dr. Laith Ali Abdul-Rahaim*** (Supervisor)
Date: / / 2022

Signature:
Name: ***Asst. Prof. Dr. Ahmed Abdulkadhim Hamad*** (Supervisor)
Date: / / 2022

Signature:
Name: ***Asst. Prof. Dr. Shamam Fadhil Alwash***
(Head of Electrical Engineering Dept.)
Date: / / 2022

Signature:
Name: ***Prof. Dr. Hatem Hadi Obeid***
(Dean of College of Engineering)
Date: / / 2022

Acknowledgments

Before anything, I praise ALLAH Almighty for providing me force and granting the ability to perform this thesis.

I would like to express my sincere and great gratitude to my supervisors: Prof. Dr. Laith Ali Abdul-Rahaim and Asst. Prof. Dr. Ahmed Abdulkadhim Hamad for their supervision, appreciable guidance and suggestions throughout this work.

The warm thank and gratitude is presented to my wife and my parents for their continuous support in all aspects of my life.

Special thank is presented to Dr.Akram Jaddoa khalaf for his advices .

Finally, thanks to all my friends, colleagues, workmate and the staff of electrical engineering for encouragement and help during the study period. Furthermore, thank all persons who directly or indirectly encouraged me to do my project.

Abstract

Energetic life-sustaining needs are essential for everyday existence, such as electrical power. It is used in residential, industrial and medical facilities. Despite the vital need for electricity demand and the evolution of bill payment ways, loss curtailments, additional energy bills, and the heist of electric energy are still problems. Power factor correction is a method to fix or minimise some mentioned problems. Automated power factor correction (APFC) will precede good contrivance for correction. On the other hand, electricity theft detection enables a more efficient and cost-effective method, as power theft is a matter for all utilities.

This thesis attends to design modern cloud computing systems for the operation centre. The first system is cloud APFC with neural network design advances to recent designs of APFC that depend on IoT and cloud. This system design used a private cloud with Node-red platform utilising Raspberry Pi and a neural network to correct the power factor of homes in a single algorithm.

Cloud is helping in hosting, processing, and accessing on-demand at any time and from anywhere as long as the Internet is accessible. Also, the neural network is used for determining the capacitance value for power factor correction. In addition, this design will minimise devices used for decision capacitance; it also minimises the bill's cost. The average power factor correction error based on real and decided capacitance via algorithm was 1.928% for trained data (active power and power factor for appliances as data set) and 2.65% for untrained. The neural network trained and tested by backpropagation on MATLAB R2020b.

While the second algorithm is a way for electricity fraud detection and energy tampering in the cloud, this design allows monitoring of the main distribution supply lines details to know future expansion if needed. It used a

private cloud with Node-red platform utilising Raspberry Pi near the main feeder to detect all homes possible larceny. In addition, this design by Raspberry Pi will minimise devices for detection to one with a single algorithm inside it by using the Node-Red platform.

The algorithm depends on the difference and disconnection of meters by sending a command from the cloud to the meters. The suggested system can detect and identify fraudulent or tampered electricity meters and meters bypassed and identify normal users around the clock. It also gives precise results, as in the case of two meters bypassed when the bypassing event started at the hour of 4:59, and the detection was done at the same time.

The monitoring process using Node-red inside the private cloud server offers flexibility in data managing and further process on it, it reads data every 10 seconds and it can be accessed via the browser with the same IP address. In addition, the mobile app Android can access from any network to monitor data.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
ANN	Artificial Neural Network
AMI	Advanced Meter Infrastructure
APFC	Automated Power Factor Correction
AWS	Amazon Web Services
CC	Cloud Computing
CPU	Central Processing Unit
CRM	Customer Relationship Management
CT	Current Transformer
DOC	Distribution Operation Centre
DB	Data Base
Dtrans	Distribution transformer
GC	Grid Computing
GND	Ground
GPIO	General Purpose Input/Output
GPS	Global Positioning System
GSM	Global System for Mobile
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IBM	International Business Machines
I/O	Input Output
IP	Internet Protocol
IR-Sensor	Infrared sensor
IT	Information Technology
JSONATA	JavaScript Object Notation Data
JSON	JavaScript Object Notation
LCD	Liquid Crystal Display
LoRaWAN	Long Range Wide Area Network
MAC	Media Access Control
MCC	Mobile Cloud Computing
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NodeMCU	Node Micro Controller Unit

OC	Operation Centre
OS	Operating System
PaaS	Platform as a Service
PC	Personal Computer
PEM	Primary Energy Meter
PF	Power Factor
PIC	Programmable Interface Circuit
PLC	Programmable Logic Controller
RAM	Random Access Memory
RMS	Root Mean Square
SaaS	Software as a Service
SD	Secure Digital
SDK	Software Development Kit
SG	Smart Grid
SMS	Short Message (or Messaging) Service
SOC	Smart Operation Centre
SoC	System-on-a-Chip
SSH	Secure Shell Protocol
TTL	Transistor-Transistor Logic
UEM	User Energy Meter
VT	Voltage Transformer
XML	Extensible Markup Language

List of Symbols

Symbol	Elaboration	Units
C	Capacitance	Farad
$\mathfrak{D}$	Current differences	Ampere
E	Energy	KWH
f	Activation function	Unitless
f	Frequency	Hz
I	Current or Primary Current	Ampere
i	Meter current	Ampere
I_L	Rated current allowed	Ampere
k	Output node number	Unitless
L	Number of meters per transformer	Unitless
n	Number of inputs	Unitless
P	Active Power	KW
Q	Reactive Power	VAR
S	Apparent Power	VA
T	Threshold	Unitless
VCC	Input voltage or PZEM	Volt
W, w	Weight	Unitless
X, x	Neural input	Unitless
Y, y	Neural output	Unitless
β	Factor control rate	Unitless
δ_{yk}	The error signal	Unitless
θ	Power factor angle	Unitless
λ	Learning rate	Unitless

Chapter One
Introduction

Chapter One

Introduction

1.1 Brief Background

The first decades of this century have been marked by rapid technical advancement, which has resulted in the modernisation of numerous services and utilities and the modernisation of electric energy. One of these upgrades in this sector is dubbed “smart grids”. Automation and telecommunications advancements are unquestionably the impetus for the construction of smart grids. They directly impact practically every service involved in network operation and force Operation Centres (OC) to undergo this change, resulting in smart network operation where OC integrates and makes sense of data from various sources through a single interface. Thus, it reduces the chaos and proliferation of data sources required for comprehension [1].

The OC assembles the processes collected from Human Machine Interfaces, cameras, geographic information systems, and other monitoring systems. In addition, it can be installed as a server on a computer and accessed remotely through another computer or device. The computer server for the OC must meet system requirements such as Linux or Windows operating systems [2] [3].

Cloud computing can offer resources that are made available only when needed architecture and support scaling solutions. End-user involvement is made possible by dynamic energy management. It bolsters an energy management system to offer an easy-to-use and superior service, escalate efficiency, and curtail the cost of running the facility. By using cloud computing in demand response systems, utilities and customers benefit from a fast response that is dependable and safe with reliable service. Cloud computing help and meets the requirements of OC [4].

The Smart Operation Centre (SOC) is a form of OC, it will maintain and

manage the Advanced Meter Infrastructure (AMI) for water, electric, gas, and among other things, that was created to combine various types of linked devices (sensors) [5]. AMI has several advantages: online billing pursuit for the client, monitoring and early discovery of faults and losses measurement, and the quick response in events of energy outage.

Furthermore, AMI enables more detailed customer profiles for actual time measures that assist the system in adopting decisions and estimating demand [1]. Smart meters must have bidirectional connectivity for real-time measurements and accept directives from the power utility. Mobile phone networks, satellite communications, RF transmissions, and Wi-Fi are examples of communication standards used by meters [6].

The Distribution Operation Centre (DOC) is a form of OC used by power companies to ensure energy delivery to all users linked to the system. Typical DOC attitude involves anticipating load, scheduling physical network events, controlling load in exigency or emergency circumstances, monitoring power quality, and coordinating system operations [1]. In addition, the DOC's network architecture should provide the following functions [7] :

1- Power or energy meter data administration, network observed and govern grid status and information communication systems management.
2- Power adjustment techniques like billing services, database updating and modification, and geographic data and position.

1.2 Problem Statement

Most OCs are utilised solely for monitoring or monitoring with fewer processes like meters arranged according to consumption. The DOC have the following:

1- The development of smart, more resilient, and less dependent on human intervention monitoring system makes it easier to integrate network

structure.

2- Reduce residential grid technical issues such as power factor improvement.
3- Reduce residential grid non-technical losses such as electric energy larceny.

Literature Review

This literature consists of previous research studies for power factor correction based on cloud or IoT and larceny of energy detection with cloud systems as in the following.

1.2.1 Cloud-Based Automated Power Factor Correction and Power Monitoring

Gunawan et al.(2018) [8] During experiments on the calibration of the current measurement in the power factor meter, the accuracy increased by utilising an SD card to store the detected data points and send them to MATLAB's user interface for monitoring. In addition, smart meter with the internet of things (IoT) framework with local storage was used. Automatic power factor adjustment was made through parallel linked capacitors; Arduino coupled to a relay circuit might control switches that activate the capacitors switch selector for the capacitor bank.

Taye (2018) [9] designed and emulated an automated power factor adjustment prototype utilising an Arduino as a microcontroller. The usage of this kit decreased expenses and helped customers because the industry power factor was enhanced from 0.66 to 0.92.

Vignesh Kumar et al.(2018) [10] constructed a scheme to reduce the penalty for industrial facilities, a set of automated power factor correction (APFC) equipment has been created around the Raspberry Pi. For safety, attention should be paid to power factor adjustment. Otherwise, the voltage and

current will increase, power system or machine components will be more likely to break, and capacitor bank life will be shortened.

Sathiyapriya et al.(2019) [11] utilised IoT and cloud computing to send and save power factor data. Alarm messages were sent to the individual with a high inductive load then an electrical relay was activated to connect the capacitor bank. This system was also tested to enhance the induction motor power factor automatically. Microcontroller and capacitor banks were used to develop power factor correction boosted by 0.21 from 0.76. About 1.7% of savings in energy consumption were achieved for the different planned loads.

Bhagavathy et al. (2019) [12] built an Android application with an open-source cloud platform; this app helped the user via text message to inspect the power factor revision and a bank capacitors misstep. When the power factor scale varies, the panel of APFC swaps capacitor banks automatically to correct the power factor, and power factor fluctuations were investigated under various load circumstances. The cloud role is hosting the data uploaded from the Android app. The maximum power factor achieved is 0.86.

Praveen et al. (2020) [13] addressed domestic load monitoring and informed the proper power factor range of the concerned load and which appliance degraded the power factor. The prototype hardware results for power factor were produced using Arduino Uno with mobile app was not exceed 0.9. IoT was helping customers and electric company employees better understand how their loads and power factors affected one another.

Mohammed et al. (2020) [14] used a Wi-Fi kit named Photon to control and monitor the Mosul University electricity plant activities remotely. Supervise voltage, devices load current, and power factor was included. Additionally, the system was developed to use an automatic power factor adjustment approach, fire detection and alarm unit, and carbon monoxide detector. In a major accident,

such as a fire, the plant's security system can lock down the facility to prevent more incidents. The equipment mentioned above was utilised to upload the sensor's data to the ThingSpeak cloud, to be processed fastly and visualised. The power factor after correction reaches 0.95.

Gomaa et al.(2020) [15] devoted a mathematical model tested on the cabling industry through a MATLAB model mason. While the IoT physical layer gathered, evaluated, and transmitted electric power characteristics associated with manufacturing process data obtained from PLC IoT nodes and the cloud for storing data. The adequate power quality was improved through manufacturing process management, so 33% in the power factor from (0.7 to 0.93) was achieved.

N. Dhamal et al.(2021) [16] suggested a system of power factor correction with cloud and IoT that will switch capacitor banks in and out of the circuit when the power factor drops below a certain point avoid power company charges. By determining the delay in the arrival of the current signal concerning voltage signal from the function generator using Arduino Uno and NodeMCU and relays. The cloud is used for saving data only. The Power Factor is improved, and the value becomes nearer to 0.9 to 0.95.

Nugroho et al. (2021) [17] used the Neural Network approach to reckon and rectify power factors automatically, and power may be monitored online via IoT. Overall, the power factor improved to 97.8% for the trained appliance's load and 94.8% of the untrained ones benefited from this power factor enhancement technology. Furthermore, using the MQTT (Message Queuing Telemetry Transport) protocol in the observation process based on IoT improved data transfer efficiency and helped in real-time monitoring.

Table 1.1 represents a comparison between systems according to specific characteristics.

Table 1.1Difference between characteristics of power factor correction systems and our system in literature review

Reference	Core hardware device	UI	Actuators or Sensors	Communication scheme	Node Type	PF Way of Correction	Messaging Protocol	System Type
[8]	Arduino	LCD	CT, VT	Wi-Fi	Arduino	Computational	-	Cloud storage
[9]	Arduino	LCD	CT, VT	-	local	Computational	-	IoT
[10]	Raspberry Pi board	PC	CT, VT	-	Raspberry Pi board	Computational	-	Local server
[11]	Arduino	Web page	CT, VT	Wi-Fi	NodeMCU	Computational	HTTP	Cloud storage
[12]	PIC-16F877A	Mobile app	CT, VT	Wi-Fi	Wi-Fi module	Computational	TCP	Cloud host data
[13]	Arduino	Mobile app	CT, VT	Wi-Fi	IoT module	Computational	TCP	IoT
[14]	HL-56S V1.0	Web page	ZMPT101B, SCT-013-030	Wi-Fi	Particle Photon	Computational	HTTP	Cloud host data
[15]	Central server	PC	CT, VT	Wi-Fi& Bluetooth	IoT beacons	Computational	MQTT	Cloud for storing data
[16]	Arduino	LCD	CT, VT	Wi-Fi	Esp8266	Computational	-	Cloud saving data
[17]	Stm32	web page	PZEM-004T	Wi-Fi	Esp8266	Neural network	MQTT	Local server
Our system	Raspberry Pi board	Web page+ Mobile app	PZEM-004T	Wi-Fi	NodeMCU	Neural network	MQTT	Cloud host and process

1.2.2 Larceny Revelations of Electric Energy with Cloud Computing

R. E. Ogu et al. (2016) [18] used an Arduino Wi-Fi Shield with Arduino Mega 2560 board for networking and controlling functions while sensing and actuating are handled by a Passive Infrared Sensor and Solid-State Relay. Hence, the meter can transmit its GPS location to the distribution company's portal over the cloud to save data. If the connectivity interface is functioning correctly, the system continuously checks for tampering with the meter and then disconnects the load attached to the meter from the distribution grid.

S. Sridhar et al. (2016) [19] devised an automatic electricity theft detection system in which an IR-Sensor is used to detect the passage of any abstract through the sensor channel. The project has the potential to significantly minimise the significant power and income losses caused by consumer theft. In addition, it makes utilisation of messages regarding transformer maintenance directed to the maintenance department.

N. Pranau et al. (2017) [20] established a summing method between the power supplied from the transformer in the distribution ends and the consumers to detect tampering. The electricity usage and distribution data are retrieved from the relevant meters, uploaded to the electrical board's monitoring portal, and then to the cloud storage for analysis. The theft is notified on the server page, and installing a suitable alarm near the server so that the theft may be prevented immediately or charged.

W. Li, T. Logenthiran et al. (2019) [21] created a system to detect and prevent energy theft using statistical models with machine learning. The system is divided into three stages. The stages are prediction, decision-making and subaltern decision-action; the last stage is responsible for energy theft decision-making. Every energy-consuming in the experimental house was equipped with an Aeon Labs Z-Wave UK Plug-in switch and energy meter. The data was then

gathered via a centralised smart device known as the VeraEdge Home Controller, with the cloud just monitoring the data from it.

K.Ashwitha et al. (2019) [22] developed a single-phase power theft identification and alert system with the assistance of the Blynk cloud. The design utilises a real-time comparison method that compares the incoming current of the energy meter with that of the load current. If the incoming current is equal to the load current, there has been no power theft; if the incoming current is greater than the load current, there is power theft, and the alert is directly posted on the internet in real-time via Blynk cloud. When the electrical board gets the notification on the authorised person's smartphone, they can disconnect the load remotely.

M. C. B. Loyola et al. (2019) [23] devised an electricity meter with warning and theft detection systems and an internet-based energy monitoring system to lessen the occurrences of power theft. To detect theft, microcontrollers and current sensors are used, while to notify others about the theft, LoRaWAN technology is employed. Illegal tapping and meter bypassing can be detected by the theft detection module. The cloud is used to collect data for monitoring energy consumption.

R. Meenal et al. (2019) [24] built a system to track and detect power theft by sending the information from the home Electricity Board to solve energy stealing in transmission lines and energy meters by several sensors that have the potential to send data in real-time. The Raspberry Pi is employed to detect energy theft and transmit a command to the GSM module, communicating the theft data to the Electricity Board. The sensor's sensitivity will increase when tapping or extra loading has occurred in the transmission lines.

R. Aswini et al. (2020) [25] built an intelligent house system that counteracts burglary by implementing IoT and cloud administration data base.

Microcontroller-based equipment links the equipment to the internet and server. The infrared sensor is contained within the metering infrastructure and is locked in as a safety measure to identify any unlawful tampering. A mobile alert is also issued to customers.

A. S. Hamid et al. (2020) [26] created a prepaid system for paying bills and devised a way to identify power theft, which helped increase the accuracy of energy meters via IoT. Another function was treated as energy usage monitoring over the cloud. An Arduino Uno with a Wi-Fi module is needed. A limit switch with a relay is used for theft detection.

M. Jeffin et al. (2020) [27] used IoT and cloud to detect and monitor power theft and online smart meter observation. The linear retraction technique is used to detect power theft by continuously observing the client's data and distribution-side intelligent meters. Furthermore, Android applications are being created to monitor user usage and billing information and inform utility in the event of a robbery; the cloud server hosts real-time events data for the database. Finally, a prototype circuit is created by an ATmega328P microcontroller and NodeMCU as a Wi-Fi module.

A. D. Attar et al. (2021) [28] utilised Arduino Uno in their experiment with traditional meters to identify and control energy meter scams to prevent any energy theft. The GSM module is configured to send an SMS to the central utility cloud server mechanically through a GSM module. In addition, the GSM module has been linked to the microcontroller, which is responsible for notifying the customer that unauthorised offers have been discovered on the cloud server used for storing data of theft events.

Table 1.2 represents a comparison between systems according to specific characteristics.

Table 1.2 Difference between characteristics of energy theft detection systems and our system in literature review

Reference	Core hardware device	UIC	Actuators or Sensors	Comm. scheme	Node Type	Tamper detection way and system type	Mess. Protocol
[18]	Arduino	Web page	IR Sensor, Relay	Wi-Fi	Arduino	Connectivity interface check, cloud storage	HTTP
[19]	89C51RD2BN microcontroller	LCD	CT, IR sensor	GSM	SIM300	Current sensing, IoT	SMS
[20]	Local Server	Web page	MOD Bus with meter	Wi-Fi	Esp8266	Current difference, cloud storage	MOD Bus
[21]	VeraEdge Home Control	-	smart plugs	Wi-Fi	Smart plug	Neural network, cloud energy monitoring	-
[22]	ATmega328-8 bit	Mobile app+ LCD	CT, VT and hall sensor	Wi-Fi	Esp8266	Subtraction of currents, Blynk cloud	TCP
[23]	Arduino Mega 2560	LCD	CT	RF 868-MHz	LoRaWAN	Compare of currents, cloud host	MAC
[24]	Raspberry pi	Web page	CT, VT	GSM	Arduino	Current sensing with threshold	HTTP
[25]	PIC16F877	LCD+ Web page	CT, VT	GSM	SIM300	Fuzzy logic, cloud administration data	SMS+ HTTP
[26]	Arduino	Mobile app	CT, VT	Wi-Fi	Wi-Fi Module	Connectivity interface check, cloud host	TCP
[27]	ATmega328P	Mobile app	CT, VT and IR sensor	Wi-Fi	NodeMCU	Linear Regression, cloud storage	TCP
[28]	Arduino	LCD	CT, VT	GSM	SIM 900	Current sensing with threshold, cloud save	SMS
Our system	Raspberry Pi board	Web page+ Mobile app	PZEM-004T	Wi-Fi	NodeMCU	Current difference with detach meters, cloud host and process	MQTT

1.3 Thesis Objectives

The primary ambitions of this thesis are to design systems for DOC as follows:

1. Electric meters and appliances data collection by using a cloud computing platform inside Raspberry Pi.
2. Reducing customer bills.
3. A power factor correction based on cloud computing and neural network serves homes.
4. Using central monitoring for all power factor correction processes.
5. A way for electricity fraud detection and tamper detection of power allows monitoring of the main distribution supply lines with cloud concept.
6. Implementing the systems on prototype AMI system with smart meters.

1.4 Thesis Outlines

Listed below are the chapters of this thesis marshalled as:

- Second Chapter

It explained the theoretical knowledge pertaining to designed systems for power factor correction and electric energy pilferage with cloud computing.

- Third Chapter

It described the design architecture, and operating aspects of all system components, with the appearance of schematics of the blocks systems.

- Forth chapter

It detailed the most significant results of the system and discussed them in comprehensive.

- Fifth Chapter

It offered the findings, conclusions and recommendations for future research that can be conducted under the opinion of the researcher.

2

Chapter Two Theoretical Background for Suggested Systems

Chapter Two

Theoretical Background for Suggested Systems

2.1 Introduction

This chapter concerns the theoretical connotations and crux subjects related to creating cloud systems for data collection and processing for Smart Operation Centre. Furthermore, this chapter is divided to comprehend the technologies and theories of the systems of power monitoring, cloud-based automated power factor correction and larceny revelations of electric energy with cloud computing.

2.2 The Smart Operation Centre

Smart Operation Centre (SOC) system takes and retains data and information and analyses it. It is sometimes using machine learning techniques to output the results like the warning of faults or errors .etc [29]. The Distribution Operation Centre (DOC) is an OC employed by power providers to guarantee energy supply to all system users. For example, DOCs are known for their proactive approach to power quality, which includes planning for and scheduling system events and limiting power usage in times of stress or emergency [1].

The DOC is related to the electric smart grid, where the electric grid is the grid that allows local power plants to distribute electricity to buildings in the region, whether residential or commercial. The upgrade of the previous grid is the Smart Grid (SG), which is composed of many components that connect with one another or with a central control centre via a bidirectional communication route, so the grid can self-monitor for faults and detect when something occurs anywhere within it. Additionally, it enables humans to monitor and respond accurately to problems, such as maintaining and balancing the electric load [30]. Figure 2.1 shows a simplified diagram illustrating smart grid technology.

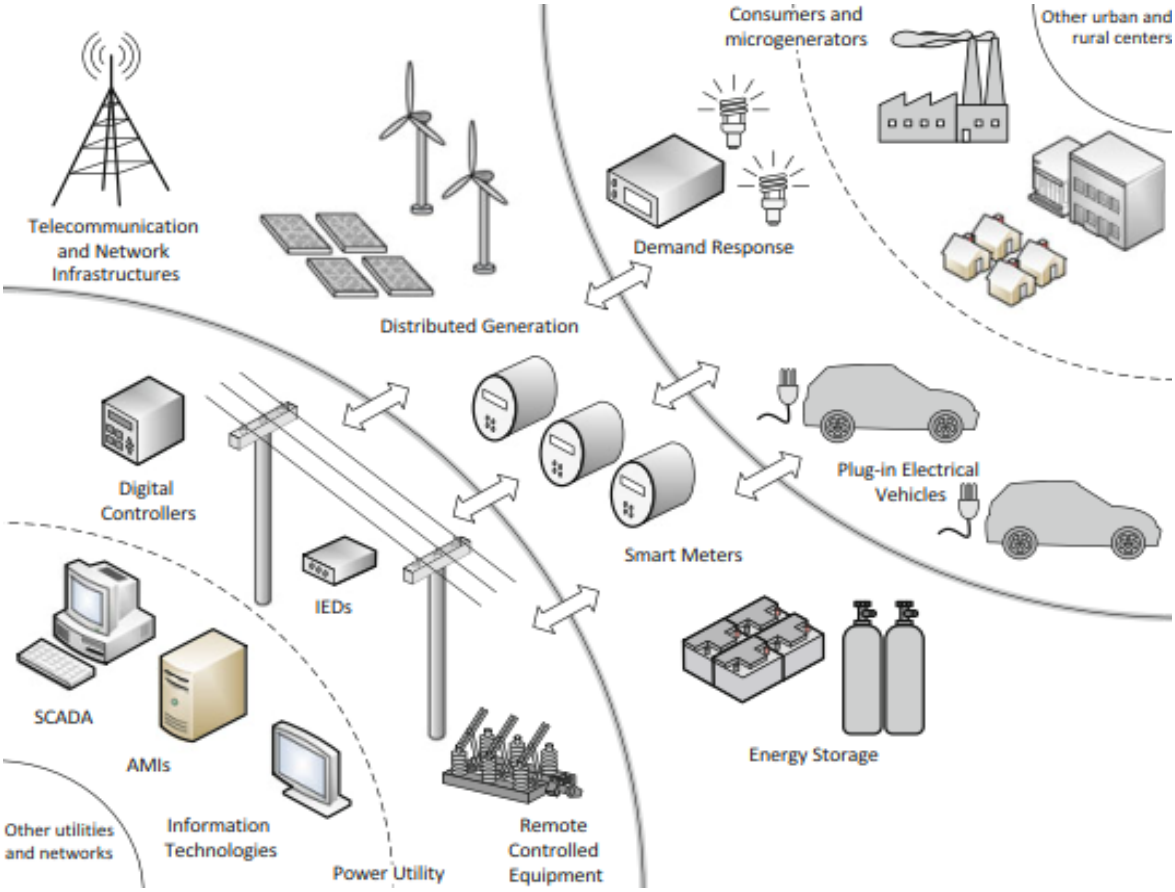


Figure 2.1: Schematic of smart grid technology [1].

The DOC framework comprises a sophisticated networked computer system in which operators and supervisors continually monitor the grid's condition and make system-level intervention choices. An intervention is anything done in the distribution system, such as expanding the network or installing new equipment. The power utility's standards govern the activities in DOC. Furthermore, it may be divided into three categories [1]:

1. Pre-operation: incorporates prior research on the network to enhance its dependability.
2. Real-time operation: incorporates technologies for monitoring energy use (network parameters, line loadings, and faults or errors).
3. Post-operation: this phase entails the compilation of reports and a

database of network events, which enables the development of diagnostics and studies for network enhancement.

2.3 Advanced Metering Infrastructure

The Advanced Metering Infrastructure (AMI) has developed into the primary network, so it is a vital component of the smart grid and is inextricably linked to daily life. AMI rejuvenates the electricity metering system by transitioning to smart meters that enable real-time communication between utility suppliers and energy consumers [31]. Gathering data at each meter enables energy providers and distribution systems to understand better the client behaviour [32]. Figure 2.2 illustrates the AMI principle.

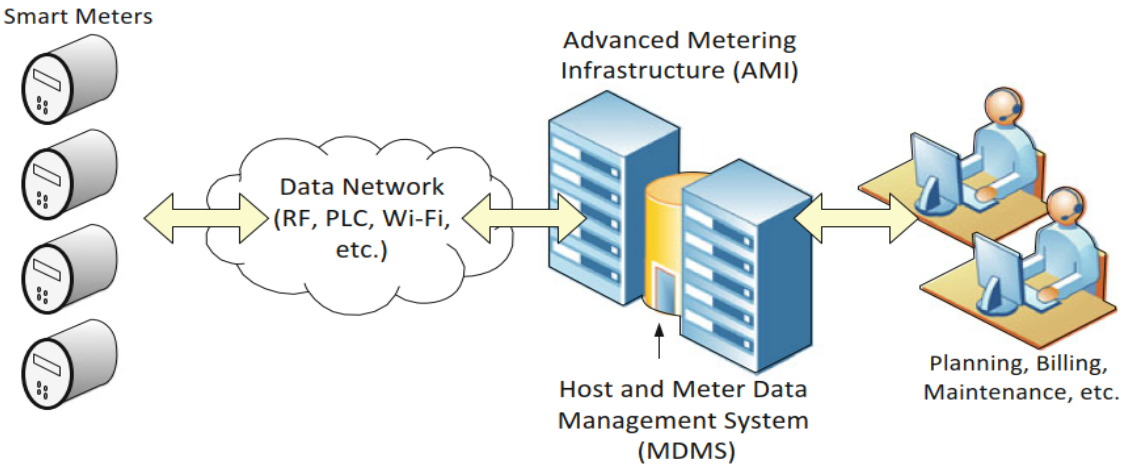


Figure 2.2: Illustration of AMI principle [1].

2.4 Cloud Computing

In the past few years, the change from offline procedures to online ones has occurred in the power systems. Cloud computing (CC) can fulfil the previous requirement [33]. Resource usage and storage capacity requirements grow in modern electrical power systems, accommodating via CC. It incorporates computer resources and virtualisation into a scalable model. CC is integrating power system resources into internal networks, known as 'clouding' them. It can

serve applications in power system analysis, including power flow computation and system monitoring, scheduling, and reliability analysis [34] [35].

Furthermore, CC is a service provided to customers that offer different capabilities like hardware, databases, storage, networks, and software applications [33] [36]. The quantity of data acquired by sensors is tremendous. The experiments emphasise that CC is an excellent solution for processing big data because of the vast amount of data handled with CC; also, it makes it ideal for condition monitoring systems, data-driven and model-based [37].

Further, the cloud platform can use different communication protocols on various devices with different techniques to get different measurements available in the grid [38]. Moreover, CC allows computing resources to be brought together, regardless of their type or the number of resources owned. Virtualisation has transformed the approach of presenting IT services with fewer demands on infrastructure, making IT services easier to introduce [39].

CC services are based on the web and maybe launched with little effort since the services are developed, to be maintained, and paid for easily [40]. Nevertheless, using CC gives significant advantages to many entities, including healthcare organisations, home automation, and innovative home systems [41]. In addition, online cloud systems allow vendors to scrutinise data regularly and fix any equipment that suffers from impairment meet or damage [42].

2.5 Cloud Computing Deployment

Four different models of CC may be used depending on the requirement. Each one has its characteristics. Public, privately owned (Private), or an admixture of the two previously described concepts dubbed Hybrid and district or community [43] [44]. Figure 2.3 states cloud computing models.

2.5.1 Public Cloud

The architecture of this type represents storage and other resources made available to the entire community via a service provider, either for free or on a pay-per-use basis. It is controlled, owned, and operated by a commercial, academic or government entity, or a hybrid of these. inside the public cloud, no

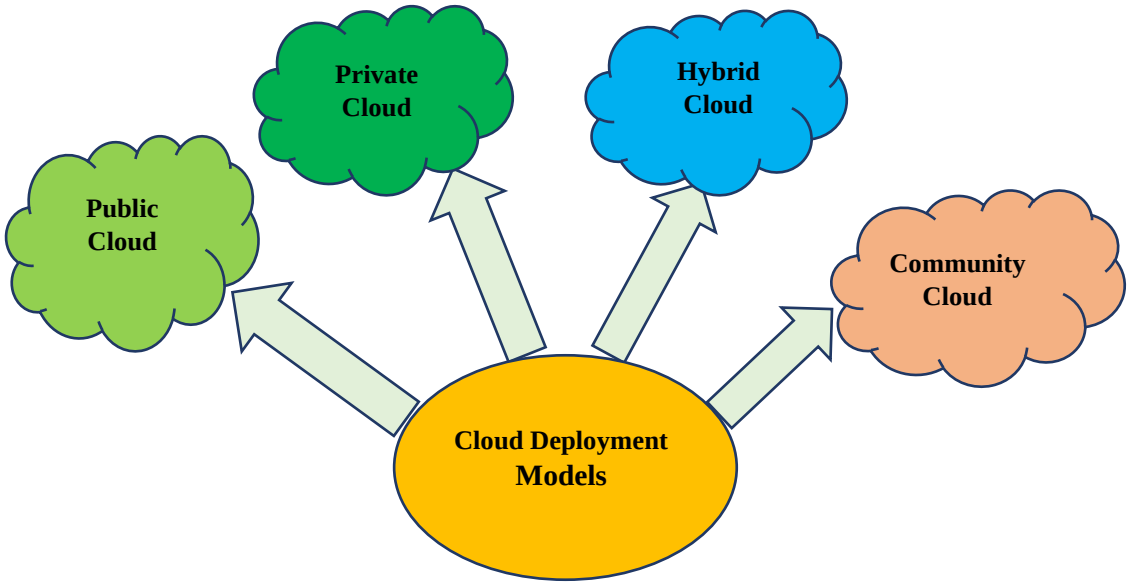


Figure 2.3: Cloud computing models [44].

pre-built infrastructure is required; all resources are ready-made on the cloud provisioner structure. Typically, cloud providers agree on all submissions, and the service provisioner resources are deemed limitless. Amazon AWS and Microsoft Azure are two well-known examples of public clouds. This model has some features [45]:

1. The public cloud services are very scalable; therefore, the supply provisioners ensure that all requirements and demands are met.
2. This cloud genre is cost-effective since users only pay for what they utilise (usually per-hour basis).
3. The public cloud poses a greater security risk because of an external provider.

4. The public cloud is more readily accessible than other models because access limitations related to geography or other factors could exist in this model.
5. The customers have more options because of the public cloud's ability to connect seamlessly with the private cloud. Figure 2.4 depicts an example of public cloud.

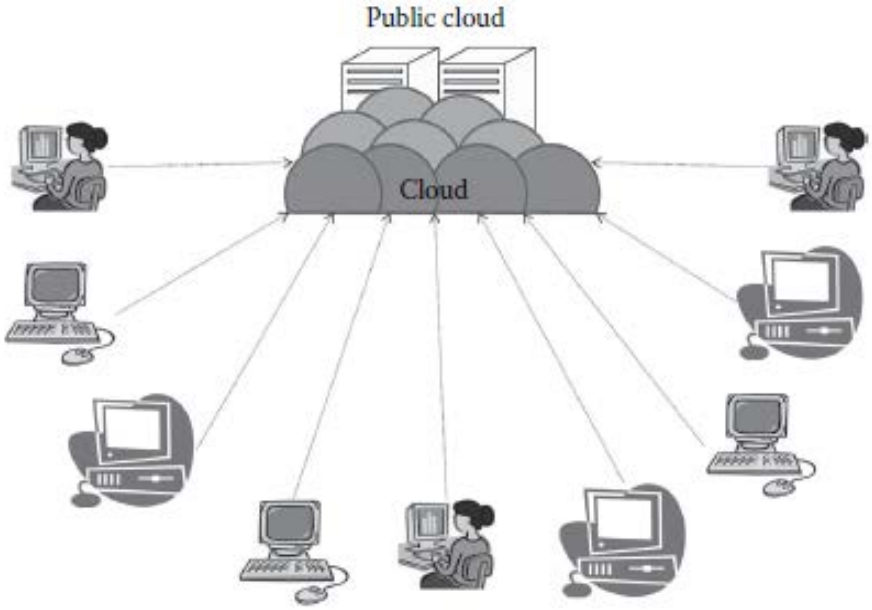


Figure 2.4: Example of a public cloud [45].

2.5.2 Private Cloud

The infrastructure of this genre is dedicated to a single organisation, whether it is managed internally or externally and whether it is hosted internally or externally. As a result, specific organisations can host mission-critical apps on private clouds with slightly fewer security concerns than on public clouds. [46]. Also, it uses a cloud infrastructure only to benefit a single business. Compared to other cloud architectures, this model is relatively modest in size. This model has some features [45]:

1. Private clouds are less vulnerable to data leaks since they are often installed and maintained by the business.

2. Central control: The organisation retains complete control over the cloud since the company often maintains the private cloud.
3. Its resources are less than those in public clouds, providing a higher efficiency level. Figure 2.5 shows an example of a private cloud.

2.5.3 Hybrid Cloud

The third kind combines private and public clouds. The hybrid cloud may be thought of as a private cloud that has been expanded to include public cloud resources; This enables the mixing between public and private cloud's capabilities or characteristics. The features of this type are as follows [46]:

1. Because of the scalability property in the public cloud, the hybrid will have the same property.
2. While the privately-owned cloud is deemed secure, the hybrid cloud also has the same property.

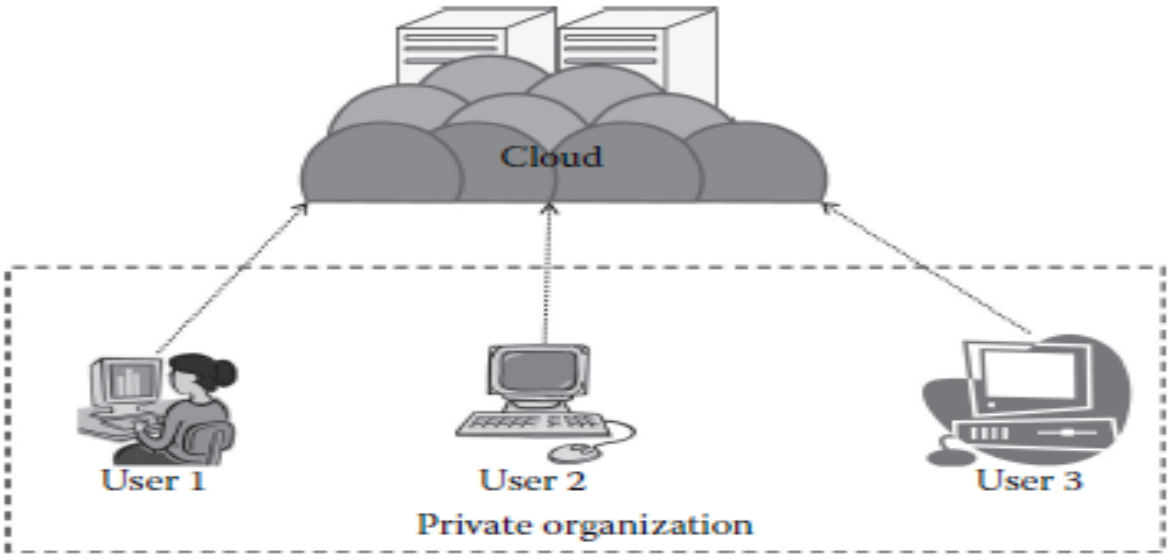


Figure 2.5: Example of a private cloud [45].

3. Compared to private clouds, public clouds are more cost-effective. Figure 2.6 states an example of a hybrid cloud.

2.5.4 Community Cloud

The last cloud type refers to a collaborative effort in which infrastructure is shared among several organisations from a particular community that share common concerns (compliance, security, jurisdiction), whether internally or externally. Also, it is an enhancement to the private cloud. This model has the following characteristics [45]:

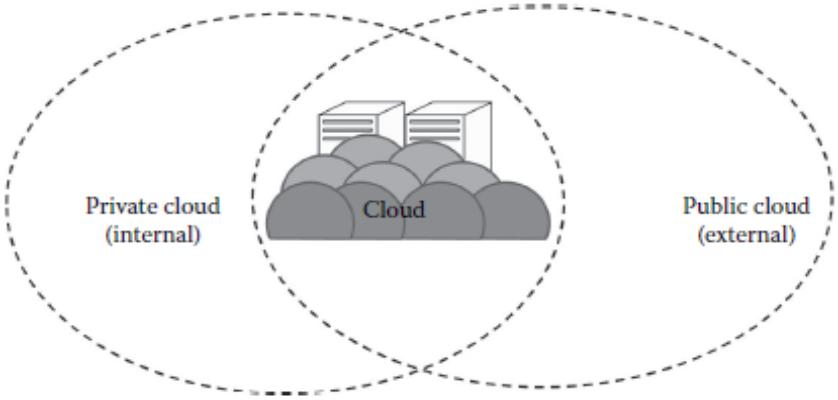


Figure 2.6: Example of a hybrid cloud [45].

1. This cloud model is highly synergistic, with neither party having unique, complete domination throughout the entire cloud.
2. It is less expensive to use this type because several companies share the entire cloud. Figure 2.7 shows an example of a community cloud.

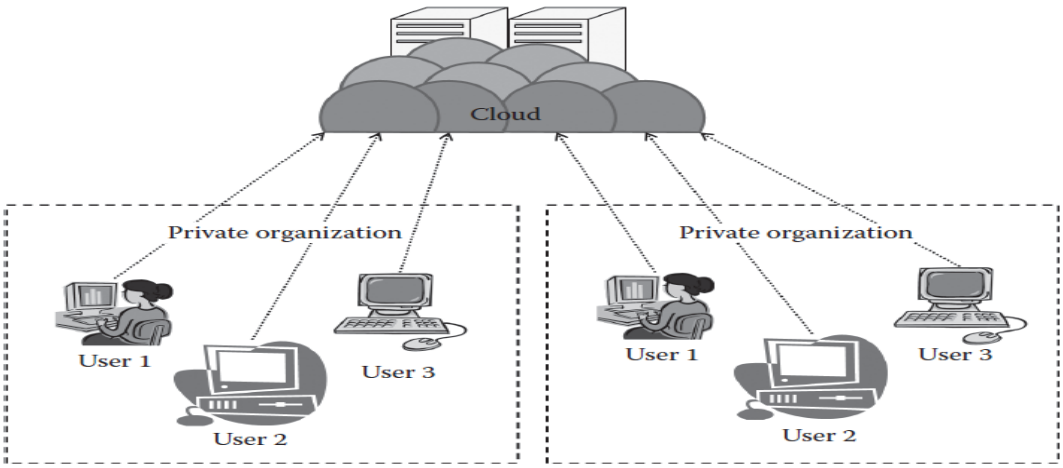


Figure 2.7: Example of a community cloud [45].

2.6 Cloud Computing Services

In addition, there are three different sorts of cloud computing services as follows [33] [44]:

2.6.1 IaaS (Infrastructure as a Service)

This service makes the consumer capable of deploying and running arbitrary software. The supplier provides capabilities such as provision processors, storage, networks, and diverse core computing supplements. The client controls the operating systems, storage, applications, and networking hardware, but they do not manage or control the underlying cloud infrastructure. [44].

2.6.2 PaaS (Platform as a Service)

This kind describes applications built using a specific development platform deployed in the cloud and hosted by the cloud service provider. For example, customer application support is only provided in the dedicated environment. In addition, the (PaaS) environment offers both a foundation of operating and development environments and an infrastructure to deploy the apps. However, the customer controls the installed programmes and presumably the configuration parameters for the application-hosting environment, not the underlying cloud infrastructure. The PaaS supplier offered networks, storage space, and servers, overseeing scalability and maintenance [33].

2.6.3 SaaS (Software as a Service)

The last providers' service can utilise the providers' applications hosted on a cloud infrastructure. The apps are available via a soft client interface, such as a web browser (e.g., e-mail based on the web) or a program interface from various client devices. The substrata cloud infrastructure is not managed or

controlled by the client. Customer relationship management (CRM), intelligence business analytics, and software for online accounting are all common examples of programmes available as a service [45]. Figure 2.8 depicts cloud computing services.

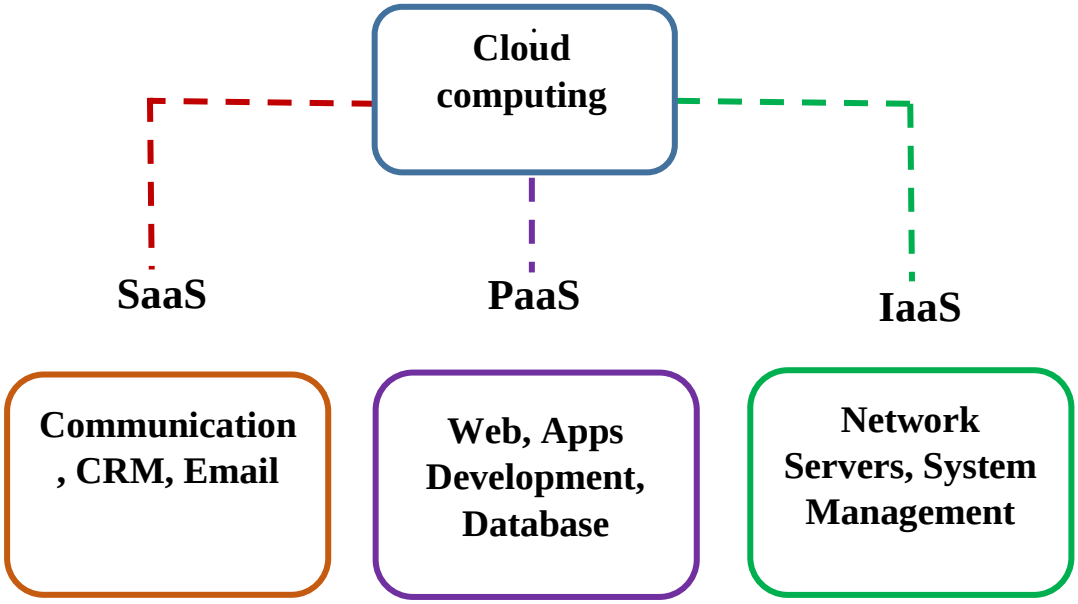


Figure 2.8: Cloud computing services [47].

2.7 The Architecture of the Cloud

There is a hierarchical perspective of describing the technology in every model, so the cloud has an architecture that outlines how it works. Figure 2.9 depicts the architecture. Four tiers of classes are found in this architecture dependent on the user to cloud access, and they are listed below [45].

2.7.1 Consumer Layer

This layer is the location from which the user establishes the cloud connection. Any device is regarded as a client, including a thin or slim client, a thicky client, or any portable device like a mobile that supports simple web app functionality [48].

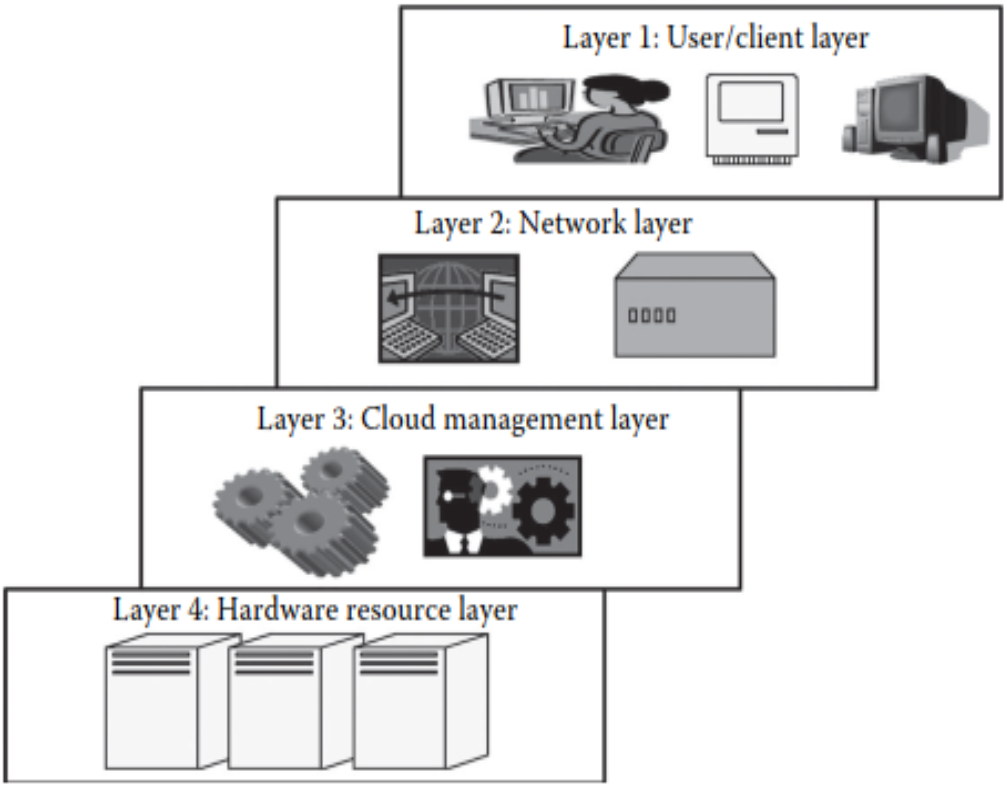


Figure 2.9: Cloud architecture [45].

2.7.2 Network Layer

This layer facilitates users to the cloud communication. The entire architecture cloud relies on this communication, which is used to deliver services to clients. When customers connect to a public or private cloud, they require a minimum amount of bandwidth, which is occasionally determined by the cloud provider [45].

2.7.3 Cloud Management Layer

This layer is comprised of software applications that control the cloud. The cloud's operating system (OS) is software which serves as a conduit between physical resources and the user. This software enables resource management, server storage optimisation, and internal cloud governance [49].

2.7.4 Hardware Resources Layer

The fourth layer comprises physical hardware resources, a collection of hardware resources connected and comprises the present configuration system [45].

2.8 Mobile Cloud Computing (MCC)

At the most fundamental stage, mobile cloud computing indicates an infrastructure where data processing and storage occur farther from the mobile device. MC applications offload processing power and data storage away from mobile phones and the cloud, presenting applications and mobile computing to a larger circle of mobile subscribers than smartphone users [45].

Moreover, MCC is essentially the nexus between CC and mobile networks. In essence, mobile networks are communications systems linking users of mobile. The advent of these ultrafast networks necessitates the integration of the cloud and networking domains of mobile. Therefore, MCC essentially facilitates the development and hosting of cloud-based mobile applications [50]. Numerous cloud-based mobile applications are available; the most popular are Google Gmail and Voice for iPhone. Figure 2.10 illustrates a general diagram of MCC [45].

2.9 Parallel Computing

This computing type is a collection of units that homogenously process data that collaborate and communicate to solve complex computational problems more quickly. A typical architecture computer consists of a memory sharing, symmetrical multi-processor, a dense machine with distributed memory, and a free linked cluster of distributed workstations. In addition, symmetrical programmes are frequently required to address computational issues [45].

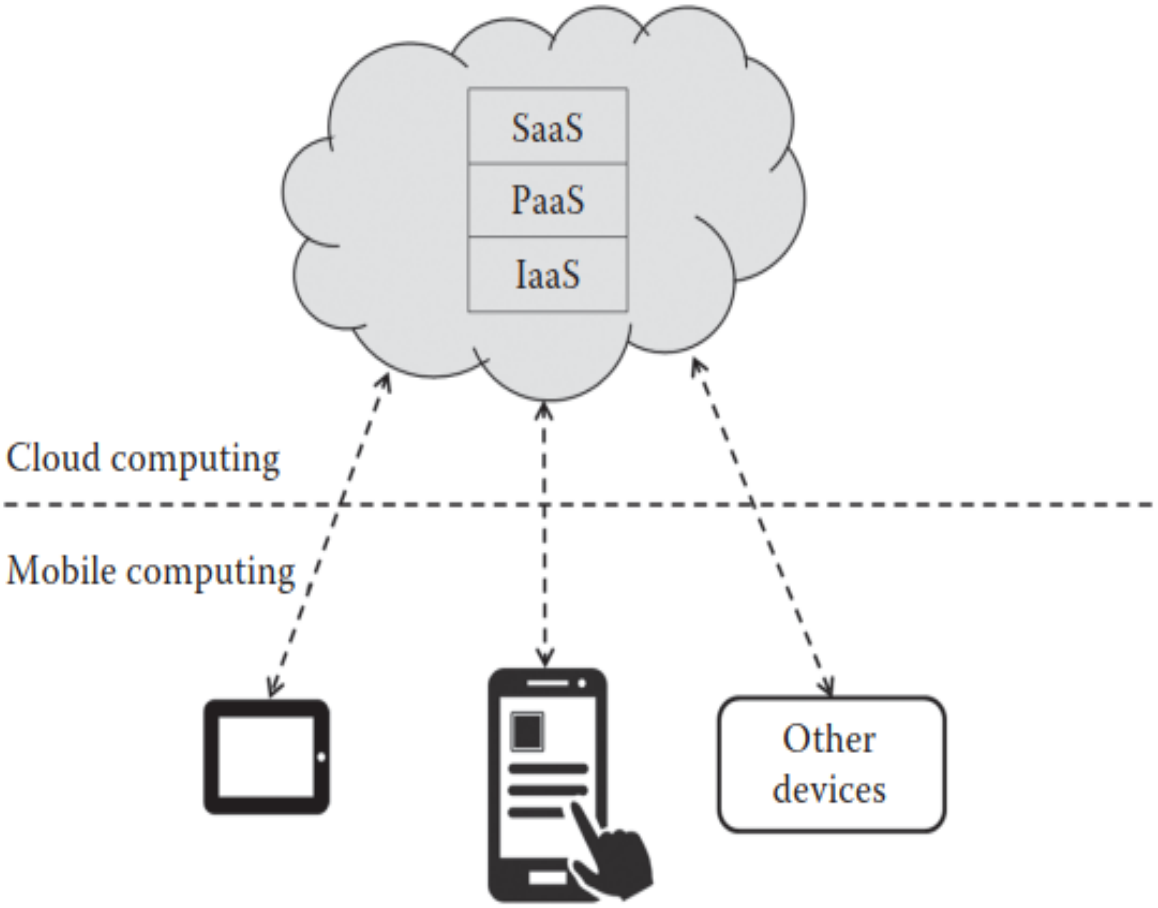


Figure 2.10: A general diagram of MCC [45].

Parallel computing might be considered a critical component of the cloud ecosystem. Like Cloud computing, the modern world is based on a network of supercomputers to assist customers with parallel computing. However, Cloud computing and classical parallel computing have substantial distinctions.

In contrast, CC must deliver a high-quality service environment to millions of various tiers of apps, enhance responsiveness in response according to user requirements, and since CC resources are distributed more widely across several different geographic sites than parallel computing [51].

2.10 Grid Computing (GC)

This type of cloud is the method of computing on a distributed basis. GC

technology combines servers, storage, and networks scattered over the entire network to produce an inclusive, integrated system that provides clients with high-performance processing and storage. Therefore, GC seems a powerful virtual machine for end-users in the grid or applications [51].

Cloud computing and grid computing have pursued similar goals: lowering computing costs while increasing flexibility and reliability. However, they differ in security, scalability, and coordination [52].

2.11 Reason for Cloud Computing

Many reasons encourage to use of CC [45]:

1. Cost optimisation is the primary objective, as cloud computing is based on the "pay as you go" approach.
2. Enhanced mobility, ease of use, optimal resource usage, and application portability. This enables users to effortlessly access information from any location without consuming valuable or unnecessary hardware resources.
3. Savings on expenses, remote workplace productivity, flexibility and future-proofing.

2.12 Pervasive Computing, IoT and Cloud Computing

Pervasive computing is a term that refers to a collection of technologies, including internet capabilities, networking, artificial intelligence, and wireless computing, that enable computing to take place everywhere. With embedded technology and connection, pervasive computing devices simplify the computing tasks. The replacement of older electric meters with smart meters is an example of an actual implementation of pervasive computing. The Internet of Things is comprised of pervasive computing [45]. The Internet has evolved into a network of all types and sizes of devices, including cars, smartphones, appliances,

cameras, and medical instruments, and it has expanded to include animals, people, and buildings. These devices communicate and share information according to predetermined protocols to achieve real-time online monitoring and upgrade [53].

Cloud computing and IoT integration would provide more storage and other significant benefits to many IoT applications. In addition, it represents an excellent solution for processing big data [54] [37]. The cloud computing and IoT architecture are illustrated in figure 2.11.

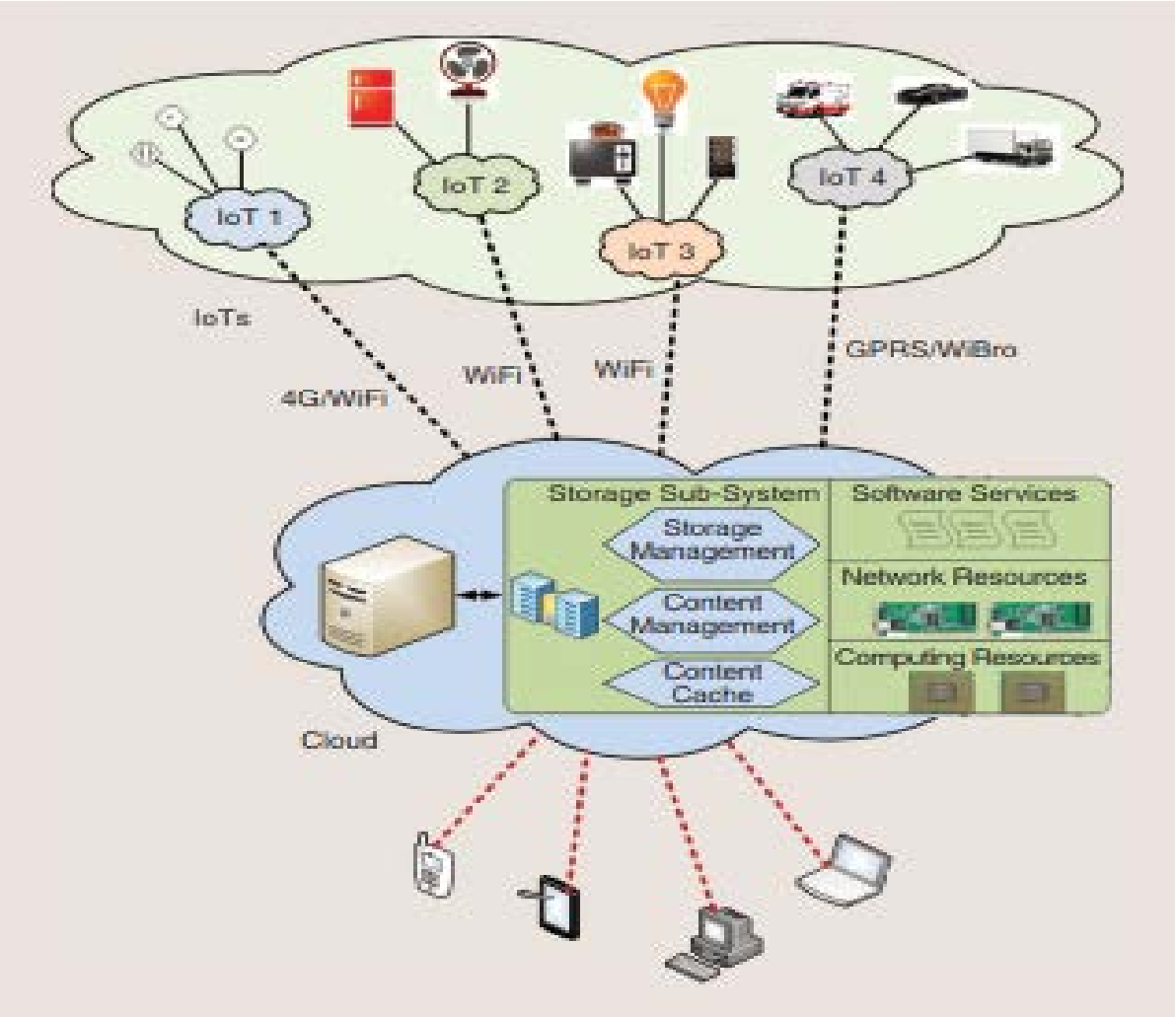


Figure 2.11: Cloud computing and IoT architecture [53].

2.13 Communication Protocols for Cloud Computing

Cloud layers support communication protocols, such as MQTT (Message Queuing Telemetry Transport) and HTTP (Hypertext Transfer Protocol) [55].

2.13.1 HTTP

Client-server models are the foundation of the web, and this protocol makes it easy for web developers to operate with the current network infrastructure. The HTTP/1.1 protocol is currently the most extensively used. The server will provide a response message with the requested resource if the request is accepted. Also, this procedure is known as request/response messaging, and it is used to communicate between clients and servers [56], as seen in figure 2.12 for the HTTP request/respond model.

The activities for generating, updating, reading, and removing coincide with the HTTP POST, GET, PUT, and DELETE techniques. The type is arbitrary because the data presentation is not predefined, with JSON and XML being the most prevalent. IoT generally adheres to the JSON over HTTP standard [55].

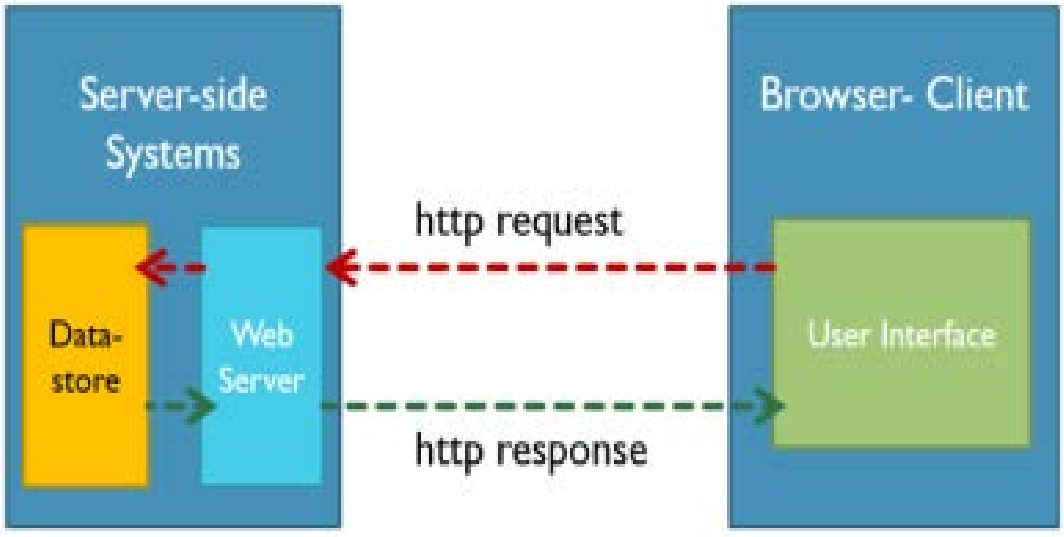


Figure 2.12 : The HTTP request/respond model [56].

2.13.2 MQTT

This lightweight messaging protocol adheres to the publish-subscribe paradigm, particularly well-suited to resource-constrained devices and less-than-optimum network connection circumstances, like little bandwidth and elevated latency. IBM developed MQTT and included two communication parties that typically act as publisher and subscriber users and servers/brokers.

Hence, clients are a device that can either publicise messages or subscribe to accept them. Further, a client subscribes to the particular subject for receiving communications related to that topic. However, other clients can subscribe to the same topic and receive notifications from the broker when new messages arrive [56] [57]. Figure 2.13 depicts the MQTT protocol model.

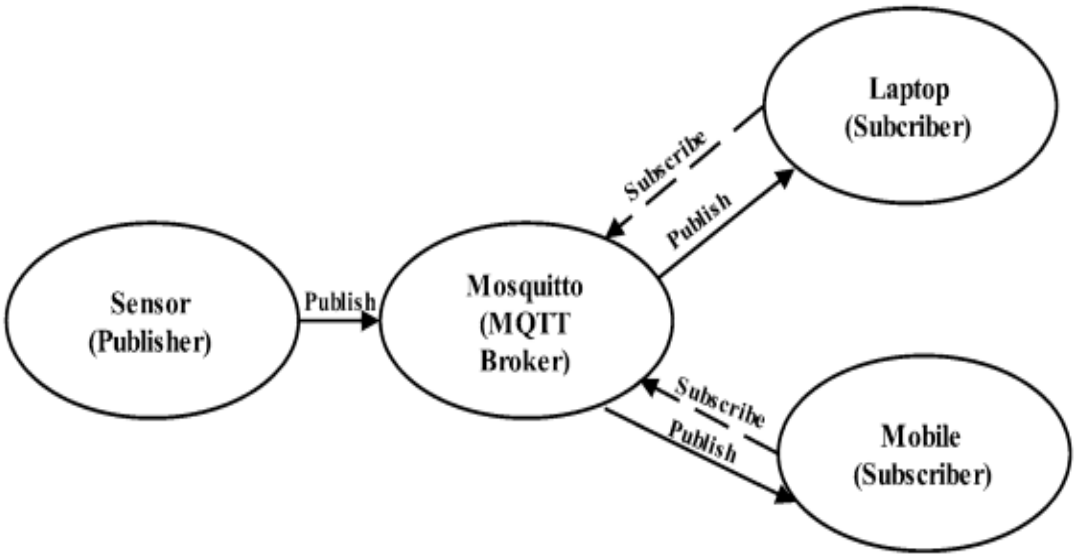


Figure 2.13 : MQTT protocol model publish /subscribe [57].

2.14 Tools for Smart Environment Technologies

Several technologies related to the smart environment, including the following [58] [59]:

2.14.1 Internet Protocol (IP)

It is a master networking protocol and unique number identification issued for networking devices that employ it as an address for communication. Host or network identification and geographic coordinates are two of the essential purposes of an IP address. IPv4 and IPv6 are two different versions of the IP, so each variant's IP addresses are distinct [58]. Figure 2.14 states the IP v4 protocol.

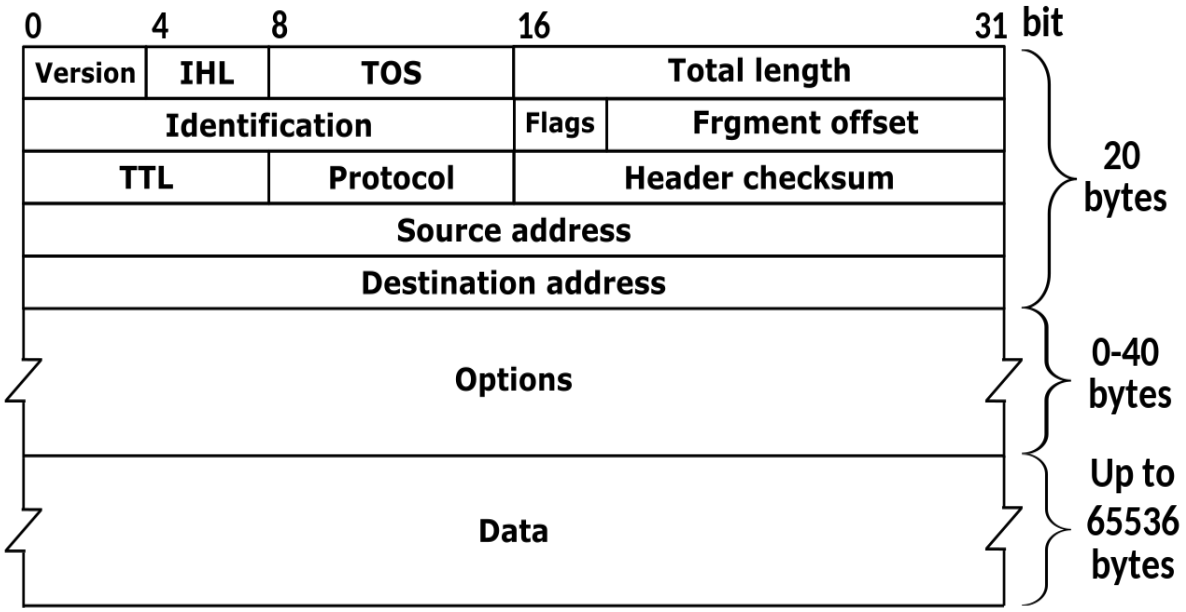


Figure 2.14: IPv4 protocol [58].

2.14.2 Wireless Fidelity (Wi-Fi)

By using Wi-Fi, computers and other devices may communicate through a network. Incorporating Wi-Fi into a wide range of everyday devices, such as smartphones and tablets, has increased Wi-Fi reliance to the point that it makes it a standard feature in these devices. The important versions of Wi-Fi are: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11af and 802.11ah. Also, the common frequencies used are 2.4,5 GHz [58]. Figure 2.15: states the relation between layers and protocols, and techniques.

2.14.3 Global System for Mobile (GSM)

In mobile telecommunications, GSM was the standard for second-generation digital cellular networks used to employ mobile phone devices, and

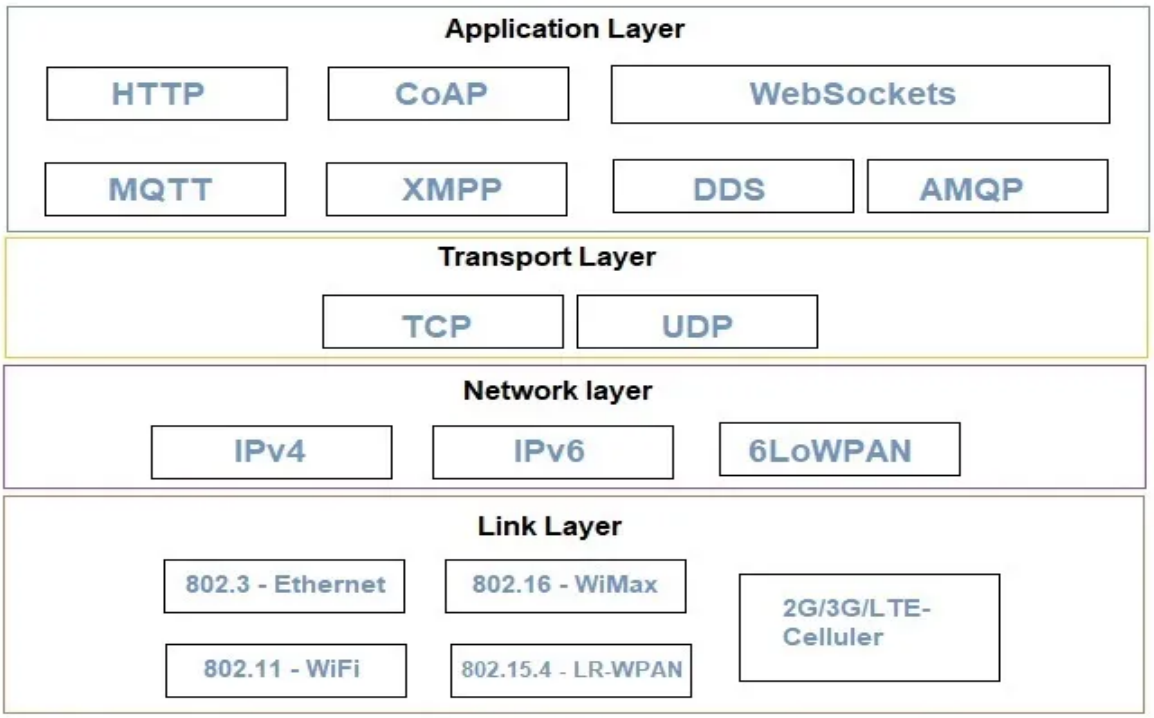


Figure 2.15: Relation between layers and protocols and techniques [58].

this expression refers to the protocols that employ a circuit switching mechanism for voice telephony by full-duplex; hence, TDMA technology employs spectrum sharing. GSM supports micro and macro cells, in addition to umbrella type. The comparable bands of 900 MHz and 1800 MHz are used by these networks [59].

2.14.4 Sensor Networks

It is a critical IoT aspect in which several autonomous devices are physically deployed. In the IoT, devices use sensors to detect various conditions such as warmth, object compression, object motion, vibrations, and electric current. These sensing tools are embedded in or attached to IoT objects to collect information about them [58].

2.15 Cloud Computing and Raspberry Pi

Raspberry Pi is an economical price computer the size of a hand palm. It can function as a full-fledged computer or a low-cost microprocessor, and with this small device, one can design and implement a variety of applications and prototype models with excellent programming capabilities. For example, Raspberry Pi can be used with a message broker like MQTT to collect and upload data as a cloud server [60]. The Raspberry Pi device is shown in figure 2.16. Other data sheet information and specifications are shown in appendix A-1. Additionally, this compact single-board computer is suited for various application domains, including private clouds and edge computing in a cruel ambience [61]. Also, It is used as an auxiliary features device with a supported operating system to create containers and virtual machines on-demand [62].

Further, it may be utilised as a cloud computing fog node and fog service, which could be exploited to reap the benefits of cloud computing [63] [64].

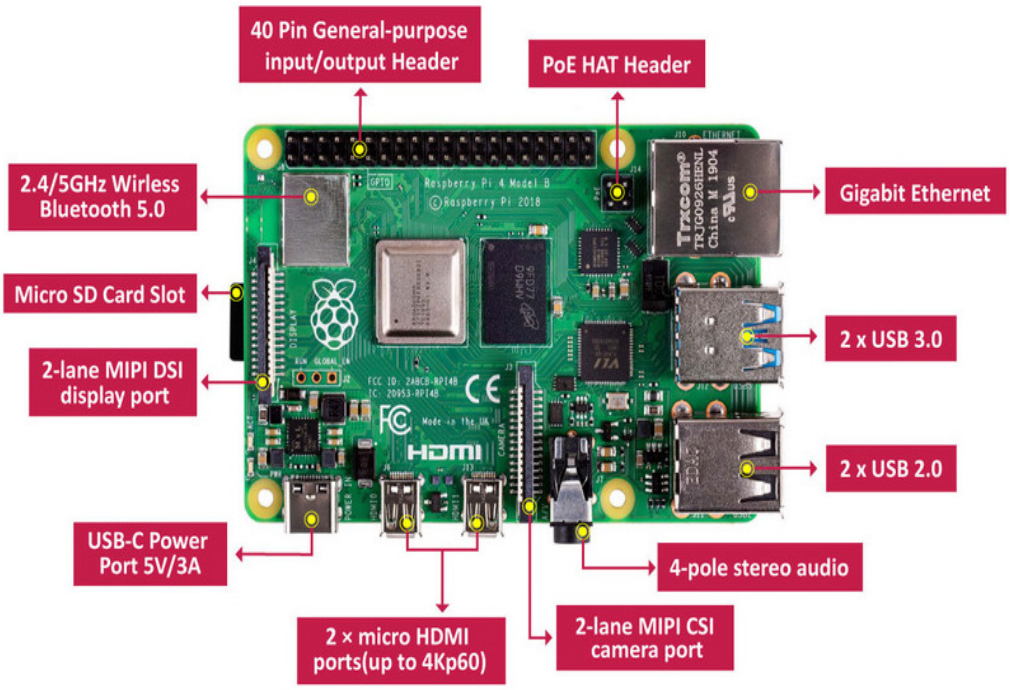


Figure 2.16: Raspberry Pi device [60].

Furthermore, on the server-side or in the cloud, it can run applications in Platforms as a Service (PaaS) [65]. Moreover, A Raspberry Pi can be used to create a private cloud server that can be used to store real-time signals. Thus, it provides cloud computing infrastructure via platforms offered by individual cloud vendors. Analogue signals from environmental sensors are used in real-time measurements. These signals are converted to digital using microcontrollers such as Arduino, analogue to digital converters or other devices, and then sent to the Raspberry Pi cloud server, which can be utilised as a storage device or server for real-time apps [66].

2.16 Smart Metering

Due to the increased use of the smart grid, the smart metering and communication systems employed in it are being intensively explored. While monitoring and control methods are widely employed in industrial systems, the energy management requirements for individuals will accelerate the growth of the smart grid [67]. Figure 2.17 depicts an example of a KWH smart meter.

AMI systems based on smart meters address the shortcomings of traditional electromechanical meters that were previously used to calculate long-term usage. Smart meters' remote monitoring and robust communication capabilities enable distribution system operators to make fast measurements for identifying demand rates and optimising particular demand-side management programmes for individual customers [68]. Figure 2.18 comprises the framework for metering and communication. The communication backbone of AMI comprises wired and wireless communication technologies such as Wi-Fi and GSM. Gateways in local area networks and routers in wide area networks handle the infrastructure. In addition, these communication systems can establish connections to sensor networks [67].

Figure 2.17: Example of a KWH smart meter [67].

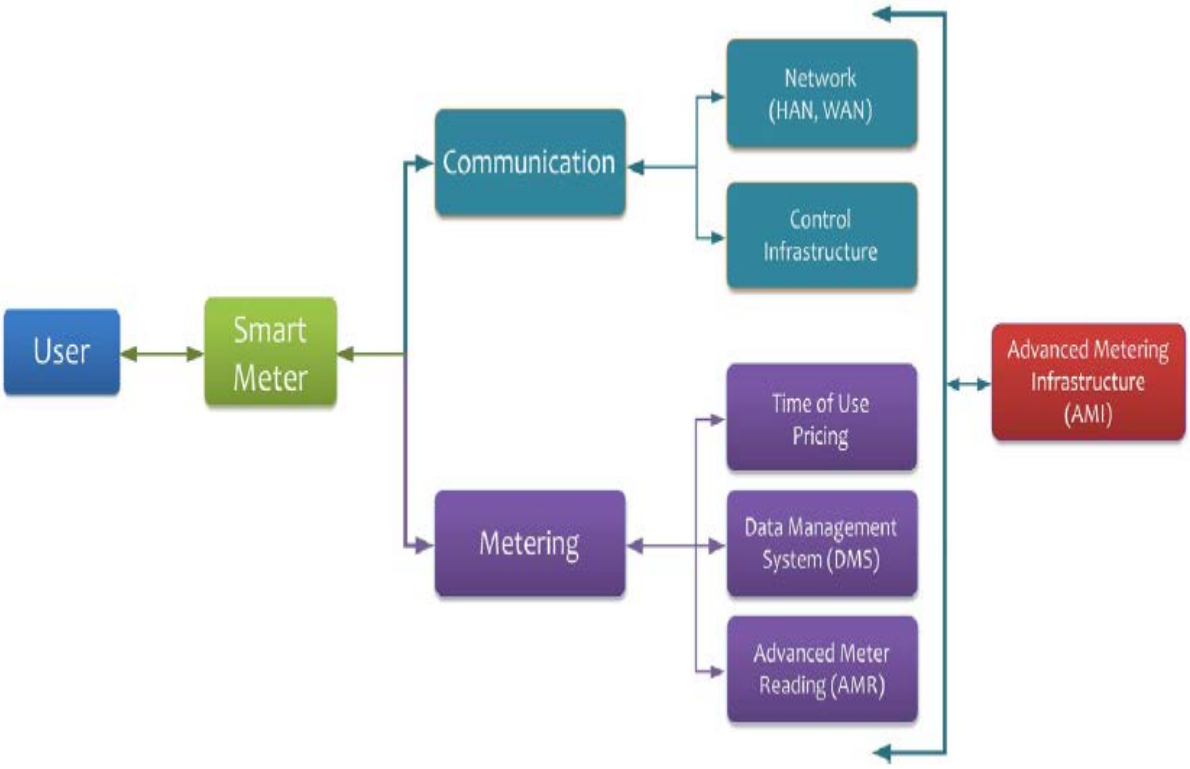


Figure 2.18: A framework for metering and communication [67].

2.17 Smart Meter Energy Sensors and Wireless

With the aid of sensors, the smart meter and its technology are growing fastly. Today's smart meters require sensors to assist in performing various beneficial and necessary duties, but these meters increase complexity. Otherwise, they make the system more intelligent, dependable, and cost-effective [69].

In addition to current and voltage sensors, smart meters may have accelerometers, Hall sensors, anisotropic magnetoresistance sensors, and passive infrared sensors. These sensors enable the meter to add new functions such as tamper detection, hide the switch of changing the meter's operating modes, and improve existing functions' reliability, size, and cost-effectiveness [69]. Some of the essential tools and sensors for prototype smart meter are:

2.17.1 PZEM

It is a module used for electrical parameters such as voltage, current, connected load, total energy consumption, frequency, and power factors. It also features a power button clear function and a power-down data storage function (accumulated power down before saving). Moreover, serial communication is also supported with serial TTL interface, via multi terminals communicate with the adapter plate, read, and set the parameters. In addition, this module comes with a spread current sensor of 100A.

It has more than one model as PZEM-004T V1.0 and PZEM-004T V3.0. Also, it can be used as a prototype smart meter. Other data sheet information and specifications are shown in appendix A-2 [70]. Figures 2.19,2.20 illustrate the mentioned module.

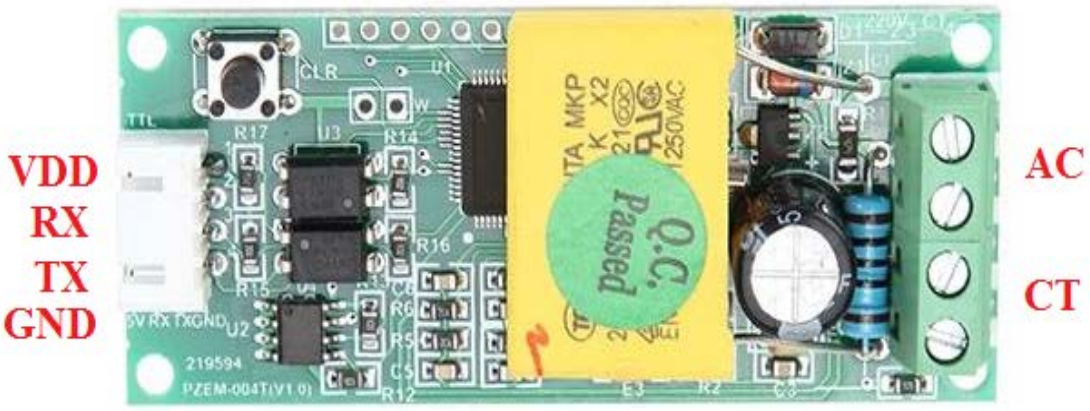


Figure 2.19 : PZEM-004 module [70].

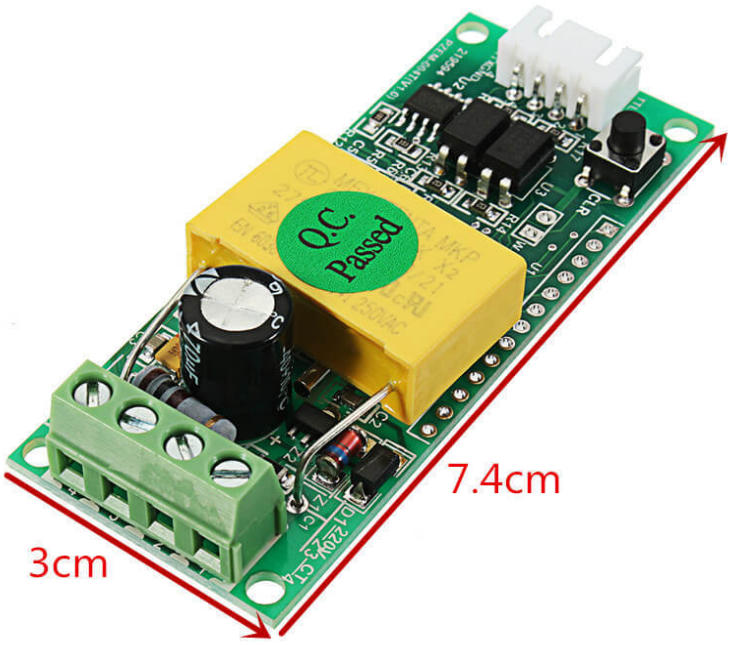


Figure 2.20 : PZEM-004 module dimensions [70].

2.17.2 NodeMCU

The NodeMCU (Node Micro Controller Unit) is an open-source software and hardware development environment centred on the ESP8266, a low-cost System-on-a-Chip (SoC). The ESP8266, developed and manufactured by

Espressif systems, includes all of the essential components of a computer as CPU, RAM, networking (Wi-Fi), and even a current operating system and SDK. As a result, it is a fantastic solution for all types of IoT projects [71].

Furthermore, the integrated Wi-Fi networking solution enables it to host the programmer or offload all Wi-Fi networking activities to another application processor. The ESP8266 NodeMCU's robust onboard processing and storage capabilities enable it to be integrated with sensor-specific devices via GPIOs with minimal development and runtime loads [71]. Figure 2.21 states the NodeMCU kit. Other data sheet information and specifications are shown in appendix A-3.

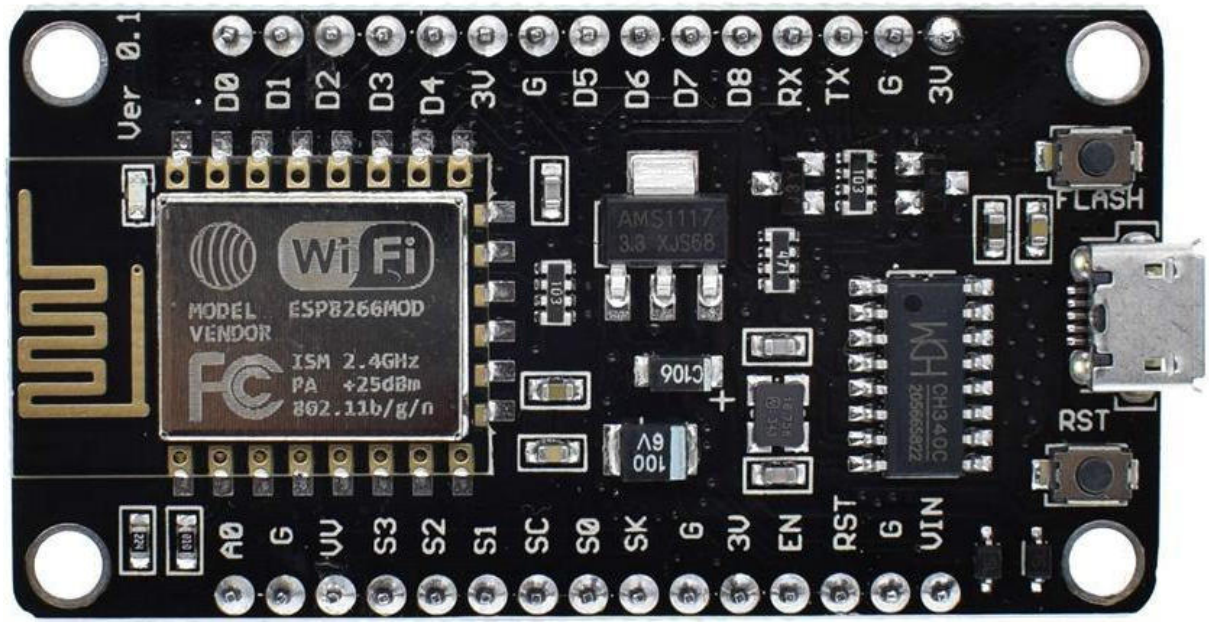


Figure 2.21 : The NodeMCU kit [71].

2.18 Technical and Non-Technical Electric Losses

Losses of energy in electric power distribution are a natural part of the service. They occur for various reasons like physical phenomena caused by the current electricity inflow or other considerations like feeble monitoring tools of

electricity companies or illegal consumer behaviour. Therefore, losses in electrical power can be categorised in this manner following their source: technical or non-technical losses [72].

2.18.1 Technical Losses

Technical losses are associated with energy losses in the various components. The energy is lost from the generation to end-users. Although removing these losses is difficult since the underlying physical phenomenality. Also, their decrease is an ongoing aim for distribution system optimisation studies. The construction of power factor adjustment algorithms to low voltage network loads is an aspect that has a significant effect on how technical losses are affected. Technical losses are caused by current passing through an electrical network and include the following types [73]:

1- Copper losses are caused by inherent in all inductors due to conductors limited resistance.
2- Dielectric losses are losses caused by the heating action of conductors on the dielectric material.
3- Losses due to induction and radiation caused by electromagnetic fields encircling conductors.

Furthermore, technical losses are calculable and controllable in the presence of known loads in the power system in question. Technical failures can be attributed to the following factors: Disturbance of Harmonics, inadequate grounding at the consumer end, extensive single-phase infrastructure, and losses incurred due to overloading and insufficient voltage.

2.18.2 Non-Technical Losses

These types of losses were calculated as the difference between total and

technical losses, representing energy distributed and expended but do not generate profit for electric companies because of various aspects. It includes theft, fraud, measurement errors, billing errors, and utility consumers who do not own meters. In addition, non-technical losses can be caused by a variety of factors as [73]:

1- Consumption readings were reduced by tampering with meters.
2- The errors were caused during the calculation of technical losses.
3- Bypassing the meter or illicit connections by hooking up to line wires.
4- Erroneous readings by meter readers or delays in meter reading and invoicing and faulty or unmetered energy places.
5- Customers refuse to pay the bill (unpaid bills).

2.19 Power Factor Correction

The power factor is defined as a voltage-versus-current phase shift in AC systems. Reactive power (Q) and power factor can affect whether the system contains a capacitive or inductive load. According to the capacitive or inductive load, the power factor may be lead or lag. On the other hand, an inductive load proposes a lagging power factor due to the retardation current, which may be compensated by switching a suitable capacitance to the system. In contrast, a capacitive load suggests a leading power factor, which may be treated by adding equivalent inductance, as shown in figure 2.22 of the power triangle [74].

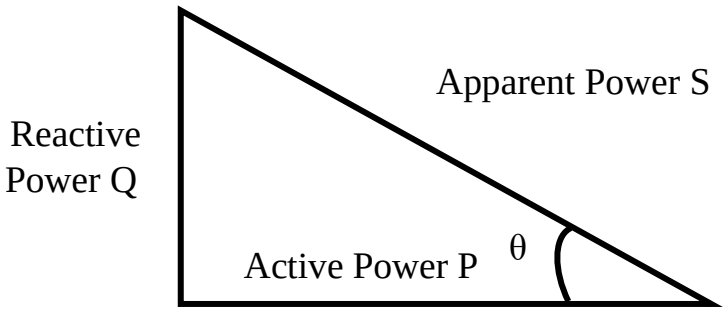


Figure 2.22: The power triangle [74].

The Power Factor (PF) also is defined as the ratio of real or active power (P) to apparent power (S). It refers to the electrical systems' ability to convert electrical current into practical work such as heat, spinning devices, or light, as in equation (2.1).

$$\mathrm{PF} = \frac{\text{Active power (P)}}{\text{Apparent power (S)}} = \cos\theta \qquad \ldots\ldots\ldots \quad 2.1$$

The PF value is between 0 and 1 and indicates whether the load is resistive, inductive, or capacitive. When the power factor is equal to one (cos θ =0), maximum power transfer occurs. If the current exceeds voltage by -90^{o}, the load is entirely capacitive. Whereas if the current is 90^{o} phase behind the voltage, the load is entirely inductive. Most electric loads have inductive nature, which means they produce a lagging power factor so that it creates a rise in the current that flows and eventuates in extra loss of the active power; hence it escalates the overall loss of power in the system [8]. For this reason, maintaining the power factor as near to unity is crucial. [75].

The capacitance bank installed parallel to the load, which provides this reactive power, is the standard method for power factor correction. Also, there are other ways like the synchronous condensers, which are three-phase synchronous motors with no load attached to their shaft. The phase advancers are another AC exciter used to improve the PF of an induction motor in industrial use [74]. The power factor adjustment has the following advantages [10]:

1- Power consumption is reduced by increasing energy efficiency, resulting in an environmental gain. Less demand equals less greenhouse gas emissions and fossil fuel depletion from power plants reducing monthly electric bills.
2- It plays a role in minimising copper distribution equipment losses which minimising the voltage drops.

3- Overall electrical equipment and components life is extended.

As mentioned previously from the power triangle, the power factor depends on S, P and Q, so to correct the lagging power factor, capacitance (C) or Q needed to be added to decrease the angle. So, according to the following equations, the PF can be corrected [9] [74].

$$P = S * \cos\theta \ , Q = S * \sin\theta \quad \ldots\ldots\ldots \quad 2.2$$

$$\tan\theta = \frac{Q}{P} \quad \ldots\ldots\ldots \quad 2.3$$

$$\Delta Q = P\,(\tan\theta_1 - \tan\theta_2) \quad \ldots\ldots\ldots \quad 2.4$$

$$\Delta C = \frac{Q}{2\pi\, f\, V^2} \quad \ldots\ldots\ldots \quad 2.5$$

Where f is the frequency, V is the phase voltage and $\cos\theta_1, \cos\theta_2$ is old and required power factor, respectively.

2.20 Electric Energy Larceny

Electricity larceny or theft is one of the issues confronting some power companies; it renders the infrastructure necessary for proper operation unsustainable, as power companies suffer from losses. Confident electricity consumers receive extreme bills for energy spent, while others may tap directly into the distribution network or circumvent their prepaid meters. As a result, most electric power distribution companies must maintain loss control [18].

Electric energy larceny is not a new thing; it is a complicated and multifaceted subject. Power theft is widespread in several nations, and a significant extent of energy is lost yearly from the low voltage distribution network. Moreover, due to the massive number of distributed endpoints, mainly unmonitored in publicly accessible locations, an electric distribution company

will never be immune to pilfering or fraud [76].

Several electric companies implement targeted strategies to cut energy losses on low voltage grids. AMI systems are one of the most critical factors in a successful ability to decrease non-technical losses associated with pilfering or fraud [77]. There are two distinct types of theft and fraud that often occur in all low voltage power grid systems [76]:

1- Fraud occurs when a consumer intentionally attempts to defraud the electric company. A widespread conventional habit is to modify or physically tinker with the meter to display lower power usage readings than is the situation in reality. There are some ways of tampering. One of them is magnetic tampering which is done by attempting to alter consumption behaviour through a magnet. Another one is meter swindling, which is done by transferring smart meter content housing to another faulty one and substituting it with non-authorised meter hardware, like inserting a resistance into the meter measurement via wiring that allows the consumption computations to be slowed down. Figure 2.23 states an example of magnetic tampering.
2- Electricity larceny can be accomplished via direct energy source line wiring to the desired area needing electrical power installation, circumventing the meter. Customers whose primary target do electricity larceny are known as bypassers. The resources and motive for tampering with analogue meter systems are highly detected in some utilities.

Reduced power theft and its containment are more likely to succeed in systems with a strong governance culture. This is because theft reduction systems seek a good environment to initiate and operate. Figure 2.24 depicts an example of a direct connection to the service line.

Figure 2.23: Example of magnetic tampering [78].

Figure 2.24: Example of a direct connection to the service line [78].

2.21 Neural Networks

The architecture of an artificial neural network (ANN) architecture is a computational model for biological neuronal, like those found in the human cerebrum. Natural neurons receive signals through synapses located on the dendrites or membrane of the neuron. When the signals received are strong enough (surpass a certain threshold), the neuron is activated and emits a signal through the axon. This signal might be sent to another synapse and activate other neurons [79].

Likewise, ANN consists of inputs (like synapses) multiplied by weights (strength of the respective signals) and computed by a mathematical function that determines the neuron's activation. Another function (which may be the identity) computes the output of the artificial neuron (sometimes in dependence on a certain threshold). ANNs combine artificial neurons in order to process information. ANN has the capability of simulating complex non-linear interactions. Additionally, the ANN is highly fault-tolerant, quick, and scalable because of its parallel processing [80]. Most aspects of neural networks are node identifiers, network architecture, learning rules and backpropagation training.

2.21.1 Node Identifier

Each node or cell receives various inputs from neighbouring nodes via connections with corresponding weights that correspond to the synaptic strength. Whenever the weighted summation of the incomings exceeds the cell threshold rate, the cell triggers and sends the signal to surrounding nodes via a transfer function, and figure 2.25 illustrates the node. The procedure can be stated mathematically as in equations (2.6),(2.7) [79]:

$$net = \sum_{i=0}^{n} w_i x_i - T \qquad \ldots\ldots\ldots \quad 2.6$$

$$y = f(\text{net}) \qquad \ldots\ldots\ldots \quad 2.7$$

where y is the cell outcome, f is the transfer function w_i is the weight of input x_i, and T is a criterion threshold value. Hence, the activation function can take on numerous shapes. Non-linear transfer functions are more valuable than linear transfer functions because:

1- the derivative of the nonlinear function would be related to the input, and it is allowed backpropagation, so it is possible to go back and understand which weights in the input neurons can provide a better prediction.
2- They allow the stacking of multiple layers of neurons as the output would be a non-linear combination of input passed through multiple layers.

The basic one is the Heaviside step function, which is defined in equation (2.8):

$$y = f(\text{net}) = \begin{Bmatrix} 1 \ldots if \ \sum_{i=0}^{n} w_i x_i \geq T \\ 0 \ \ldots if \sum_{i=0}^{n} w_i x_i < T \end{Bmatrix} \quad \ldots\ldots \quad 2.8$$

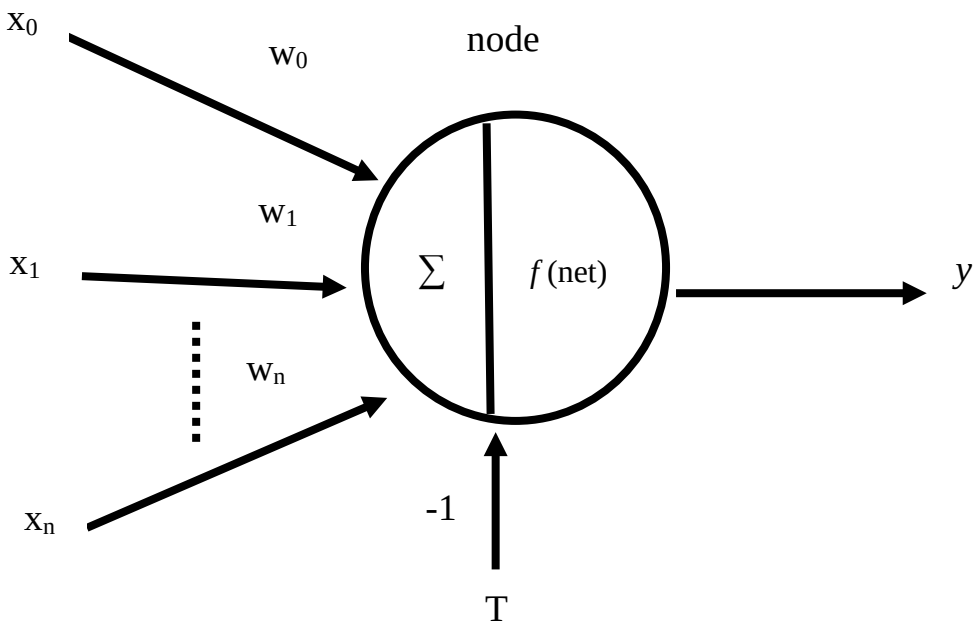


Figure 2.25: Neural network node [79].

The sigmoidal or logistic is another activation function. It is frequently employed as a transfer function because the function type and its derivation are continual; the function is depicted as seen in equation (2.9):

$$f(\text{net}) = \frac{1}{1+e^{-\beta\,\text{net}}} \qquad \ldots\ldots\ldots \quad 2.9$$

where β is a factor that controls the rate of learning derivative.

2.21.2 Network Architecture

Layers are used to organise the nodes into linear arrays. Typically, there are three-layer types: input, output, and hidden layers. The last one may be single or multiple. The network topology composition entails identifying the count of cells at every tier, the total count of levels, and the route taken by the node interconnections. Typically, these parameters are determined intuitively and then optimised through numerous cycles of experimentation.

Finally, there are two distinct forms of node-to-node connections. One is a one-way connection that does not include feedback. The second type of connection consists of a feedback link; hence, the node output is linked as an input to earlier or same stage nodes [79].

Neural networks can be classed into two groups based on their types of connections: feedforward and feedback networks. The feedforward network is a fixed structure since the signal only goes in one direction. Otherwise, in the feedback network, a single input has applied, and the state of the feedback network varies for several cycles until it reaches an equilibrium point which results in a sequence of outputs from a single input [80]. Figure 2.26 shows the architecture of feedforward neural networks.

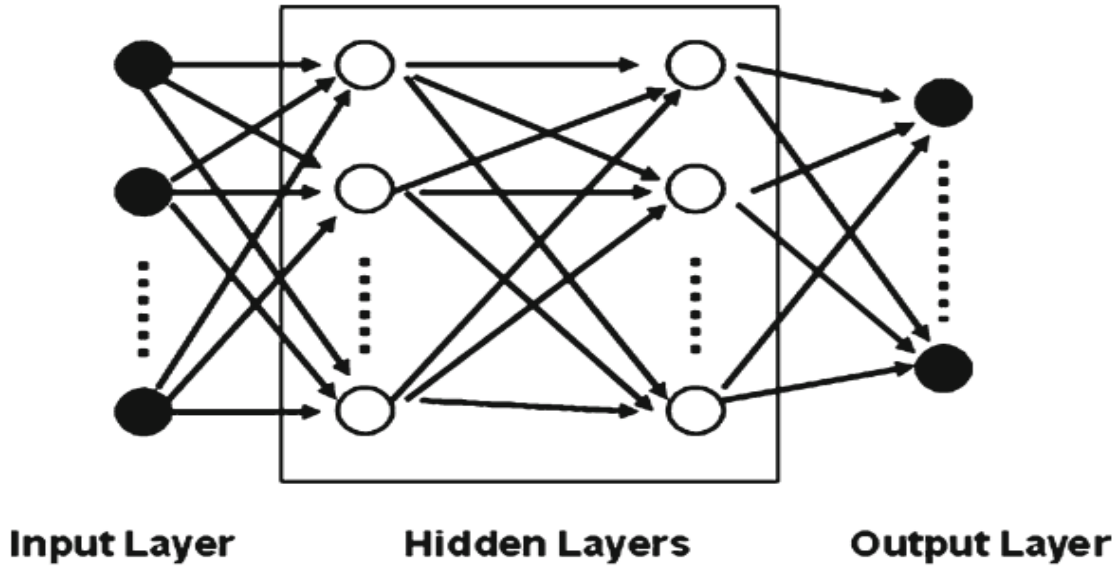


Figure 2.26: The architecture of feedforward neural networks [79].

2.21.3 Learning Rules

A neural network employs a learning technique for training the network to adjust weights to the suitable values during that operation. Two main categories of learning have existed: supervised and unsupervised. A training set consisting of a table of inputs and intended outputs is prepared for supervised learning. Adjusting the weights reduces the error between the network and desired outputs. Constructing the training set requires particular thought. A training set that is not representative cannot yield a reliable model [79].

The network must first be trained to use supervised learning on a network. Whenever the ANN generates the prospective outputs from the input set, the network is regarded as trained and the weight extracted to fix use.

On the other hand, unsupervised learning does not predict output values from the training set, but only inputs are used to deduce the tacit paradigm [79]. Numerous learning ways developed for a variety of learning objectives. The error correction and closest neighbour methods are widely used [33].

2.21.4 Back Propagation and Learning Rate

Typically, error correction techniques include the back-propagation technique. Then the error function kth cell output node, which is known as the difference between the actual and the desired node output or the error as in equation (2.10) [79]:

$$E=\sum \frac{1}{2}(\text{target}-\text{output})^2 \quad \ldots\ldots\ldots \quad 2.10$$

The error equation for the sigmoid function in equation (2.9) is depicted in equation (2.11)

$$\delta_{yk} = (d_k - y_k)y_k(1-y_k) \quad \ldots\ldots\ldots \quad 2.11$$

where δ_{yk} is the error signal, d_k and y_k is the kth desired value and neural output, respectively.

The new weight for input x_i is $w_{k\,i+1}$, it can be updated each step until a convergent state is reached; this convergence is affected significantly by the learning rate λ, the update weight computed according to the equation depicted in equation (2.12)

$$w_{k\,i+1} = w_{ki} + \lambda\delta_{yk}x_i \quad \ldots\ldots\ldots \quad 2.12$$

The equation (2.12) can further be modified for the case of the hidden layers.

The back-propagation technique can be employed to train multi-layer neural networks. This algorithm starts by propagating the input through the network and then calculates the output. The difference between the calculated and desired output values is the cost function, which is promulgated reversely to the input coming from the output to update the weight.

3

Chapter Three
The Proposed Systems

Chapter Three

The Proposed Systems

3.1 Introduction

This chapter addresses the proposed cloud systems for smart operation centre, including hardware, software, and cloud-based monitoring and algorithms. The hardware layer is made up of numerous elements and components. All of these parts and components will be thoroughly detailed in the sections on design tools. This system depends on the cloud with IoT and data sensors. Other architecture essentials and operations are presented later.

3.2 Cloud Operation Centre

As mentioned earlier, most OCs are utilised only for monitoring or monitoring with fewer processes. However, systems are invented with the development of smarter life, more resilient, and less dependent on human intervention, making life easier. According to the ministry of electricity of Iraq's annual report in 2018, it is a demand to build a new centre monitoring residential grids and solve some technical and non-technical losses, so two systems are proposed here in this thesis.

3.3 Cloud-Based Automated Power Factor Correction and Power Monitoring System

This first cloud system design aims to improve power factor and contribute to the contraction of some technical losses and energy monitoring.

3.3.1 Stimulus

According to the annual statistic report from the Iraqi ministry of electricity in 2018, many clients are in the residential sector. In addition, a large amount of energy is around 59% in this sector. The value of energy and percentage of it for three provinces are shown on the map in figure 3.1.

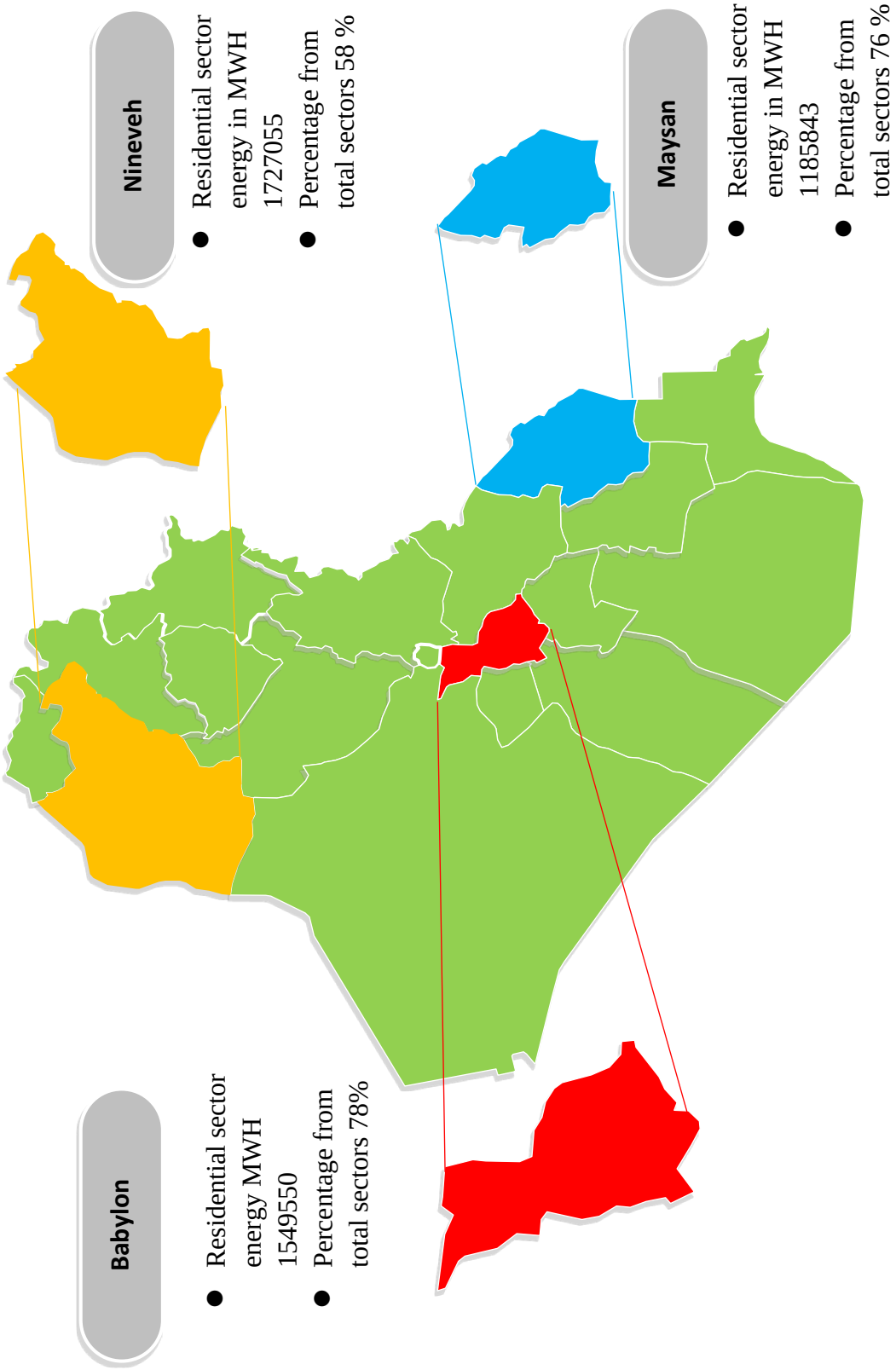


Figure 3.1: Consuming value of energy map of residential and its percentage in three provinces

Furthermore, many appliances or devices have an inductive nature, so the power factor was lagging and needed to be corrected by reactive power or calculated that reactive to determine the required capacitance for correction. Also, it allowed updating residential grid power minoring.

3.3.2 Proposed System Description

The main goal of the future system is to provide knowledge concerned with cost reduction, multi-home process assistance, and core device decision-making. In addition, the new automatic power factor correction will be constructed to increase the monitoring and power quality benefits by reducing bills and losses. Following the advances in electrical networks, the solution will be widely agreed upon and will have less cost for the user and need less reactive power. It uses the private cloud idea as PaaS and may be expanded to accommodate hybrid cloud scenarios.

A pre-test will be run in the system to identify combinations of common devices to all homes in nonequal houses residential areas. For example, in the primary typical process device, appropriate choices during the creation of training data (actual power and power factor) are made by the neural network algorithm so that each house offers the best option for improving the power factor by picking the perfect value of capacitance based on the algorithm decision.

The system works after measuring the voltage, actual power, and power factor of a sample of household appliances by PZEM; the measured data was transmitted to the Raspberry Pi, which plays the role of cloud server via NodeMCU. Finally, the power factor data is displayed inside the platform of Node-red.

Further, the neural network was used to compute the suitable capacitance for APFC, the capacitance value saved in Raspberry Pi. This value of the amount

of capacitance can be later sent to the capacitor selector for adding it to the correct power factor. The block diagram for the two home appliances is shown in figure 3.2. Also, the system expected block diagram is depicted in figure 3.3.

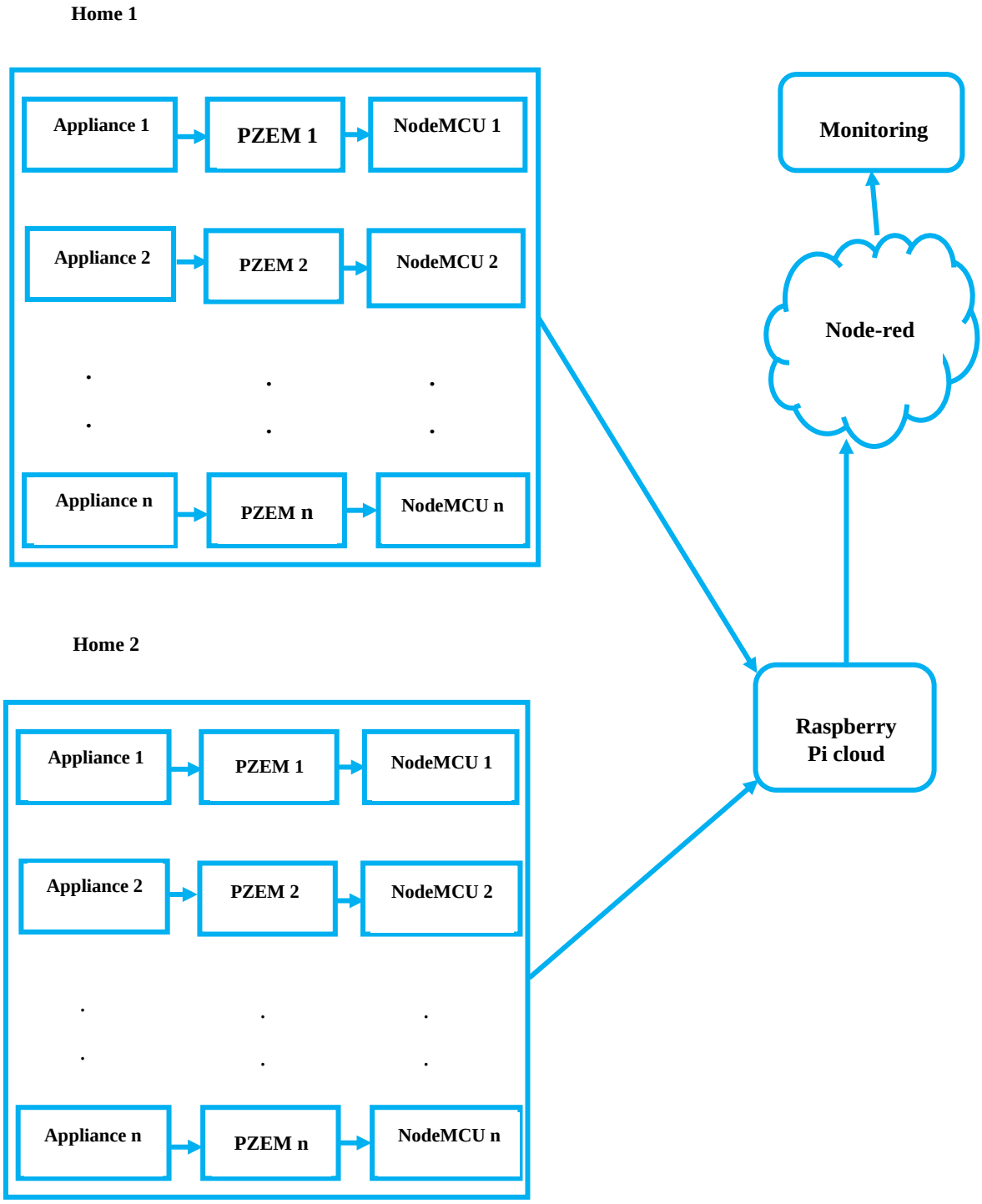


Figure 3.2: The block diagram for two homes.

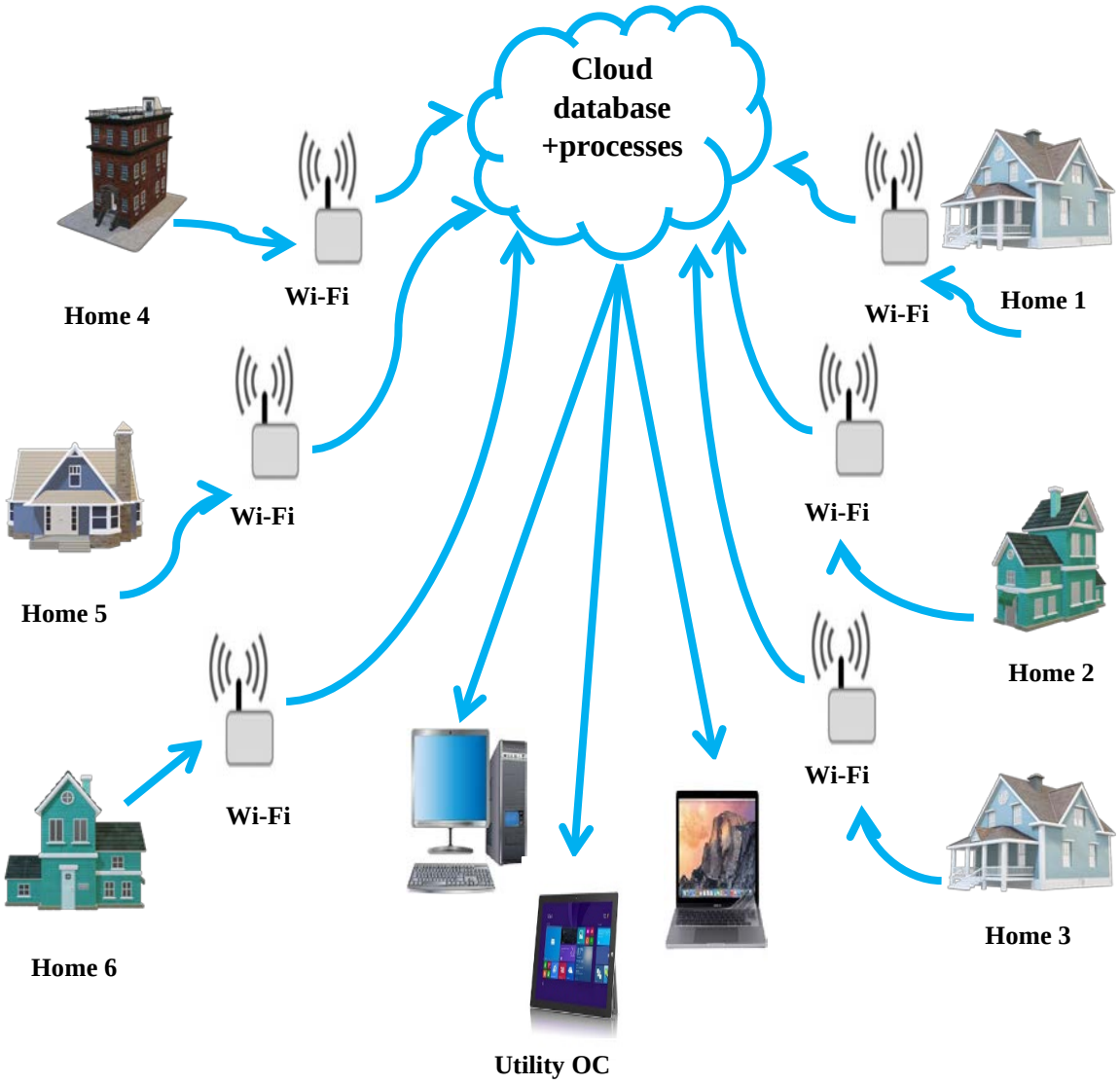


Figure 3.3: The block diagram system imagination.

3.3.3 Instrument Layer

This layer consists of the data sensor and the device that sends data to the cloud. Hence, NodeMCU represents a data-sending node unit. The NodeMCU or ESP8266 is a special internal processing and storage device that permits a connection with a sensor-specific device via its GPIOs with minimal development and runtime loads, and it is programmed in C language.

Furthermore, the PZEM-004t sensor device reads power values

parameters with current transformer (CT) and voltage transformer (VT). Also, this module is used to extract electrical parameters such as voltage, current drawn by the load, total energy expenditure, frequency, and power factors. It also has a power knob to reset the cumulative energy, and PZEM-004t can be connected serially over an adapter or via the device NodeMCU over Tx and Rx of the device for data with any digital I/O of NodeMCU and VCC and GND for a power device, as in figure 3.4.

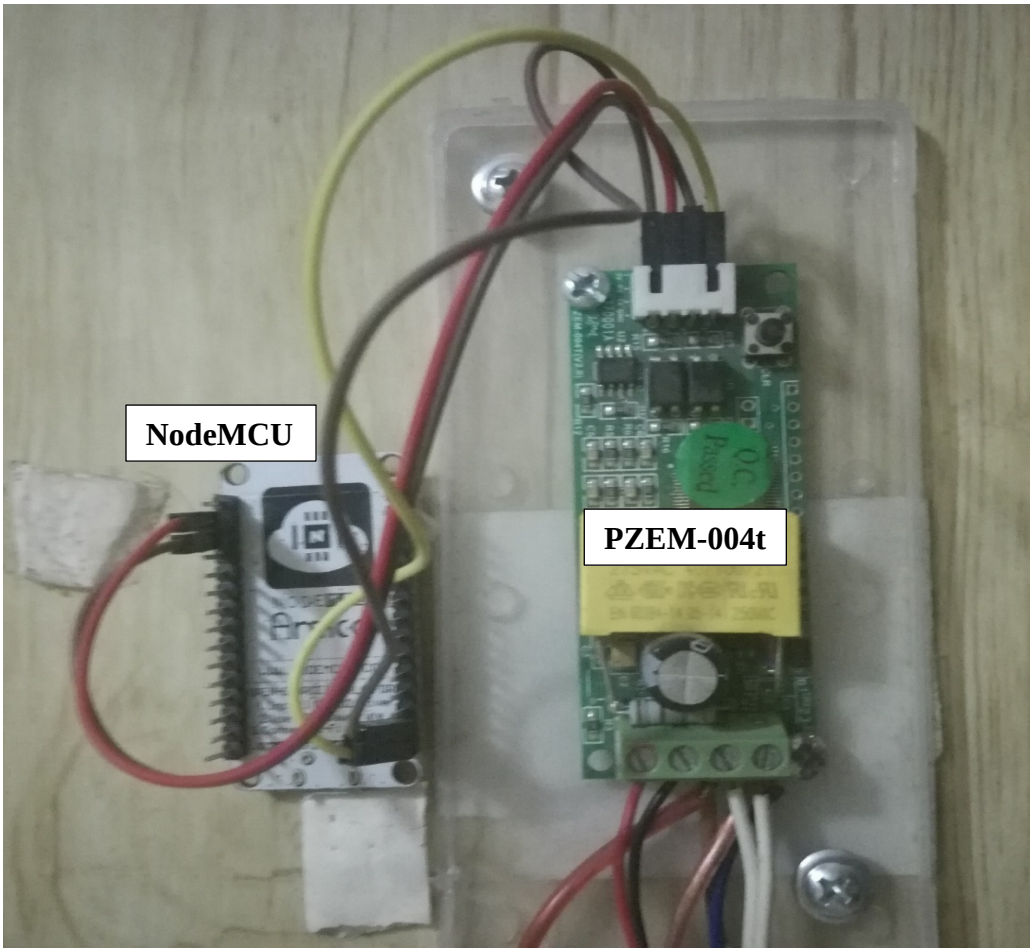


Figure 3.4: The connection of PZEM-004t with NodeMCU.

3.3.4 Cloud Layer

This layer is represented by the private cloud server, in which the Raspberry Pi plays the role of a central unit cloud that runs the algorithm of a

neural network that decides the appropriate value of condensation for all homes in one algorithm. In addition, the power monitoring readings for all parameters are inside it. The Raspberry Pi is an economical price computer of size less than the hand palm.

Raspberry Pi can be used with a message broker like MQTT to collect and upload data and create a private cloud server. It can run applications in the form of Platforms as a Service (PaaS). Cloud helps in hosting and accessing on-demand and from anywhere as long as the Internet is accessible. Figure 3.5 shows the system layers, and Figure 3.6 illustrates the block diagram showing this system's hardware.

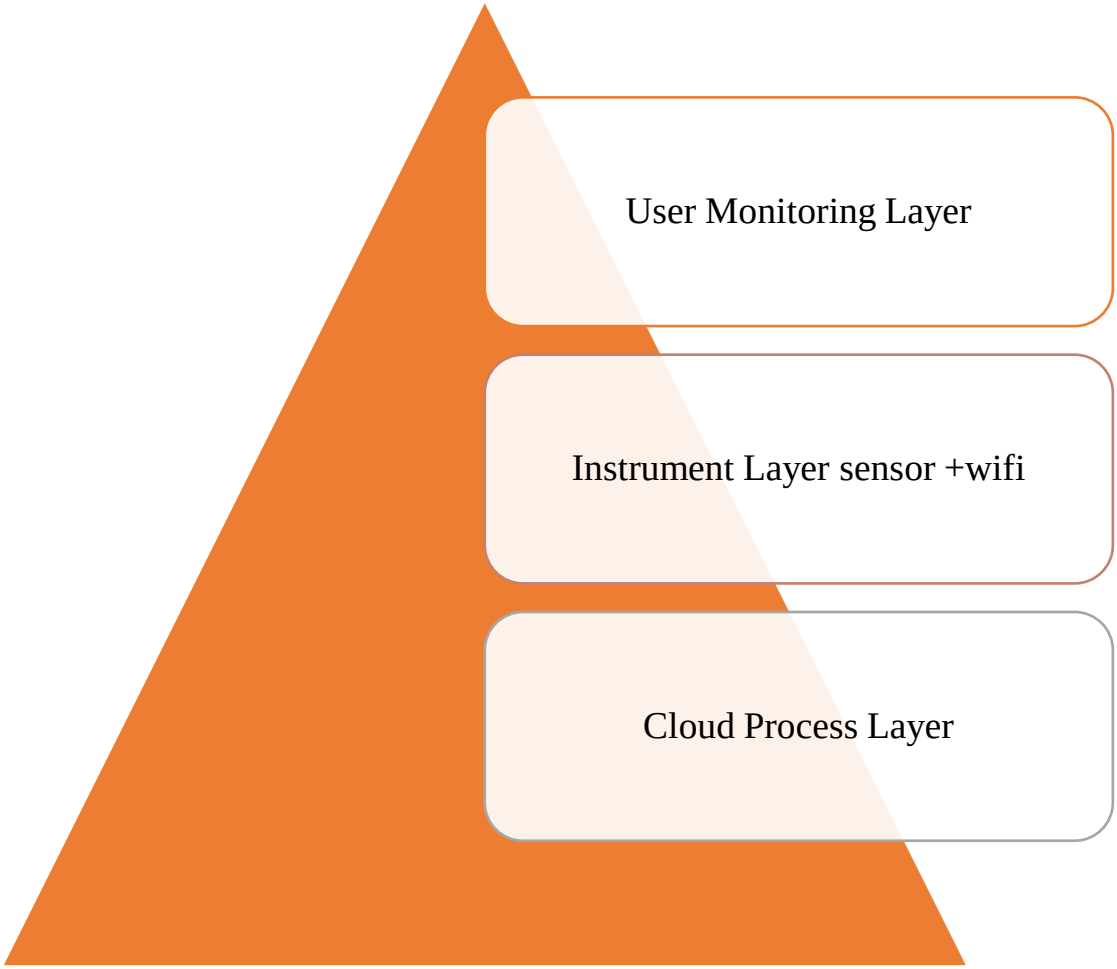


Figure 3.5: The system layers.

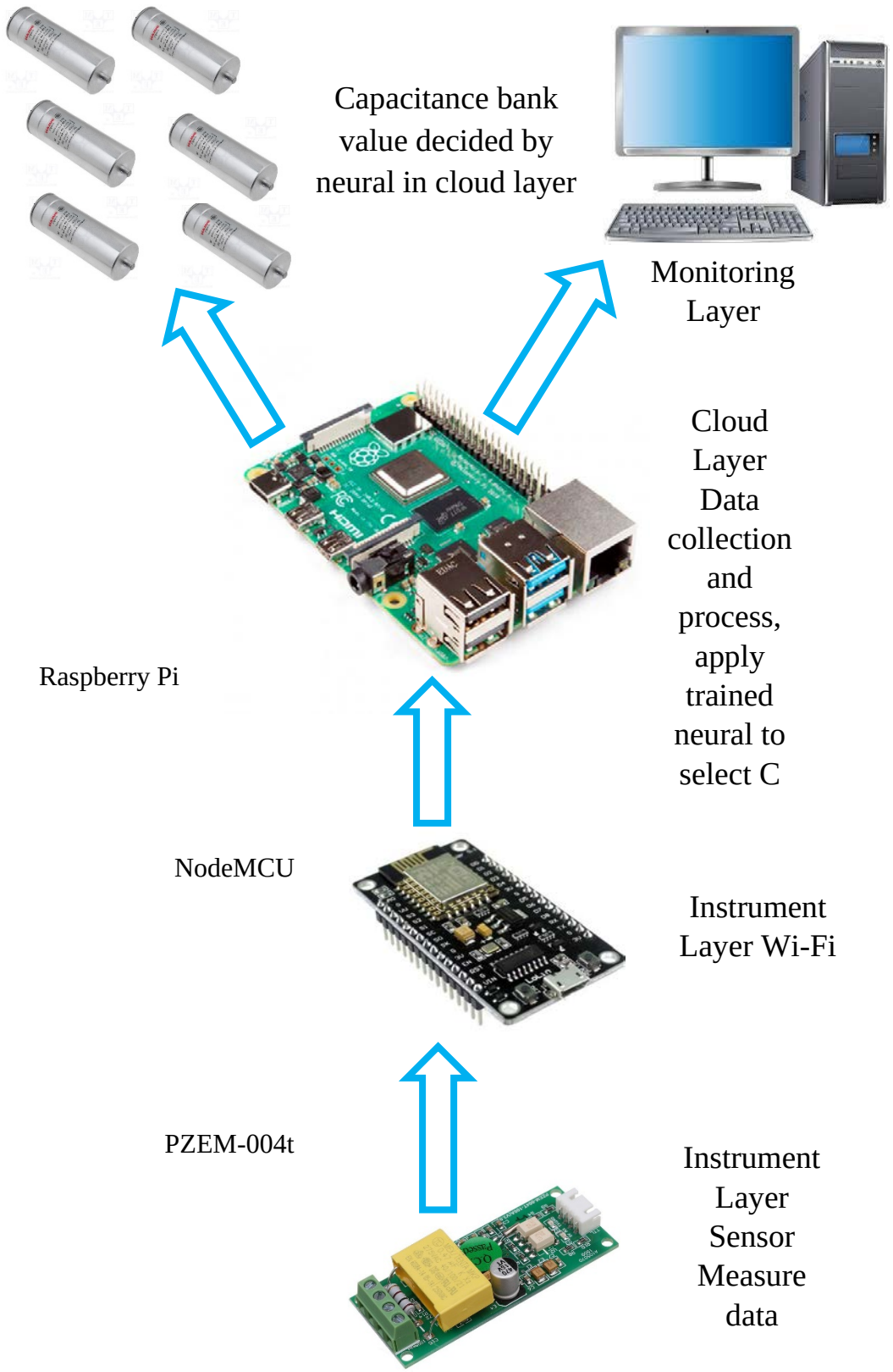


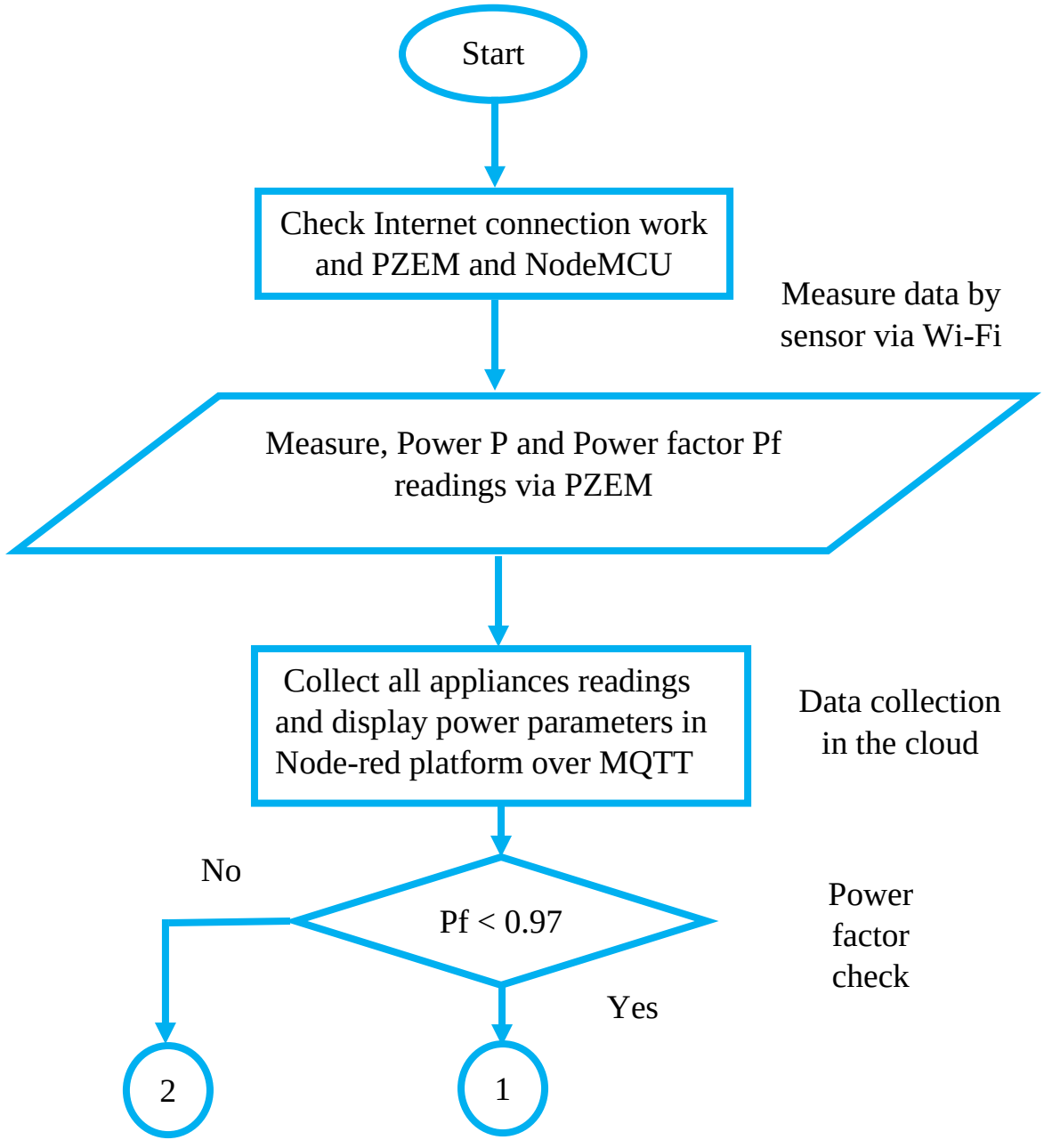
Figure 3.6: The block diagram shows the hardware of this system.

3.3.5 Monitoring Layer

In this layer, the client or the supervisor can observe the power parameters or the result of the cloud process through the web directly via the IP of Raspberry Pi.

3.3.6 The Algorithm of Proposed System

The flowchart for the process algorithm of the proposed system can be shown in figure 3.7.



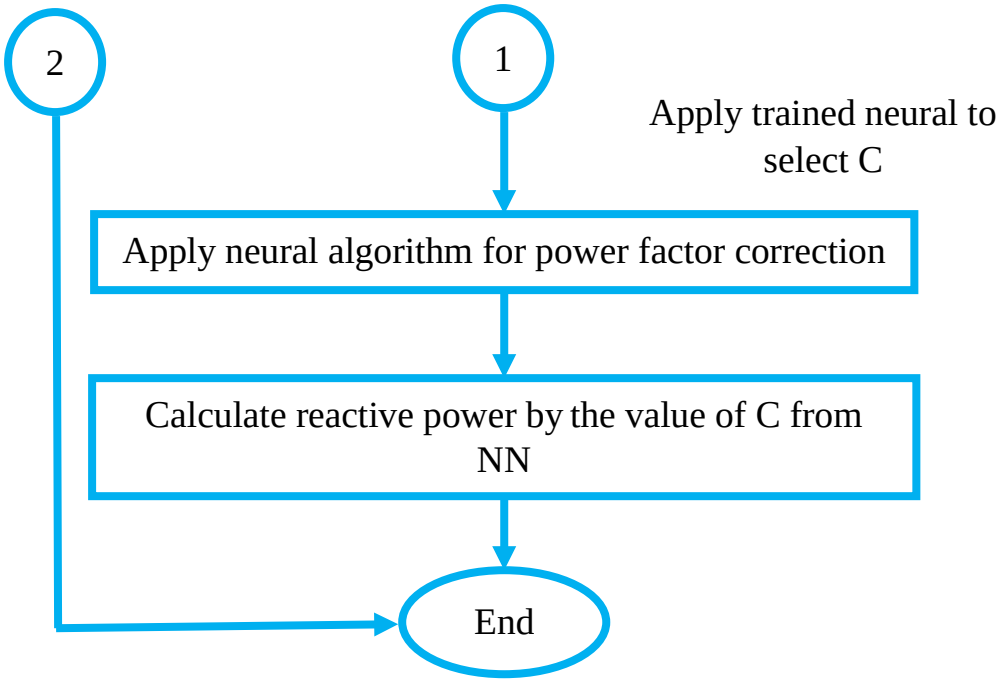


Figure 3.7: The schematic algorithm of the proposed system.

3.3.7 The Neural Network Design for Power Factor Correction

Here the neural network design will use some values of actual loads as input data set. These values have been obtained by us from a practical reading of real home appliances loads, as shown in Table 3.1 below:

Table 3.1: Different loads with power and power factor.

Load device	Power (W)	pf
LED light lamp Ingco	30	0.55
LED light Ingco	80	0.58
Stand Fan Gosonic GSF-165	55	0.82
Freezer Iceberg 10302	155	0.46
Fridge Concord 540L TE1900-W	237	0.64
LED light Ingco	140	0.55
Gaming console Sony Ps4 pro	88	0.78
LED light Aswar	64	0.55
home random loads 1	266	0.67
home random loads 2	181	0.73
home random loads 3	377	0.61
home random loads 4	688	0.72

3.3.8 System Features

The proposed system has many features as follows:

1- This system can be applied in a typical residential area with appliances served with internet access as proposed.
2- Support multi-home power factor correction in one central device.
3- With the cloud concept employed, the system supports scaling to manage big data or big district power quality enhancement.
4- It consists of accurate determination of capacitance power factor correction.
5- Neural network function.
6- It allows monitoring power and correction processes in a central unit in real-time.
7- Smart grid concept support.

3.4 Larceny Revelations of Electric Energy with Cloud Computing

This second cloud system design desires to detect electricity fraud and estimate the cost of frauded power. Also, it allows monitoring of main distribution supply lines details to know future expansion if needed.

3.4.1 Stimulus

According to the annual statistic report from the Iraqi ministry of electricity in 2018, the non-technical losses, which is a type of loss in the distribution network as shown in figure 3.8, represent major types of losses that around 58% of received energy from the transmission side. This amount consists of a part of these losses in the form of fraud meters and other metering losses. An example of losses in three provinces and three districts in Babylon province is indicated in figure 3.9. and figure 3.10 which different from figure 3.1.

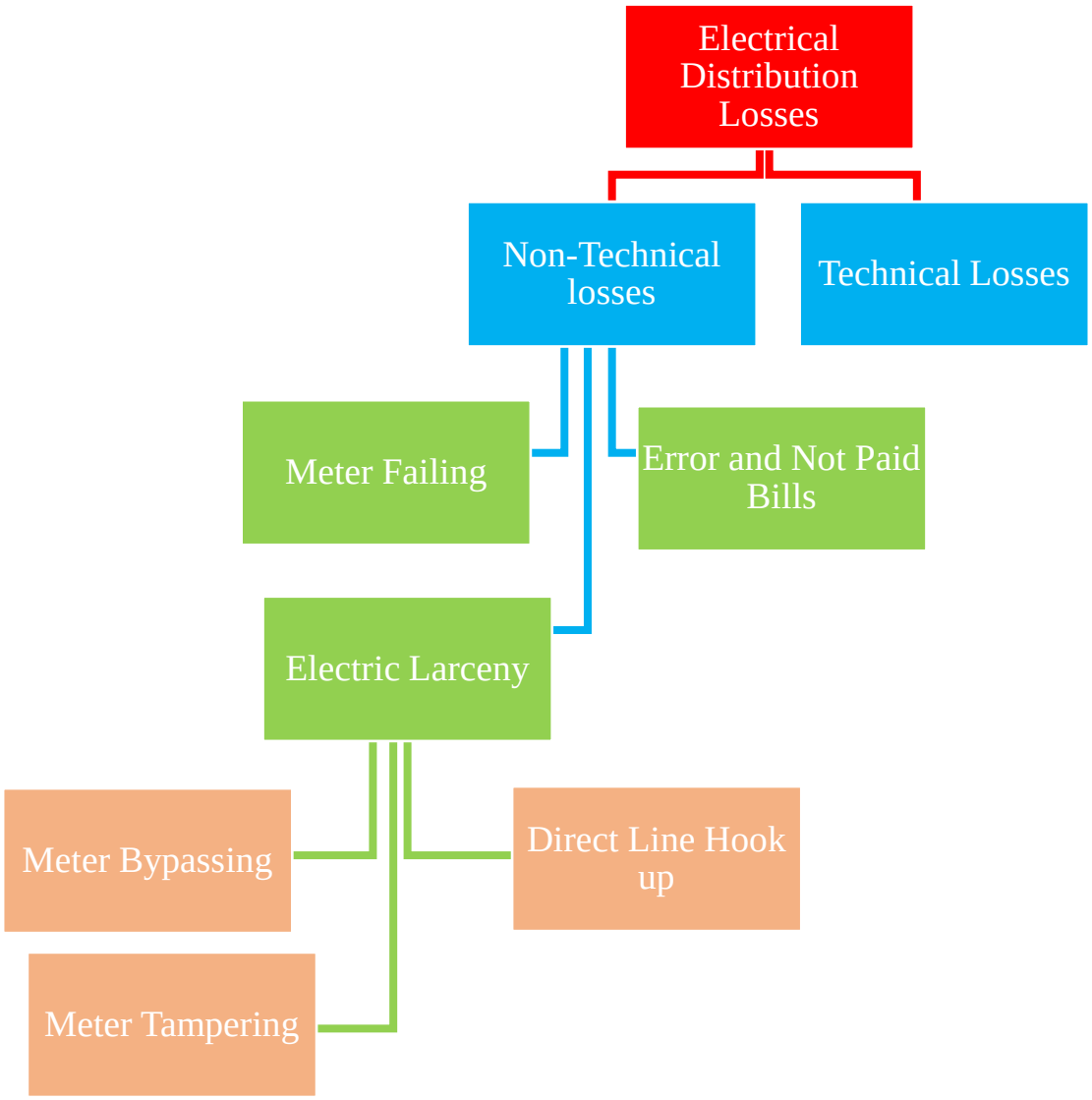


Figure 3.8: Electrical distribution losses.

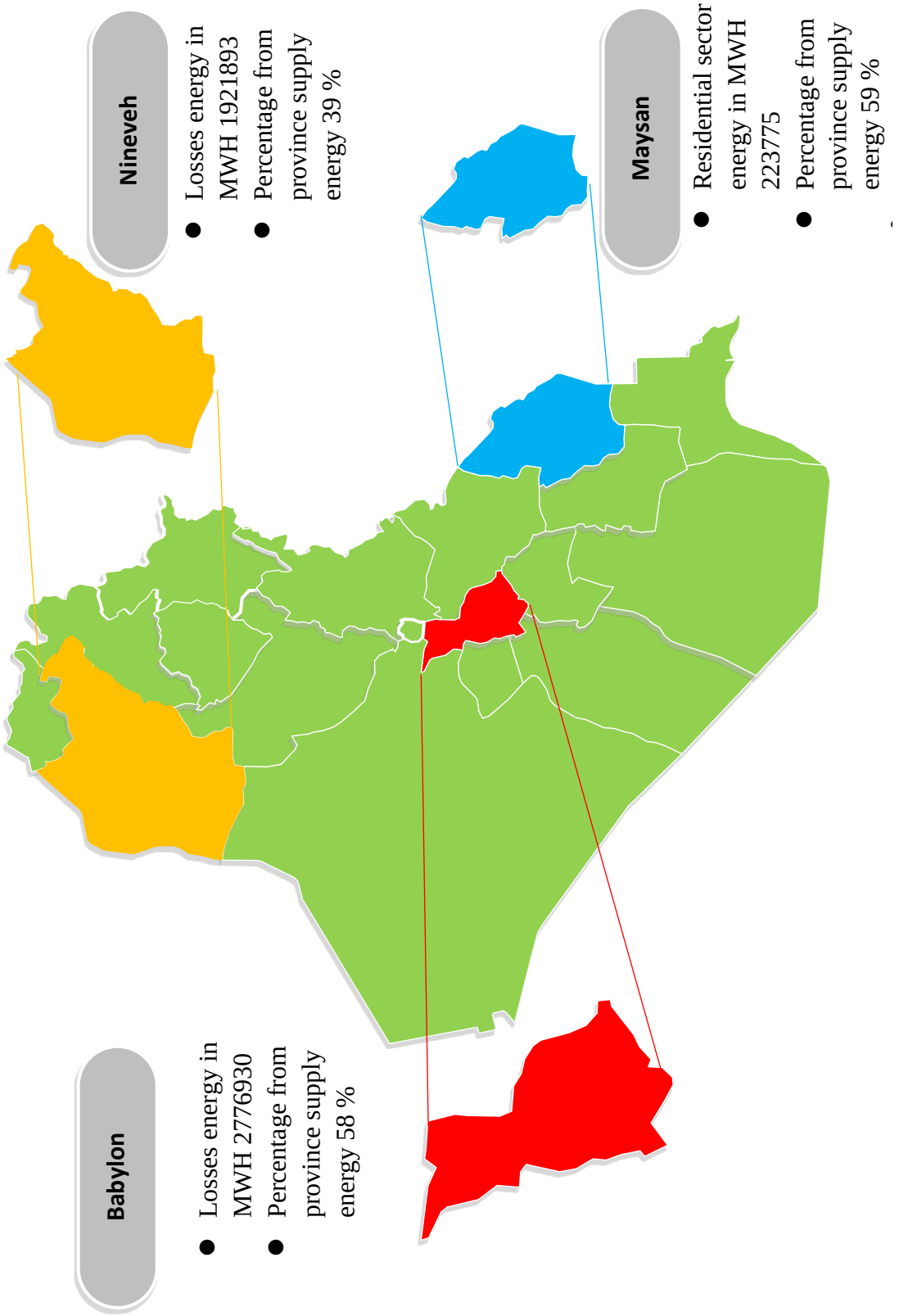


Figure 3.9: A map of example for losses in three provinces

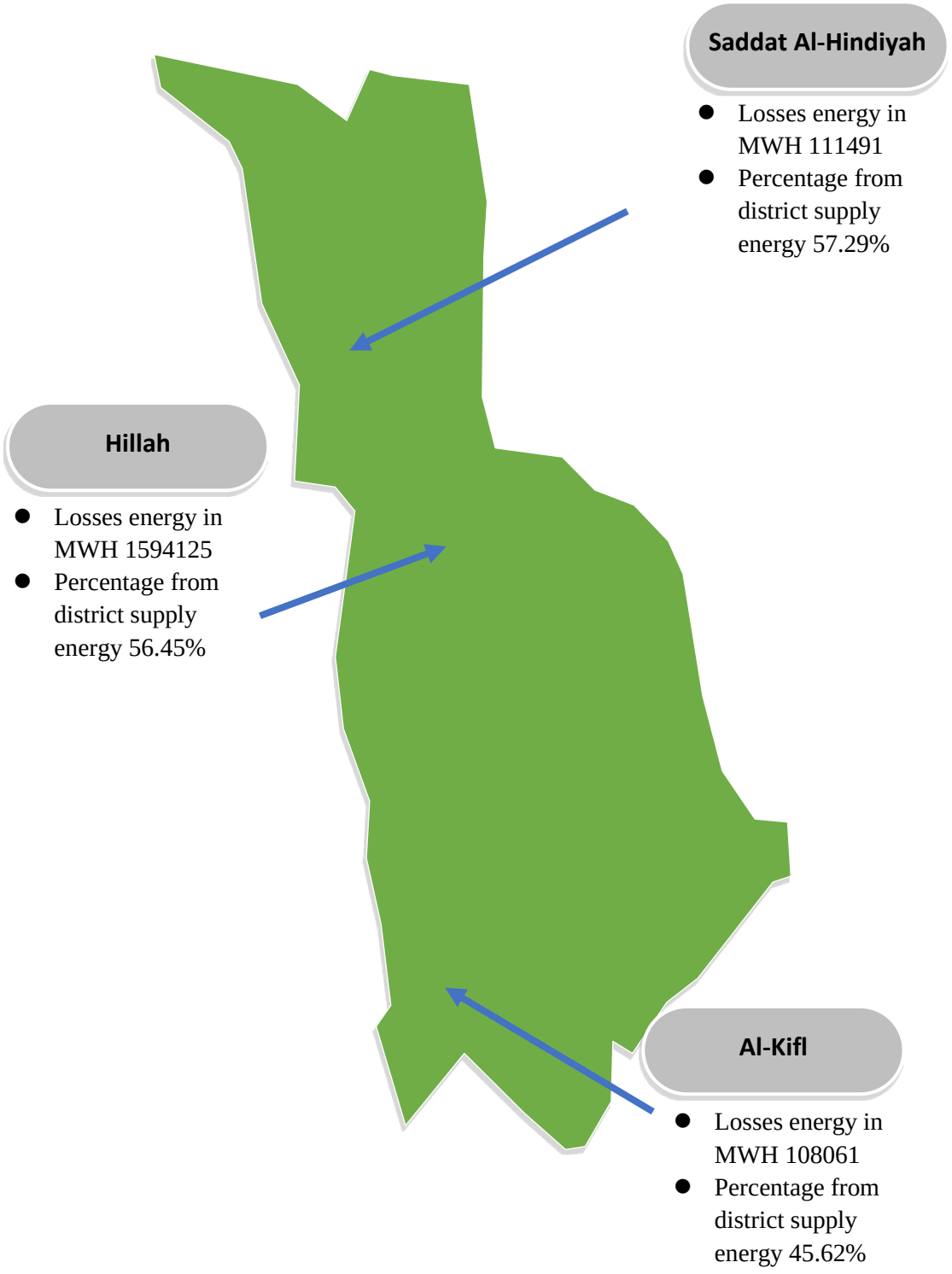


Figure 3.10: A map of example for losses in three districts in Babylon province.

3.4.2 Proposed System Description

The main aim of this system is the larceny revelation of electric energy based on cloud computing (PaaS). The suggested system overcomes the meter bypassing, fraudulent users and direct line theft; also, it provides good imagination on electric sources providers that need to expand. The Raspberry Pi works as a private cloud central unit to perform and run the algorithm. In addition, this system is provided knowledge about electrical user networks via monitoring and support of advanced metering.

The system emphasizes on the cost of loss reduction and multi-home processing in one system process with cloud assistant. The proposed system uses the main meter on a transformer, and the meter has a role of control and, with the help of a server, it collects the reading of user meters (intelligent meters or upgraded conventional meters) in the grid. The algorithm depends on the current difference between the primary meter reading and the sum of secondary meters. The suggested system can detect fraudulent electricity meters and direct line hookups around the clock.

In order to make the theft detection system, a main or Primary smart Energy Meter (PEM) which has current (I) must be put in the primary distribution source like a transformer or (Dtrans). In addition, if found, each electronic energy meter or mechanical meter must be upgraded to be smart. Therefore, User Energy Meters (smart meters and upgraded) are symbolled as (UEM) and the current of each meter (i).

The systematic system block diagram is in figure 3.11, and the imagination of the overall system is in figure 3.12

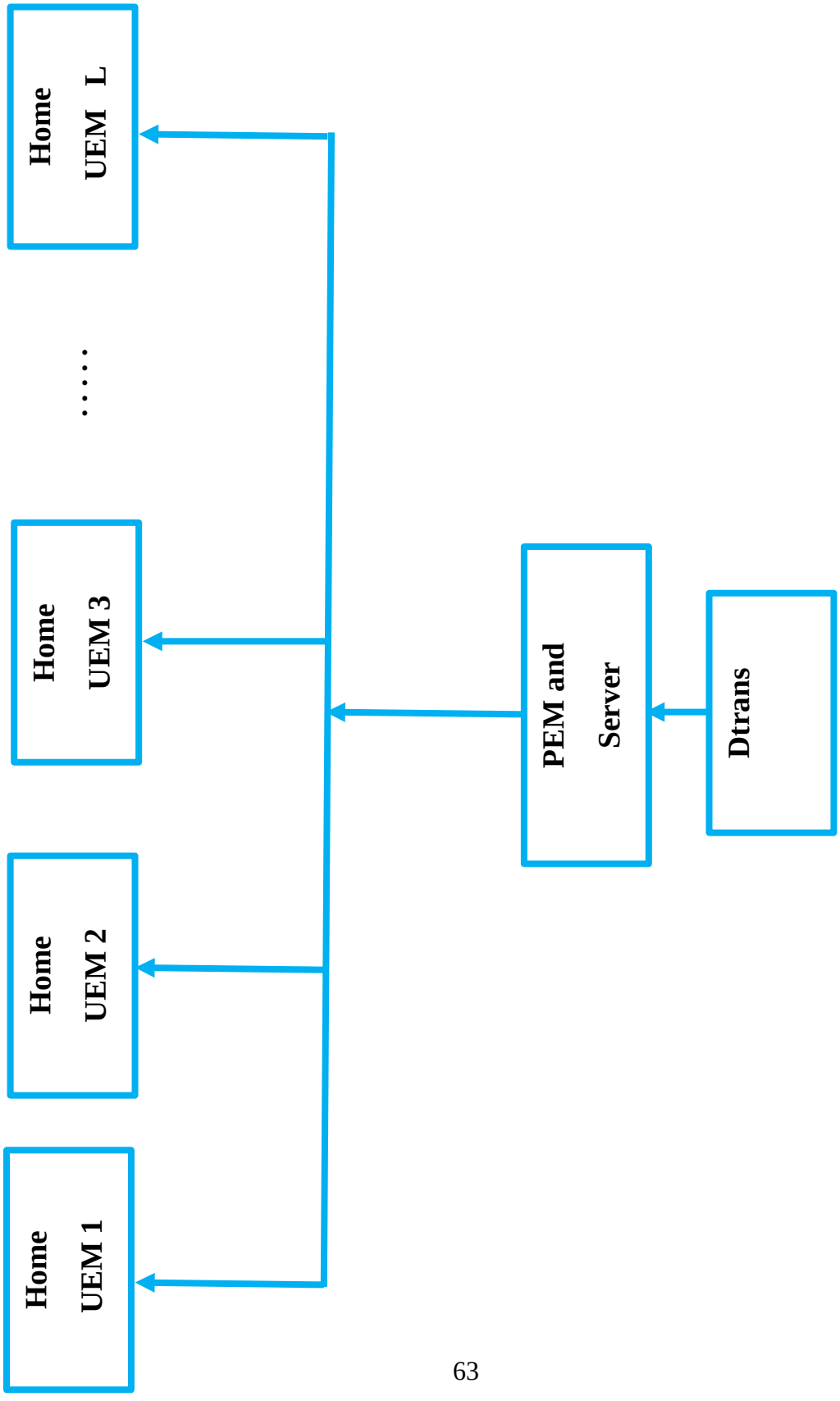


Figure 3.11: The systematic system block diagram

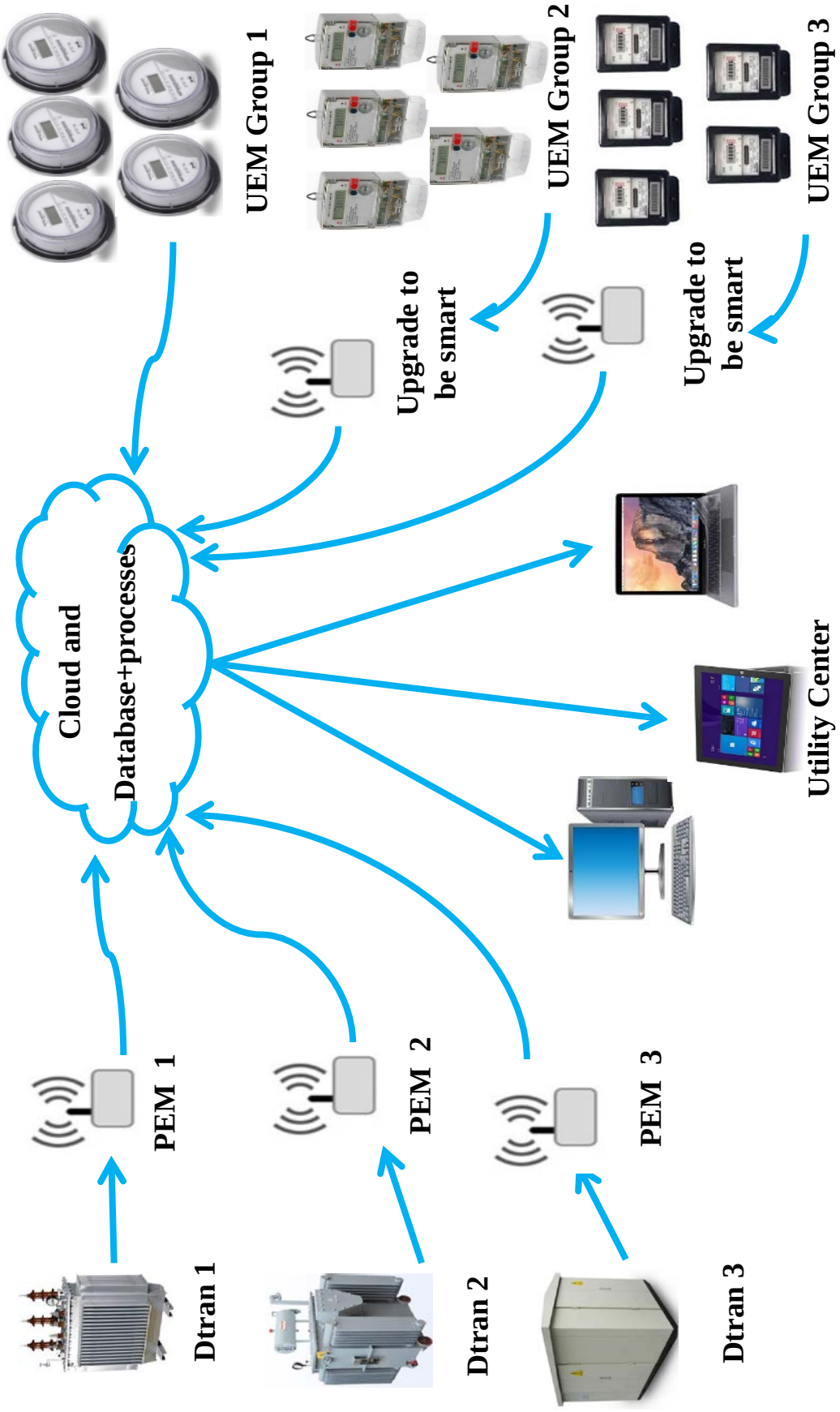


Figure 3.12: The imagination of overall system

3.4.3 Instrument Layer

Like the first system instrument layer description, this layer contains the data sensor and the device that sends data to the cloud. Hence, NodeMCU represents a data-sending node unit. The PZEM-004t sensor device reads power values parameters with current transformer (CT) and voltage transformer (VT). Also, this module is used for electrical parameters such as voltage, current, connected load, total energy consumption, frequency, and power factors. The PZEM-004t is also connected with NodeMCU in the same manner. The difference between the previous and this system for this layer is that each combination of the PZEM-004t and NodeMCU represents a home smart meter or what is symbolled (PEM and UEM).

3.4.4 Cloud layer

This layer takes into account the instrument layer of the first system, and it is represented by the private cloud server, in which the Raspberry Pi plays the role of the central unit cloud that runs the algorithm that decides the theft type according to the flowchart that explained later also it gives an alarm. Raspberry Pi can be used with a message broker like MQTT to collect and upload data. A Raspberry Pi can be used to create a private cloud server. The main difference between the first system and the second one is the process done among meters and the main meter in the cloud for larceny detection in the first system, while the process on appliances data is in the cloud in the second system. The system hardware figure is the same as figure 3.6. Furthermore, choosing two different systems is that each one can be used in different user environments and privacy in the smart grid.

3.4.5 Monitoring Layer

In this layer, the supervisor can observe the energy larceny in all cases or the cloud process through the web directly via the IP of Raspberry Pi.

3.4.6 System Details

The system consists of collecting and sending the information measured by the primary energy meter from distribution transformers (DTrans) as (voltage, current, power, energy) to the central process server represented here by Raspberry Pi, also check if the DTrans current is in a reasonable load manner and suitable for rated. Then collect and send the information from (UEM) that is connected with corresponding Dtrans to the same server to calculate the difference between a load of Dtrans and the sum of loads of UEM. The proposed system then will determine if there is a theft in energy (fraud in UEM, or meter bypassed via direct line hook up).

The system was designed as a prototype. The primary current of the transformer (PEM) is symbolled as (I), and the current each for UEM (i) and the difference is $\mathfrak{D}$, No. of Dtras =K, num of meter/trans=L, and the rated current of each Dtras = I_L. The system treats the following points:

- Overload alarm for source and inform the utility.
- Larceny of energy by meter bypassing.
- Energy hooks up of line.
- The system can deal with the fraud of meter

The following equations are designed for this system and used in the calculation process. The difference equation is for each Dtrans:

$$\mathfrak{D} = I - \sum_1^L i \qquad \ldots\ldots\ldots \quad 3.1$$

The difference $\mathfrak{D}$ for two times now and preceding name new and old $\mathfrak{D}$ new, $\mathfrak{D}$old is

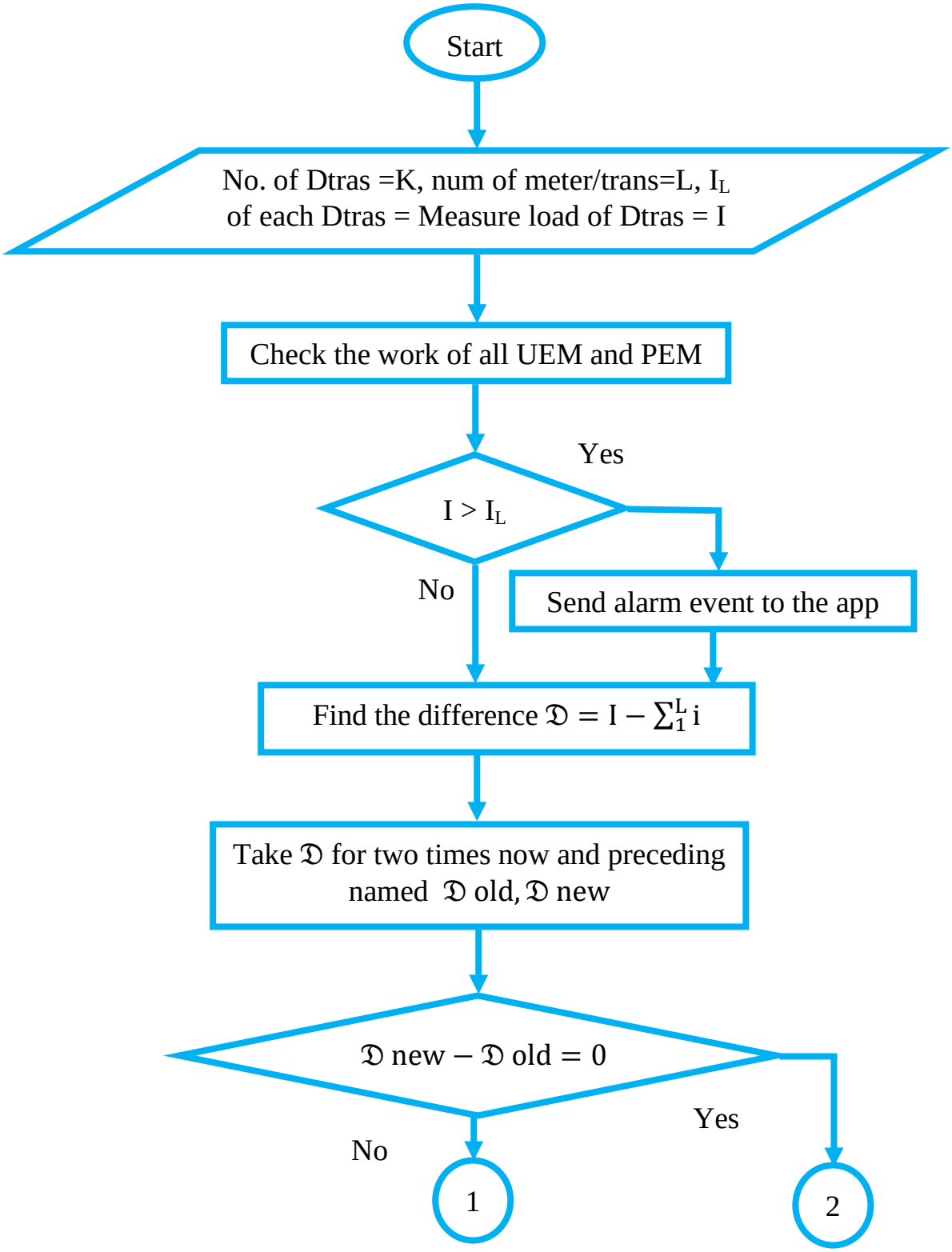
$$\mathfrak{D}\,\text{new} - \mathfrak{D}\text{old} = 0 \qquad \ldots\ldots\ldots \quad 3.2$$

The main current difference equation

$$I\,\text{old} - I\,\text{new} = 0 \qquad \ldots\ldots\ldots \quad 3.3$$

3.4.7 The Algorithm of Proposed System

The flowchart for the process algorithm of the proposed system can be shown in figure 3.13.



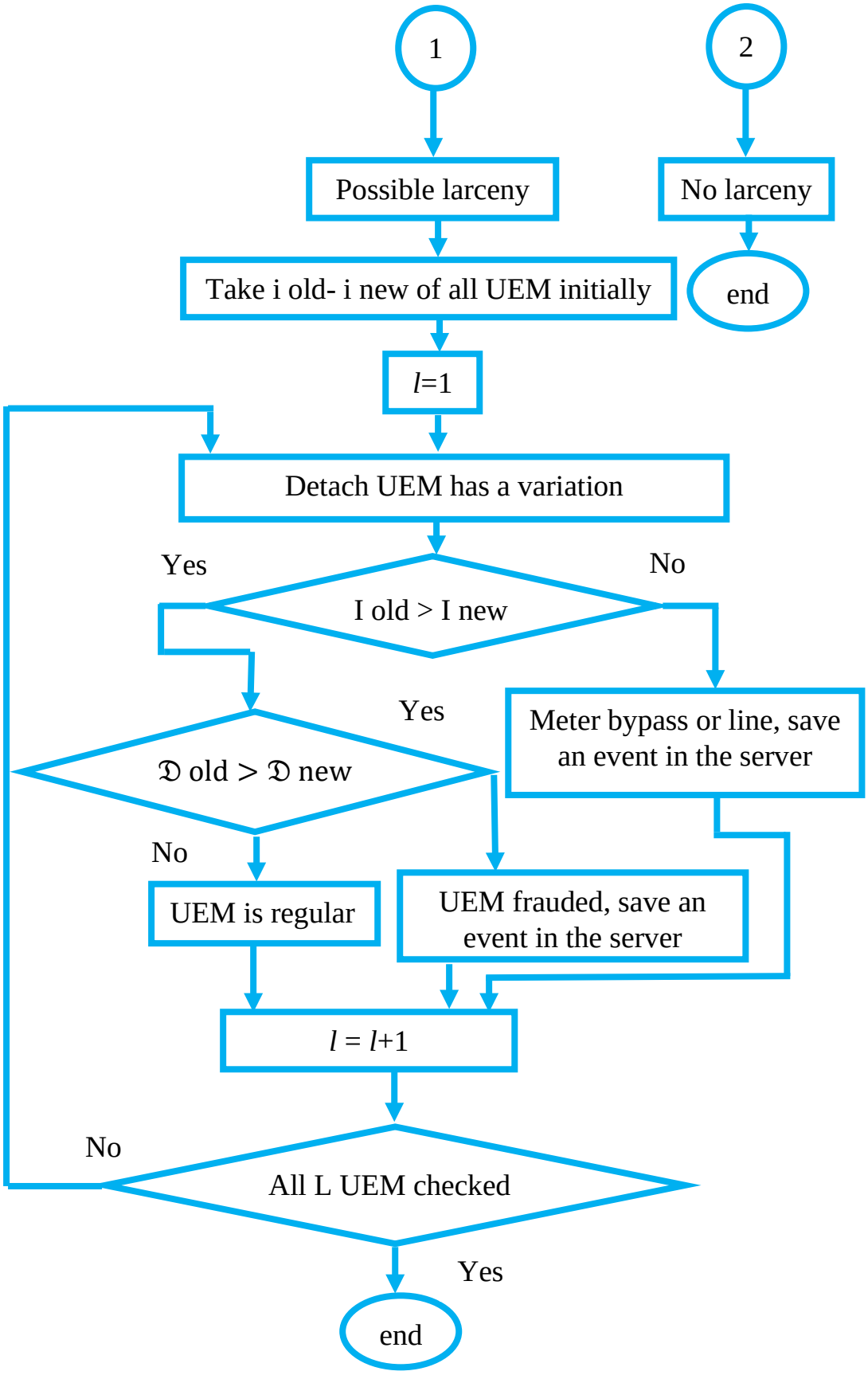


Figure 3.13: The flowchart for the process algorithm.

3.4.8 System Features

The system has the following features:

1- The system was designed for medium evolution smart grid without smart appliances in the previous system.
2- It represents a general solution for consumer distribution network electric power theft.
3- It helps in upgrading conventional meter to be a smart meter
4- It solves full and partial fraud electricity meter bypass.
5- It offers to fix feeder line direct hacking or consuming without meter alert.
6- It allows monitoring transformer distribution power supplied lines details for the current expansion.
7- It enables central process and monitoring over the cloud.
8- The system solves some non-technical losses by fraudulent users.

4

Chapter Four
Results and Discussions

Chapter Four

Results and Discussions

4.1 Introduction

This chapter states the description of system connections and implementations test results. These results from different cases with their discussions to illustrate the features of these systems.

4.2 Power and Energy Monitoring

The previous monitoring method used for energy is via local web page (webserver) or IoT platform web hosting, using the NodeMCU and PZEM-004t connection described in section 3.3.3 and figure 3.4. In the webserver monitoring, the web browser shows the PZEM data extracted by NodeMCU over the local IP of the device, and the IP can fetch from the internet gateway or the router, as in figure 4.1.

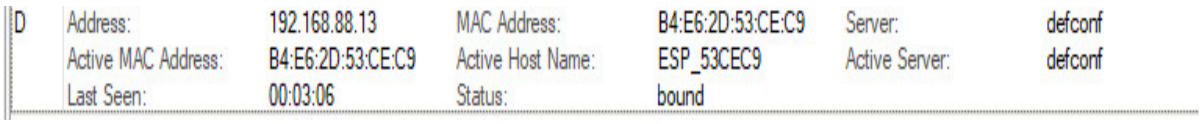
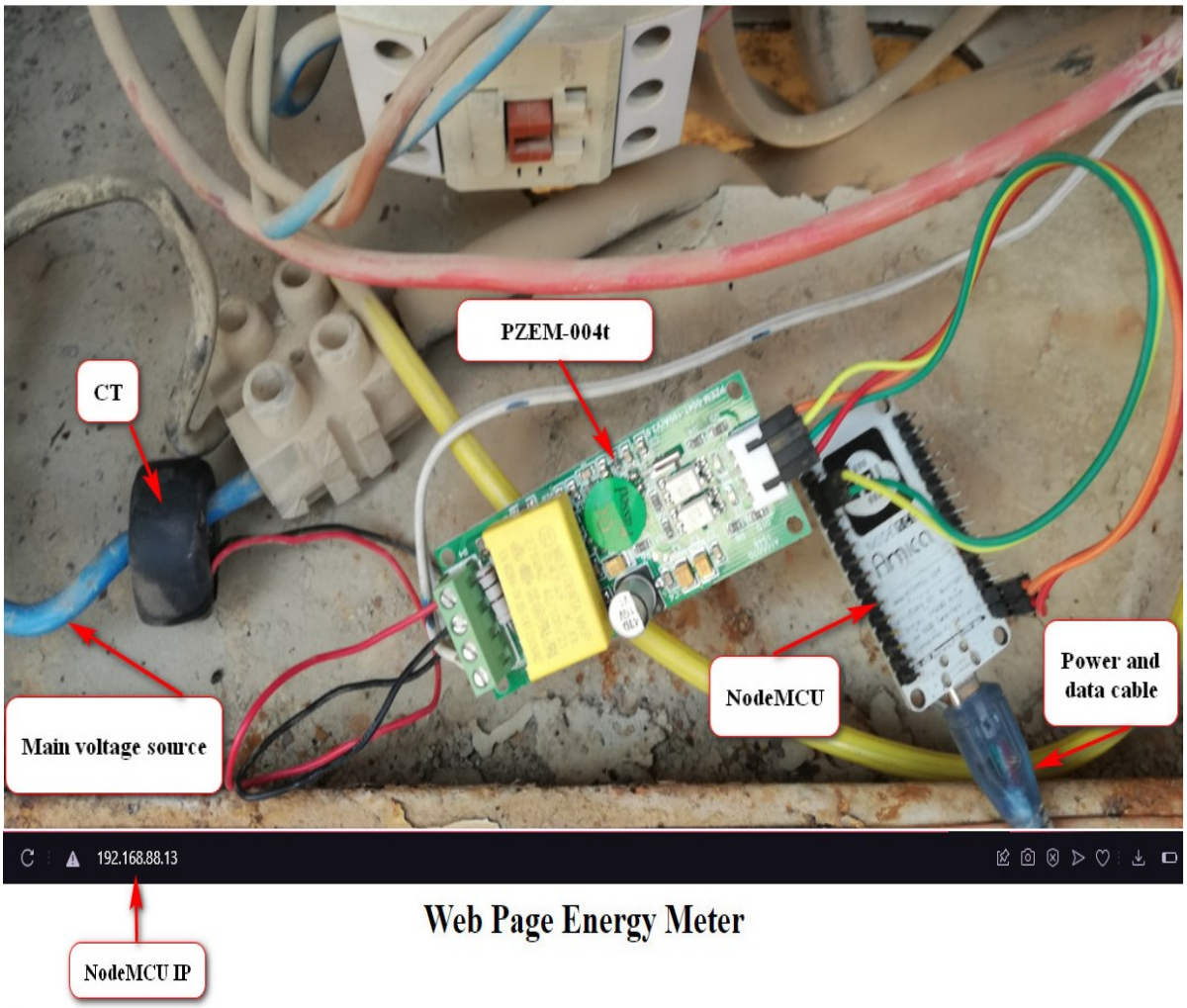


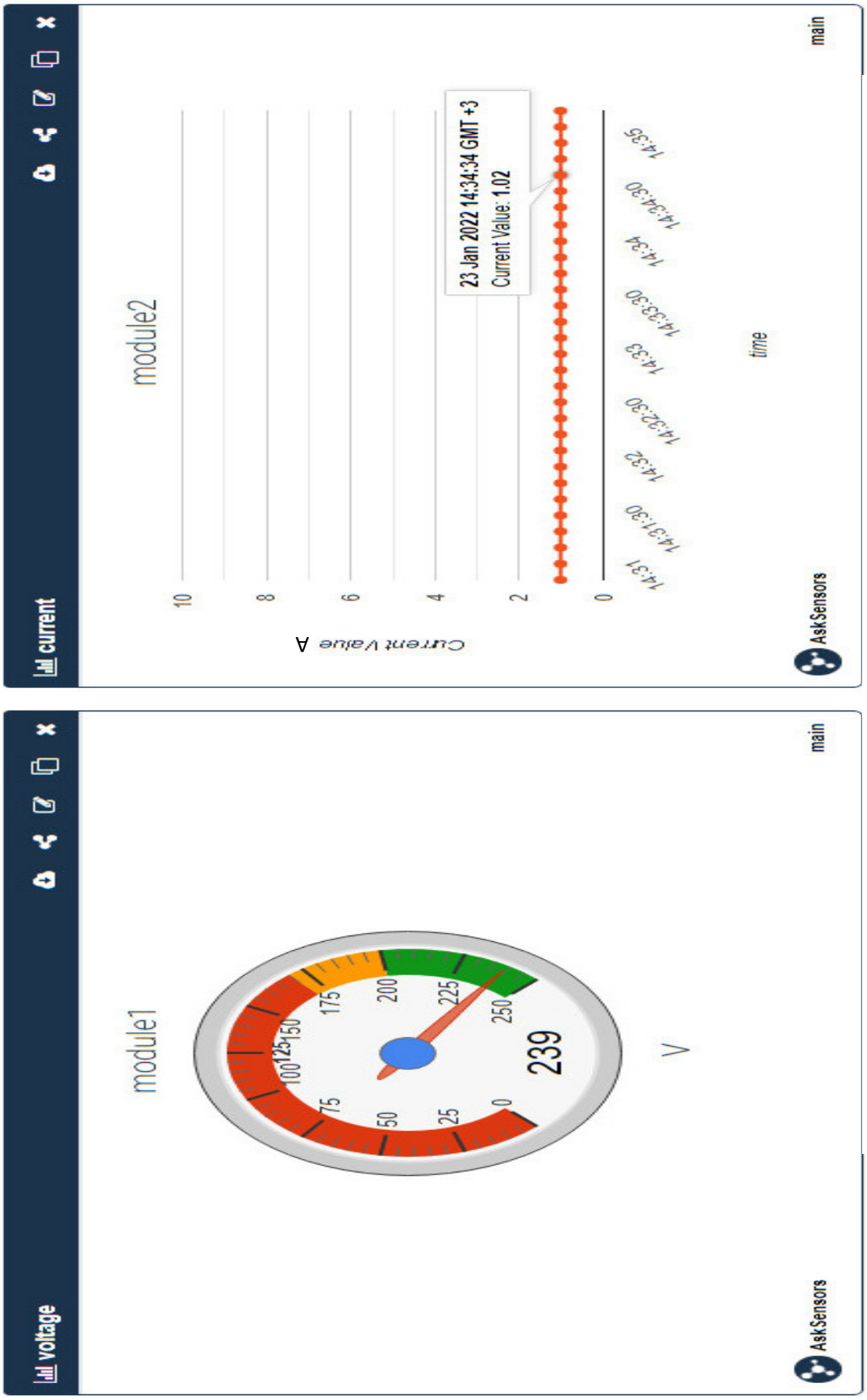
Figure 4.1: NodeMCU IP fetches from the router.

In this way, the data can only be shown in the web browser with values only, as in figure 4.2, so that the table made in HTML inside NodeMCU for the energy parameters mentioned previously. Here, an example for three lamps of 140 W only in the home is stated. Other appliances like (heaters, fans, refrigerators, and other devices) are taken but not mentioned. IoT web platform monitoring offers good features and additional functions like the map of the sensor site and gives visualised data and time curves. With the same connection in figure 3.4 and the same load of 140 W lamps, the results depicted in figure 4.3 (a,b,c) using the Askedsensors platform for energy monitoring of lamps of 140W the reading is taken every 10 seconds.

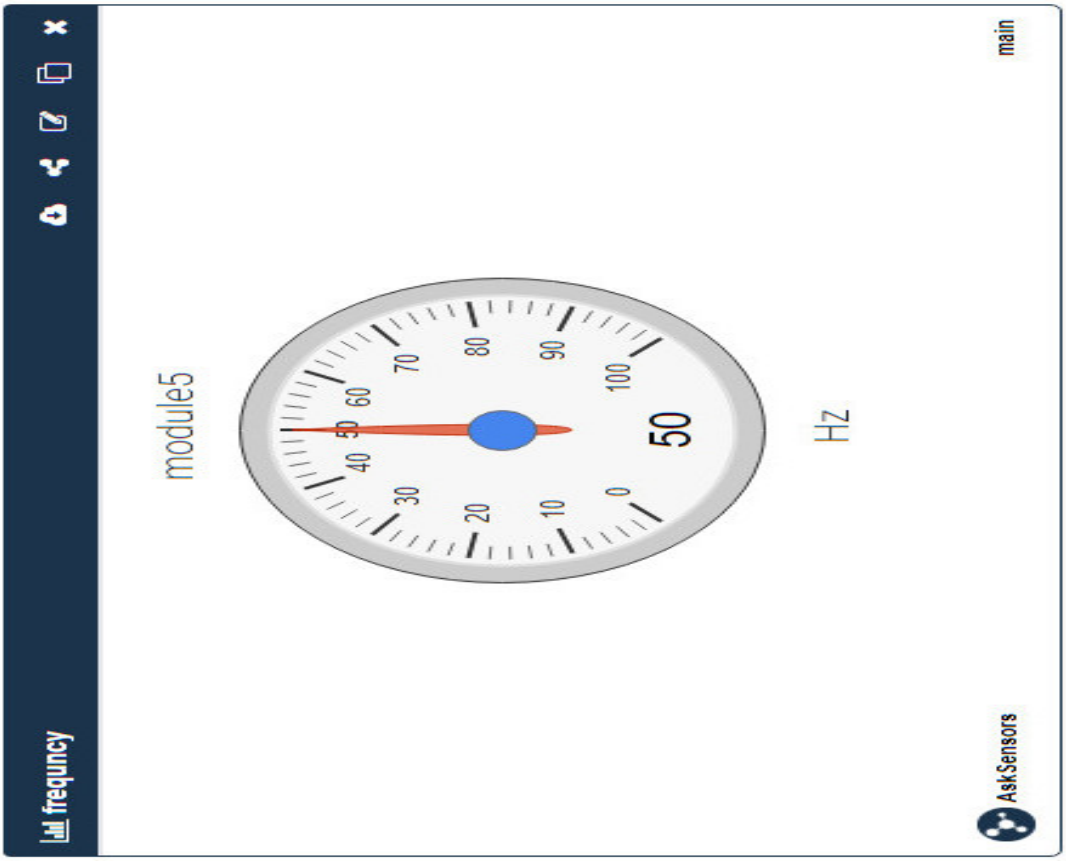


Parameters	Value	Units
Voltage	239.40	Volts
Current	1.06	Amperes
Power Factor	0.55	unitless
Power	140.50	Watts
Frequency	48.9	Hz

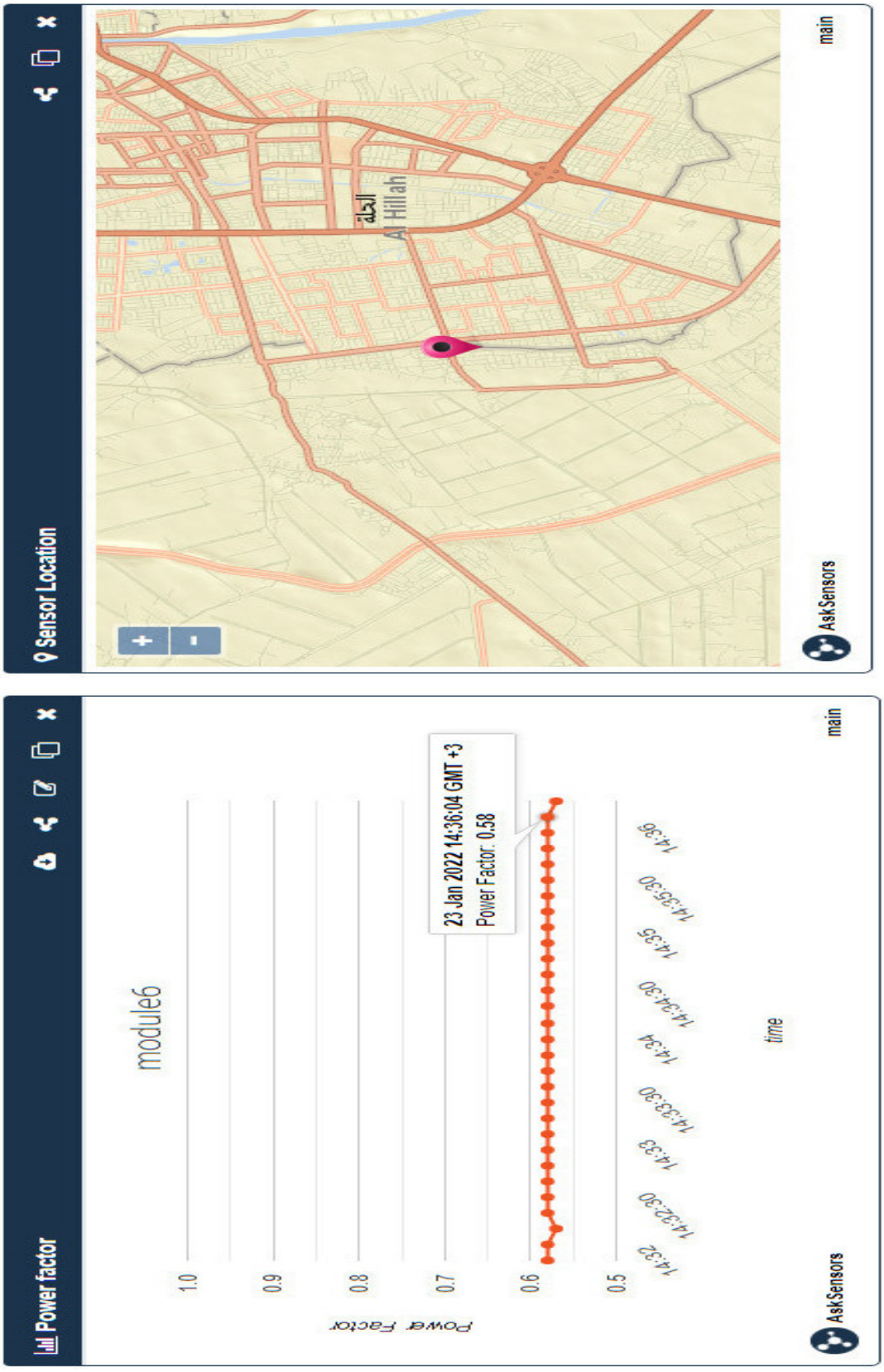
Figure 4.2: Webserver values of PZEM-004 sensor parameters with device connection on home main source.



(a) Voltage and current reading in Askedsensors every 10 seconds



(b)Power and frequency results in Askedsensors every 10 seonds



(c) Power factor and the map of home position

Figure 4.3: (a,b,c) results of IoT platform for energy parameters of 140W lamps.

This way of monitoring is also limited by the number of nodes for data collection or restricted to further processes on data in the cloud. In addition, the processes are limited to IoT devices only, and most services need to pay to use them. Also, these ways gave ripple variation in electric data readings.

4.3 Power and Energy Monitoring using Cloud Platform

In the monitoring using cloud vision, the MQTT discussed previously in section 2.14.2 will be employed with the external or internal(local) broker to get the data of PZEM from NodeMCU, and the data will be brought inside the server as PC or Raspberry Pi that will run IBM platform of Node-red. This platform is based on backend node.js with JavaScript language. In this monitoring, the raspberry pi 4 with (4Gb RAM) is used with an external MQTT is employed, and the Pi is used without peripherals and can be accessed through its IP from another PC via putty SSH software, as depicted in figure 4.4.

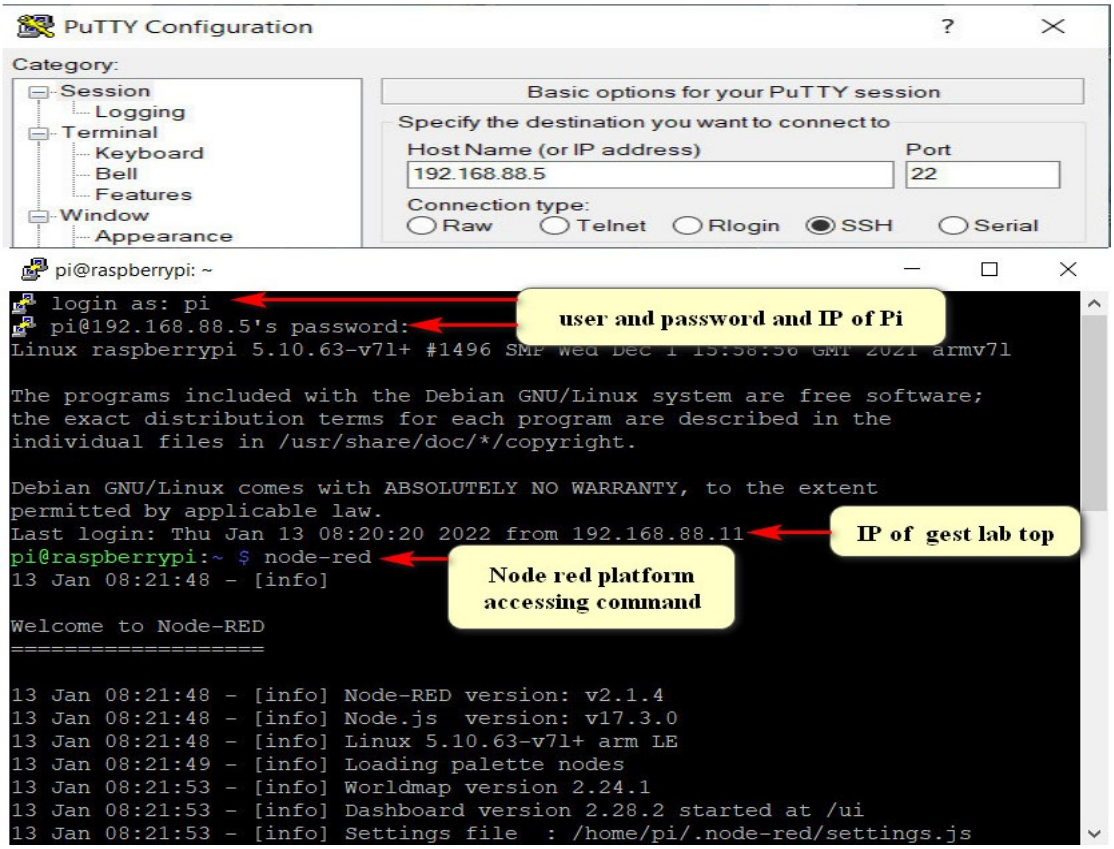


Figure 4.4: SSH accessing to the Raspberry Pi.

The monitoring page in the server can be accessed via the browser with the same IP address. Also, the same hardware connection in figure 4.2 is used to give the data to design a flow of processes inside the Node-red platform. This flow is a canvas in Node-red with icons or nodes set to perform a specific job as in figure 4.5.

The MQTT in nodes as mentioned in comment icon of "PZEM reading from nodeMCU" like UEM/voltage, UEM/current and other MQTT in here bring the data from MQTT broker that extracted the data from PZEM-004 and NodeMCU group to Raspberry Pi Node-red platform.

Further, the functions made using JavaScript language to exchange the float of other nodes named values that used to draw the data and the debug node to show the readings data inside the platform.

The remote access node that links the platform flow to the Android app for anywhere access, also a map function node of the world map was designed and built via JavaScript function gives green and red icons with a home name where sensor placed for normal voltage and voltage below 190V. In addition, the function gives longitude and latitude inserted for each PZEM-004 sensor. The function and its results are shown in figure 4.6.

The monitoring results of the same loads of 140W got in a separate web page called a dashboard consist voltage gauge and curve, current gauge and curve, and current gauge and curve also power factor and frequency gauges and these results are shown in figure 4.7.

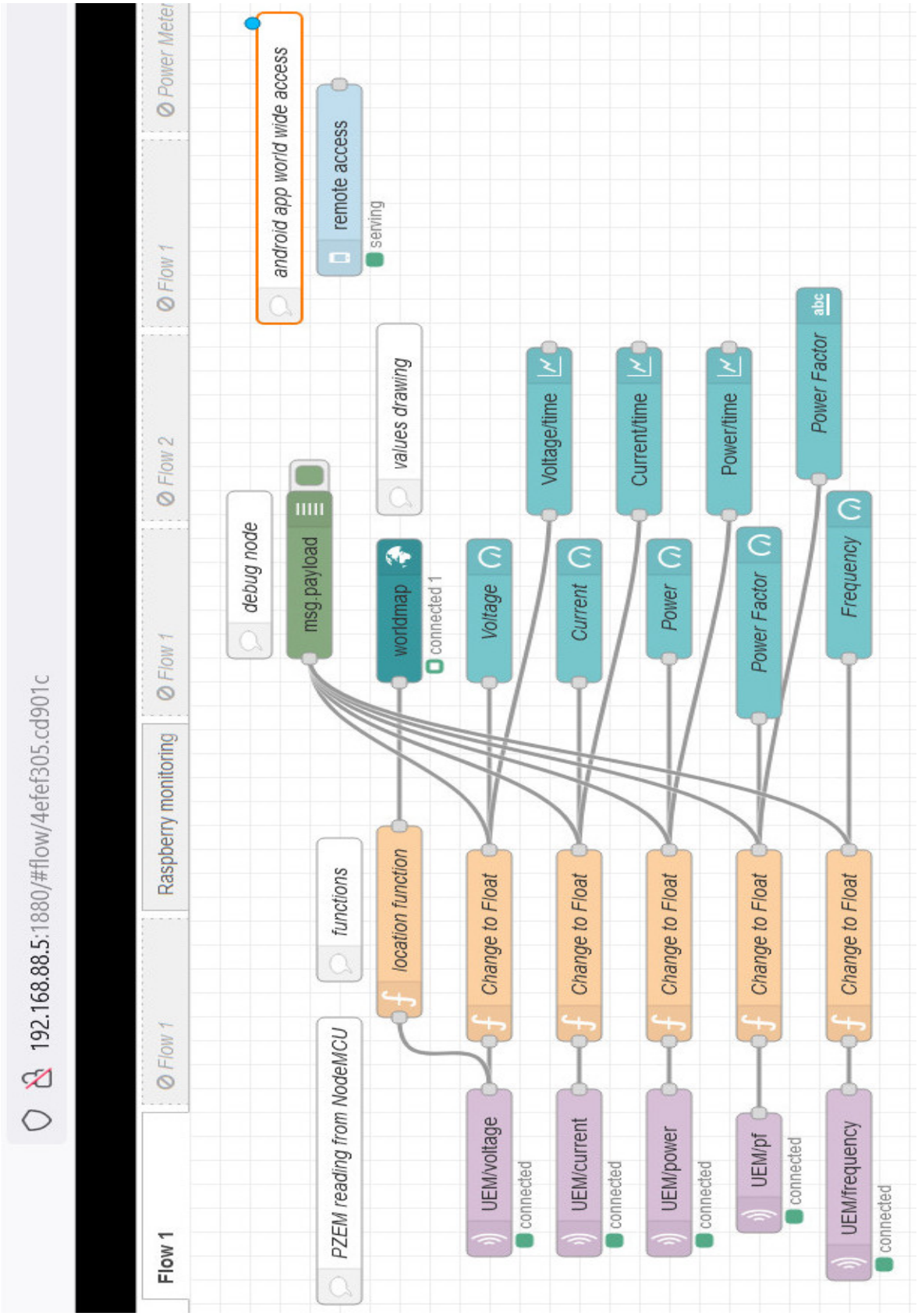


Figure 4.5: Energy Monitoring implementation inside Raspberry Pi.

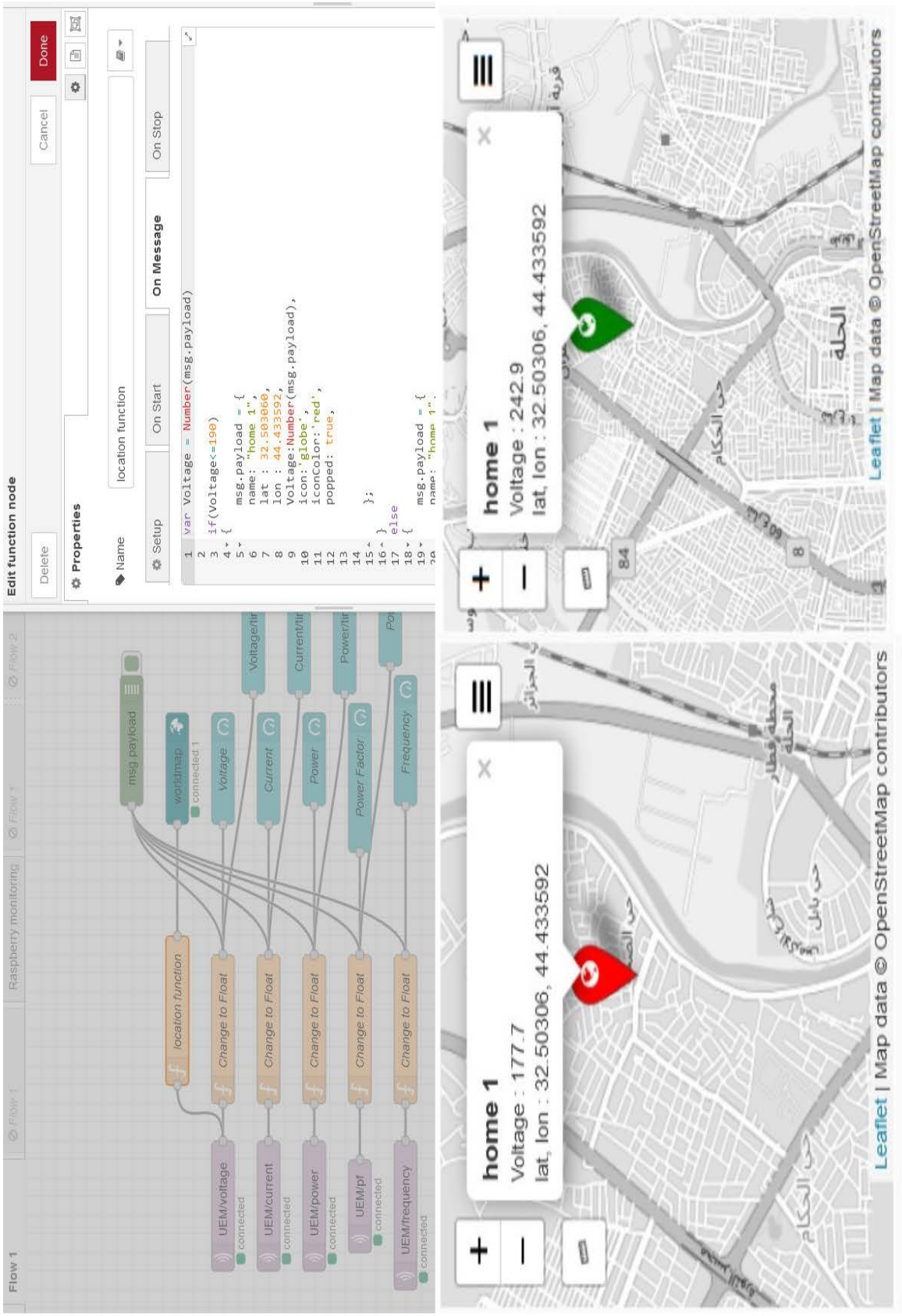


Figure 4.6: Map function code in JavaScript, Node-red and its results.

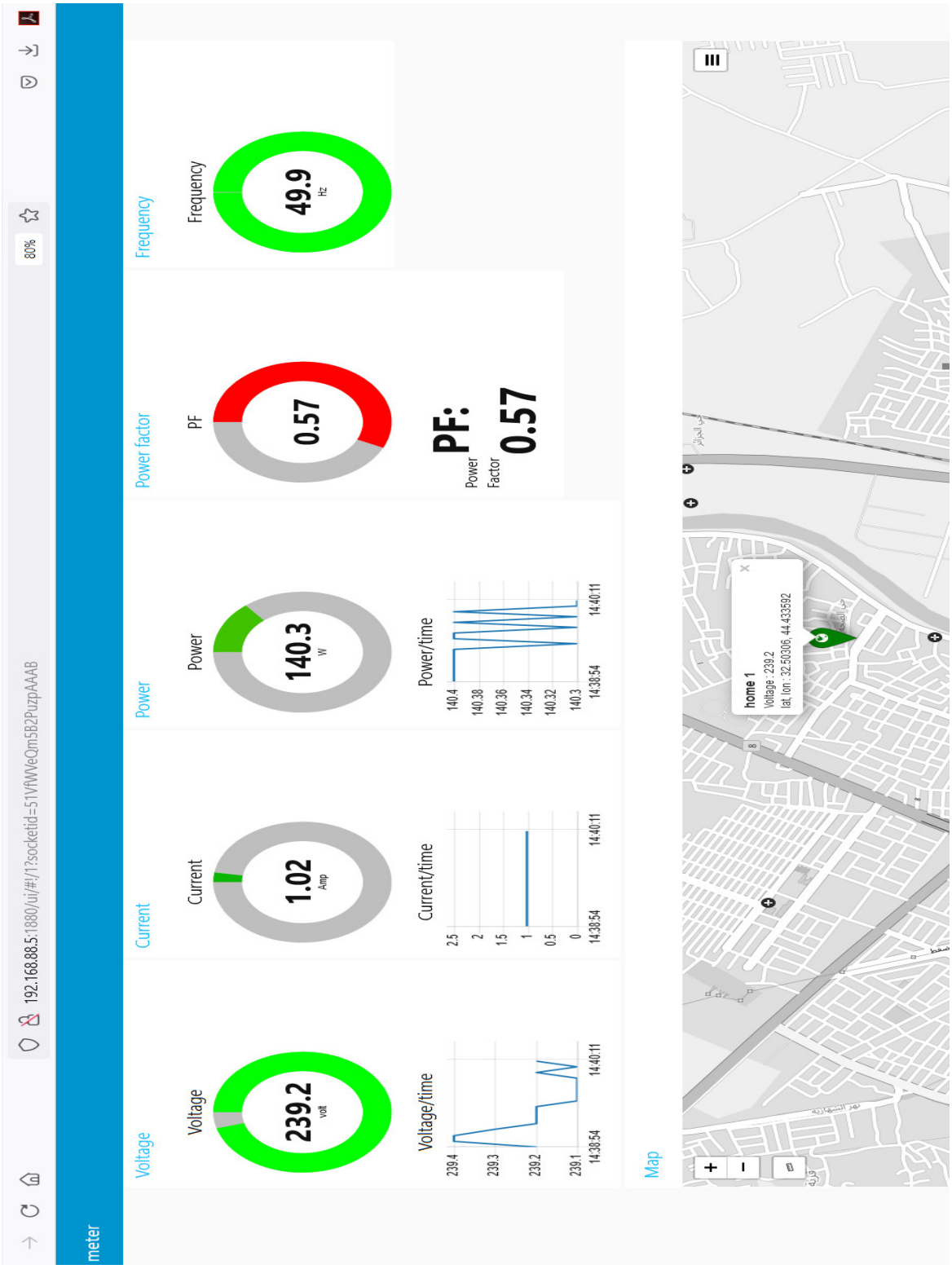


Figure 4.7: Monitoring results of the lamps of 140W using Node-red.

The mobile app on Android and for results the same 140 W are shown in figure 4.8.

Figure 4.8: Monitoring results of the lamps of 140W with the Android app.

The monitoring using this platform inside the private cloud server is different from the two previous ways of monitoring by offering flexibility in data managing and further process on it, it reads data every 10 second and the page of monitoring from the server can be accessed via the browser with the same IP address. In addition, the mobile app Android from IBM company that related to Node-red platform can access from any network to monitor data. This way of monitoring will be used later in the other suggested objectives.

The state of Raspberry Pi, like disk space, free memory, CPU temperature, and utilisation of CPU results for this monitoring process can be seen in figure 4.9.

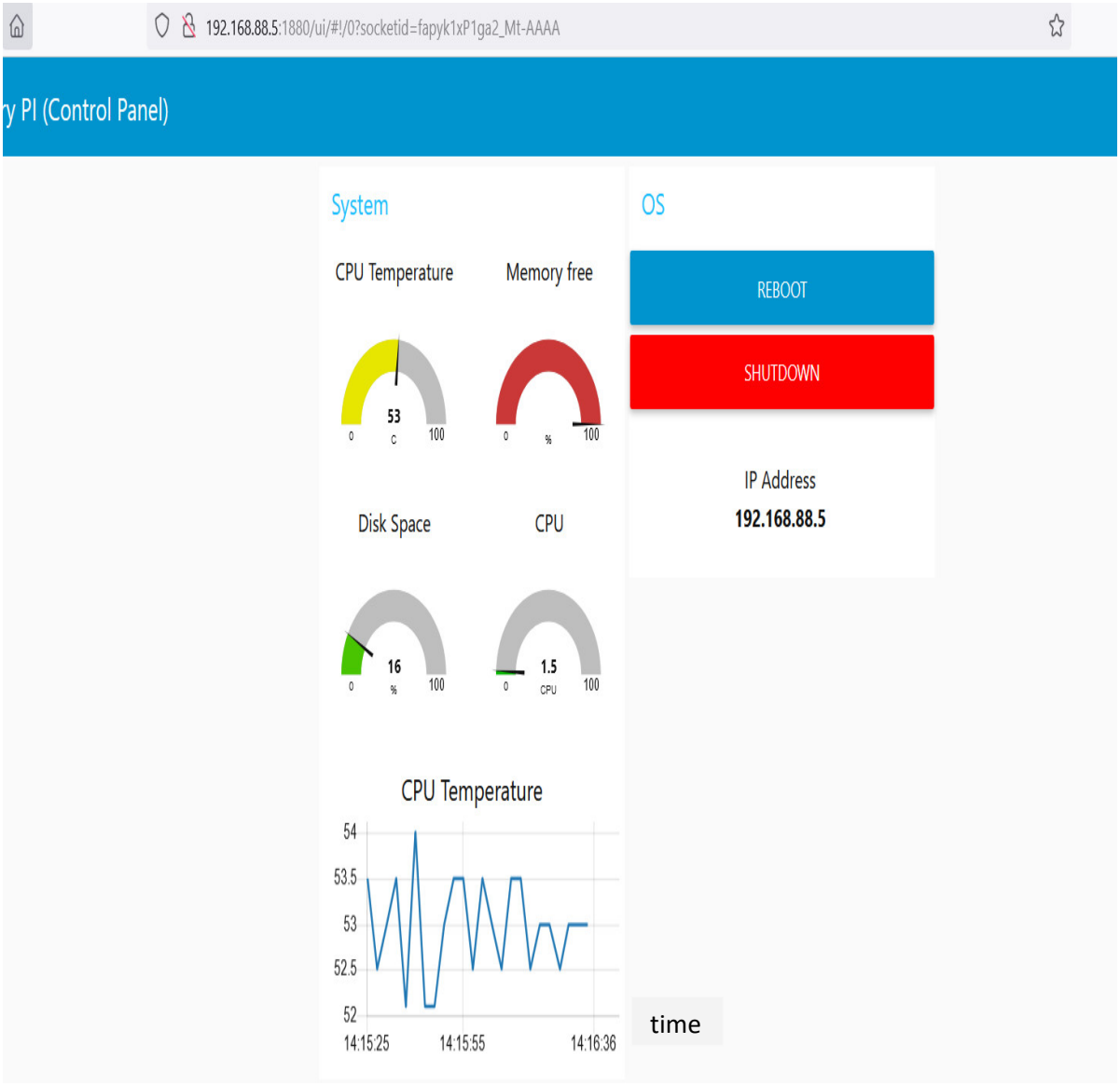


Figure 4.9: Raspberry Pi status during the monitoring process.

This panel was designed in a different node.js flow design with Linux commands to track the state of the server, and it helped to give the IP address and enable shutdown or reboot.

4.4 Power and Energy Monitoring using Cloud Platform with Database

The previous monitoring process can be modified to be more useful by adding a database like influx DB, a type of database, and using a more detailed visualisation dashboard like Grafana design, as in figure 4.10.

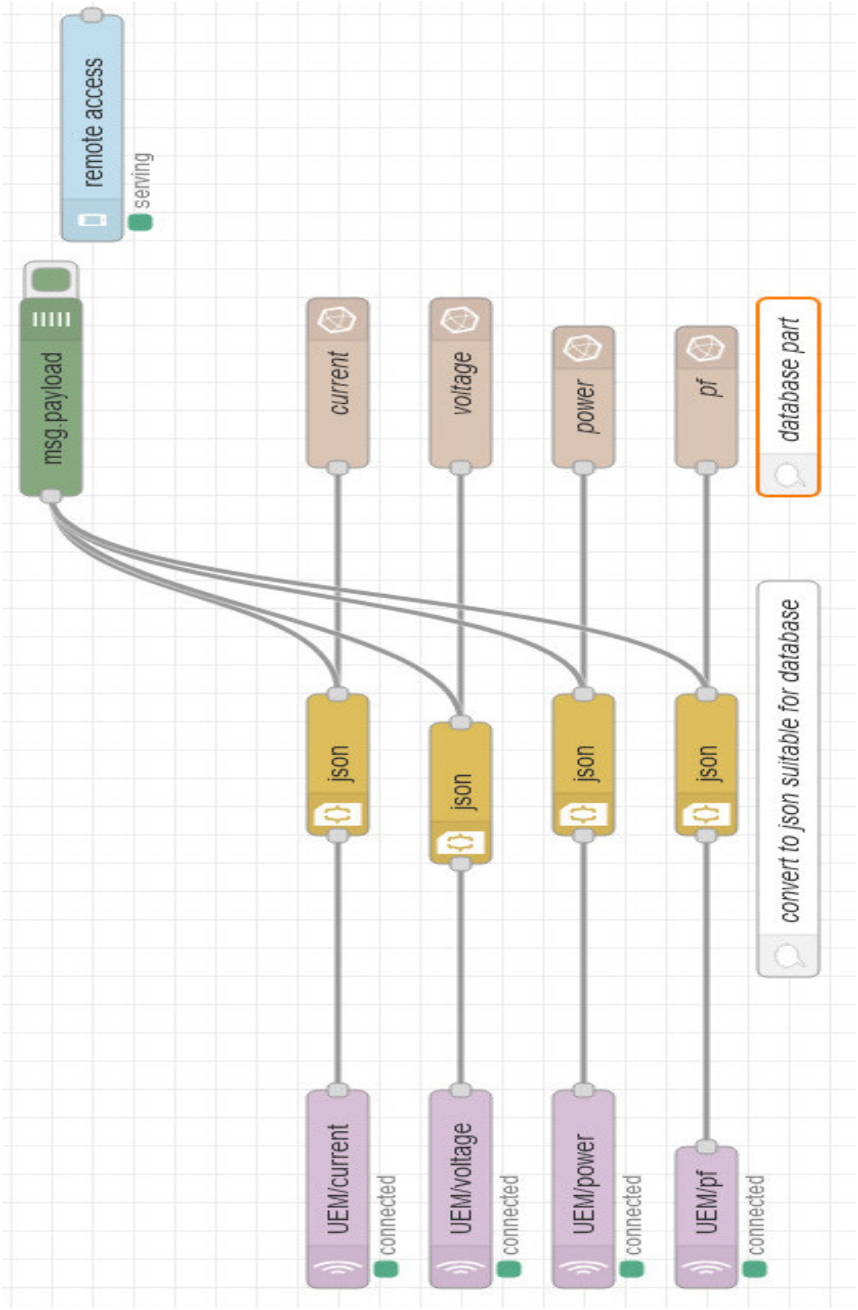


Figure 4.10: Energy monitoring implementation with database in Raspberry Pi.

The MQTT in nodes measurements data is converted to JSON using JSON node to suit the database. The database node named voltage, current and others represent the influx DB in the Raspberry Pi server. It collected the data in the database and linked it to the Grafana dashboard to draw it more configurable. The Grafana and influx DB installed inside Raspberry Pi can be accessed via the same Raspberry Pi IP with different ports for each one. An example of the power parameter showed value and query from UEM/power MQTT for 140 W lights is shown in figure 4.11. This result has some fluctuation or ripple of ±2W in the curve due to the database reading latency. All parameter results of monitoring are depicted in figure 4.12, also A ripple of ±1V in the curve of voltage due to the database reading latency

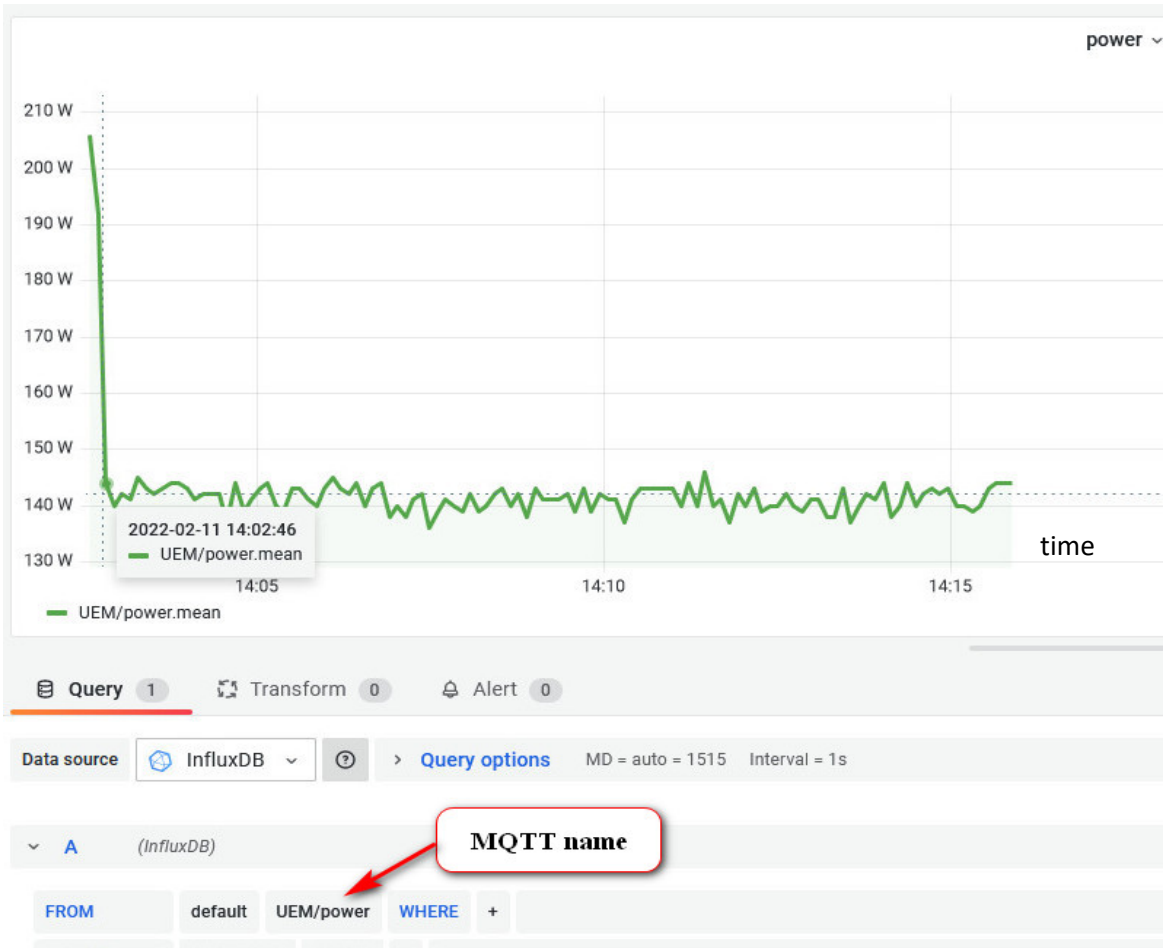


Figure 4.11: Power monitoring using Grafana and influx DB.

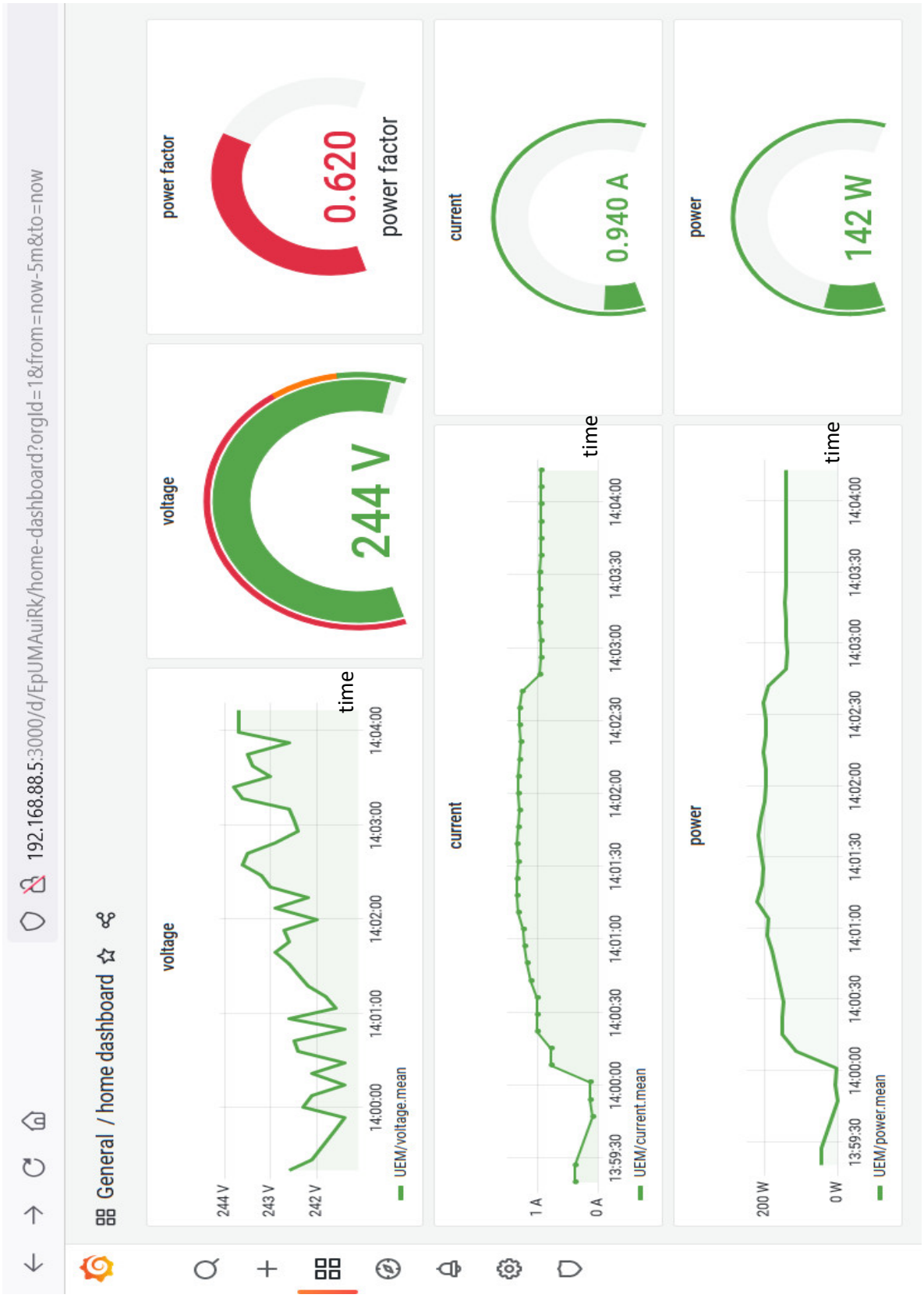


Figure 4.12: Power monitoring using Grafana and influx DB for 140w lights.

The database of influx DB for parameters is named sensors. It contains all power and voltage and current and power factor parameters. Also, it is essential for linking with a dashboard. Some values are of mentioned parameters versus Unix time are shown in figure 4.13.

```
Connected to http://localhost:8086 version 1.8.10
InfluxDB shell version: 1.8.10
> use sensors
Using database sensors
> show measurements
name: measurements
name
----
PEM/current
UEM/current
UEM/pf
UEM/power
UEM/voltage
UEM1/current
UEM2/current
UEM3/current
> SELECT * FROM "UEM/voltage","UEM/current","UEM/power","UEM/pf" WHERE time >
44578100s
name: UEM/current
time                value
----                -----
1644578104280953631 0.95
1644578111240745226 0.96

name: UEM/pf
time                value
----                -----
1644578104281530526 0.61
1644578111241548858 0.6

name: UEM/power
time                value
----                -----
1644578104281293235 140
1644578111241105663 140

name: UEM/voltage
time                value
----                -----
1644578104055417230 242.1
1644578111055661685 241.9
>
```

Figure 4.13: Influx DB data for 140w lights.

4.5 Power Factor Correction with Cloud

The system proposed in chapter three in the flow chart depicted figure 3.7 of and the block diagram in figure 3.2 was implemented using the same way mentioned in section 4.4 in figure 4.10. The power and power factor data were extracted from MQTT, and the mentioned flow was modified by adding a simple time and templet node to link the data with time to be suitable to save in a file inside raspberry pi. Finally, the file node (File save in) writes data to a text file that can be used later to process the modified design shown in figure 4.14.

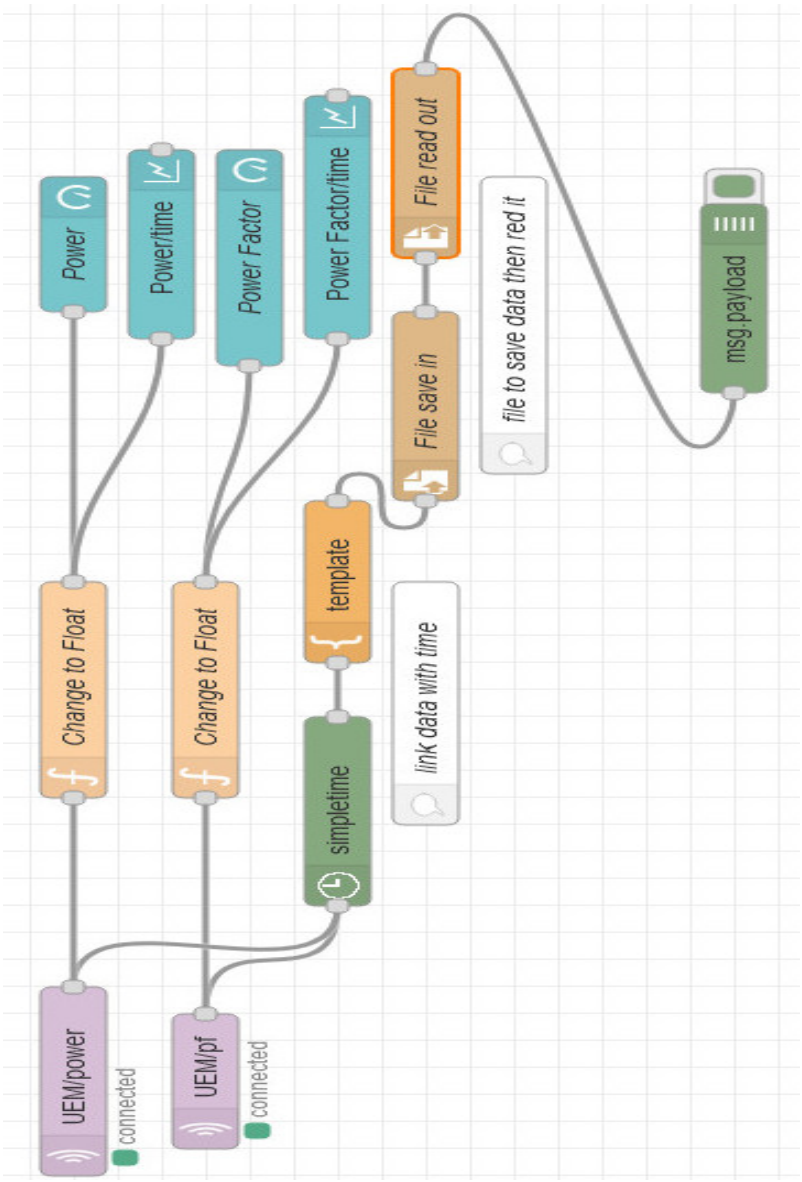


Figure 4.14: Design for power and power factor appliance data save in a file.

The processing of neural will be done using MATLAB R2020b.A sample of the execution of the previous flow is stated in figure 4.15. The data read from a file by file read node (File read out) from a text file

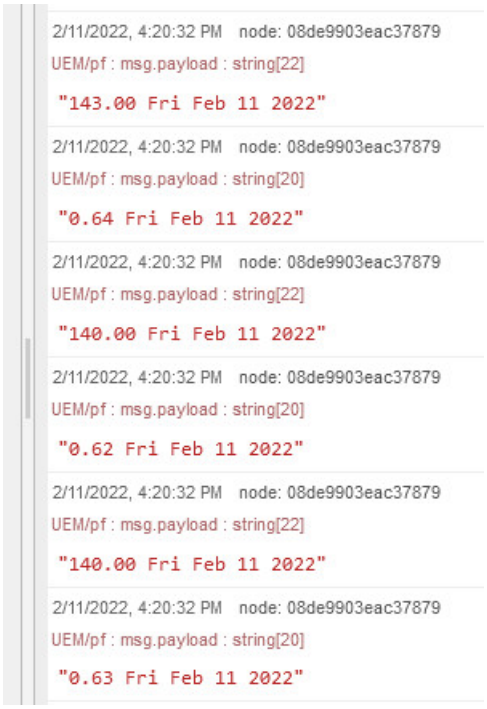


Figure 4.15: A data sample of power and power factor appliance read from a file.

4.5.1 Neural Capacitance Decision for Power Factor Correction

The neural network training table was created from the power and power factor of the first five appliances from table 3.1, and the untrained test data was also selected from the remaining data in the same table. The training appliances are switched alternately to give thirty-one cases of actual reading power and power factor gained by the ways in the previous sections. The required capacitance value was calculated using the equations (2.4), (2.5) to get the supposed power factor of 0.97 as desired value. Six levels of actual hardware capacitance values are proposed from a combination of (2,5,10,15) µF. These levels as (2,5,10,12,22,27) µF and in numbers (1,2,5,3,4,6) as in table 4.1. The task of the neural network circumscribes the level of capacitance nearest or the

same value from mentioned levels to give real power factor correction.

Table 4.1 Power and power factor and capacitance training data of neural network.

ID	Load device	Power (W)	Pf original	Pf desired	C calculated Farad	C real Farad	level	Pf for real C	Q VAR
1	(**A**) Led light	30	0.55	0.97	2.1e-6	2e-6	1	0.95	38.03
2	(**B**) Led light	80	0.58	0.97	5.1e-06	5e-6	2	0.96	92.31
3	(**C**) stand fan	55	0.82	0.97	1.35e-06	2e-6	1	0.99	24.60
4	(**D**) Freezer	155	0.46	0.97	1.43e-05	12e-6	3	0.88	260.34
5	(**E**) Fridge	237	0.64	0.97	1.24e-5	12e-6	3	0.96	225.14
6	**A+B**	110	0.62	0.97	6.1e-06	5e-6	2	0.91	111.63
7	**A+C**	85	0.79	0.97	2.46e-06	2e-6	1	0.94	44.66
8	**A+D**	185	0.53	0.97	1.37e-05	12e-6	3	0.92	249.63
9	**A+E**	267	0.69	0.97	1.17e-05	12e-6	3	0.97	213.16
10	**B +C**	135	0.76	0.97	4.5e-06	5e-6	2	0.98	81.61
11	**B +D**	235	0.62	0.97	1.31e-05	12e-6	3	0.94	238.49
12	**B +E**	317	0.75	0.97	1.1e-05	10e-6	5	0.95	200.12
13	**C+D**	210	0.6	0.97	1.25e-05	12e-6	3	0.95	227.36
14	**C+E**	292	0.74	0.97	1.06e-05	10e-6	5	0.96	192.22
15	**D+E**	392	0.54	0.97	2.83e-05	27e-6	6	0.95	512.74
16	**A+ B +C**	165	0.74	0.97	6 e-06	5e-6	2	0.94	108.62
17	**A+ B +D**	265	0.66	0.97	1.3e-05	12e-6	3	0.95	235.22
18	**A+B+E**	347	0.76	0.97	1.15e-05	12e-6	3	0.97	209.77
19	**A+C+E**	322	0.79	0.97	9.35e-06	10 e-6	5	0.97	169.19
20	**A+D+E**	422	0.56	0.97	2.86e-05	27e-6	6	0.95	518.56
21	**A+C+D**	240	0.65	0.97	1.21e-05	12e-6	3	0.96	220.44
22	**B +C+D**	290	0.72	0.97	1.14e-05	12e-6	3	0.97	206.83
23	**B +C+E**	372	0.82	0.97	9.2e-06	10 e-6	5	0.98	166.42
24	**B +D+E**	472	0.61	0.97	2.73e-05	27e-6	6	0.96	494.84
25	**C+D+E**	445	0.6	0.97	2.66e-05	27e-6	6	0.97	481.80
26	**A+ B +C+D**	320	0.75	0.97	1.11e-05	10 e-6	5	0.95	202.01
27	**A+ B +C+E**	400	0.83	0.97	9.31e-06	10 e-6	5	0.98	168.55
28	**A+ B +D+E**	502	0.64	0.97	2.63e-05	27e-6	6	0.97	476.88
29	**A+C+D+E**	477	0.63	0.97	2.6 e-05	27e-6	6	0.98	468.44
30	**B +C+D+E**	527	0.68	0.97	2.4 e-05	22e-6	4	0.95	436.16
31	**A+B +C+D+E**	557	0.7	0.97	2.3 e-05	22e-6	4	0.95	428.65

The training workout process of neural uses two input cells as power and power factor with one hidden layer of six cells and one cell as outcome layer that gives the appropriate level of simulated capacitance as in figure 4.16. In the first, the thirty-one cases of data for appliances are used to train the neural

network, then after equilibrium, the weight was extracted, and the neural be ready for later use for any appliances load with any power. The practising of neural was done by backpropagation with a sigmoidal function and six levels of capacitance, the levels can increase to train other high loads.

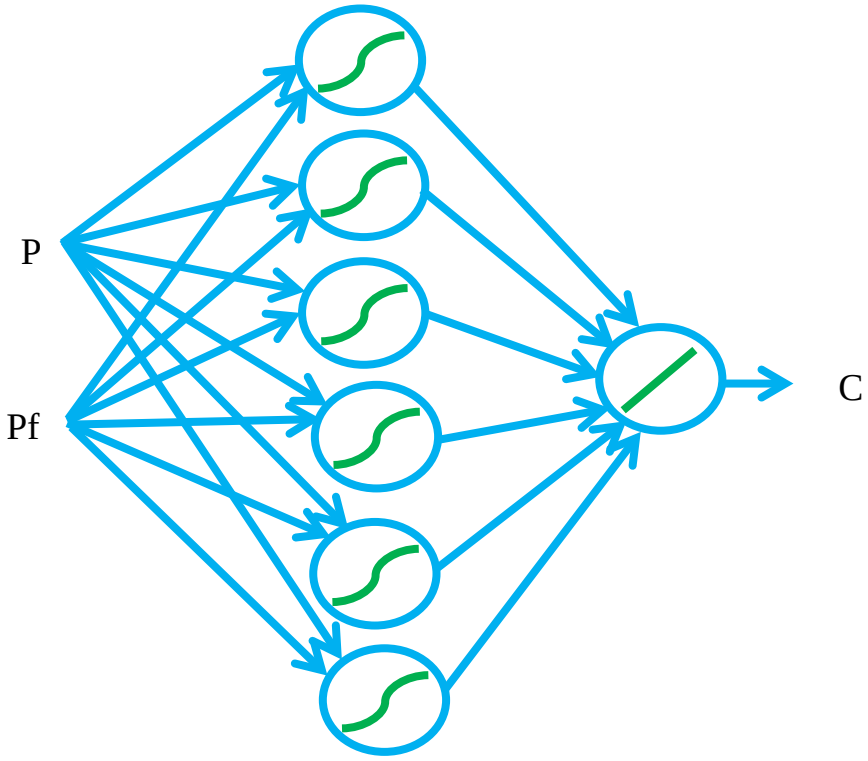


Figure 4.16: Neural network design for capacitance decision.

4.5.2 The Error of Power Factor and Neural

After creating a table for the desired power factor, the neural training error was 8.76 *$10^{-4,}$ and the testing error was 0.0014 for 186epoch, as in figure 4.17. The average power factor is 0.95. Also, the power factor error can be calculated as [(desired – actual)/ desired] power factor. The average error was 1.928%. The error, the average error and the average power factor are shown in table 4.2. The average error result of the power factor is less than the value in [17] that achieved an average error of 2.2%. The neural fabrication was simplified by one hidden layer with six cells concerning the same reference. Also, the capacitance level

was reduced to six from eight and the neural trained with higher load appliances than the mentioned reference. In our way, the power factor can be correct from 0.46, overcoming [9] that start correction from 0.64.

Table 4.2: Power factor and capacitnce error.

ID	Load device	Pf desired (pf_d)	C calculated Farad	C Real Farad	Pf corrected real C (pf_r)	Pf Error approximate %= (pf_d-pf_r)/pf_d	C error in µF C calc-C real
1	(**A**) Led light	0.97	2.1e-6	2e-6	0.95	2.061	0.1
2	(**B**) Led light	0.97	5.1e-06	5e-6	0.96	1.030	0.1
3	(**C**) stand fan	0.97	1.35e-06	2e-6	0.99	2.061	0.65
4	(**D**) Freezer	0.97	1.43e-05	12e-6	0.88	9.287	2.3
5	(**E**) Fridge	0.97	1.24e-5	12e-6	0.96	1.030	0.4
6	**A+B**	0.97	6.1e-06	5e-6	0.91	6.185	1.1
7	**A+C**	0.97	2.46e-06	2e-6	0.94	3.092	0.46
8	**A+D**	0.97	1.37e-05	12e-6	0.92	5.154	1.7
9	**A+E**	0.97	1.17e-05	12e-6	0.97	0	0.3
10	**B +C**	0.97	4.5e-06	5e-6	0.98	1.030	0.5
11	**B +D**	0.97	1.31e-05	12e-6	0.94	3.092	1.1
12	**B +E**	0.97	1.1e-05	10e-6	0.95	2.061	1
13	**C+D**	0.97	1.25e-05	12e-6	0.95	2.061	0.5
14	**C+E**	0.97	1.06e-05	10e-6	0.96	1.030	0.6
15	**D+E**	0.97	2.83e-05	27e-6	0.95	2.061	1.3
16	**A+ B +C**	0.97	6 e-06	5e-6	0.94	3.092	1
17	**A+ B +D**	0.97	1.3e-05	12e-6	0.95	2.061	1
18	**A+ B +E**	0.97	1.15e-05	12e-6	0.97	0	0.5
19	**A+C+E**	0.97	9.35e-06	10 e-6	0.97	0	0.65
20	**A+D+E**	0.97	2.86e-05	27e-6	0.95	2.061	1.6
21	**A+C+D**	0.97	1.21e-05	12e-6	0.96	1.030	0.1
22	**B +C+D**	0.97	1.14e-05	12e-6	0.97	0	0.6
23	**B +C+E**	0.97	9.2e-06	10 e-6	0.98	1.030	0.8
24	**B +D+E**	0.97	2.73e-05	27e-6	0.96	1.030	0.3
25	**C+D+E**	0.97	2.66e-05	27e-6	0.97	0	0.4
26	**A+ B +C+D**	0.97	1.11e-05	10 e-6	0.95	2.061	1.1
27	**A+ B +C+E**	0.97	9.31e-06	10 e-6	0.98	1.030	0.69
28	**A+ B +D+E**	0.97	2.63e-05	27e-6	0.97	0	0.7
29	**A+C+D+E**	0.97	2.6 e-05	27e-6	0.98	1.030	1
30	**B +C+D+E**	0.97	2.4 e-05	22e-6	0.95	2.061	2
31	**A+ B +C+D+E**	0.97	2.3 e-05	22e-6	0.95	2.061	1
Average pf					0.95		
Average error %						1.928	
Average capacitance error							0.824 µF

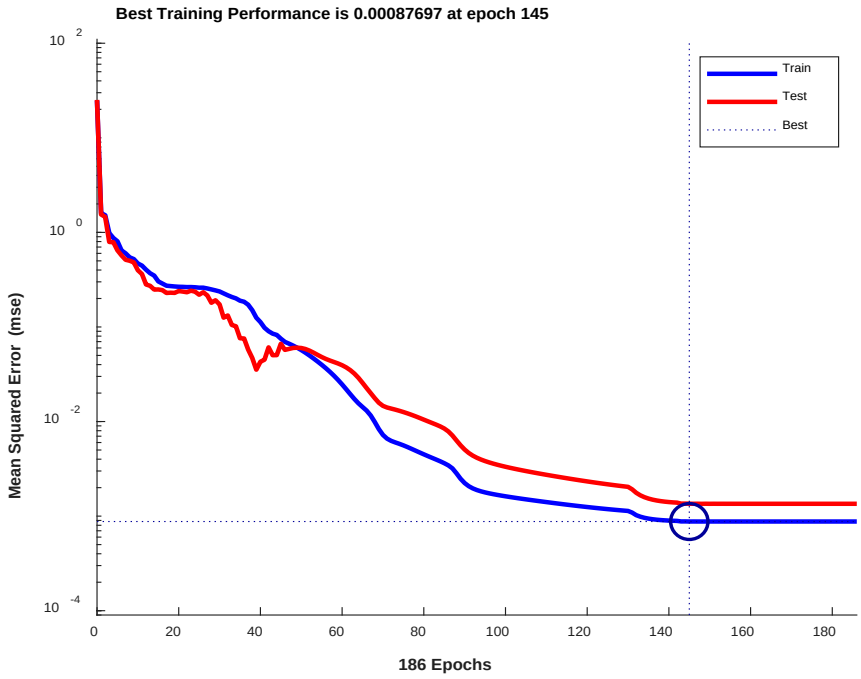


Figure 4.17: Neural network errors.

4.5.3 The Untrained Loads or Appliances Power Factor Correction

The neural network tested by untrained devices or loads from table 3.1 and the results of capacitance level is seen in table 4.3.

Table 4.3: Untrained power, pf and capacitance data of neural network.

ID	Load device	power (W)	Pf original	C calculated Farad	C Real By neural Farad	level	Pf corrected real C (pf_r)	Pf Error approximate %= (0.97-pf_r)/0.97	C error in µF C calc-C real
1	Led light	140	0.55	10.1e-06	12e-6	3	0.99	2.061	1.9
2	Gaming console	88	0.78	2.6e-06	2e-6	1	0.93	4.123	0.6
3	Led light	64	0.55	4.4e-06	5e-6	2	0.99	2.061	0.6
4	home random loads 1	266	0.67	1.26e-05	12e-6	3	0.96	1.030	0.6
5	home random loads 2	181	0.73	6.7e-06	5e-6	2	0.92	5.154	1.7
6	home random loads 3	377	0.61	21.8e-06	22e-6	4	0.97	0	0.2
7	home random loads 4	688	0.72	26.4e-06	22e-6	4	0.93	4.123	4.4
Average pf							0.95		
Average error %								2.650	
Average capacitance error									1.428 µF

The neural network achieved error in power factor from desired as 2.65% for untrained data superior the reference [17] of error 5.2%. The average corrected

power factor of the neural network is 0.95 for untrained data supreming [17] , which has an average power factor of 0.94.

4.6 Cloud Larceny Revelation with Cloud Computing

The system proposed in chapter three in figure 3.13 of the flow chart and the block diagram stated in figure 3.11 was implemented using a prototype environment, which is assumed to be equivalent to transformer source with some users. Suppose 3 meters are taken called UEM and main meter PEM as in the hardware design in figure 4.18.

The currents of mentioned meters i_1, i_2, i_3, and the main meter $\mathcal{I}$ and loads of these meters are proposed heaters with currents i_1= 2.56A, i_2=3.57A, i_3=4.89A. These values were proposed for the calculation process and taken from actual loads at a specific time. These currents are during experiments to avoid latency in an external broker. The overall design inside Node-red was mentioned in figure 4.19.

In this design, the meters data was collected using the ways mentioned in power monitoring, so the current here got from the MQTT of each meter. In this system, there are some JSONATA nodes to store in a variable, join and filter node to clear save values or track the change in values, also these nodes suitable with delay node. In addition to functions nodes to perform the algorithm.

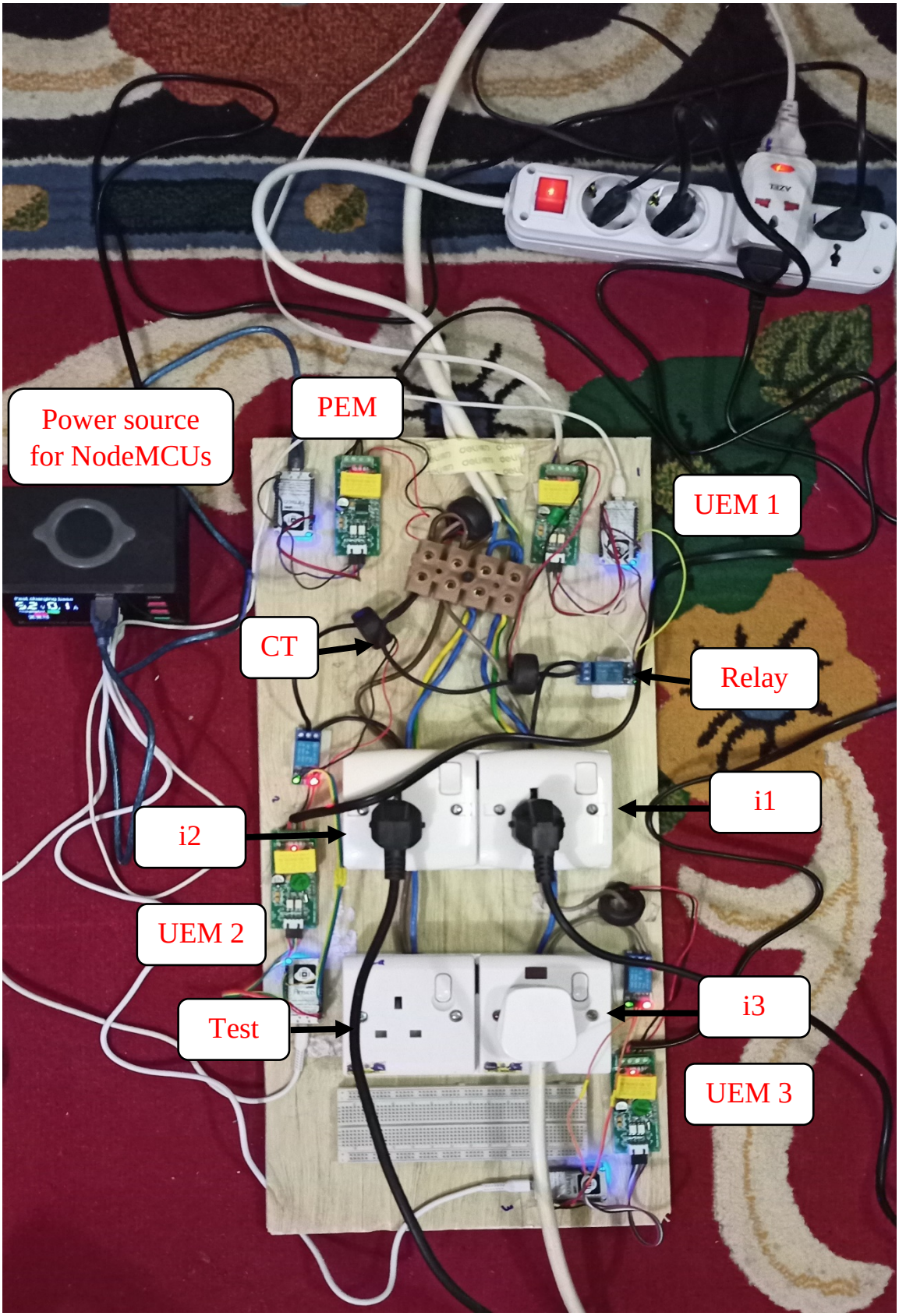


Figure 4.18: A Prototype hardware design for electric larceny detections.

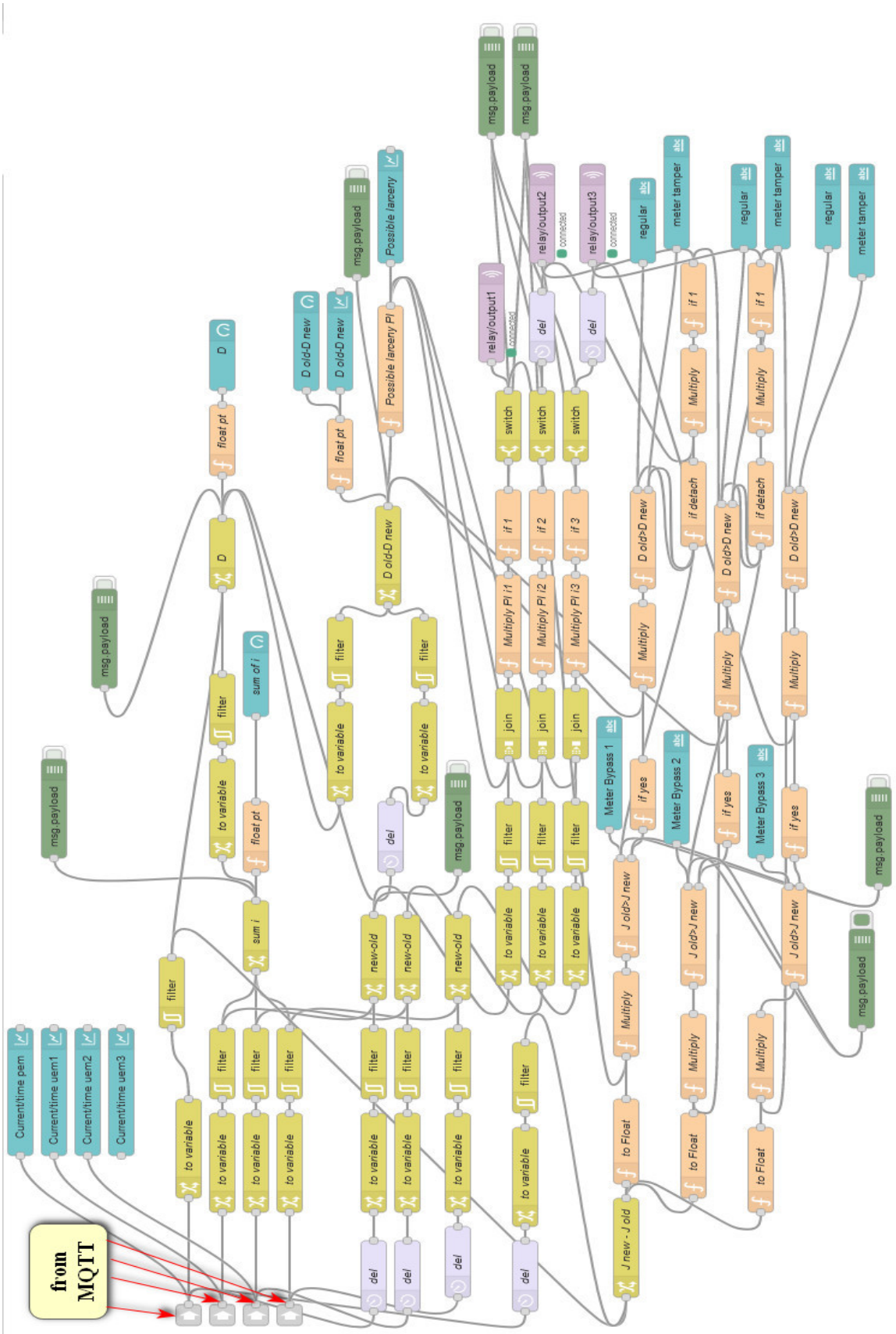


Figure 4.19: Overall design of electric larceny detections inside Node-red.

4.6.1 Data Fetching and Over Load Notification

The meters data are collected using the ways mentioned in power monitoring, so the current here got from MQTT of each meter then converted to JSON and stored in the database with the same name of each meter. Also, due to many nodes and saving space in the Node-red canvas, a link between the flow MQTT data collection and larceny detection flow was created like the flow chart link in two pages. The overload notification model and data are depicted in figure 4.20, the messages send of overload via the Android app are in the same way in the power monitoring section here. For assumption the current exceeds I_L=10A so, $I > I_L$ which gives notification every 20 seconds and the notification is shown in figure 4.21.

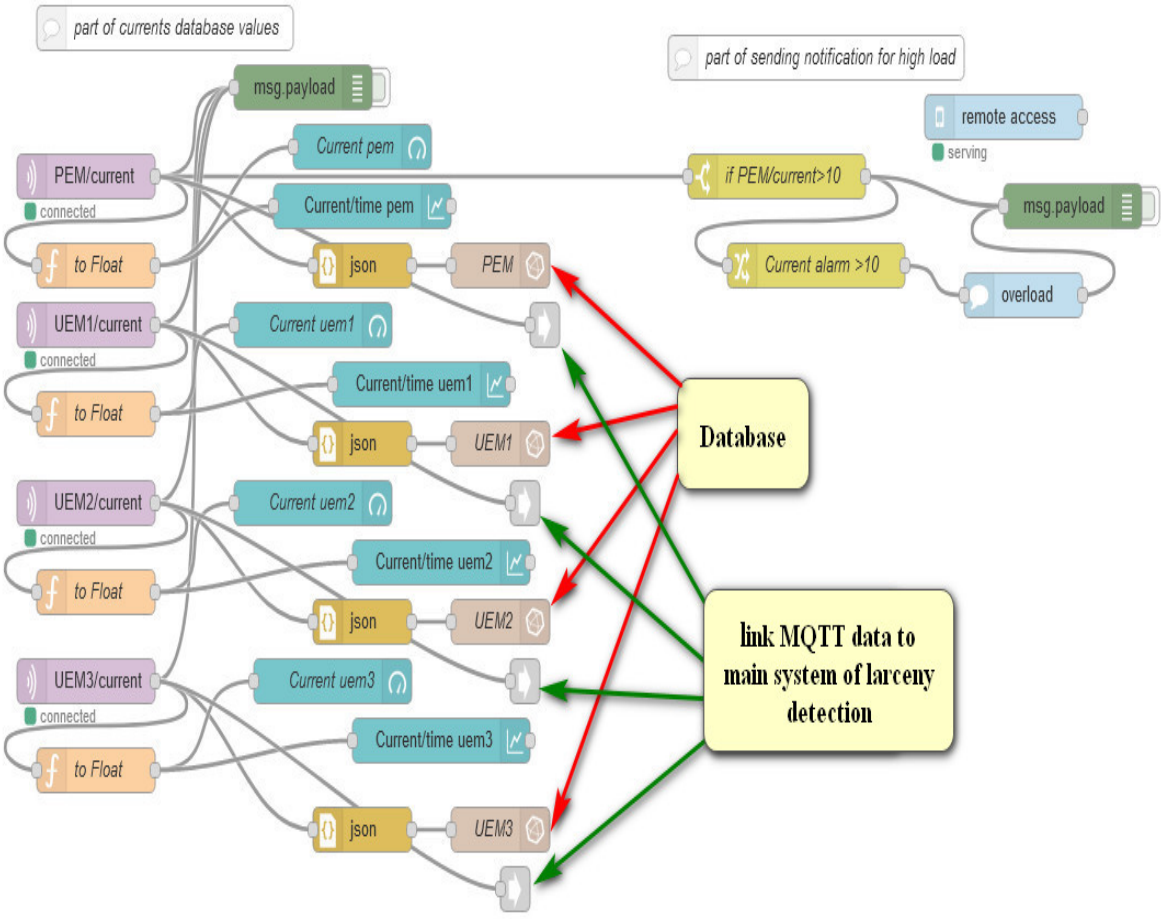


Figure 4.20: Overload notification model inside Node-red.

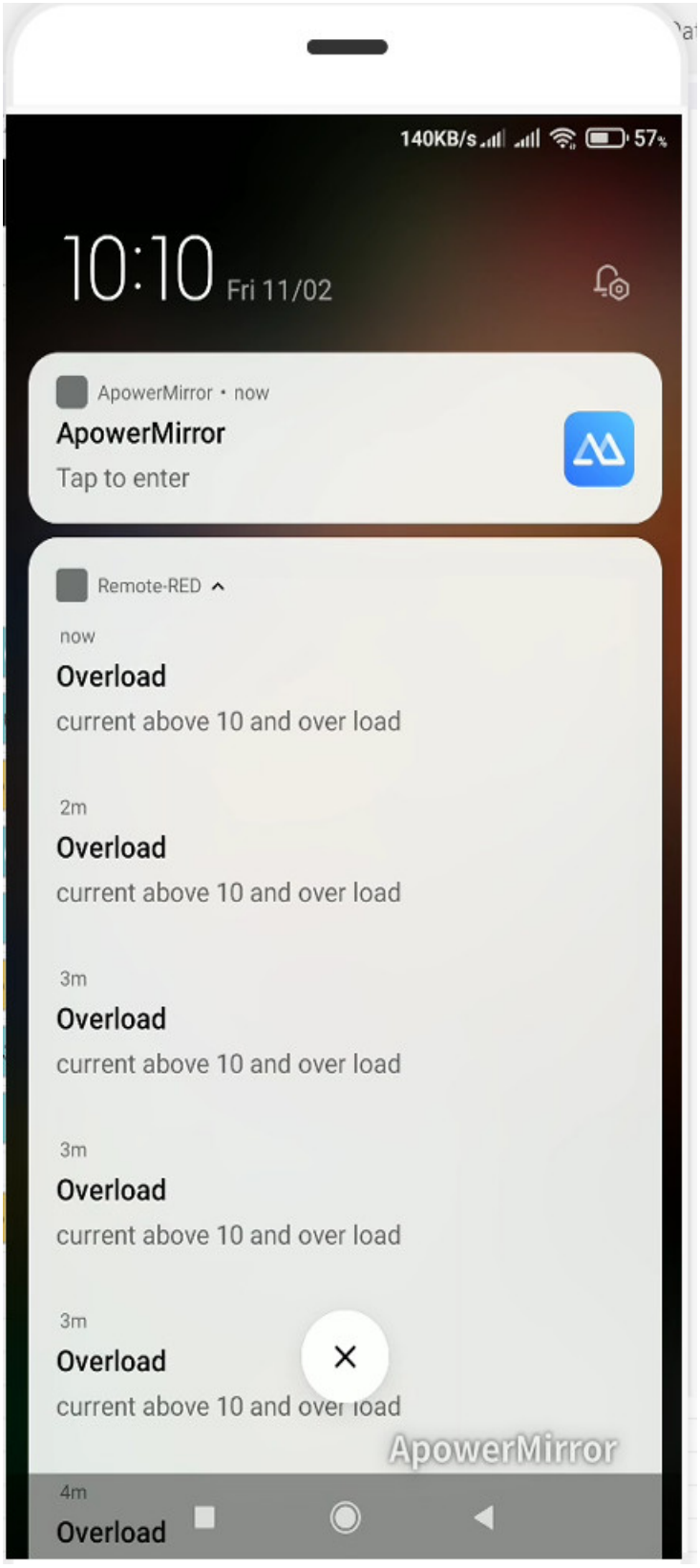


Figure 4.21: Notification results over Android app.

4.6.2 Meter Bypassed Case

In this system, no theft was supposed to start at precisely the same time, and an example for larceny via bypassing one meter is in figure 4.22 and for two meters in figure 4.23. Here the bypassing practically in the experiment is done by shunting the CT terminal or connecting without meter like shunting in a real case and detach done by the relay in the way of the input current of each meter.

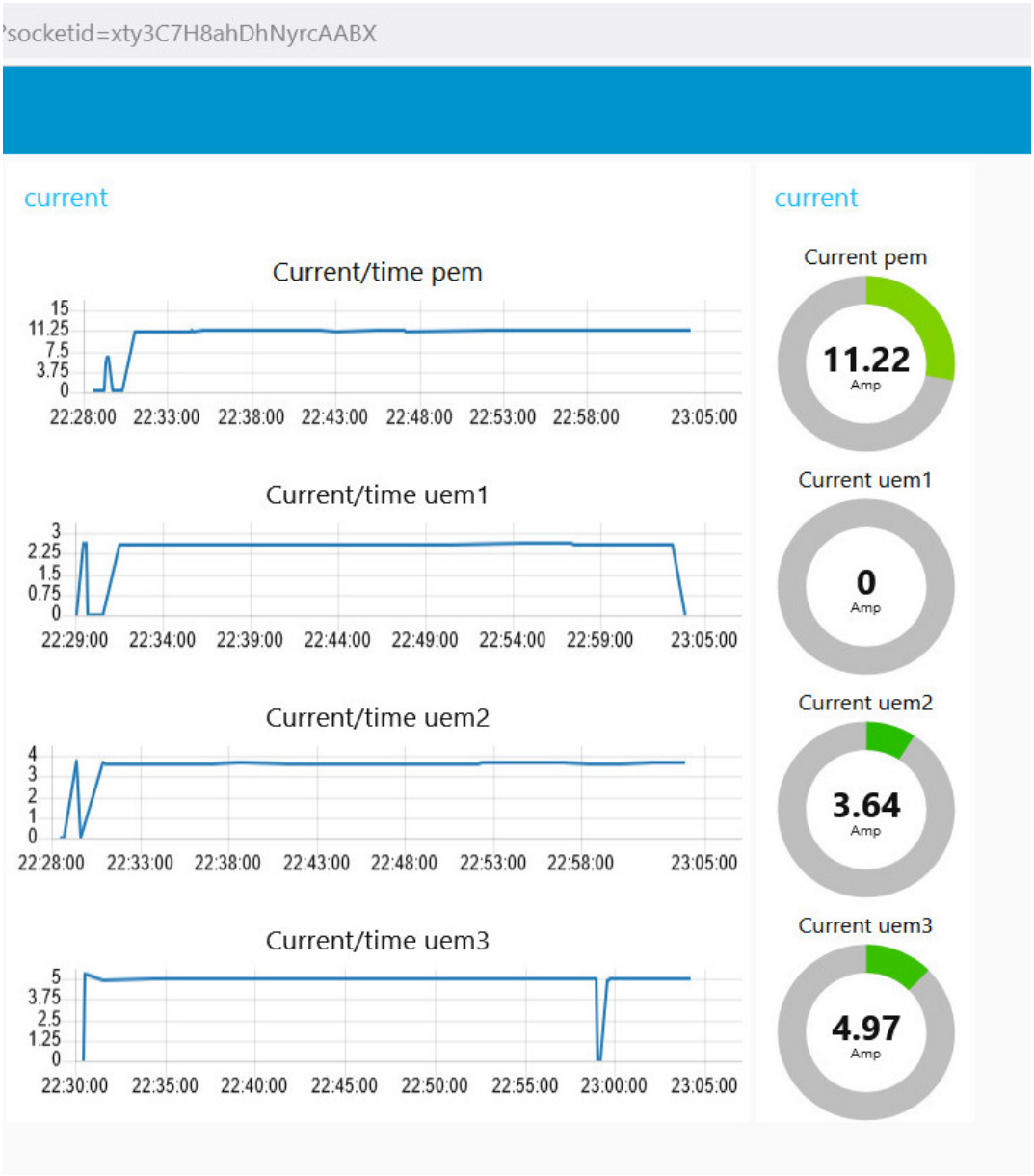


Figure 4.22**:** An example for larceny via bypassing meter UEM1.

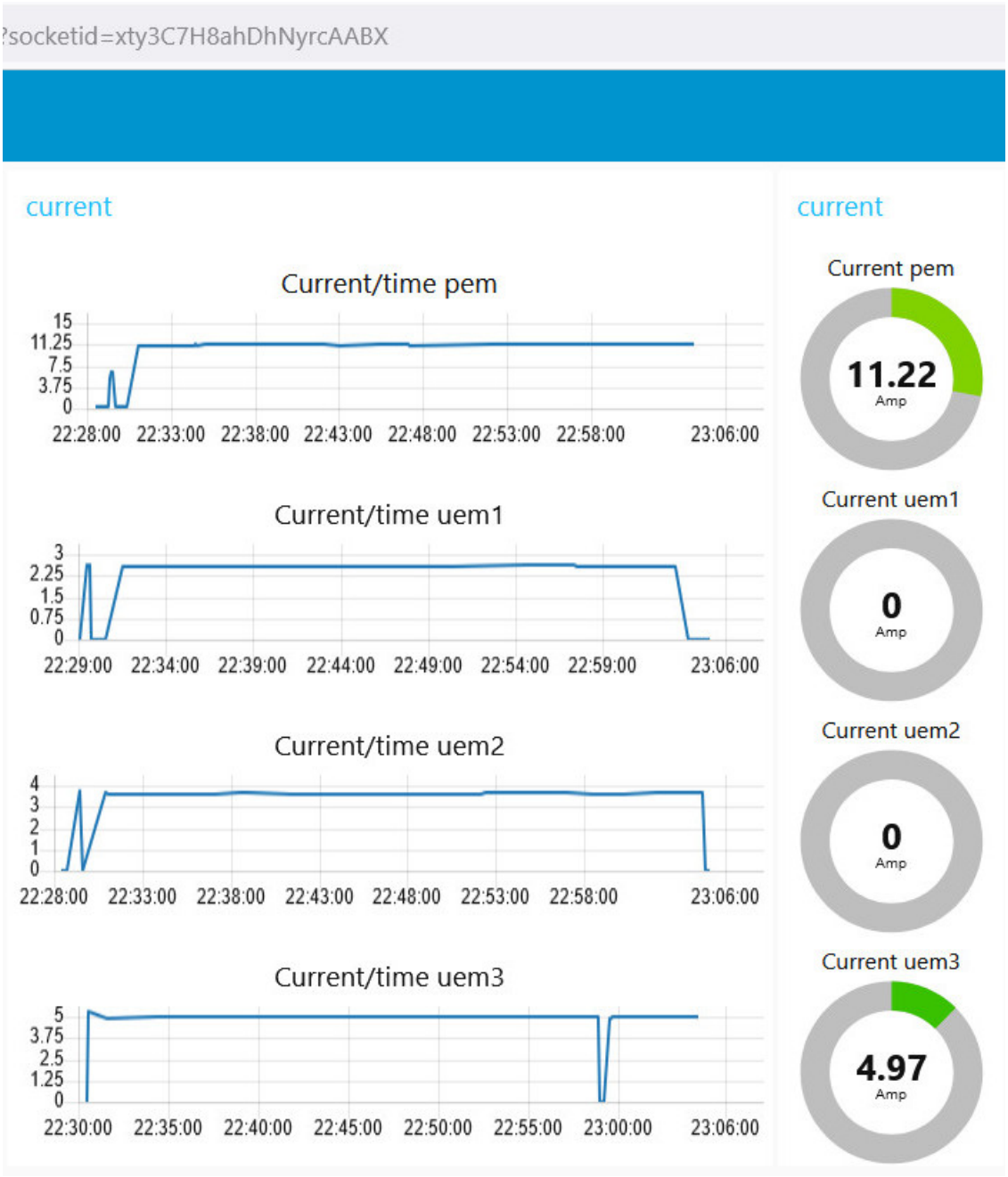


Figure 4.23**:** An example for larceny via bypassing meters UEM1 and UEM2.

In typical case by applying equation 3.1, $\mathfrak{D} = I - (i_1 + i_2 + i_3)$

$\mathfrak{D} = 11.02 - (2.56 + 3.57 + 4.89) = 0A.$

and according to equation 3.2 $\mathfrak{D}$ new $-$ $\mathfrak{D}$old=0A.

Here, the losses do not affect the algorithm and are supposed to be fixed because of subtraction of two different samples in equation 3.2, but it is supposed =0 for experimental because there is no real transformer source.

For example, let the main current I=11.52A, and the 0.5 is losses by applying equation 3.2 in the typical case without larceny $\mathfrak{D}\,\text{new} - \mathfrak{D}\text{old}$=0.5-0.5=0. So, the losses do not affect the algorithm.

In a larceny case, if one-meter UEM1 or i_1 was proposed to start theft so the equation 3.1 of reading values $\mathfrak{D} = 11.02 - (0 + 3.57 + 4.89) = 2.56\text{A}$, so equation 3.2 became 2.56-0 =2.56A and according to flow chart in figure 3.13 there is possible larceny because $\mathfrak{D}\,\text{new} - \mathfrak{D}\,\text{old} \neq 0$,

This thing was assigned as 1 for possible larceny and 0 for no larceny in algorithm then with this condition checking the variations of meters as on condition to detection (i old- i new) for all meters this thing was done by using delay node in algorithm so read values of differences ($i_1$old-i_1 new) =2.56-0=2.56A, (i_2 old-i_2 new) =3.57-3.57=0A. and (i_3 old-i_3 new) =4.89-4.89=0A.

After detaching the meter that has a difference in the condition of possible larceny, this possible case was mentioned as a multiplication process of the meter difference value and the 1 of possible larceny. After relay detaches so the meter UEM1, taking previous and now reading difference of main meter I, the $\text{I old} = 11.02\text{A}$ then $\text{I new} = 11.02\text{A}$ after that the meter UEM1 was in bypassing according to algorithm. The result of this case is depicted in figure 4.24. The figure was aggregated from results, and the second group of gauges represents the moment of start larceny, which is at time 4:31. The larceny detach and meter bypassed event is just trigger without units.

Figure 4.24**:** Larceny detection of bypassing meter of UEM1.

In case of two meters, start pilfering UEM1 or i1 and UEM2 or i2 after detaching UEM1 as previous, so the equation 3.1 of reading values $\mathfrak{D} = 11.02 - (0 + 4.89) = 6.13$ A, so equation 3.2 became 6.13-0 =6.13A and according to mentioned flow chart there is possible larceny because $\mathfrak{D}$ new $- \mathfrak{D}$ old $\neq 0$ then read values of differences after UEM1 detached previously.

(i_2 old-i_2 new) =3.57-0=3.57A,

(i_3 old-i_3 new) =4.89-4.89=0A

by detaching the meter UEM2 and taking previous and now reading difference of main meter I the Iold $= 11.02$ A, and I new $= 11.02$A, so the meter UEM2 was bypassing according to algorithm. The results of this case are shown in figure 4.25 at time 4:59 the indication for meter bypass is depicted.

4.6.3 Meter Tampering Case

In the larceny case of tampering, for example, the tampering of one meter is in figure 4.26 or for two meters, as shown in figure 4.27.

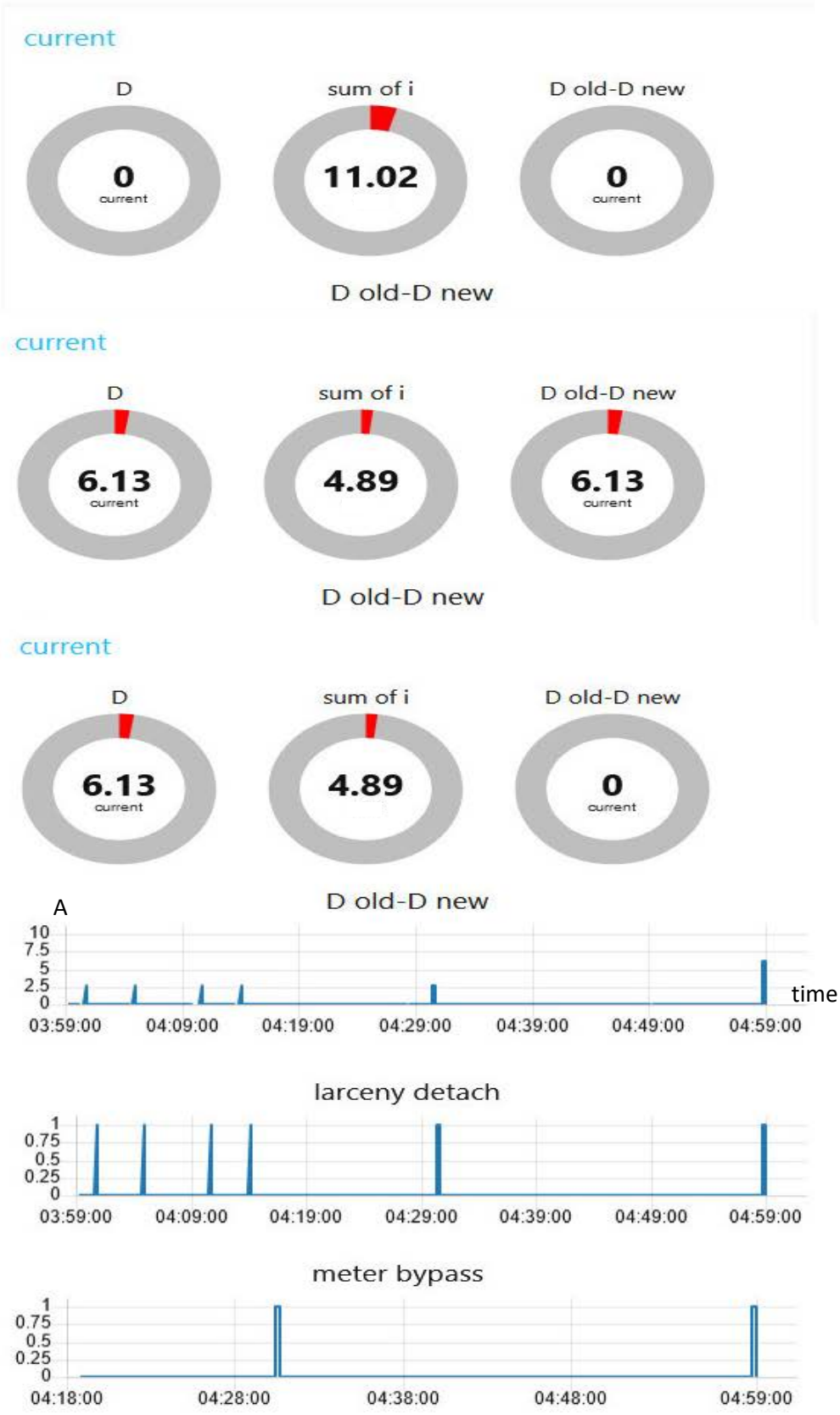


Figure 4.25**:** Larceny detection of bypassing meters of UEM1 and UEM2.

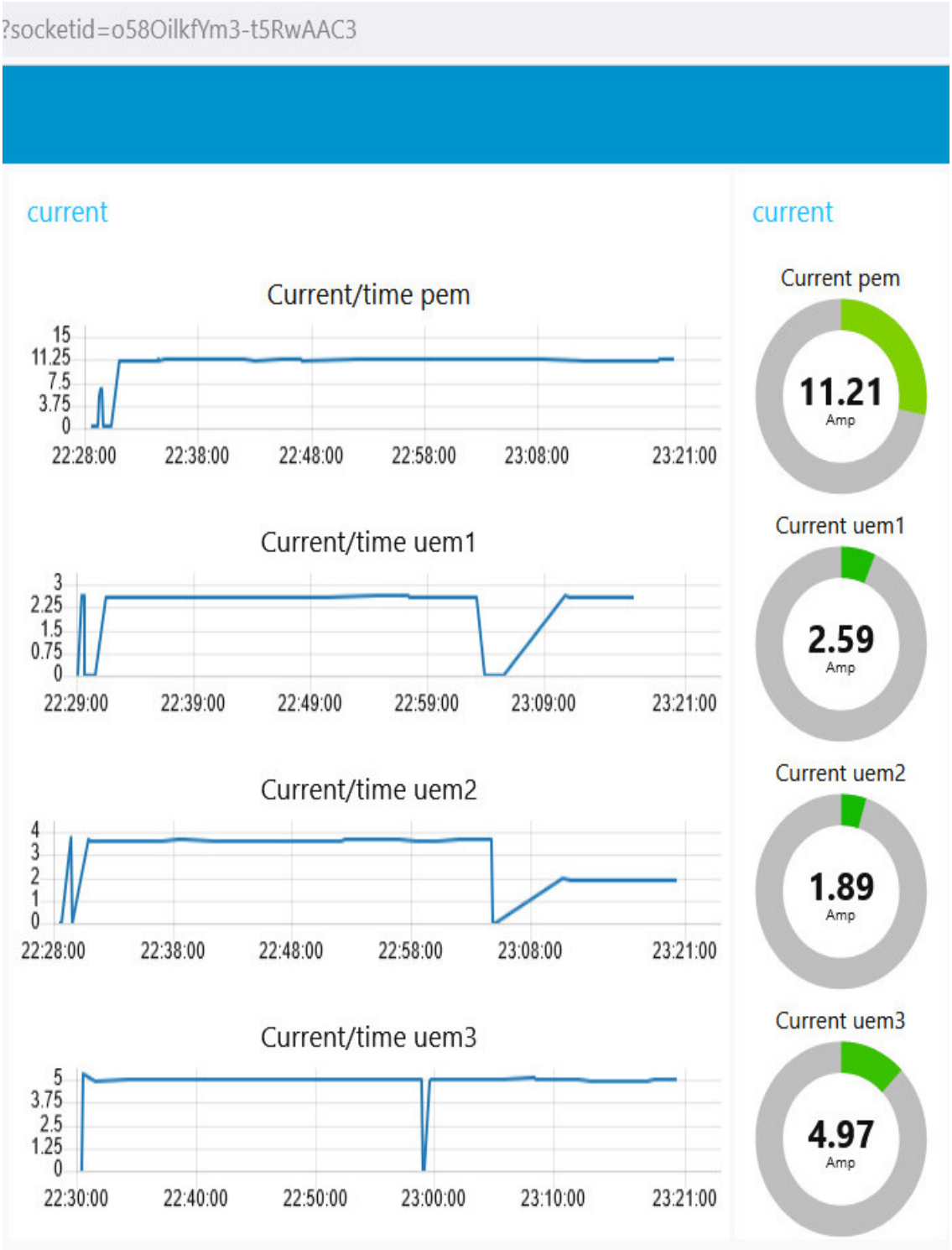


Figure 4.26**:** An example for larceny tamper meter UEM2.

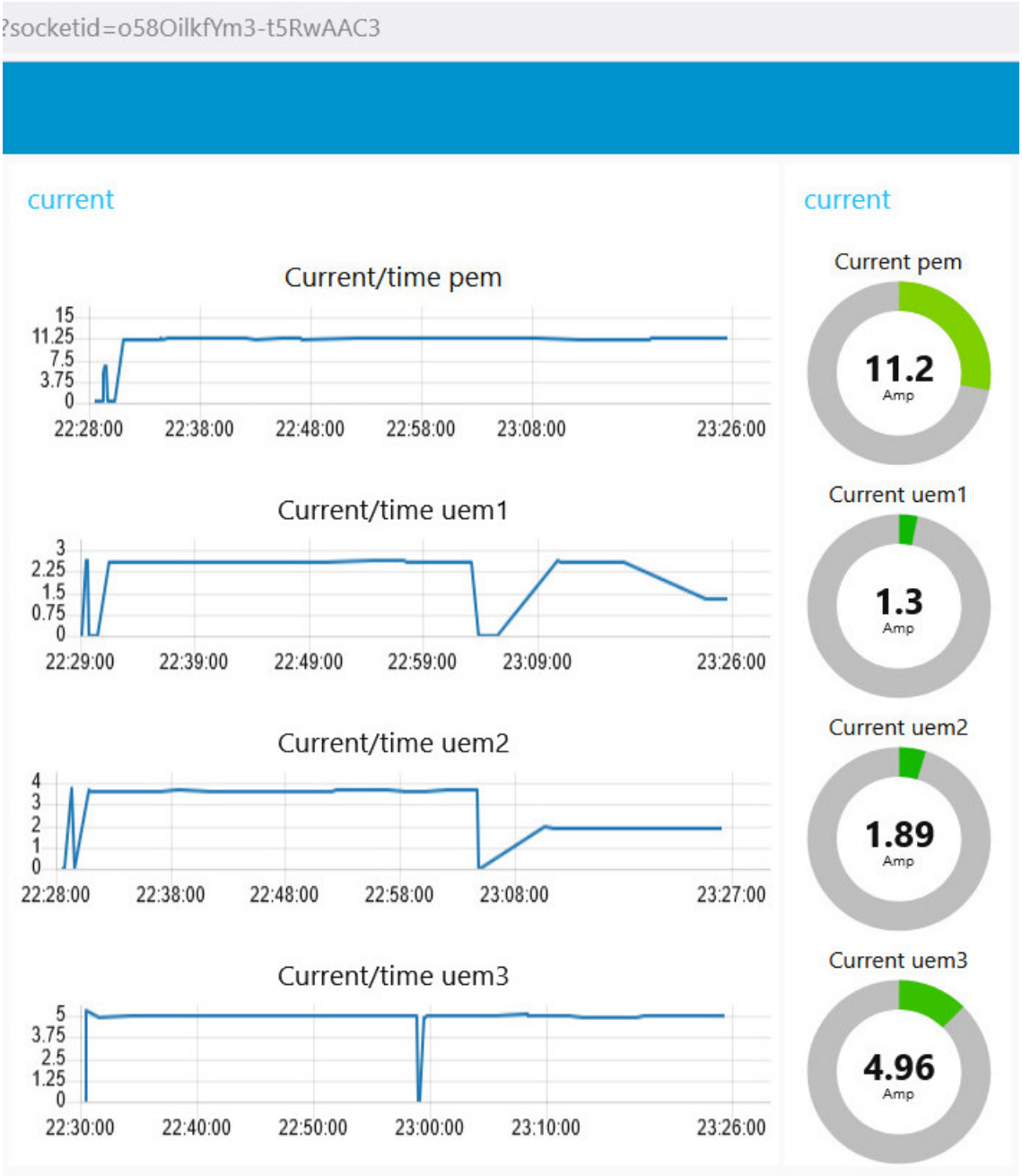


Figure 4.27**:** An example for larceny via tampering meters UEM1 and UEM2.

Supposing one-meter UEM1 or i_1 start tampering for test (here tampering done by using not correct reading CT), then the equation 3.1 output reading values $\mathfrak{D} = 11.02 - (1.28 + 3.57 + 4.89) = 1.28A$ and the previous value of $\mathfrak{D} = 11.02 - (2.56 + 3.57 + 4.89) = 0$, so equation 3.2 became 1.28-0 =1.28

and according to the mentioned flow chart there is possible larceny because $\mathfrak{D}$ new $-$ $\mathfrak{D}$ old $\neq 0$ .In addition ,the current differences are:

($i_1$old-i_1 new) =2.56-1.28=1.28, (i_2 old-i_2 new) =3.57-3.57=0 and (i_3 old-i_3 new) =4.89-4.89=0, then by detaching the meter UEM1 and taking previous and now reading difference of main meter I the I old $= 11.02$ while I new $= 8.46$ after that because this decision of I that give yes or one according to the algorithm so checking of $\mathfrak{D}$ old $>$ $\mathfrak{D}$ new, so 1.28>0, the decision will give one so that an indicator for meter UEM1 was in tampering at time 5:28. The result of this case is illustrated in figure 4.28.

In the same way, two-meters UEM1 or i_1 and UEM2 or i_2 are supposed to start tampering, so the equation 3.1 of reading values $\mathfrak{D} = 11.02 - (1.28 + 1.78 + 4.89) = 3.07$A so equation 3.2 became 3.07-1.28 =1.79A and according to the mentioned flow chart there is possible larceny because $\mathfrak{D}$ new $-$ $\mathfrak{D}$ old $\neq 0$ so read values of differences after UEM1 detached previously.

(i_2 old-i_2 new) =3.57-1.78=1.7A.

and (i_3 old-i_3 new) =4.89-4.89=0A.

Later by detaching the meter UEM2 and take previous and now reading difference of main meter I the I old $= 8.46$A while I new $= 4.89$A. After that because this decision of I that give yes or one according to the algorithm and by checking if $\mathfrak{D}$ old $>$ $\mathfrak{D}$ new so (1.79>0), the decision will give one an indicator for meter UEM2 was in tampering at time 5:39. The result of this case is depicted in figure 4.29.

Figure 4.28**:** Larceny detection of tamper meter UEM1.

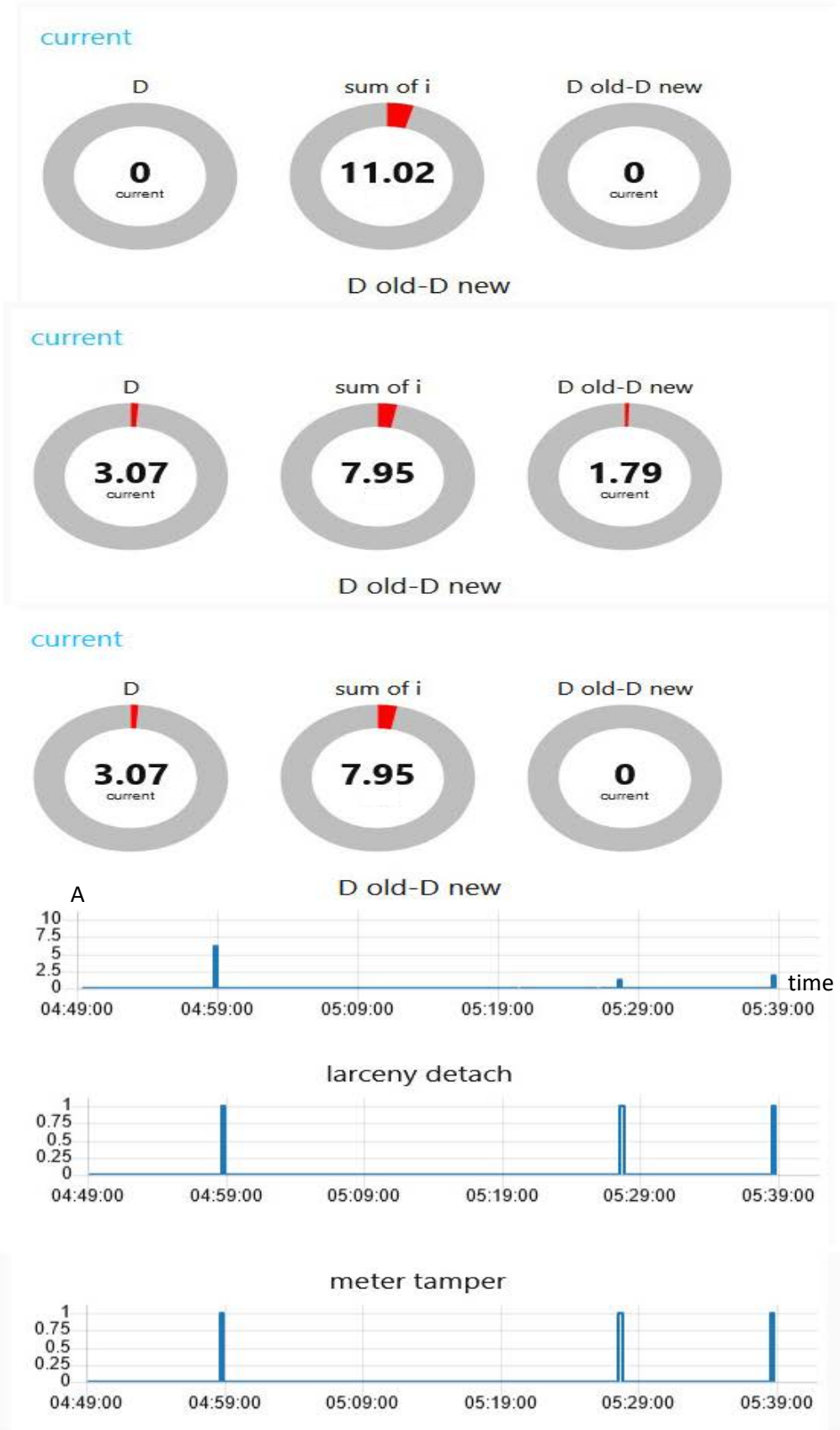


Figure 4.29**:** Larceny detection of tampering meters of UEM1 and UEM2.

4.6.4 Meter Tampering and Normal User Consuming Variation Case

Supposing a user of UEM1, i_1 has lowered the consuming and one-meter UEM2 or i_2 start tampering, so the equation 3.1 of reading values with $\mathrm{I\,new} = 9.74\mathrm{A}$, $\mathfrak{D} = 9.74 - (1.28 + 1.78 + 4.89) = 1.79\mathrm{A}$, and the previous value of $\mathfrak{D} = 11.02 - (2.56 + 3.57 + 4.89) = 0$, so equation 3.2 became 1.79-0 =1.79A.

According to the mentioned flow chart, there is possible larceny because $\mathfrak{D}\,\mathrm{new} - \mathfrak{D}\,\mathrm{old} \neq 0$ so read values of differences

($i_1$old-i_1 new) =2.56-1.28=1.28 A,

(i_2 old-i_2 new) =3.57-1.78=1.79A

and (i_3 old-i_3 new) =4.89-4.89=0A.

By detaching the meter UEM1 and taking previous and now reading difference of main meter I the $\mathrm{I\,old} = 9.74\mathrm{A}$, while $\mathrm{I\,new} = 8.46\mathrm{A}$. This value of I leads to decision that give yes or one according to the algorithm so checking of $\mathfrak{D}\,\mathrm{old} > \mathfrak{D}\,\mathrm{new}$ so [8.46- (1.78+4.89)], [9.74- (1.28+1.78+4.89)] and, 1.79>1.79, this decision will give 0 an indicator for meter UEM1 was in normal or regular according to algorithm. Moreover, if the system continues detaching UEM2 according to previous equations $\mathrm{I\,new} = 4.89\mathrm{A}$, $\mathrm{I\,old} = 8.46\mathrm{A}$ and $\mathfrak{D}\,\mathrm{old} > \mathfrak{D}\,\mathrm{new}$, 0<1.79, the meter UEM2 was in tampering at time 6:12 according to algorithm. The result of this case is stated in figure 4.30.

The KWH cost can be calculated by time to get energy if multiplied by tariff gained cost of frauded energy.

Figure 4.30**:** Larceny detection of tampering meter UEM2 and while UEM1 normal.

In this work, the Raspberry Pi used for the core process is positioned near the transformer or feeder source. Also, the algorithm depends on the initial detachment of meters to detect fraud and tampering according to using the Node-red platform inside the Raspberry Pi.

In contrast, with [24] where the Raspberry Pi is put in each home with an Arduino device to measure and detect theft and send information to the electric board, which is costly due to the number of devices. Other systems in literature depended on either local infrared sensor or threshold on device process for each home only without using the process for all homes or even using cloud concept or database.

5

Chapter Five
Conclusions and Future Work

Chapter Five

Conclusions and Future Work

5.1 Conclusions

In this thesis and the scheme and accomplishment of the proposed systems, abundant knowledge has been gained in sundry disciplines like software and platform programming, Linux operation system experience, control, electronics, and communications. Furthermore, the following points are concluded:

1- The average power factor correction error based on real and decided capacitance via neural power factor correction algorithm was 1.928% for trained data and 2.65% for untrained or tested data.

2- The power factor corrected from 0.46 to 0.97 with an average power factor of 0.95 for trained and untrained data.

3- The average capacitance error for trained data is 0.824 µF and 1.428 µF for untrained or tested data.

4- The larceny detections system gives precise results; for example, the case of two meters bypassed when the bypassing event started at the hour of 4:59, and the detection was done at the same time.

5- The training of neural network using backpropagation succeeded for the decision of capacitance value with a training error of $8.76 * 10^{-4}$, and a testing error of 0.0014 for 186 epochs.

6- In power monitoring with cloud and database, the result has some fluctuation or ripple of ±2W in the curve due to the database reading latency. Also, A ripple of ±1V in the voltage curve is due to the same reason.

7- During the monitoring process, the cloud server during monitoring process takes 1.5%from the Raspberry Pi CPU with a CPU temperature of 53 C at room temperature.

5.2 Future Works

Some points state some testaments for future work as listed below:

1- Load identification or forecasting system with the cloud
2- Home load pattern for larceny detection with neural network
3- Dynamic pricing and demand with cloud computing
4- Power factor correction with other types of neural networks or nonlinear power factor correction
5- Harmonic Effect and loss analysis with the cloud.
6- Cloud system for appliance label of power-saving agreement.
7- Cloud system for hybrid sourced (renewable and traditional) load pattern analysis.
8- The larceny detection system can extend to calculate the cost of frauded energy.

References

[1] L. L. Pfitscher, A. R. Abaide, D. P. Bernardon, and V. J. Garcia, "Introduction to Smart Operation Centers," in *Smart Operation for Power Distribution Systems: Concepts and Applications*, D. P. Bernardon and V. J. Garcia Eds. Cham: Springer International Publishing, pp. 1-14,2018.

[2] " Unified Operations Center."AVEVA™.https://www.aveva.com/en/ solutions/operations/unified-operations-center/ (accessed at May 2022).

[3] "System requirements for the Operations Center."IBM. https:// www. ibm.com/docs/en/spectrum-protect/8.1.9?topic=center-system-requirements-operations (accessed at May 2022).

[4] Y. Allahvirdizadeh, M. P. Moghaddam, and H. Shayanfar, "A survey on cloud computing in energy management of the smart grids," *International Transactions on Electrical Energy Systems*, vol. 29, no. 10, p. e12094, 2019.

[5] P. Yong. "Intelligent Operations Center: A Smart Brain for City Management." Smart City Solution Department, Enterprise Business Group, Huawei Technologies Co., Ltd. https://e.huawei.com/en/ publications/global/ict_insights/201908281022/focus/201911081641(acc-essed at May 2022).

[6] F. Bouhafs, M. Mackay, and M. Merabti, "Links to the future: Communication requirements and challenges in the smart grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 24-32, 2011.

[7] S. Heidari, M. Fotuhi-Firuzabad, and M. Lehtonen, "Planning to equip the power distribution networks with automation system," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3451-3460, 2017.

[8] T. S. Gunawan, M. H. Anuar, M. Kartiwi, and Z. Janin, "Development of Power Factor Meter using Arduino," in *2018 IEEE 5th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA)*: IEEE, pp. 1-4, 2018.

[9] A. Taye, "Design and Simulation of Automatic Power Factor Correction for Industry Application," *International Journal of Engineering Technologies and Management Research,* vol. 5, no. 2, pp. 10-21, 2018.

[10] M. D. M. Vignesh Kumar, Y. Pavithra, S. Vedha Varshini, "Automatic Power Factor Controller Using Raspberry Pi " *International Journal of Electrical, Electronics and Data Communication (IJEEDC)-IJEEDC,* vol. 6, no. 4 (Apr, 2018), pp. 42-44, 2018.

[11] R. D. P. Sathiyapriya, S. Dhanasooryaa, S. Gokulakrishnan "Power Factor Monitoring and Controlling for Industrial Load using IoT," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* vol. 8, no. 3, pp. 555 -559, 2019

[12] P. Bhagavathy, R. Latha, and E. Thamizhmaran, "Development of IoT Enabled Smart APFC Panel for Industrial Loads," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*: IEEE, pp. 1-5, 2019.

[13] A. A. A. Praveen, M. M. Kumaran, A. N. Ali, and K. Premkumar, "Minimization of Power Factor Penalty Charges for Non-Linear Domestic Loads with IOT Technology," in *IOP Conference Series: Materials Science and Engineering*, vol. 937, no. 1: IOP Publishing, p. 012011, 2020.

[14] E. A. Mohammed, A. F. Al-Allaf, and B. R. Altamer, "IoT-Based Monitoring and Management Power Sub-Station of the University of

Mosul," in *IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 2, p. 022061, 2020.

[15] N. N. Gomaa, K. Y. Youssef, and M. Abouelatta, "On design of IoT-based power quality oriented grids for industrial sector," vol. 5, no. 6, pp. 1634-1642, 2021.

[16] N. Dhamal, "IoT Cloud-Based PF Controller," *Journal of Science and Technology*, vol. 6, no. 1, pp. 268-272, 2021.

[17] D. Nugroho *et al.*, "Household electricity network monitoring based on IoT with of automatic power factors improvement using neural network method," in *IOP Conference Series: Materials Science and Engineering* vol. 1010, no. 1, p. 012045, 2021,.

[18] R. E. Ogu, G. Chukwudebe, and I. A. Ezenugu, "An IoT Based Tamper Prevention System for Electricity Meter," *American Journal of Engineering Research*, vol. 5, no. 10, pp. 347-353, 2016.

[19] S. Sridhar, H. Bharath, V. Vishvesh, K. Gowtham, and H. Girish, "IoT based-Transformer power theft detection and protection," *International Journal of Engineering Research*, vol. 5, no. 4, pp. 992-1128, 2016.

[20] N. Pranau, T. Raghuraman, S. Vishnuguhan, and B. Meenakshi, "Load Monitoring and Detection of Tampering in Power Lines Using Internet of Things (Iot)," *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN*, vol. 12, no. 2, pp. 2278-1676, 2017.

[21] W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, "A novel smart energy theft system (SETS) for IoT-based smart home," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5531-5539, 2019.

[22] K. Ashwitha, A. Gracy, M. Poojasree, B. Somashekar, and R. DhayanandB, "Power Theft Preventation System Using IoT,"

International Journal of Current Engineering And Scientific Research, vol. 6, no. 6, pp. 118-125, 2019.

[23] M. C. B. Loyola, J. B. Bueno, and R. Leon, "Internet-based electric meter with theft detection, theft notification and consumption monitoring for residential power lines using wireless network technology," *Int. Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 8, no. 5, pp. 238-246, 2019.

[24] R. Meenal, K. M. Kuruvilla, A. Denny, R. V. Jose, and R. Roy, "Power Monitoring and Theft Detection System using IoT," in *Journal of Physics: Conference Series*, vol. 1362, no. 1, p. 012027, 2019.

[25] R. Aswini and V. Keerthihaa, "IoT Based Smart Energy Theft Detection and Monitoring System for Smart Home," in *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)*: IEEE, pp. 1-6, 2020.

[26] A. S. Hamid, "IoT based Smart Energy Meter using Theft Detection for Home Management System," *Journal of emerging technologies and innovative research*, vol. 7, no. 8, pp. 1681-1684, 2020.

[27] M. Jeffin, G. Madhu, A. Rao, G. Singh, and C. Vyjayanthi, "Internet of Things Enabled Power Theft Detection and Smart Meter Monitoring System," in *2020 International Conference on Communication and Signal Processing (ICCSP)*, 2020: IEEE, pp. 0262-0267.

[28] A. D. Attar, D. D. Patil, V. B. Patil, and M. M. C. Butale, "GSM Based Advance Monitoring and Metering System with Power Theft Detection," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 3, no. 3, pp. 247-253, 2021.

[29] Tawatchai T and S. K, "Smart Technology in Water Disaster Management in Thailand and Research Collaboration," in *Research of Earth Sciences*

and Smart Disaster Reduction in Southeast Asia Taipei, Taiwan: Institute of Earth Sciences, pp. 1-10, 2019.

[30] C. WON, "Smart Grid," in *https://sites.tufts.edu/eeseniordesignhandbook /2015/smart-grid/, The Electrical and Computer Engineering Design Handbook,* 2015.

[31] R. Iniyanathan, B. Balaramakrishnan, and S. Vanila, "Energy Theft Detection Issues For Advanced Metering Infrastructure Using IoT In Smart Grid," *International Journal of Electrical Engineering and Technology,* vol. 12, no. 3, pp. 62-67, 2021.

[32] P. Mack, "Chapter 35-big data, data mining, and predictive analytics and high performance computing," *Renewable Energy Integration, Academic Press, Boston,* pp. 439-454, 2014.

[33] M. P. Raju and A. J. Laxmi, "IoT based online load forecasting using machine learning algorithms," *Procedia Computer Science,* vol. 171, pp. 551-560, 2020.

[34] N. Mishra, V. Kumar, and G. Bhardwaj, "Role of Cloud Computing in Smart Grid," in *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*: IEEE, pp. 252-255, 2019.

[35] F. Q. Kamal and A. A. Betti, "Towards securing cloud data in the multi-cloud scenario," *Periodicals of Engineering and Natural Sciences (PEN),* vol. 9, no. 2, pp. 868-872, 2021.

[36] H. El-Sayed *et al.*, "Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment," *IEEE Access,* vol. 6, pp. 1706-1717, 2017.

[37] P. Qian, D. Zhang, X. Tian, Y. Si, and L. Li, "A novel wind turbine condition monitoring method based on cloud computing," *Renewable energy*, vol. 135, pp. 390-398, 2019.

[38] M. Pau *et al.*, "Design and accuracy analysis of multilevel state estimation based on smart metering infrastructure," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 11, pp. 4300-4312, 2019.

[39] A. A. Mohammed, M. A. N. Al-hayanni, and H. M. Azzawi, "Detection and segmentation the affected brain using ThingSpeak platform based on IoT cloud analysis," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 9, no. 2, pp. 858-867, 2021.

[40] N. Sultan, "Making use of cloud computing for healthcare provision: Opportunities and challenges," *International Journal of Information Management*, vol. 34, no. 2, pp. 177-184, 2014.

[41] Y. H. Lin, "Novel smart home system architecture facilitated with distributed and embedded flexible edge analytics in demand-side management," *International Transactions on Electrical Energy Systems*, vol. 29, no. 6, p. e12014, 2019.

[42] I. Korkmaz, S. K. Metin, A. Gurek, C. Gur, C. Gurakin, and M. Akdeniz, "A cloud based and Android supported scalable home automation system," *Computers & Electrical Engineering*, vol. 43, pp. 112-128, 2015.

[43] S. Muralidharan, G. Song, and H. Ko, "Monitoring and managing iot applications in smart cities using kubernetes," in *The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 1-6, 2019.

[44] S. Goyal, "Public vs private vs hybrid vs community-cloud computing: a critical review," *International Journal of Computer Network and Information Security*, vol. 6, no. 3, pp. 20-29, 2014.

[45] K. Chandrasekaran, *Essentials of cloud computing*. CrC Press, 2014.

[46] T. Abd, Y. S. Mezaal, M. S. Shareef, S. K. Khaleel, H. H. Madhi, and S. F. Abdulkareem, "Iraqi e-government and cloud computing development based on unified citizen identification," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 7, no. 4, pp. 1776-1793, 2019.

[47] C. M. Mohammed and S. R. Zebaree, "Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review," *International Journal of Science and Business*, vol. 5, no. 2, pp. 17-30, 2021.

[48] W. Xu, D. Yuan, and L. Xue, "Design and implementation of intelligent community system based on thin client and cloud computing," *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, vol. 5, no. 4, pp. 1-10, 2014.

[49] I. Odun-Ayo, B. Udemezue, and A. Kilanko, "Cloud service level agreements and resource management," *Adv. Sci. Technol. Eng. Syst.*, vol. 4, no. 2, pp. 228-236, 2019.

[50] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future generation computer systems*, vol. 29, no. 1, pp. 84-106, 2013.

[51] W. D. Tian and Y. D. Zhao, *Optimized cloud resource management and scheduling: theories and practices*. Morgan Kaufmann, 2014.

[52] S. M. Hashemi and A. K. Bardsiri, "Cloud computing vs. grid computing," *ARPN journal of systems and software*, vol. 2, no. 5, pp. 188-194, 2012.

[53] M. Aazam and E.-N. Huh, "Fog computing: The cloud-iot\/ioe middleware paradigm," *IEEE Potentials*, vol. 35, no. 3, pp. 40-44, 2016.

[54] M. M. Sadeeq, N. M. Abdulkareem, S. R. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, "IoT and Cloud computing issues, challenges and

opportunities: A review," *Qubahan Academic Journal,* vol. 1, no. 2, pp. 1-7, 2021.

[55] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," *ACM Computing Surveys (CSUR),* vol. 51, no. 6, pp. 1-29, 2019.

[56] K. Afsari, C. M. Eastman, and D. R. Shelden, "Data transmission opportunities for collaborative cloud-based building information modeling," in *Proceedings of the 20th Conference of the Iberoamerican Society of Digital Graphics*, pp. 907-913, 2016.

[57] S. Gomathi, T. Venkatesan, and D. S. Vidhya, "Design and implementation of fault current limiters in distribution system using internet of things," *Wireless Personal Communications,* vol. 102, no. 4, pp. 2643-2666, 2018.

[58] D. Sehrawat and N. S. Gill, "Deployment of IoT based smart environment: key issues and challenges," *International Journal of Engineering & Technology,* vol. 7, no. 2, pp. 544-550, 2018.

[59] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends," *Wireless communications and mobile computing,* vol. 2018, pp. 1-24 ,2018.

[60] F. B. Poyen, "Raspberry Pi and its Use in IoT Applications," *Annual Technical Volume of Computer Engineering Division Board,* vol. 2, pp. 42-47, 2018.

[61] L. Miori, J. Sanin, and S. Helmer, "A platform for edge computing based on Raspberry Pi clusters," in *British International Conference on Databases*: Springer, pp. 153-159, 2017.

[62] R. Botez, V. Strautiu, I.-A. Ivanciu, and V. Dobrota, "Containerized Application for IoT Devices: Comparison between balenaCloud and Amazon Web Services Approaches," in *2020 International Symposium on Electronics and Telecommunications (ISETC*: IEEE, pp. 1-4), 2020.

[63] P. D. Bharathi, V. Ananthanarayanan, and P. Bagavathi Sivakumar, "Fog Computing-Based Environmental Monitoring Using Nordic Thingy: 52 and Raspberry Pi," Singapore: Springer Singapore, in Smart Systems and IoT: Innovations in Computing, pp. 269-279, 2020.

[64] C. Pahl, S. Helmer, L. Miori, J. Sanin, and B. Lee, "A container-based edge cloud paas architecture based on raspberry pi clusters," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*: IEEE, pp. 117-124, 2016.

[65] T. Hagino, *Practical Node-RED Programming*. Packt, p. 326, 2021.

[66] S. E. Princy and K. G. J. Nigel, "Implementation of cloud server for real time data storage using Raspberry Pi," in *2015 Online International Conference on Green Engineering and Technologies (IC-GET)*: IEEE, pp. 1-4, 2015.

[67] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews,* vol. 57, pp. 302-318, 2016.

[68] E. Kabalcı, Y. Kabalcı, and P. Siano, "Design and implementation of a smart metering infrastructure for low voltage microgrids," *International Journal of Electrical Power & Energy Systems,* vol. 134, pp. 1-13, 2022.

[69] S. Hallur, "Smart Components for a Smart Energy Mete," *International Journal of Advance Research in Engineering Science and Technology,* vol. 4, no. 3, pp. 544-556, 2017.

[70] https://innovatorsguru.com/pzem-004t-v3/ (accessed at May 2022).

[71] Y. S. Parihar, "Internet of Things and Nodemcu," *Journal of Emerging Technologies and Innovative Research*, vol. 6, no. 6, p. 1085, 2019.

[72] C. E. Moreira Rodrigues *et al.*, "Technical Loss Calculation in Distribution Grids Using Equivalent Minimum Order Networks and an Iterative Power Factor Correction Procedure," *Energies*, vol. 14, no. 3, p. 646, 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/3/646.

[73] J. Navani, N. Sharma, and S. Sapra, "Technical and non-technical losses in power system and its economic consequence in Indian economy," *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 2, pp. 757-761, 2012.

[74] V. Ananthapadmanabhan, I. Tenison, and T. Shanavas, "Automated Power Factor Improvement Based on Artificial Neural Networks," in *2018 International Conference on Intelligent Autonomous Systems (ICoIAS)*: IEEE, pp. 170-174, 2018.

[75] N. N. Gomaa, K. Y. Youssef, and M. Abouelatta, "An IoT-based Energy Efficient System for Industrial Sector," in *2019 15th International Computer Engineering Conference (ICENCO)*: IEEE, pp. 132-137, 2019.

[76] T. Ahmad and Q. U. Hasan, "Detection of frauds and other non-technical losses in power utilities using smart meters: a review," *International Journal of Emerging Electric Power Systems*, vol. 17, no. 3, pp. 217-234, 2016.

[77] M. S. Saeed *et al.*, "Detection of non-technical losses in power utilities—a comprehensive systematic review," *Energies*, vol. 13, no. 18, p. 4727, 2020.

[78] "Energy Theft and Fraud Reduction." https://networkedenergy.com/en/news-events/energy-theft-and-fraud-reduction (accessed at May 2022).

[79] J. Zou, Y. Han, and S.-S. So, "Overview of Artificial Neural Networks," in *Artificial Neural Networks: Methods and Applications*, D. J. Livingstone Ed. Totowa, NJ: Humana Press, pp. 14-22, 2009.

[80] M. S. Ibrahim, W. Dong, and Q. Yang, "Machine learning driven smart electric power systems: Current trends and new perspectives," *Applied Energy*, vol. 272, pp. 1-19, 2020.

APPENDICES

Appendix(A)

APPENDIX A-1: Raspberry Pi Specification and Datasheet.

APPENDIX A-2: PZEM-004T Specification and Datasheet.

APPENDIX A-3: NodeMCU Specification and Datasheet.

APPENDIX A-1

Raspberry Pi 4 Model B Specification and Datasheet

1. Introduction

The Raspberry Pi 4 Model B (Pi4B) is the first of a new generation of Raspberry Pi computers supporting more RAM and with significantly enhanced CPU, GPU and I/O performance; all within a similar form factor, power envelope and cost as the previous generation Raspberry Pi 3B+.The Pi4B is available with either 1, 2 and 4 Gigabytes of LPDDR4 SDRAM.

2. Features

2.1 Hardware

- Quad core 64-bit ARM-Cortex A72 running at 1.5GHz
- 1, 2 and 4 Gigabyte LPDDR4 RAM options
- H.265 (HEVC) hardware decode (up to 4Kp60)
- H.264 hardware decodes (up to 1080p60)
- Video Core VI 3D Graphics
- Supports dual HDMI display output up to 4Kp60

2.2 Interfaces

- 802.11 b/g/n/ac Wireless LAN
- Bluetooth 5.0 with BLE
- 1x SD Card
- 2x micro-HDMI ports supporting dual displays up to 4Kp60 resolution
- 2x USB2 ports
- 2x USB3 ports
- 1x Gigabit Ethernet port (supports PoE with add-on PoE HAT)

- 1x Raspberry Pi camera port (2-lane MIPI CSI)
- 1x Raspberry Pi display port (2-lane MIPI DSI)
- 28x user GPIO supporting various interface options:
  – Up to 6x UART
  – Up to 6x I2C
  – Up to 5x SPI
  – 1x SDIO interface
  – 1x DPI (Parallel RGB Display)
  – 1x PCM
  – Up to 2x PWM channels
  – Up to 3x GPCLK outputs

2.3 Software

- ARMv8 Instruction Set
- Mature Linux software stack
- Actively developed and maintained
  – Recent Linux kernel support
  – Many drivers upstreamed
  – Stable and well supported userland
  – Availability of GPU functions using standard APIs

3. Mechanical Specification

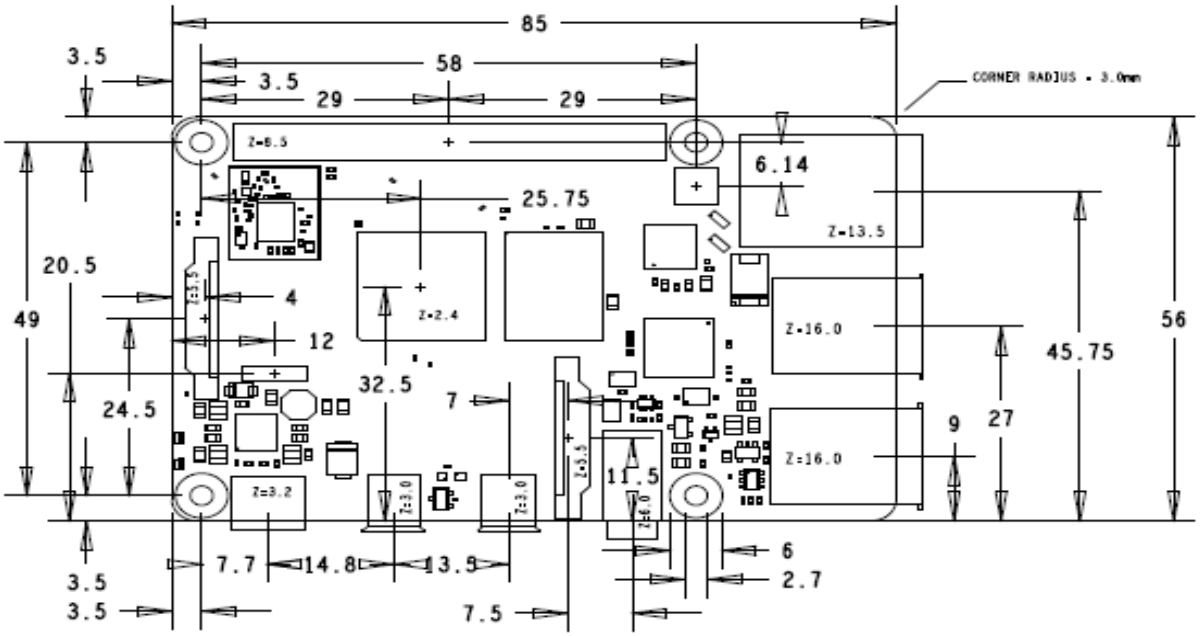


Figure 1: Mechanical Dimensions

4. Electrical Specification

Caution! Stresses above those listed in Table 2 may cause permanent damage to the device. This is a stress rating only; functional operation of the device under these or any other conditions above those listed in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Table 2: Absolute Maximum Ratings

Symbol	Parameter	Minimum	Maximum	Unit
VIN	5V Input Voltage	-0.5	6.0	V

Please note that VDD IO is the GPIO bank voltage which is tied to the on-board 3.3V supply rail.

Table 3: DC Characteristics

Symbol	Parameter	Conditions	Minimum	Typical	Maximum	Unit
V_{IL}	Input low voltage[a]	VDD_IO = 3.3V	-	-	TBD	V
V_{IH}	Input high voltage[a]	VDD_IO = 3.3V	TBD	-	-	V
I_{IL}	Input leakage current	TA = +85°C	-	-	TBD	μA
C_{IN}	Input capacitance	-	-	TBD	-	pF
V_{OL}	Output low voltage[b]	VDD_IO = 3.3V, IOL = -2mA	-	-	TBD	V
V_{OH}	Output high voltage[b]	VDD_IO = 3.3V, IOH = 2mA	TBD	-	-	V
I_{OL}	Output low current[c]	VDD_IO = 3.3V, VO = 0.4V	TBD	-	-	mA
I_{OH}	Output high current[c]	VDD_IO = 3.3V, VO = 2.3V	TBD	-	-	mA
R_{PU}	Pullup resistor	-	TBD	-	TBD	kΩ
R_{PD}	Pulldown resistor	-	TBD	-	TBD	kΩ

[a] Hysteresis enabled

[b] Default drive strength (8mA)

[c] Maximum drive strength (16mA)

Table 4: Digital I/O Pin AC Characteristics

Pin Name	Symbol	Parameter	Minimum	Typical	Maximum	Unit
Digital outputs	t_{rise}	10-90% rise time[a]	-	TBD	-	ns
Digital outputs	t_{fall}	90-10% fall time[a]	-	TBD	-	ns

[a] Default drive strength, CL = 5pF, VDD IO = 3.3V

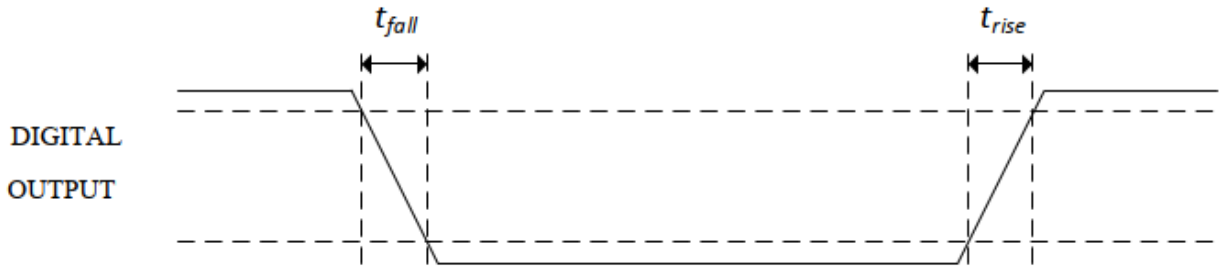


Figure 2: Digital IO Characteristics

4.1 Power Requirements

The Pi4B requires a good quality USB-C power supply capable of delivering 5V at 3A. If attached downstream USB devices consume less than 500mA, a 5V,2.5A supply may be used.

5. Peripherals

5.1 GPIO Interface

The Pi4B makes 28 BCM2711 GPIOs available via a standard Raspberry Pi 40-pin header. This header is backwards compatible with all previous Raspberry Pi boards with a 40-way header.

5.1.1 GPIO Pin Assignments

As well as being able to be used as straightforward software-controlled input and output (with programmable pulls), GPIO pins can be switched (multiplexed) into various other modes backed by dedicated peripheral blocks such as I2C, UART and SPI. In addition to the standard peripheral options found on legacy Pis, extra I2C, UART and SPI peripherals have been added to the BCM2711 chip and are available as further mux options on the Pi4. This gives users much more flexibility when attaching add-on hardware as compared to older models.

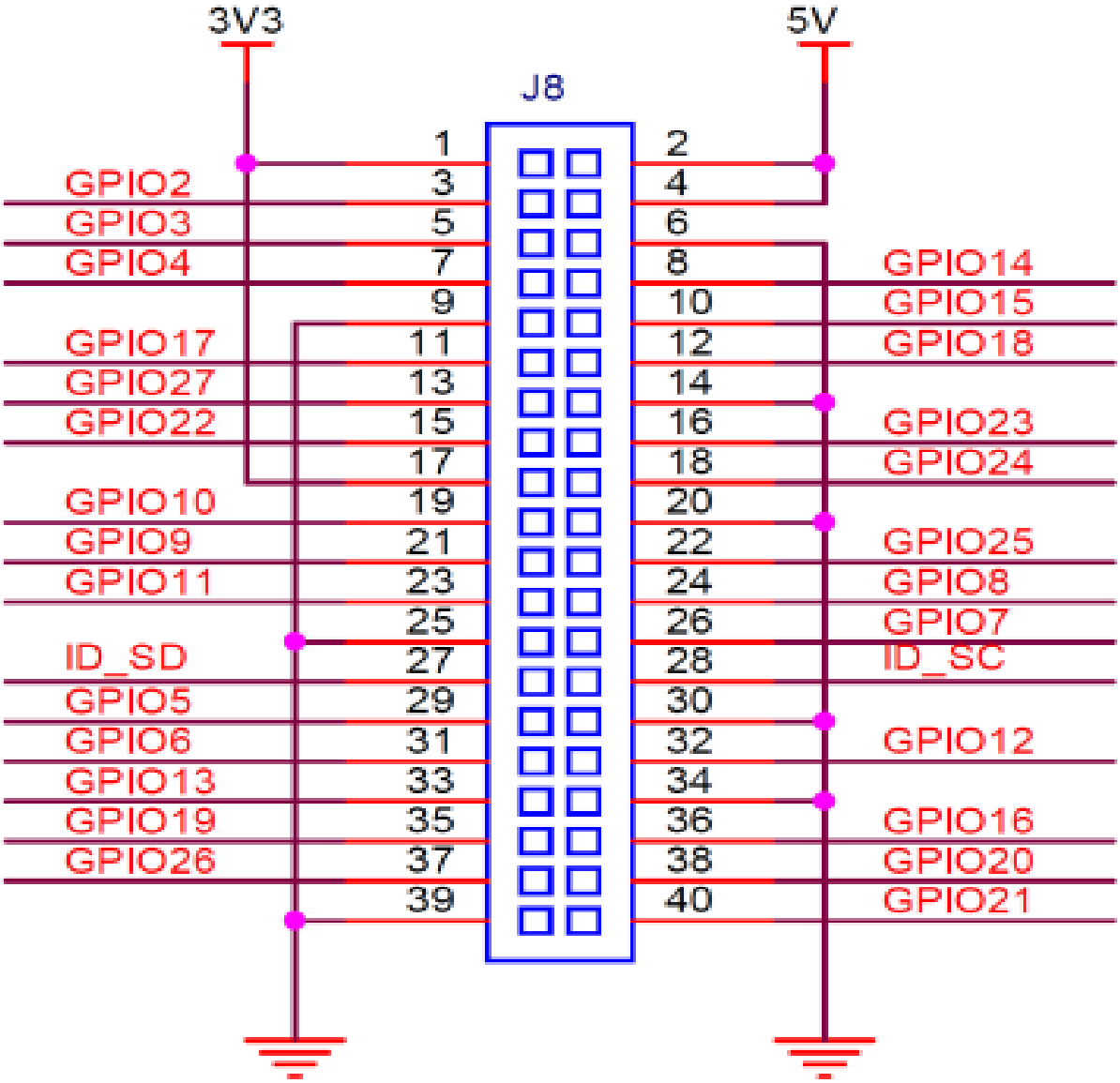


Figure 3: GPIO Connector Pinout

5.1.2 GPIO Alternate Functions

Table 5 details the default pin pull state and available alternate GPIO functions. Most of these alternate peripheral functions are described in detail in the BCM2711 Peripherals Specification document which can be downloaded from the hardware documentation section of the website.

Table 5: Raspberry Pi 4 GPIO Alternate Functions

GPIO	Default Pull	ALT0	ALT1	ALT2	ALT3	ALT4	ALT5
0	High	SDA0	SA5	PCLK	SPI3_CE0_N	TXD2	SDA6
1	High	SCL0	SA4	DE	SPI3_MISO	RXD2	SCL6
2	High	SDA1	SA3	LCD_VSYNC	SPI3_MOSI	CTS2	SDA3
3	High	SCL1	SA2	LCD_HSYNC	SPI3_SCLK	RTS2	SCL3
4	High	GPCLK0	SA1	DPI_D0	SPI4_CE0_N	TXD3	SDA3
5	High	GPCLK1	SA0	DPI_D1	SPI4_MISO	RXD3	SCL3
6	High	GPCLK2	SOE_N	DPI_D2	SPI4_MOSI	CTS3	SDA4
7	High	SPI0_CE1_N	SWE_N	DPI_D3	SPI4_SCLK	RTS3	SCL4
8	High	SPI0_CE0_N	SD0	DPI_D4	-	TXD4	SDA4
9	Low	SPI0_MISO	SD1	DPI_D5	-	RXD4	SCL4
10	Low	SPI0_MOSI	SD2	DPI_D6	-	CTS4	SDA5
11	Low	SPI0_SCLK	SD3	DPI_D7	-	RTS4	SCL5
12	Low	PWM0	SD4	DPI_D8	SPI5_CE0_N	TXD5	SDA5
13	Low	PWM1	SD5	DPI_D9	SPI5_MISO	RXD5	SCL5
14	Low	TXD0	SD6	DPI_D10	SPI5_MOSI	CTS5	TXD1
15	Low	RXD0	SD7	DPI_D11	SPI5_SCLK	RTS5	RXD1
16	Low	FL0	SD8	DPI_D12	CTS0	SPI1_CE2_N	CTS1
17	Low	FL1	SD9	DPI_D13	RTS0	SPI1_CE1_N	RTS1
18	Low	PCM_CLK	SD10	DPI_D14	SPI6_CE0_N	SPI1_CE0_N	PWM0
19	Low	PCM_FS	SD11	DPI_D15	SPI6_MISO	SPI1_MISO	PWM1
20	Low	PCM_DIN	SD12	DPI_D16	SPI6_MOSI	SPI1_MOSI	GPCLK0
21	Low	PCM_DOUT	SD13	DPI_D17	SPI6_SCLK	SPI1_SCLK	GPCLK1
22	Low	SD0_CLK	SD14	DPI_D18	SD1_CLK	ARM_TRST	SDA6
23	Low	SD0_CMD	SD15	DPI_D19	SD1_CMD	ARM_RTCK	SCL6
24	Low	SD0_DAT0	SD16	DPI_D20	SD1_DAT0	ARM_TDO	SPI3_CE1_N
25	Low	SD0_DAT1	SD17	DPI_D21	SD1_DAT1	ARM_TCK	SPI4_CE1_N
26	Low	SD0_DAT2	TE0	DPI_D22	SD1_DAT2	ARM_TDI	SPI5_CE1_N

APPENDIX A-2

PZEM-004T Specification and Datasheet

PZEM-004T-10A: Measuring Range 10A (Built-in Shunt)

PZEM-004T-100A: Measuring Range 100A (external transformer)

1.Function Description

1.1 Voltage

1.1.1 Measuring range:80～260V

1.1.2 Resolution: 0.1V

1.1.3 Measurement accuracy: 0.5%

1.2 Current

1.2.1 Measuring range: 0～10A(PZEM-004T-10A); 0～100A (PZEM-004T-100A)

1.2.2 Starting measure current: 0.01A(PZEM-004T-10A); 0.02A(PZEM-004T-100A)

1.2.3 Resolution: 0.001A

1.2.4 Measurement accuracy: 0.5%

1.3 Active Power

1.3.1 Measuring range: 0～2.3kW (PZEM-004T-10A); 0～23kW (PZEM-004T-100A)

1.3.2 Starting measure power: 0.4W

1.3.3 Resolution: 0.1W

1.3.4 Display format:

＜1000W, it displays one decimal, such as: 999.9W

≥1000W, it displays only integer, such as: 1000W

1.3.5 Measurement accuracy: 0.5%

1.4 Power Factor

1.4.1 Measuring range: 0.00～1.00

1.4.2 Resolution: 0.01

1.4.3 Measurement accuracy: 1%

1.5 Frequency

1.5.1 Measuring range: 45Hz～65Hz

1.5.2 Resolution: 0.1Hz

1.5.3 Measurement accuracy: 0.5%

1.6 Active Energy

1.6.1 Measuring range: 0～9999.99kWh

1.6.2 Resolution: 1Wh

1.6.3 Measurement accuracy: 0.5%

1.6.4 Display format:

＜10kWh, the display unit is Wh(1kWh=1000Wh), such as: 9999Wh

≥10kWh, the display unit is kWh, such as: 9999.99kWh

1.6.5 Reset energy: use software to reset.

1.7. Over Power Alarm

Active power threshold can be set, when the measured active power exceeds the threshold, it can alarm

1.8. Communication Interface

RS485 interface.

2. Communication Protocol

2.1. Physical Layer Protocol

Physical layer use UART to RS485 communication interface

Baud rate is 9600, 8 data bits, 1 stop bit, no parity

2.2. Application Layer Protocol

The application layer uses the Modbus-RTU protocol to communicate. At present, it only supports function codes such as 0x03 (Read Holding Register), 0x04 (Read Input Register), 0x06 (Write Single Register), 0x41 (Calibration), 0x42 (Reset energy). etc.

0x41 function code is only for internal use (address can be only 0xF8), used for factory calibration and return to factory maintenance occasions, after the function code to increase 16-bit password, the default password is 0x3721.

The address range of the slave is 0x01 ~ 0xF7. The address 0x00 is used as the

broadcast address, the slave does not need to reply the master. The address 0xF8 is used as the general address, this address can be only used in single-slave environment and can be used for calibration operation.

2.3. Read the Measurement Result

The command format of the master reads the measurement result is (total of 8 bytes):

Slave Address + 0x04 + Register Address High Byte + Register Address Low Byte + Number of Registers High Byte + Number of Registers Low Byte + CRC check high Byte + CRC check low Byte.

The command format of the reply from the slave is divided into two kinds:

Correct Reply: Slave Address + 0x04 + Number of Bytes + Register 1 Data High Byte + Register 1 Data Low Byte + ... + CRC Check High Byte + CRC Check Low Byte

Error Reply: Slave address + 0x84 + Abnormal code + CRC Check High Byte + CRC Check Low Byte

Abnormal code analysed as following (the same below)

- 0x01, Illegal function
- 0x02, Illegal address
- 0x03, Illegal data
- 0x04, Slave error

The register of the measurement results is arranged as the following table

Register address	Description	Resolution
0x0000	Voltage value	1LSB correspond to 0.1V
0x0001	Current value low 16 bits	1LSB correspond to 0.001A
0x0002	Current value high 16 bits	
0x0003	Power value low 16 bits	1LSB correspond to 0.1W
0x0004	Power value high 16 bits	
0x0005	Energy value low 16 bits	1LSB correspond to 1Wh
0x0006	Energy value high 16 bits	
0x0007	Frequency value	1LSB correspond to 0.1Hz
0x0008	Power factor value	1LSB correspond to 0.01
0x0009	Alarm status	0xFFFF is alarm ? 0x0000is not alarm

For example, the master sends the following command (CRC check code is replaced by 0xHH and 0xLL, the same below)

0x01 + 0x04 + 0x00 + 0x00 + 0x00 + 0x0A + 0xHH + 0xLL

Indicates that the master needs to read 10 registers with slave address 0x01 and the start address of the register is 0x0000

The correct reply from the slave is as following:

0x01 + 0x04 + 0x14 + 0x08 + 0x98 + 0x03 + 0xE8+0x00 + 0x00 +0x08 + 0x98+ 0x00 + 0x00 + 0x00 + 0x00 + 0x00 + 0x00 + 0x01 + 0xF4 + 0x00 + 0x64 + 0x00 + 0x00 + 0xHH + 0xLL

The above data shows:

Voltage is 0x0898, converted to decimal is 2200, display 220.0V

- Current is 0x000003E8, converted to decimal is 1000, display 1.000A
- Power is 0x00000898, converted to decimal is 2200, display 220.0W.

- Energy is 0x00000000, converted to decimal is 0, display 0Wh.
- Frequency is 0x01F4, converted to decimal is 500, display 50.0Hz.
- Power factor is 0x0064, converted to decimal is 100, display 1.00.
- Alarm status is 0x0000, indicates that the current power is lower than the alarm power threshold.

2.4. Read and Modify the Slave Parameters

At present, it only supports reading and modifying slave address and power alarm threshold. The register is arranged as the following table:

Register address	Description	Resolution
0x0001	Power alarm threshold	1LSB correspond to 1W
0x0002	Modbus RTUaddress	The range is 0x0001~0x00F7

The command format of the master to read the slave parameters and read the measurement results are same (described in details in Section 2.3), only need to change the function code from 0x04 to 0x03.

The command format of the master to modify the slave parameters is (total of 8 bytes):

Slave Address + 0x06 + Register Address High Byte + Register Address Low Byte + Register Value High Byte + Register Value Low Byte + CRC Check High Byte + CRC Check Low Byte.

The command format of the reply from the slave is divided into two kinds:

Correct Response: Slave Address + 0x06 + Number of Bytes + Register Address

Low Byte + Register Value High Byte + Register Value Low Byte + CRC Check High Byte + CRC Check Low Byte.

Error Reply: Slave address + 0x86 + Abnormal code + CRC Check High Byte + CRC check Low Byte.

For example, the master sets the slave's power alarm threshold:

0x01 + 0x06 + 0x00 + 0x01 + 0x08 + 0xFC + 0xHH + 0xLL

Indicates that the master needs to set the 0x0001 register (power alarm threshold) to 0x08FC (2300W).

Set up correctly, the slave returns to the data which is sent from the master. For example, the master sets the address of the slave

0x01 + 0x06 + 0x00 + 0x02 + 0x00 + 0x05 + 0xHH + 0xLL

Indicates that the master needs to set the 0x0002 register (Modbus-RTU address) to 0x0005

Set up correctly, the slave returns to the data which is sent from the master.

2.5. Reset Energy

The command format of the master to reset the slave's energy is (total 4 bytes): Slave address + 0x42 + CRC check high byte + CRC check low byte. Correct reply: slave address + 0x42 + CRC check high byte + CRC check low byte.

Error Reply: Slave address + 0xC2 + Abnormal code + CRC Check High Byte + CRC Check Low Byte

2.6. Calibration

The command format of the master to calibrate the slave is (total 6 bytes):

0xF8 + 0x41 + 0x37 + 0x21 + CRC check high byte + CRC check low byte. Correct reply: 0xF8 + 0x41 + 0x37 + 0x21 + CRC check high byte + CRC check low byte.

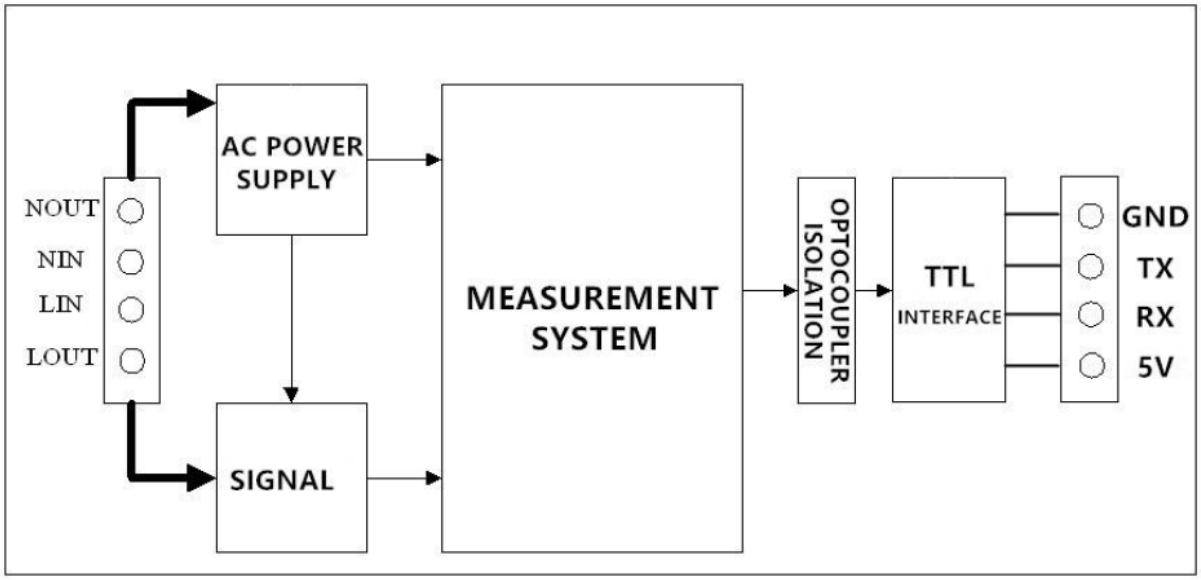
Error Reply: 0xF8 + 0xC1 + Abnormal code + CRC check high byte + CRC check low byte.

It should be noted that the calibration takes 3 to 4 seconds, after the master sends the command, if the calibration is successful, it will take 3 ~ 4 seconds to receive the response from the slave.

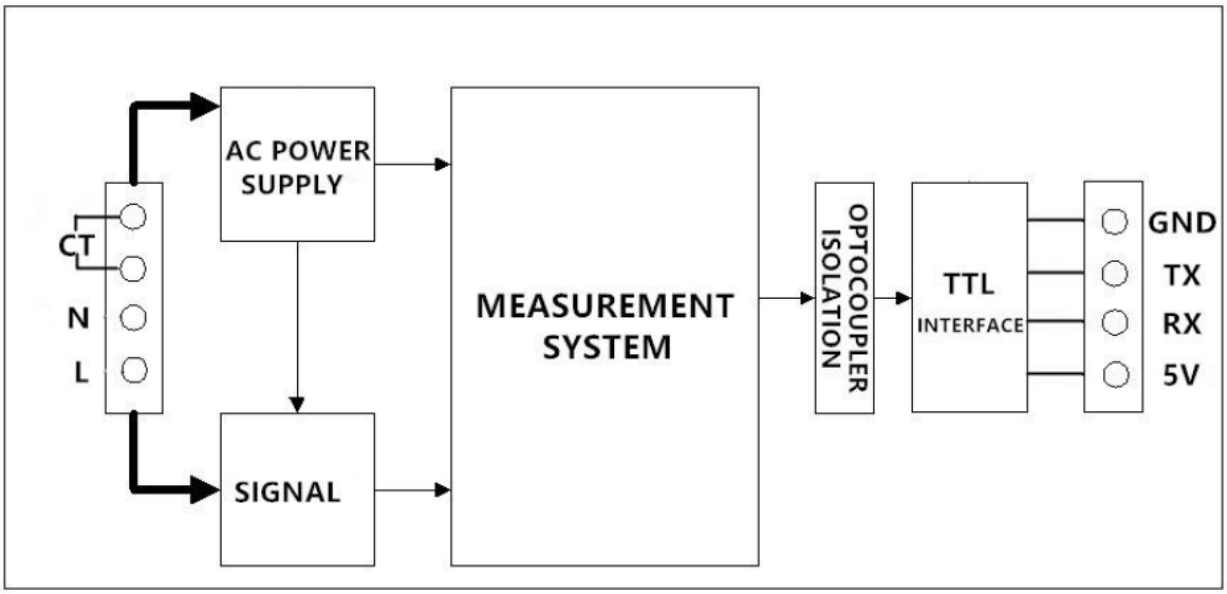
2.7 CRC check

CRC check use 16bits format, occupy two bytes, the generator polynomial is X16 + X15 + X2 +1, the polynomial value used for calculation is 0xA001. The value of the CRC check is a frame data divide all results of checking all the bytes except the CRC check value.

3.Functional block diagram



Picture 3.1 PZEM-004T-10A Functional block diagram



Picture 3.2 PZEM-004T-100A Functional block diagram

4. Other Instructions

The TTL interface of this module is a passive interface, it requires external 5V power supply, which means, when communicating, all four ports must be connected (5V, RX, TX, GND), otherwise it cannot communicate, and the working temperature is between -20 C ~ +60 C.

APPENDIX A-3

NodeMCU Specification and Datasheet

1. Overview

Espressif's ESP8266EX delivers highly integrated Wi-Fi SoC solution to meet users' continuous demands for efficient power usage, compact design and reliable performance in the Internet of Things industry. With the complete and self-contained Wi-Fi networking capabilities, ESP8266EX can perform either as a standalone application or as the slave to a host MCU. When ESP8266EX hosts the application, it promptly boots up from the flash. The integrated high-speed cache helps to increase the system performance and optimize the system memory. Also, ESP8266EX can be applied to any microcontroller design as a Wi-Fi adaptor through SPI/SDIO or UART interfaces. ESP8266EX integrates antenna switches, RF balun, power amplifier, low noise receives amplifier, filters and power management modules. The compact design minimizes the PCB size and requires minimal external circuitries. Besides the Wi-Fi functionalities, ESP8266EX also integrates an enhanced version of Tensilica's L106 Diamond series 32-bit processor and on-chip SRAM. It can be interfaced with external sensors and other devices through the GPIOs. Software Development Kit (SDK) provides sample codes for various applications. Espressif Systems' Smart Connectivity Platform (ESCP) enables sophisticated features including:

- Fast switch between sleep and wakeup mode for energy-efficient purpose.
- Adaptive radio biasing for low-power operation.
- Advance signal processing.
- Spur cancellation and RF co-existence mechanisms for common cellular, Bluetooth, DDR, LVDS, LCD interference mitigation.

1.1. Specifications

Table 1.1. Specifications

Categories	Items	Parameters
Wi-Fi	Certification	Wi-Fi Alliance
	Protocols	802.11 b/g/n (HT20)
	Frequency Range	2.4 GHz ~ 2.5 GHz (2400 MHz ~ 2483.5 MHz)
	TX Power	802.11 b: +20 dBm
		802.11 g: +17 dBm
		802.11 n: +14 dBm
	Rx Sensitivity	802.11 b: –91 dbm (11 Mbps)
		802.11 g: –75 dbm (54 Mbps)
		802.11 n: –72 dbm (MCS7)
	Antenna	PCB Trace, External, IPEX Connector, Ceramic Chip
Hardware	CPU	Tensilica L106 32-bit processor
	Peripheral Interface	UART/SDIO/SPI/I2C/I2S/IR Remote Control
		GPIO/ADC/PWM/LED Light & Button
	Operating Voltage	2.5 V ~ 3.6 V
	Operating Current	Average value: 80 mA
	Operating Temperature Range	–40 °C ~ 125 °C
	Package Size	QFN32-pin (5 mm x 5 mm)
	External Interface	-
Software	Wi-Fi Mode	Station/SoftAP/SoftAP+Station
	Security	WPA/WPA2
	Encryption	WEP/TKIP/AES
	Firmware Upgrade	UART Download / OTA (via network)
	Software Development	Supports Cloud Server Development / Firmware and SDK for fast on-chip programming
	Network Protocols	IPv4, TCP/UDP/HTTP
	User Configuration	AT Instruction Set, Cloud Server, Android/iOS App

1.2. Wi-Fi Key Features

- 802.11 b/g/n support.
- 802.11 n support (2.4 GHz), up to 72.2 Mbps.

- Defragmentation.
- 2 x virtual Wi-Fi interface.
- Automatic beacon monitoring (hardware TSF).
- Support Infrastructure BSS Station mode/SoftAP mode/Promiscuous mode.

2. Pin Layout

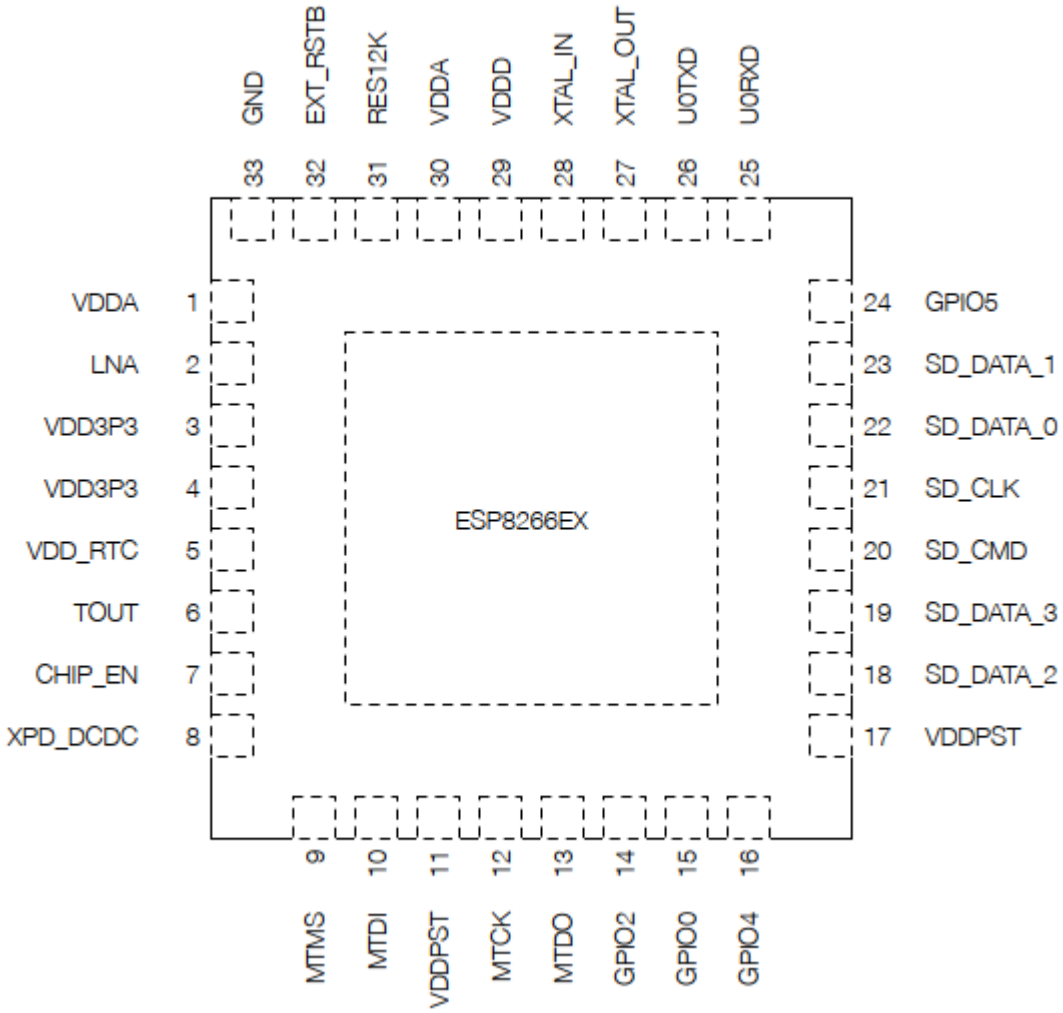


Figure 2-1 shows the pin layout for 32-pin QFN package.

3. Electrical Specifications

3.1. Electrical Characteristics

Table 3-1. Electrical Characteristics

Parameters		Conditions	Min	Typical	Max	Unit
Operating Temperature Range		-	–40	Normal	125	°C
Maximum Soldering Temperature		IPC/JEDEC J-STD-020	-	-	260	°C
Working Voltage Value		-	2.5	3.3	3.6	V
I/O	V_{IL}	-	–0.3	-	0.25 V_{IO}	V
	V_{IH}		0.75 V_{IO}		3.6	
	V_{OL}	-	-	-	0.1 V_{IO}	
	V_{OH}		0.8 V_{IO}		-	
	I_{MAX}	-	-	-	12	mA
Electrostatic Discharge (HBM)		TAMB = 25 °C	-	-	2	KV
Electrostatic Discharge (CDM)		TAMB = 25 °C	-	-	0.5	KV

3.3. Wi-Fi Radio Characteristics

The following data are from tests conducted at room temperature, with a 3.3V power supply.

Table 3-2. Wi-Fi Radio Characteristics

Parameters	Min	Typical	Max	Unit
Input frequency	2412	-	2484	MHz
Output impedance	-	39 + j6	-	Ω
Output power of PA for 72.2 Mbps	15.5	16.5	17.5	dBm
Output power of PA for 11b mode	19.5	20.5	21.5	dBm
Sensitivity				
DSSS, 1 Mbps	-	–98	-	dBm
CCK, 11 Mbps	-	–91	-	dBm
6 Mbps (1/2 BPSK)	-	–93	-	dBm
54 Mbps (3/4 64-QAM)	-	–75	-	dBm
HT20, MCS7 (65 Mbps, 72.2 Mbps)	-	–72	-	dBm
Adjacent Channel Rejection				
OFDM, 6 Mbps	-	37	-	dB
OFDM, 54 Mbps	-	21	-	dB
HT20, MCS0	-	37	-	dB
HT20, MCS7	-	20	-	dB

الخلاصة:

الاحتياجات الحيوية لاستمرار الحياة مثل الطاقة الكهربائية أصبحت ضرورة يومية حيث تستخدم بشكل واسع في المرافق السكنية والصناعية والحيوية وعند فقد هذه الطاقة تصبح الحياة بدائية.

على الرغم من تلك الحاجة للكهرباء وتطور طرق دفع الفواتير وسهولتها لاتزال بعض المشاكل الموجودة مثل الخسائر التي تحتاج الى تقليل والفواتير الاضافية التي تحتاج الى معالجة إضافة الى اخذ الطاقة الكهربائية مباشرة بدون مقياس.

تصحيح معامل القدرة هو طريقة لتقليل بعض المشاكل المذكورة. حيث ان تصحيح معامل القدرة المؤتمت هو اختراع جيد. من ناحية أخرى يتيح اكتشاف انتحال الطاقة الكهربائية طريقة أكثر كفاءة وفعالية من حيث الكلفة حيث ان انتحال الطاقة هو مشكلة في اغلب مؤسسات الطاقة.

غرض هذه الاطروحة هو تصميم أنظمة سحابية لمركز تشغيل ذكي. النظام الأول هو سحابة لتحسين معامل القدرة مع الشبكة العصبية هذا النظام يستخدم سحابة خاصة بالاستفادة من Raspberry Pi والشبكة العصبية لتصحيح معامل القدرة للمنازل بخوارزمية واحدة. السحابة ستساعد في الاستضافة والمعالجة والوصول عند الطلب وفي أي وقت طالما توفر الانترنت. الشبكة العصبية ستستخدم لإيجاد قيمة المتسعة اللازمة للتصحيح. هذا التصميم سيقلل الأجهزة المستخدمة ويساعد في تقليل الفاتورة إضافة الى دقة النتائج. كان معدل خطا تصحيح معمل القدرة خلال الشبكة العصبية بالاعتماد على قيمة المتسعة الحقيقية والمحسوبة للبيانات المدربة 1.928% والغير مدربة 2,5% تم التدريب باستخدام MATLAB R2020b.

بينما النظام الثاني هو طريقة مبتكرة للكشف عن التحايل على في الطاقة الكهربائية وتقدير كلفة الطاقة المفقودة في تلك العملية مع مراقبة خط التوزيع الرئيسي لمعرفة الحاجة للتوسع المستقبلي.

يستخدم هذا النظام أيضا سحابة خاصة بواسطة Raspberry Pi ومنصة Node-redعند المصدر الرئيسي مع خوارزمية مركزية واحدة للكشف مما سيقلل الأجهزة المستخدمة النظام المقترح يمكنه أيضا كشف وتشخيص المقاييس التي يتم التحايل عليها والربط المباشر بدون مقياس والخوارزمية تعتمد على نظام فرق التيار مع فصل المقاييس بأرسال أوامر من السحابة للمقاييس وتعطي نتائج دقيقة ويسهل على المؤسسة مراقبة هذه الطاقة الضائعة على مدار اليوم كمثال حالة تجاوز مقياسين حيث تم الكشف آنيا بنفس الوقت. نظام المراقبة بالاعتماد على السحابة الخاصة ومنصة Node-red يوفر مرونة وقدرة على إدارة البيانات ومعالجتها لاحقا حيث يمكن الوصول اليها اما عن طريق المتصفح او تطبيق الجوال.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل / كلية الهندسة
قسم الهندسة الكهربائية

تصميم وتنفيذ نظام حوسبة سحابية لجمع البيانات ومعالجتها لمركز تشغيل ذكي

اطروحة

مقدمة إلى كلية الهندسة في جامعة بابل

كجزء من متطلبات الحصول على درجة الدكتوراه

فلسفة في الهندسة \ الهندسة الكهربائية \ إلكترونيك واتصالات

من قبل

مفاز محمد عبد جعفر

بأشراف

أ. د. ليث علي عبد الرحيم

أ. م. د. احمد عبد الكاظم حمد

٢٠٢٢ م