©IDOSR PUBLICATIONS
International Digital Organization for Scientific Research
IDOSR JOURNAL OF COMPUTER AND APPLIED SCIENCES 7(1):109-118,2022. ISSN: 2579-0803

Enhanced Security Monitoring System for the Pay Card Energy Meter

George Kasamba and Anthony Ejeh

Department of Electrical and Telecommunications Engineering, School of Engineering & Applied Sciences, Kampala International University, Uganda.

ABSTRACT

The problem of poor payment of electricity bills has been thing of concern for research for some years now. In the context of energy meters the concept of meter security is of great concert due to tempering of the energy meters presented a GSM-Based Smart Energy Meter with Arduino Uno that could enable users to monitor their current power consumptions (bill) anytime from anywhere by using their mobile phone via Short Message Services (SMS). Enhanced Security monitoring system that detects energy meter tampering anytime from anywhere by using the Global Positioning System (GPS) was design. It would be a huge benefit for the utility companies if energy meter tampering is detected on real-time basis. ATMEG328p main controller, was the interface between energy meter and Global Positioning System (GPS) module sound an alarm.

Keywords: Energy Meter, Global Position System (GPS), ATMEGA328p, and Real Time.

INTRODUCTION

In Uganda today, UMEME expects to address some challenges like poor payment of electricity bills, current high cost of billing as well as create an opportunity for easier monitoring of consumers' meters and energy consumption. It was also anticipated that this new system will reduce the fraud that has been largely peddled by illegal electricity technicians who prey on unsuspecting customers by extorting money out of them under the guise of disconnecting and reconnecting them. By the first half of 2013, the company had 32,000 customers converted to the pre-paid Yaka system a number that is likely to have doubled by the close of 2014 [1].

A good look at how Smart Meters operate shows a heavy reliance on ICT systems. A meters usually an electronic device that records consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing purposes [2].

Governments globally are rooting for Smarter metering systems to encourage better and sustainable usage of the limited electricity energy available. This has led to a sudden boom in the production of smart meters as utility companies are buoyed to take on this direction in response to Government support. However, these smart meters have been found vulnerable and subject to tampering by intruders with the wrong intentions. The lack of proper security controls can make them susceptible attacks [3]. Now hackers can carry out billing related fraud and shutdown electricity supplies at will. By accessing their memory chips, one can carry out some re-programming as well as exploit any flawed code there-in to tamper with meter readings, transfer readings to other customers as well as insert network worms that can potentially leave entire neighborhoods in a blackout. This is easily achievable if one takes control of the meter box since they can switch its unique ID to mimic another customer's or use it to launch attacks on the network [4].

In IT security, physical access to the hardware is one of the loopholes one can use to initiate any compromise. The fact that these meters are easily accessible to the consumers means a lot. Access to the onboard software (firmware) of these meters can enable one find the encryption keys used to scramble all the information that the meter shares with hosts found higher up in the power distribution network. One can then fool the hosts and send them false data [5].

Other flaws these meters are likely to have are shared IDs like factory default passwords (I recall this with Cisco networking gear at the turn of this

century) and poor protection from tampering. Some of the quick hacks one can use to render a smart meter dumb are; attacking its memory through hardware; with insufficient protective features, all that one needs is to insert a needle on each side of the device's memory chip. The needle intercepts the electrical signals in the memory chip. From these signals, a device's programming can be determined [6,7,8].

Use of a digital radio; the two-way radio chip in a smart meter allows the device to be read remotely and receive commands over the network. Once one has cracked the smart meter's programming, they can use security codes from the software in the chip to get network access thereby issuing commands at will.

Interfering the Smart Meter's energy monitoring; by placing strong magnets on the devices, it can cause the meter to stop measuring usage while still providing electricity to the customer.

UMEME has a big challenge ahead considering that meter tampering is likely to be facilitated by collusion between meter manufacturing employees, current or former UMEME employees and consumers. In Puerto Rico, it costs between US$ 300 – US$ 1000 to tamper with a residential smart meter while industrial ones cost up to US$ 3000. So, while UMEME expects to have higher payment compliance by customers, there is a real possibility of this not achieving the expected levels. Several cases have been registered of current and former UMEME employees and contractors that are already involved in this lucrative illicit activity [9,10,11,12].

At a higher level, concern arises with the national security. What is likely to happen if a hacker breaks into the national electricity grid and shuts it down? Currently the likely purveyors of such an attack are driven by mere profit and thus may not be of much concern to our internal security organs. However, as these skills become more mainstream, those driven with more political motives like terrorists and rebels could swap their gun totting activities for infrastructure based attacks using available electronic systems that are easily procurable on websites like e-bay among others [8].

METHODOLOGY

DATA COLLECTION.

Experimental data collection method was used in this project. It is data produced by a measurement, test method, experimental design or quasi-experimental design. Also, it is data produced as a result of a clinical trial. Experimental data may be qualitative or quantitative, each being appropriate for different investigations. The data there-in used in this project is both qualitative and quantitative where qualitative data is considered more descriptive and can be subjective in comparison to having a continuous measurement scale that produces numbers normally experimentally repeatable. Qualitative information is usually more closely related to phenomenal meaning and is, therefore, subject to interpretation by our observations as it will be shown in the experiments and block diagrams in this and the next chapters.

METHODS

Examining the existing system

Experimentation

This involves the deliberate manipulation of an intervention in order to determine its effects.

Reason why experimentation was used

An experiment may compare a number of interventions with each other, or may compare one (or more) to a control group. Issues of generalizability (often called 'external validity') are usually important in an experiment, so the same attention must be given to sampling, response rates and instrumentation as in a survey (see above). It is also important to establish causality ('internal validity') by demonstrating the initial equivalence of the groups (or attempting to make suitable allowances), presenting evidence about how the different interventions were actually implemented and attempting to rule out any other factors that might have influenced the result.

SYSTEM PROGRAMMING

All these functions were coordinated by a C code running in an Integrated Development Environment called ATMEL

STUDIO. This software uses a programming board called POLORU AVR PROGRAMMER which programs AVR microcontrollers like ATMEGA32.

Current bypassing

Intrusive tampering methods include current bypassing, reversing connections and bypassing leads. In current bypassing, which is one of the most common tampering techniques, a metal object is placed against the meter terminal block. The object forms a current divider with the current-sensing circuitry, causing the metal object to bypass the current and leading to a smaller active energy reading than actual consumption, and thus a less expensive utility bill. Through the interface of a current sensor with the atmega328p microcontroller, any current division will be detected and an alarm will be triggered for warning purposes first, if the action persists the meter will be deactivated by turning off the relay switch that supplies power the energy meter.

Magnetic intrusion tampering

On the transformers inside the electronic meter, placement of a magnet as close to this transformer as possible could cause over fluxing every half a cycle, this could cause a diode like effect in the meter electronics, a very powerful magnet might harm your GPS unit. For example, the magnet would have to be strong enough to disturb electrons to affect GPS and similar devices and if a magnetic sensor is interfaced with a MCU magnetic intrusion can be detected and mediate action is taken to deactivate the system for that period of time and on a real time basis an SMS will be sent to the management team reporting the problem.

ENERGY METER DISPLACEMENT CONTROL AFTER TAMPERING

It is known that people who tend to practice energy meter tampering have a tendency of changing locations with intentions of hiding away from the electric company security teams after being detected doing the act, so to eliminate this, using the initial set GPS coordinates an algorithm was designed to monitor location of the meter and deactivate the meter in case location is changed after the act of tampering.

Block diagram

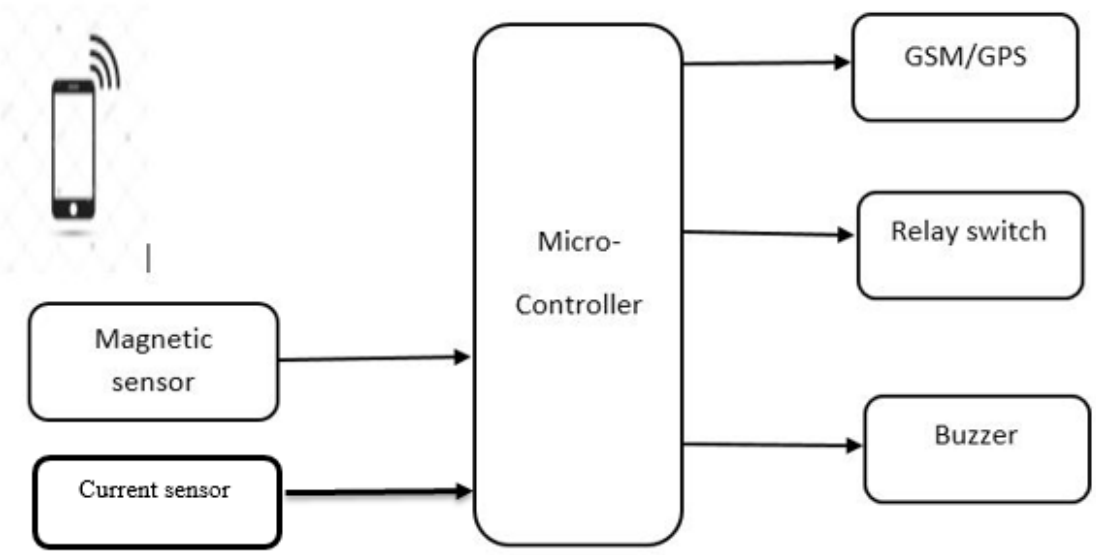


Figure 1: Block diagram.

A MICROCONTROLLER

A microcontroller is a computer-on-a-chip used to control electronic devices. It is a type of microprocessor emphasizing self-sufficiency and cost-effectiveness, in contrast to a general- purpose microprocessor. A typical microcontroller contains all the memory and interfaces needed for a simple application. A microcontroller is a single

integrated circuit with the following key features: Central processing unit - ranging from small and simple 8-bit processors to sophisticated 32- or 64-bit processors, input/output interfaces such as serial ports, peripherals such as timers, RAM for data storage, ROM, EEPROM or Flash memory for program storage, clock generator often an oscillator for a quartz timing crystal and resonator or RC circuit. This integration drastically reduces the number of chips and the amount of wiring and Printed Circuit Board (PCB) space that would be needed to produce equivalent systems using separate chips.

Figure 2: Microcontroller

THE SMS AND CALL SYSTEM

This was achieved through interfacing a GSM modem which is a highly flexible plug and play modem based on tri-band sim900. Sim900 can fit almost all the space requirements in much real-time application. This global system for mobile communication technology made it very easy to send and receive the messages by the support of the AT commands. These commands were implemented by interfacing to the receiver and transmitter pins of microcontroller.

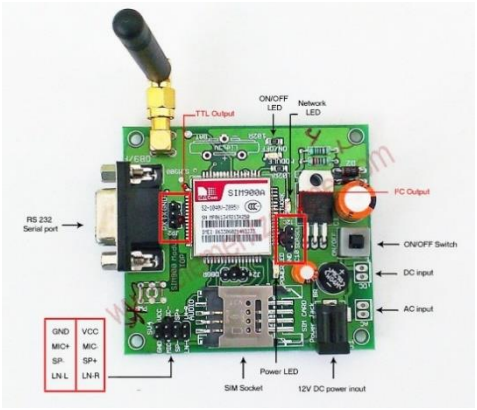


Figure 3: The SMS and call system

LCD JHD162A

A liquid crystal display is a flat panel, an electronic visual display that uses the light modulating properties of liquid crystals. Liquid crystal does not emit light directly. The working of LCD depends on two sheets of polarizing material with a liquid crystal solution in between them. When an electric current is passed through the liquid, it causes the crystals to align so that it blocks out light and does not allow it to pass. Each crystal behaves like a shutter; it either allows light to pass through or blocks the light. It can function properly in the temperature range of -10°C to 60°C and has an operating lifetime of longer than 50000 hours (at room temperature without direct irradiation of sunlight).

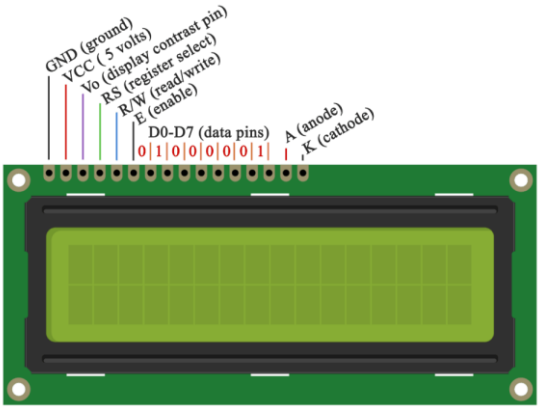


Figure 4: LCD JHD162A

BUZZER SYSTEM

Buzzer is used for alerting purpose. It convert electrical energy into sound energy by using transistor and capacitor. It produces high frequency for hearing purpose.

Figure 5: Buzzer system

MAGNETO RESISTANCE SENSOR

Magneto resistive sensors are based on a property of several materials called magneto resistance**,** consisting in the variation of their electrical resistivity when placed in a magnetic field. In practice, the current flow through a magneto resistive wire depends on the strength and on the orientation of an external magnetic field. The adjective "digital" in the name of these sensors refers to the fact that they provide just two states: either they are sensing a magnetic field or they are not. In other words, they are not able to provide a precise and accurate measurement of the strength of any external magnetic field: they only *react* to magnetic fields stronger than a given threshold, providing a sort of signal that can be, in some cases, somewhat proportional to its strength.

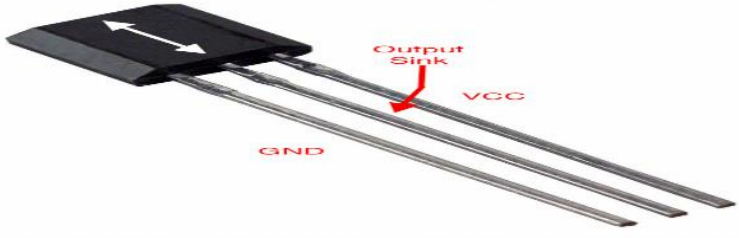


Figure 6: Magneto Resistance Sensor

Global Positioning System (GPS) Module

GPS or Global Positioning System is a satellite navigation system that furnishes location and time information in all climate conditions to the user. GPS is used for navigation in planes, ships, cars, and trucks also. The system gives critical abilities to military and civilian users around the globe. GPS provides

continuous real-time, 3-dimensional positioning, navigation and timing worldwide.

Figure 7: Global Positioning System (GPS) Module

How does GPS System Work?

The GPS consists of three segments:

1) The space segment: the GPS satellites
2) The control system, operated by the U.S. military,
3) The user segment, which includes both military and civilian users and their GPS equipment.

Space Segment

The space segment is the number of satellites in the constellation. It comprises of 29 satellites circling the earth every 12 hours at 12,000 miles in altitude. The function of the space segment is utilized to route/navigation signals and to store and retransmit the route/navigation message sent by the control segment. These transmissions are controlled by highly stable atomic clocks on the satellites. The GPS Space Segment is formed by a satellite constellation with enough satellites to ensure that the users will have, at least, 4 simultaneous satellites in view from any point at the Earth's surface at any time.

GPS Control Segment

The control segment comprises of a master control station and five monitor stations outfitted with atomic clocks that are spread around the globe. The five monitor stations monitor the GPS satellite signals and then send that qualified information to the master control station where abnormalities are revised and sent back to the GPS satellites through ground antennas. The control segment also referred to as a monitor station.

User Segment

The user segment comprises of the GPS receiver, which receives the signals from the GPS satellites and determines how far away it is from each satellite. Mainly this segment is used for the U.S military, missile guidance systems, civilian applications for GPS in almost every field. Most of the civilian use this from survey to transportation to natural resources and from there to agriculture purpose and mapping too.

How GPS Determines a Position

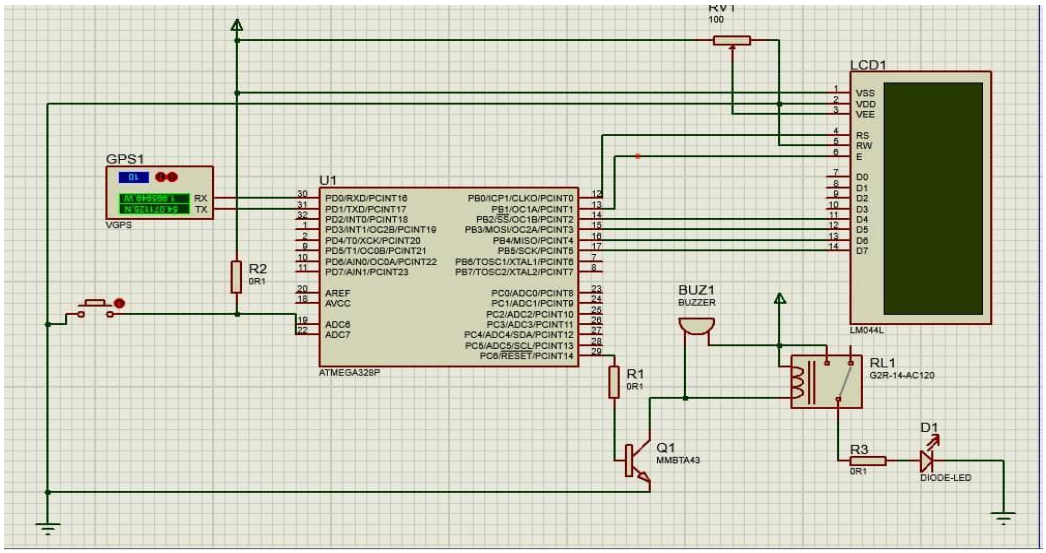
The working/operation of the Global positioning system is based on the 'trilateration' mathematical principle. The position is determined from the distance measurements to satellites. From the figure, the four satellites are used to determine the position of the receiver on the earth. The target location is confirmed by the 4th satellite. And three satellites are used to trace the location place. A fourth satellite is used to confirm the target location of each of those space vehicles. The global positioning system consists of satellite, control station and monitor station and receiver. The GPS receiver takes the information from the satellite and uses the method of triangulation to determine a user's exact position.

GPS is used on some incidents in several ways, such as:

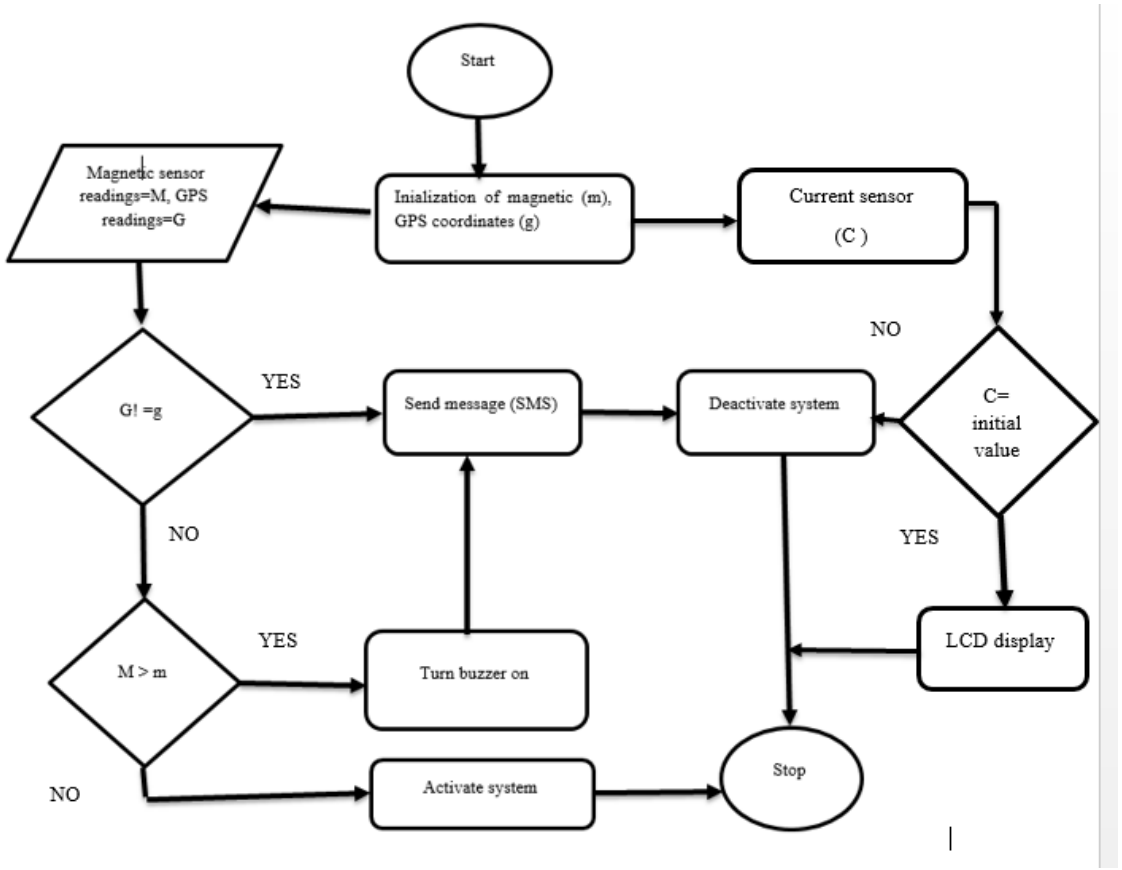
1) To determine position locations; for example, you need to radio a helicopter pilot the coordinates of your position location so the pilot can pick you up.
2) To navigate from one location to another; for example, you need to travel from a lookout to the fire perimeter.
3) To create digitized maps; for example, you are assigned to plot the fire perimeter and hot spots.
4) To determine the distance between two different points.

RESULTS AND DISCUSSION

WORKING PRINCIPLE



FLOW CHART



Software

Proteus Arduino IDE.

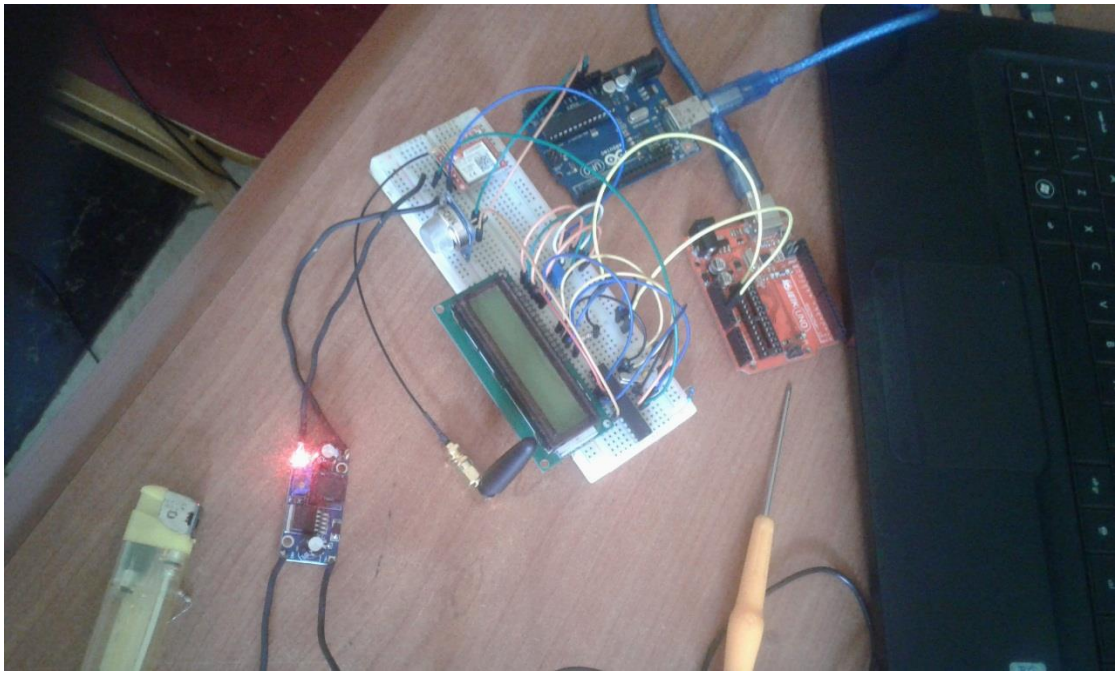


Figure 8: breadboard assembling

The results were positive as all components performed their tasks as expected, right from the +5v power source tapped from the laptop with the aid of Arduino Uno power cable (USB), through the board to all other components.

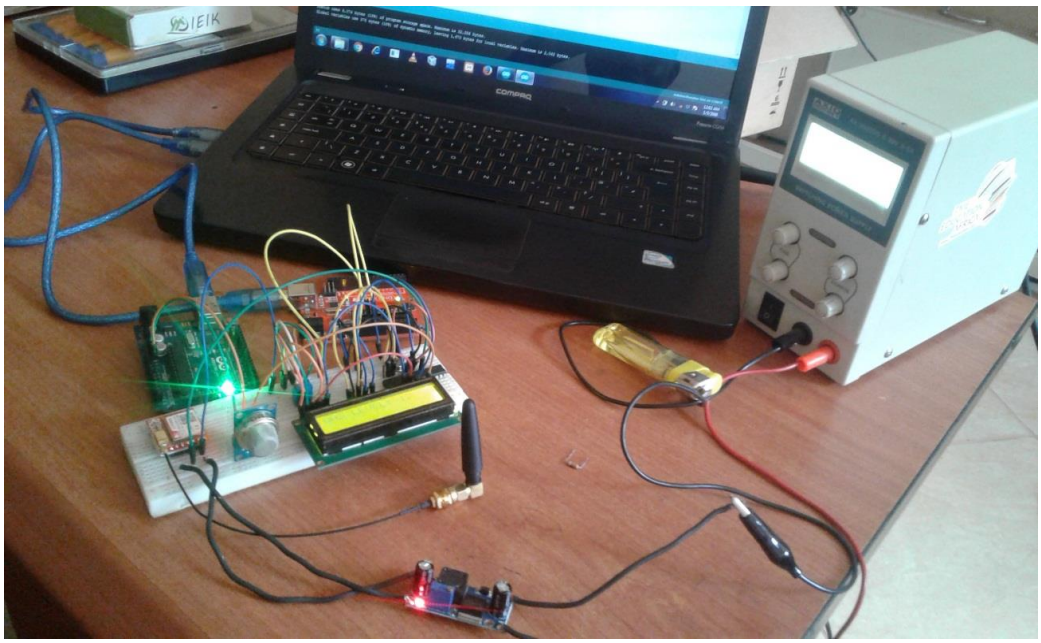


Figure 9: Breadboard components assembling

This involved, placing components on a PCB and soldering them on with the aid of a soldering gun and lead. This marked a strong continuous outline of the circuit whereby all components were connected from point to point, from Vcc to ground and microcontroller connections.

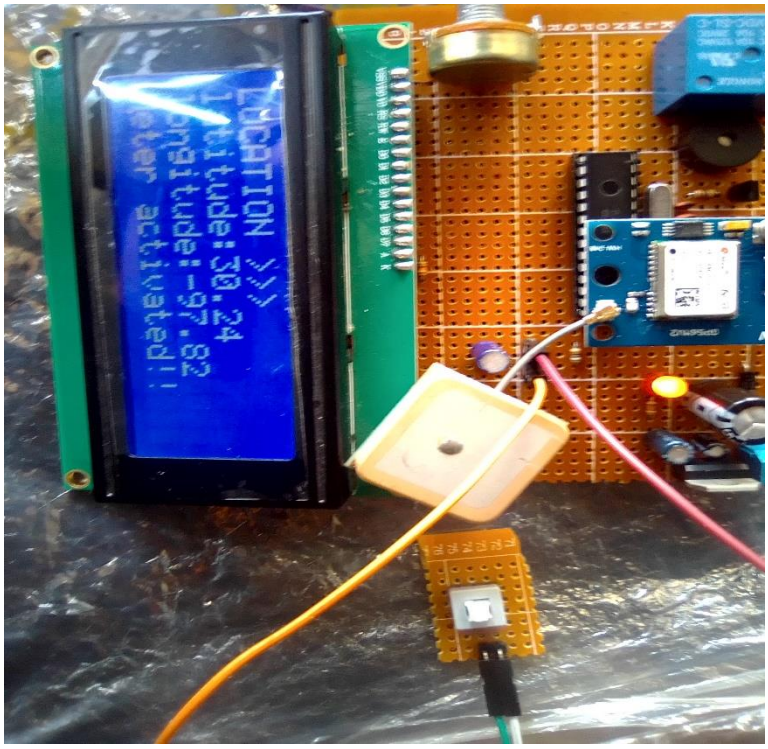


Figure 10: Results on PCB

PRECAUTIONS WERE TAKEN WHILE SOLDERING

- Keeping the heated/hot soldering gun tip away from body contact.
- Placing the hot soldering gun on a stand to prevent it from burning surrounding stuff.
- Ensuring the gun doesn't burn the components as a result of overheating

CONTINUITY TESTING

After soldering was done, the continuity test was crucial for testing whether a line was continuous from one point to another and also to ensure there are no short circuits as a result of continuity between Vcc and ground.

RESULTS ON PCB

A successful continuity test gave a go forward to power the circuit and hence all components successfully performed as anticipated and the figures A and B show the results after soldering on PCB and powering the device.

CONCLUSION

An enhanced security monitoring system for the pay card energy meter will revolutionaries the power meter industry. It will offer a better, inexpensive method to reduce power theft. This project offer the following facility GPS monitoring of the meter and deactivation of compromised nodes

REFERENCES

1. Edward, O. O. (2014). An energy meter reader with a microcontroller based logic methodology fused with a building automation system to implement remote load control by home owners using SMS from a GSM phone.
2. H.G.Rodney, T. I. (2007). Automatic Power Meter Reading system using GSM Network.
3. Abhinandan, J. (2012). A complete Automated Energy Meter.
4. Syed Shahbaz Ali, S. h. (December 2010). Smart energy meters for

energy conservation & minimizing errors.
5. Md.Masudur Ramhman, N.-E. M. (2015). An arduino and GSM based smart energy meter for advanced metering and billing system .
6. Win Adiyansyah Indra, F. M. (2018). A GSM-Based Smart Energy Meter with Arduino Uno.
7. Paraskevakos. (1972). *Automatic Meter Reading system.*
8. Sonali, S. and Wagh, S. P. (2017). An Intelligent Energy Meter Using GSM Modem with Arduino.
9. Masisani William Mufana and Adabara Ibrahim (2022). Monitoring with Communication Technologies of the Smart Grid. *IDOSR Journal of Applied Sciences* 7(1) 102-112.
10. Nabiryo Patience and Itodo Anthony Ejeh (2022). Design and Implementation of Base Station Temperature Monitoring System Using Raspberry Pi. *IDOSR Journal of Science and Technology* 7(1):53-66.\
11. Masisani William Mufana and Adabara Ibrahim (2022). Implementation of Smart Grid Decision Support Systems. *IDOSR Journal of Scientific Research* 7(1) 50-57, 2022.
12. Natumanya Akimu (2022). Design and Construction of an Automatic Load Monitoring System on a Transformer in Power Distribution Networks. *IDOSR Journal of Scientific Research* 7(1) 58-76, 2022.