IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 10, Issue 8, August 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.282

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15662/IJAREEIE.2021.1008029 |

Fault Data Detection in Smart Grid

Prakyath D, Deepak.B, Mahesh D Chaubey, Vinay, Yashwanth Kumar M

Asst. Professor, Dept. of EEE, SJB Institute of Technology, Bangalore, Karnataka, India

Dept. of EEE, SJB Institute of Technology, Bangalore, Karnataka, India

Dept. of EEE, SJB Institute of Technology, Bangalore, Karnataka, India

Dept. of EEE, SJB Institute of Technology, Bangalore, Karnataka, India

Dept. of EEE, SJB Institute of Technology, Bangalore, Karnataka, India

ABSTRACT: Security of the smart metering infrastructure, which is a part of the smart grid initiative, intended at transitioning the legacy power grid system into a robust, reliable, adaptable and intelligent energy utility, is an imminent problem that needs to be addressed quickly. Moreover, the increasingly dependency on digital system such as smart meter with communication network forcing both the consumer and the utility provider to meticulously look into the security and privacy issues of the smart grid. To achieve this, improvements on the existing architecture that uses smart meters interacting with smart grid is needed. This architecture makes the ease of work for the utility provider & helps to save energy by giving regular consumption reading. The study presented in the project analyses the various existing smart metering infrastructure, threats and vulnerabilities that has the potential to disrupt the operation and deployment of automation systems in smart grids. We are implementing system for track the receive data for smart meter. If any unformatted and wrong data will receive, it will detected by this system and update on IOT cloud app using Esp82266 module.

I. INTRODUCTION

In today's scenario, the security of smart metering infrastructures is a very critical issue and plays an important role. In this project, the analysis is made on a live consumer meter setup, The effort of collecting electricity utility meter reading. Internet of Things (IoT)is used where it is efficient to transfer the meter data of consumer effectively through wirelessly & also provide to detect the usage of electricity. The main intention of this project is measure electricity consumption in home appliances and to detect the fault data intrude by the attacker. Where the meter is serially connected with a communication modem. The meter data through serial communication reaches to the microcontroller. The interim data packets have been captured and analyzed from the live consumer meter setup using embedded c program, which is uploaded in atmega328 microcontroller. The data is sent in a special format which is understood only by the aggregation system and processed in a proprietary manner. But there is a possibility of tampering the meter data. Because the billing of the consumer consumption depend on meter data. If the meter reading data is tampered it highly affect the utility provider and also effect the economy of the country. The number of services like meter reading, online pricing, information security or load control, which is the part of the energy ecosystem could get effected. Thus, security system as to be built in such a way that it prevent any fraud & make difficulty to the attacker to manipulate the data. Since the power utility is one of the most mission critical infrastructure services today, the comprehensive security and privacy mechanisms are needed to ensure reliable and smooth operation of the smart grid.

II. LITERATURE SURVEY

Topic: "Smart Energy Metering And Power Theft Control Using Arduino&Gsm" By (Kamal Sandeep K Assistant Professor, Zeal College Of Engineering & Research, Pune. 2017)

Energy theft is a very common problem in countries like India where consumers of energy are increasing consistently as the population increases. Utility are getting affected by the energy theft which inturn affect the revenue of the country. In this paper, a new steps are followed based on MICROCONTROLLER Atmega328P to detect the energy theft and control the energy meter from power theft. Where in this paper GSM module is used to send the message to utility provider to central server whenever the unauthorized activities is detected and a control action in the form of message is sent back to microcontroller to utility in order to disconnect the unauthorized supply.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15662/IJAREEIE.2021.1008029 |

Topic:"Development Of Iot Based Smart Energy Meter Reading And Monitoring System" by M. Mohamed Mufassirin1, and A. L. Hanees, Department of Mathematical Sciences, Faculty of Applied Sciences, South Eastern University of Sri Lanka.

In the most of the developing countries, the effort of collecting electricity utility meter reading and detecting illegal usage of electricity is a very difficult and time consuming task which requires a lot of human resources. Monitoring of meter data is done through IOT which is efficient & cost effective way to transfer the data wireless and also provide option to detect the illegal usage or manipulating of data.The main aim of this study is to measure electricity consumption in the household and to detect the unauthorized activity in the comminucation network where the microcontroller is used to transfer the data to IOT module where it is connected to wifi which send the data to server. Also this study aims to detect and control the energy theft. The Arduino microcontroller is employed to coordinate the activities with digital energy meter system and to connect the system to a WiFi network and subsequently to the Internet and Server. A passive infrared sensor is engaged with the system to detect when any illegal alteration happen in the metering system. In such case, system will send an alert to the server as well as it has the facility to disconnect and re-connect the electricity supply automatically. The proposed system is capable of continuously monitor and being notified about the number of units consumed to the energy provider and consumer. The energy consumptions are calculated automatically and the bill is updated on the internet by using a network of Internet ofThings. This automation can reduce the needs of the manual labours.

III. PROPOSED WORK

The main objective is implement a method for modeling functionalities of energy meters. This system will track the receive data from communication protocol and after track data, this system will trigger alarm and IOT update using this implementation design.In this paper, we propose a systematic way of designing the procedures implemented for the smart meter and performing security analysis of these procedures. By systematic, we mean a design-based, step by step approach that is for tracking the receive data. Building a design for performing the security analysis will remove the errors data and provide an accurate way to perform penetration error. With this system the authorized person will able to monitor data from remote location using IOT platform.

A. Hardware Design:

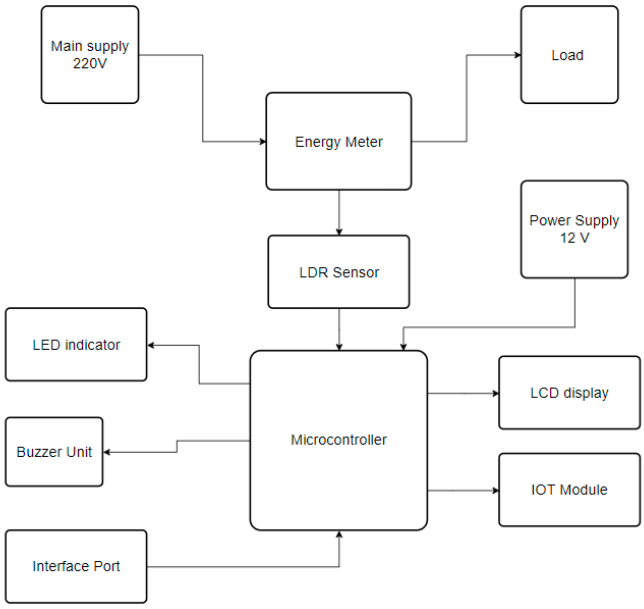


Fig 1: Block Diagram

B. Energy Meter

The energy meter work is measure the load consumption and based on consumption calculate the unit. But manually we have to read unit count. To make it advance we can make automatic reading system also with help of

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15662/IJAREEIE.2021.1008029 |

microcontroller LDR and a resistor. The electricity meter is owned by the utility company and so cannot be modified in any way. Therefore a reliable but non-permanent way has to be found to position the light detector over the LED and shield it from ambient light.

Fig 2: Energy Meter

C. Arduino UNO

Arduino is an open-source electronics platform based on easy-to-use hardware and software.The Uno is a great choice for your first Arduino. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a USB connection, a power jack, a reset button and more. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with AC-to-DC adapter or battery to get started

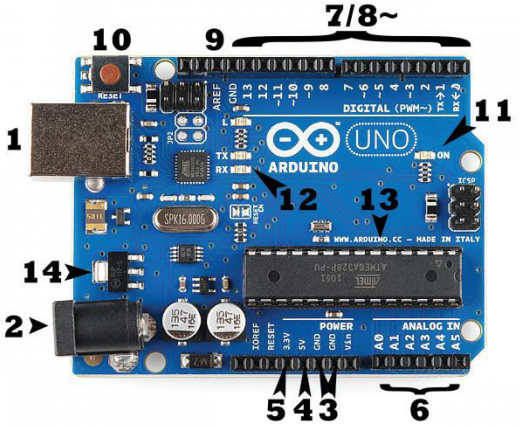


Fig 3:Arduino Uno

D. LDR Sensor

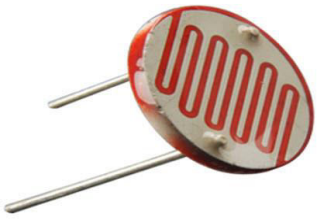


Fig 4: LDR Sensor

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15662/IJAREEIE.2021.1008029 |

An LDR or light dependent resistor is also known as photo resistor, photocell, and photo conductor. It is a one type of resistor whose resistance varies depending on the amount of light falling on its surface. When the light falls on the resistor, then the resistance changes.These resistors are often used in many circuits where it is required to sense the presence of light.

E.IOT Module

IOT Module Node MCU is an excellent hardware, which provides just enough versatility for us to do a majority of our developments. It is Arduino compatible, has a Wi-Fi on board and has enough kick to power our IOT devices. Whether connecting to gateway or connecting to our cloud solutions. Node MCU is an open source IOT platform. It includes firmware which runs on the ESP8266 Wi-Fi SoC from Espress if Systems, and hardware which is based on the ESP-12 module. The term "Node MCU" by default refers to the firmware rather than the development kits. The firmware uses the Lua scripting language.

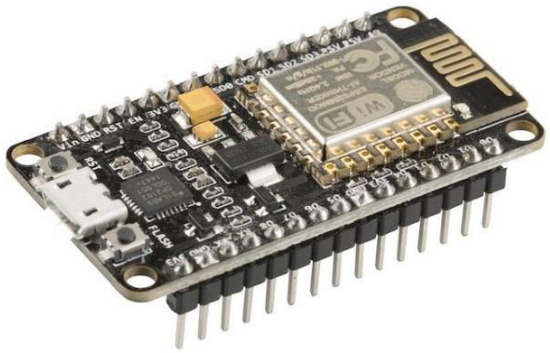


Fig 5:ESP8266 Module

F.Software Design

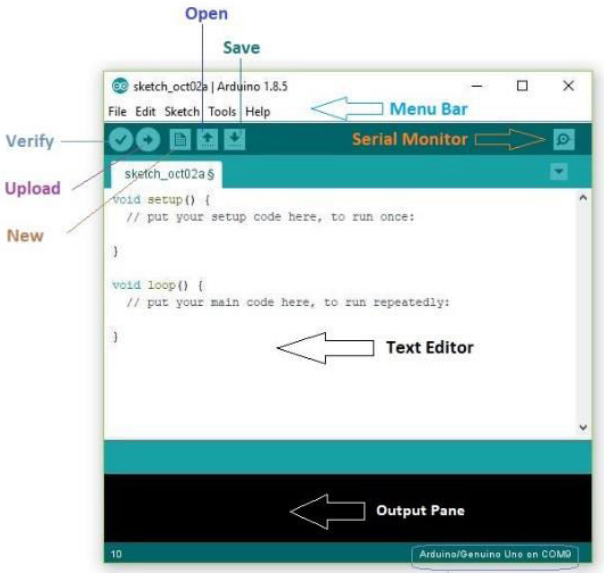


Fig 6: Arduino IDE

1. Arduino IDE

The Arduino incorporated improvement environment (IDE) is a crossplatform application (for Windows, macOS, Linux) this is written withinside the programming language Java. It is used to put in writing and add applications to Arduino well suited boards, however also, with the assist of third birthday birthday celebration cores, different dealer improvement boards. The supply code for the IDE is launched below the GNU General Public License, model 2. The Arduino IDE helps the languages C and C++ the usage of unique regulations of code structuring. The Arduino IDE

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15662/IJAREEIE.2021.1008029 |

elements a software program library from the Wiring project, which affords many not unusualplace enter and output procedures

2. *Blynk Application*

Configure the Blynk App:

- Download the Blynk App from Google play store or Apple store.
- Create a new project in the Blynk app. Enter the project name and choose the device. In this IoT project, I have used NodeMCU, so I have selected NodeMCU.
- After that Blynk will send an Auth Token to the registered email id. The Auth Token will be required while programming the ESP8266.

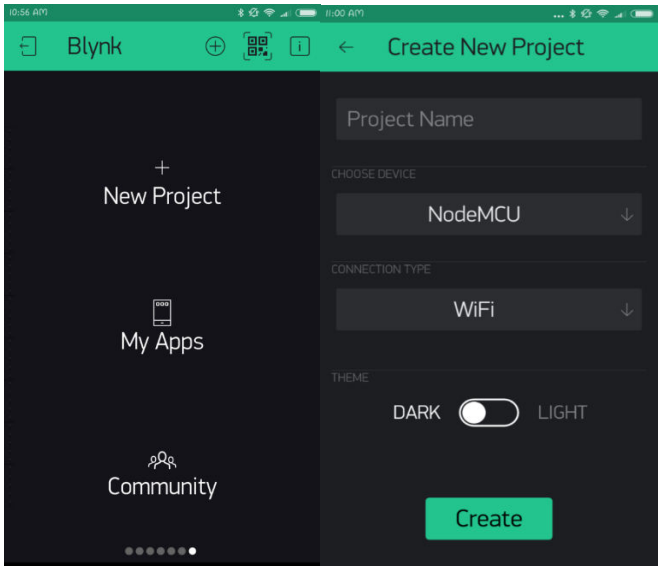


Fig 7: Configure Blynk App

IV. IMPLEMENTATION

- Main power 220 volt supply will get connected with energy meter input pin. There will be two pin terminal neutral and phase.
- Energy meter output neutral and phase output will be connected with load.
- Based on load the blink rate will be execute.
- LDR sensor is mounted on the unit LED, for count the blink led.
- LDR is connected with microcontroller analog pin.
- In microcontroller we have uploaded embedded c code for count the LDR signal and based on this we will maintain unit count.
- USB port of system is used for interface communication with external source. Here we are using Laptop as an external source for communication.
- Once USB will receive any external data using serial communication, Program code will execute and start operation on data.
- After process the data we are alerting buzzer, LCD display, LED and updating on IOT cloud service.
- This alert and update will be depends on received data.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15662/IJAREEIE.2021.1008029 |

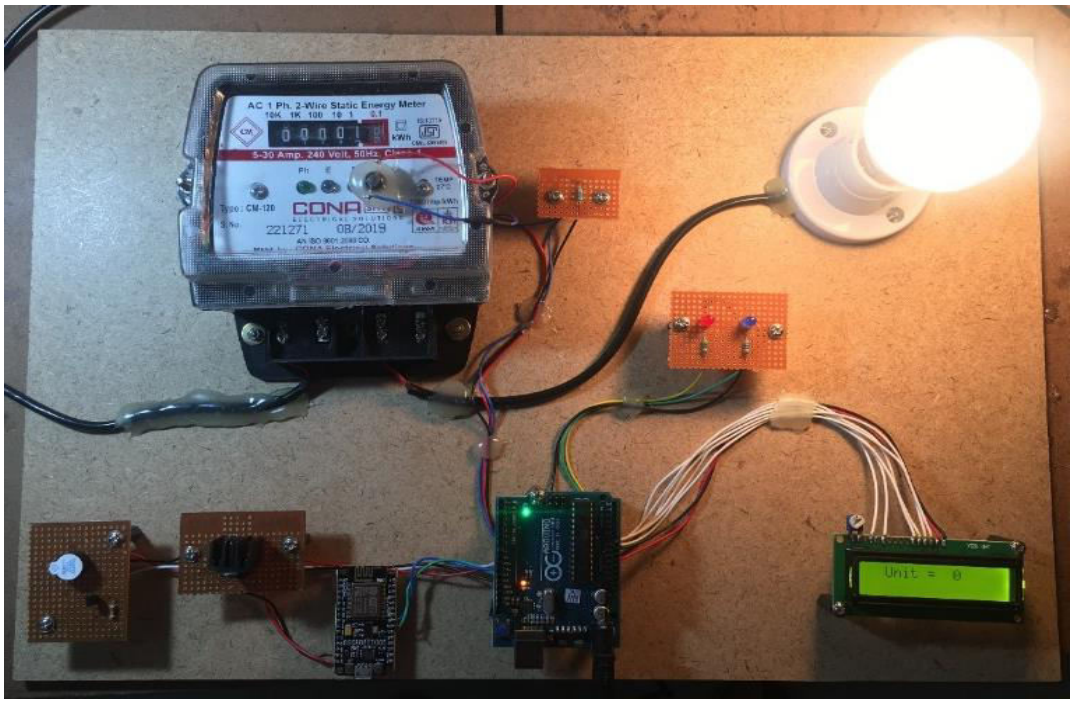


Fig 8: Working Model

A. Flow Chart

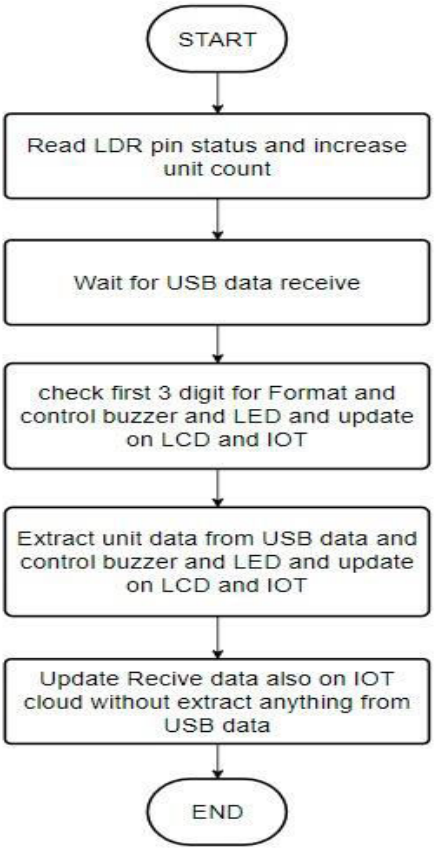


Fig 9:Flow Chart

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 8, August 2021 ||

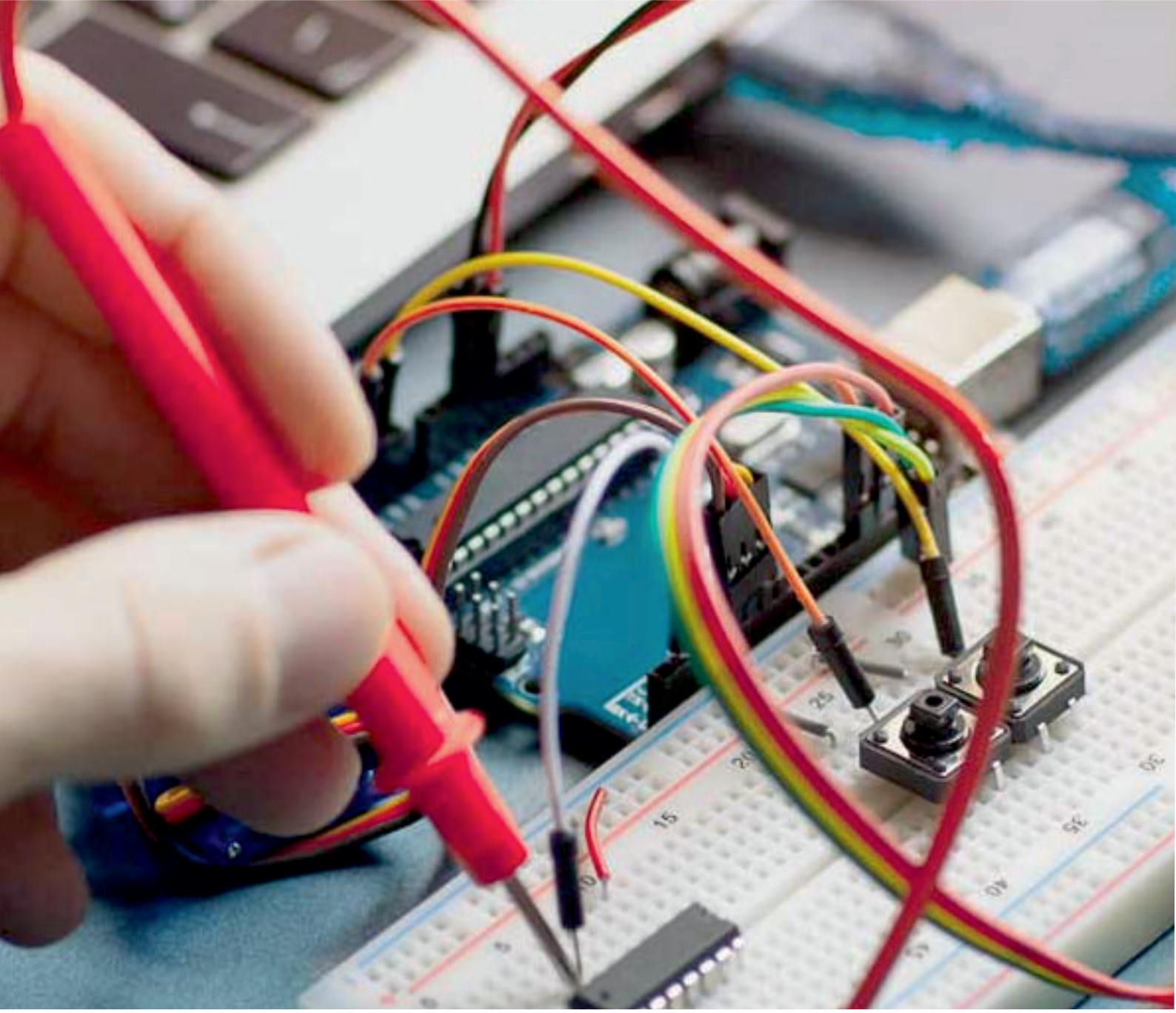
| DOI:10.15662/IJAREEIE.2021.1008029 |

V. RESULT&CONCLUSION

The implemented device we tested with different data insertion and implemented device model working fine and we are able to see result by LED indicator, LCD display and we are getting update on IOT app. The complete system working fine for different data condition. As per required task hardware and code program working successfully
Energy meter fault data insertion and automatic detected by system was out main task in this project implementation. In this paper, we have investigated the advanced metering infrastructure from security perspective being the most critical matter to consider. We have evaluated the attack surface and vulnerabilities associated with each, and recommended proper security requirements respectively. The paper findings the early fault data by design and implemented this embedded system

REFERENCES

1. “A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids”(Ahmed S. Musleh, Member, IEEE (Corresponding author: Guo Chen) School of Electrical Engineering and Telecommunications, Sydney 2019)
2. “A Survey on Bad Data Injection Attack in Smart Grid” (Ting Liu, School of Electronic and Information Engineering, china 2013)
3. S. Sridhar and M. Govindarasu, "Cyber–physical system security for the electric power grid," member of the IEEE, vol.100, pp. 210-224, 2012.
4. R. Kumar and B. Sikdar, “Efficient detection of false data injection attacks on AC state estimation in smart grids,” in IEEE Conference on Communications and Network Security (CNS), 2017
5. A.Tajer, “False Data Injection Attacks in Electricity Markets by Limited Adversaries: Stochastic Robustness,” IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 128 - 138, 2019



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 7.282

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details