

MAKERERE



UNIVERSITY

**COLLEGE OF ENGINEERING, DESIGN, ART AND
TECHNOLOGY
DEPARTMENT OF ELECTRICAL AND
COMPUTER ENGINEERING**

**DEVELOPMENT OF A LORA-BASED TAMPER MONITORING SYSTEM
FOR UTILITY METERS**

CASE STUDY: UMEME YAKA METERS

MATOVU DERRICK VICTOR

18/U/22517/PSA

Supervisors

**MAIN SUPERVISOR: MR. DAVID MARTIN AMITU
CO-SUPERVISOR: MR. INNOCENT OKETCH**

*Final year project report submitted in partial fulfillment of the Requirement for the award of the degree of
Bachelor of Science in Electrical Engineering of Makerere University*

SEPTEMBER 2022

Approval

This is to certify that the project report under the title "Development of a Lora-based tamper monitoring system for utility meters" has been done under my supervision and is now ready for examination.


Signed: 

Date: ...23/09/2022.....

Mr. David Martin Amitu

Department of Electrical Engineering,

Makerere University.

Signed: 

Date:23, 09, 2022.....

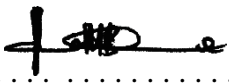
Mr. Innocent Oketch

Department of Electrical Engineering,

Makerere University.

Declaration

I MATOVU DERRICK VICTOR sincerely declare that to the best of my knowledge, the information presented in this project report is an original work resulting from my sole effort and intellect. Except for extracts whose references are stated herein, it has never been published or submitted to this organization or any other institution of training for any academic reward.

Signature.......... Date :23/09/2022.....

Dedication

I dedicate this report to my family and friends who morally, financially, and spiritually supported me throughout the execution of the project.

I also dedicate it to my project partner Nekesa Racheal with whom I shared experiences and combined knowledge to accomplish the project.

Specially, I dedicate this report to the Electrical and Telecommunications Engineering class of 2018-2023 for it generally made my pursuit of the Bachelor's degree worthwhile.

Acknowledgments

I thank the Almighty God for giving me the courage, strength, wisdom, understanding, guidance, and the ability to successfully complete my final year project and report writing. I extend my sincere gratitude to my project supervisors Mr. David Martin Amitu and Mr. Innocent Oketch for their tireless effort in guiding the direction of implementation of this project. I also thank Mr. Hillary Arinda from UMEME for the technical and non-technical support he rendered during the execution of the project. I also specially thank Mr. Sonko and Mr. Mpaddwa Enock for the technical assistance rendered throughout the project execution.

Special gratitude goes to Mr. Mukasa Victor, Ms. Namuli Reginah, and all my family members for motivating me in several ways all through my academic journey.

Lastly, I appreciate the department of Electrical and Computer Engineering staff members for the guidance and knowledge they have equipped me with as it came in handy to see the fruition of the project.

Abstract

The recent rapid rate of load growth has made the electrical crisis a severe issue. Every year, roughly 125,000 new users join the grid, which presents a load control difficulty for the company. Due to the difficulty of monitoring meters, many consumers turn to power theft. The technical creation of a Lora-based system for utility meters is accomplished in the project document. The suggested remedy aims to create a prototype device that can recognize several prepaid meter tampering scenarios, such as magnetic, opening, and displacement, and report them to a centralized system using Lora technology. It is utilizing a 433 MHz E32-433T30D matched Lora pair with a maximum communication distance of up to 8km. The real-time tamper detection and reporting system is intended for use in Yaka prepaid residential meter cases, as UMEME, the energy service provider, has dubbed them. The information is gathered into a web application database that has been created, and the graphic user interface shows the site and technique of meter manipulation. Additionally, power to the consumer is immediately turned off when a tamper is discovered.

List of abbreviations

MCU – Microcontroller Unit

HES – Hall Effect Sensor

LPU- Large Power Users

LDR – Light Detecting Resistor

LoRa – Long Range

I2C – Inter-Integrated Circuit

RTC – Real Time Clock

AMR – Automated Meter Reader

RISC- Reduced Instruction Set Computer

GSM- Global System for Mobile

AVR- Alf and Vegard's

LPWAN- Low Power Wide Area Network

RENU- Research and Education Network for Uganda

IoT- Internet of Things

SF- Spreading Factor

AMI- Advanced Metering Infrastructure

SMS- Short Message Service

LED- Light Emitting Diode

XAMPP- Cross-platform, Apache, MySQL, PHP, And Perl

MySQL- My Structured Query Language

IC- Integrated Circuit

DC- Direct Current

UART- Universal Asynchronous Receiver Transmitter

Contents

List of Figures	ix
List of tables	x
Chapter 1: Introduction	1
1.1 Project background.	2
1.2 Problem statement.....	4
1.3 Justification.....	6
1.4 Project objectives	7
1.4.1 Main Objective.....	7
1.4.2 Specific Objectives.....	7
Chapter 2: Literature review	8
2.1 Lora Technology.....	8
2.1.1 The Lora Architecture.....	8
2.1.2 Why LoRa.....	9
2.1.3 LoRa Technology in Uganda.....	10
2.2 Meter tampering.....	10
2.2.1 Ways of meter tampering.....	11
2.3 Related works.....	12
2.3.1 LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid.....	12
2.3.2 Development of an SMS-Based Prepayment Energy Meter Monitoring System for Consumers and Utility Companies.....	13
2.3.3 Web-based Prepaid Energy Meter with theft control.....	13
2.3.4 IoT-Based Energy Meter Reading, Theft Detection, and Disconnection.....	14
Chapter 3: Methodology	15
3.1 Work package, deliverable, and tools.....	15
3.2 Proposed system architecture	16
3.2.1 Control System.....	17
3.2.2 Communication Layer.....	18
3.3.3 User Interface Layer.....	18
3.4 Steps to accomplish the project.....	18
Test stage.....	19
Chapter 4: Results and Discussion	20
4.1 Circuit design	20
4.1.1 Schematic design.....	20
4.2 Construction of the tamper-proof and monitoring device.....	20
4.2.1 Power supply.....	21

4.2.2 The Control System.....	22
4.2.3 Communication layer.....	27
4.2.4 The relaying system.....	29
4.3 Web interface.....	30
4.3.1 Home page.....	30
4.3.2 Records page.....	30
4.3.3 Users page.....	31
4.4 Tamper scenarios.....	31
4.5 Cost-benefit analysis.....	33
4.5.1 Objective.....	33
4.5.2 Costs.....	34
4.5.3 Benefits.....	34
4.5.4 Assessment and Comparative Cost-Benefit Analysis.....	35
Chapter 5: Conclusion, Challenges, and Recommendations.	36
5.1 Conclusion.....	36
5.2 Challenges.....	36
5.3 Recommendation.....	37
References	38
Appendix	40

List of Figures

Figure 1: Single phase prepaid meters retrieved.....	4
Figure 2: Three phase meters faulty due to tampering	4
Figure 3: Five-year loss target set by ERA for 2020 to 2025	5
Figure 4: Lora Architecture	9
Figure 5: Comparison of LoRa technology and other technologies	9
Figure 6: Proposed System Architecture	16
Figure 7:Steps to accomplish the project	18
Figure 8:System schematic design.....	20
Figure 9: Back view of the device prototype.	21
Figure 10: Device prototype	21
Figure 11: 5V power supply circuit diagram	21
Figure 12: Power supply section of the device	22
Figure 13: Illustration of the Atmega microcontroller Unit.....	23
Figure 14: Pull-up resistor connected to pin 1	24
Figure 15: Schematic diagram of pull-up resistor circuit connected to MCU	24
Figure 16: Schematic diagram of Oscillator connection to MCU	25
Figure 17: Crystal oscillator connected to the MCU	25
Figure 18: LDR sensor and potentiometer on device	26
Figure 19: Schematic diagram showing the connection of the LDR sensor.....	26
Figure 20: Hall effect sensor.....	26
Figure 21: Schematic diagram of HES connection to MCU.....	26
Figure 22: Tilt sensor connection to MCU	27
Figure 23: Tilt Sensor	27
Figure 24: E32 433T30D LoRa module	28
Figure 25: LoRa module pin configuration	28
Figure 26: LoRa module plugged into a computer on the Utility side	28
Figure 27: LoRa module on the device (Yaka meter side)	28
Figure 28: Liquid Crystal Display	29
Figure 29: Relaying system on the device	29
Figure 30:Schematic diagram of the relaying system.....	29
Figure 31: Web- interface login page	30
Figure 32: Web-interface home page.....	30
Figure 33: Web interface records page	31
Figure 34: Home page during a tamper due to magnetic interference.....	32
Figure 35:Records page during a tamper due to magnetic interference	32
Figure 36:Records page during a tamper due to meter-tilt	32
Figure 37: Home page during a tamper due to meter-tilt.....	32
Figure 38: Records page for a tamper due to light exposure.	33
Figure 39: Home page for a tamper due to light exposure	33

List of tables

Table 1: Methodology15
Table 2: Methodology16
Table 3: Costs incurred34

Chapter 1: Introduction

Energy theft is a serious worry for government organizations (Public Utility Boards) all over the world as a result of the rising cost of electricity. The hacker may want to extract data from utility metering software or change the internal settings. Changing the time to trick the system is a common component of these techniques. [1] Because electricity distribution firms may charge various rates based on the time of day, peak demand, load, etc., the real-time clock (RTC) is needed to provide precise time information. To trick the system into charging differently, one can tamper with the clock or alter the time, such as changing PM to AM so that the metering firmware charges less because nonpeak load tariff is in effect at that time. The RTC typically uses an external crystal oscillator running at 32.768 kHz, however a hacker might alter the RTC crystal to make it run slower and countless cycles, producing errors in measurement and billing. [2] By installing electronic energy meters which, unlike electromechanical meters, can detect tamper circumstances and guarantee appropriate billing, a significant percentage of these revenue losses can be recovered. The extent of the loss in such meter settings can, however, also increase if tamper awareness is delayed. Utility companies would gain from immediately recognizing any remote tampering occurrences as these meters become networked with the adoption of improved metering technology like AMR or smart grid in the developed countries. Utility smart grid metering, however, has not yet been assumed. [2]

1.1 Project background.

The Yaka smart power meters, as we know them now, were introduced thanks to a tender that was issued in 2010 by Uganda's largest electricity distribution company, UMEME, for a comprehensive business solution for pre-payment metering.

As a business, UMEME hopes to solve issues including slow payment of electricity bills, the existing high cost of billing, and the need to make it simpler to monitor customer meters and energy usage. It was also hoped that this new approach would lessen the fraud that has primarily been perpetrated by unlicensed electrical workers who prey on unwary customers by demanding money while purporting to disconnect and reconnect them.

The company converted 32,000 clients within the first half of 2013.[3]

A close examination of how Smart Meters work reveals a significant reliance on ICT infrastructure. A smart meter is often an electronic device that monitors electric energy consumption at intervals of an hour or less and transmits that data back to the utility at least once per day for monitoring and billing reasons. To promote better and more sustainable use of the limited supply of electrical energy available, governments all over the world are supporting smarter metering systems. The manufacture of smart meters has suddenly increased as a result of the utility companies being encouraged to follow this course in response to government backing. [4]

However, it has been shown that these smart meters are weak and open to manipulation by trespassers with malicious intent. They may be vulnerable to assaults if there are inadequate security safeguards in place. Hackers are now able to commit billing fraud and turn off the electricity at will. By gaining access to their memory chips, one can perform some reprogramming and use any defective code therein to tamper with meter readings, transfer readings to other customers, and install network worms that might potentially cause a blackout to spread throughout entire neighborhoods. This is simple to accomplish if one gains access of the meter box since they can change its unique ID to imitate the ID of another client or use it to launch network attacks.

One of the gaps in IT security that one might utilize to start any attack is physical access to the hardware. It is also important that consumers may easily access these meters. The encryption keys used to scramble all the information that the meter shares with hosts situated higher up in the power

distribution network can be found by gaining access to the onboard software (firmware) of these meters. The hosts can then be duped by sending them bogus data. These meters may also have had issues with shared IDs, weak anti-tampering measures, and factory default passwords.[5]

1.2 Problem statement.

Energy losses are due to both technical and non-technical causes. The technical is due to physical parameters of the components for example resistance of Transmission lines and transformer winding resistance and non-technical causes are mainly due to power theft.

In the six months to June 2020, UMEME registered an increase in energy losses to 17.4 percent compared to 16.9 percent for the same period in 2019 and this increase in losses was attributed to the reduction in the number of anti-power theft drives during the COVID-19-induced lockdown as per the UMEME report. These energy losses cause heavy revenue losses to the utility [6].

For February and March 2022, some data was also sampled for faulty meters that were retrieved by UMEME between February & March 2022. After the retrieved meters were stress tested, it was found that of 1027 single-phase prepaid meters that were retrieved, 316 of them were faulty due to tampering resulting in 30.76%. 30 three-phase meters were retrieved and 3 of them were faulty due to tampering resulting in 10% as illustrated below.

Single phase prepaid meters retrieved

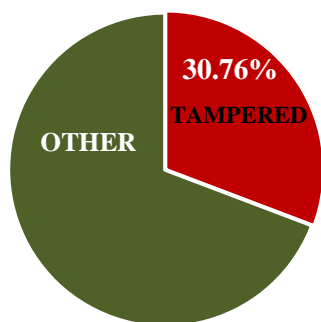


Figure 1: Single phase prepaid meters retrieved

Retrieved three phasemeters

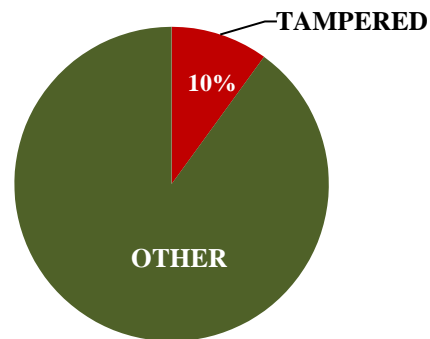


Figure 2: Three phase meters faulty due to tampering

As reported from an interview with the Principle metering Engineer, Research and development of UMEME, he noted that the energy losses as of the end of March 2022 were at 17.6%.

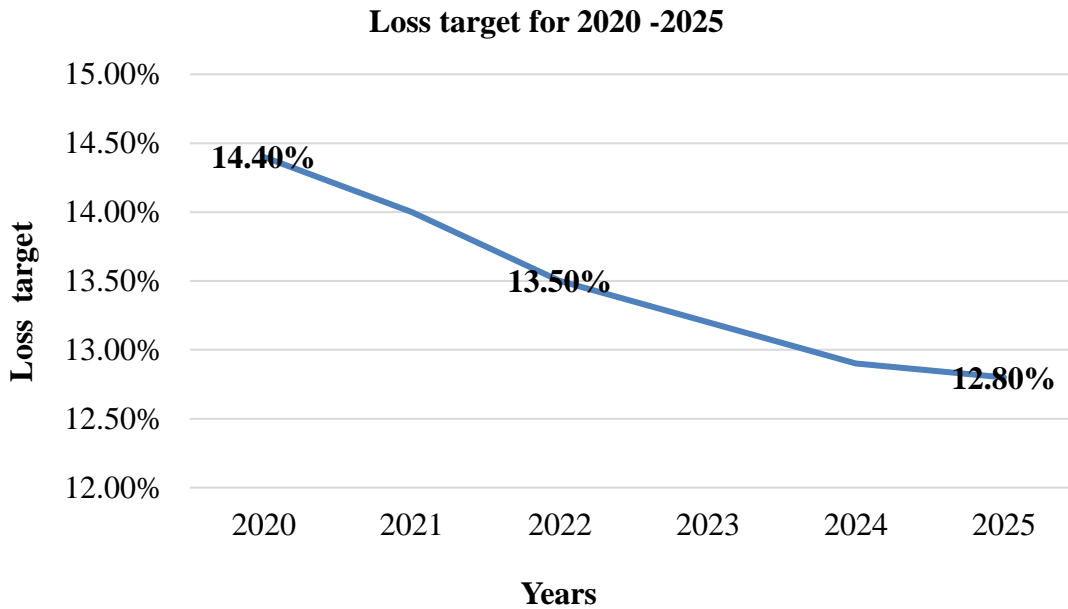


Figure 3: Five-year loss target set by ERA for 2020 to 2025

As compared to the Electricity Regulatory Authority set loss target which is 13.5% by end of 2022 as per the graph above, this shows a large gap to the set target. There is therefore an urgent need for more measures to reduce energy losses, hence the need for ways of making meter tampering undesirable to the end customer and therefore the need for a low-cost real-time monitoring system to report these tampers.

1.3 Justification.

Whereas the majority of customers are households, industrial and commercial customers (0.5 percent of the total customer database) account for over 70 percent of UMEME's sales and revenue. Tackling losses from this customer segment could drive significant revenue increases, which in turn can help UMEME connect more households [UMEME, 2017]. Particularly on the demand side, for example, communication infrastructure is incomplete, a low-power wide-area network (LPWAN) is a new solution in the context of a wireless breakthrough in the communication sector. Two representative technologies of LPWAN are the narrow-band Internet of Things (NB- IoT) and Long Range (LoRa) technology the power distribution level, and even less communication infrastructure is available for utilization systems at lower voltage levels. [7] UMEME had proposed Yaka meters with GSM connectivity to monitor and report meter tamper and vandalism activity. However, it was realized to be a non-cost-effective solution since it wasn't feasible to sustain connectivity as some prepaid meters are running dormant with no subscription over a long time. [8]To overcome this barrier. The NB-IoT is inherited from cellular communication and seamlessly works on the existing global system for mobile (GSM) and long-term evolution (LTE)networks in licensed frequency bands. In contrast, LoRa technology operates in the unlicensed frequency band, so that end users are free to build up LoRa gateways that are similar to house-owned WIFI routers. Therefore, LoRa technology is perfect for outlying regions without cellular network coverage, or for establishing private networks with specific requirements for quality andsecurity. [9]

This is a cost-effective solution as Lora will not require communication subscription costs as the case with the pre-tested GSM.

1.4 Project objectives

1.4.1 Main Objective.

To design and construct a regional centralized Yaka LoRa-based tamper monitoring system for Yaka Utility meters.

1.4.2 Specific Objectives.

- ❖ To design the tamper-proof prototype.
- ❖ To construct the tamper-proof and monitoring device.
- ❖ To design and develop the service provider Web interface.
- ❖ Integration of the device and developed interface.

Chapter 2: Literature review

2.1 Lora Technology.

IoT is gaining high popularity in today's world. Embedded systems have become a major part of our lives. People can control, monitor, and do a lot more from a remote distance. This is done by connecting various objects and reducing physical distance. IoT is the connectivity of various objects with network connectivity.

The LoRa technology is a long-range low-power technology. LoRa employs the chirp spread spectrum modulation technique. The chirp spread spectrum has a low transmission power requirement. Chirp is a signal whose frequency increases or decreases over time. Thus, a chirp signal can be up-chirp and down-chip. The chirp spread spectrum also provides immunity to multipath and fading.

The LoRa technology addresses the needs of a battery-operated embedded device. A comparison of Lora and other existing technologies entails that they are well-established networks traditionally built for high data throughput and so these do not optimize the power consumption.

These technologies consume too much power and are not a good option when a small amount of data is to be transmitted less frequently. [10]

2.1.1 The Lora Architecture.

LoRa defines the physical link that provides a long-range communication link while LoRa WAN defines the communication protocol and the network architecture.

LoRa WAN is based on a star topology. This topology decreases the power consumption and battery life requirement to a great extent in comparison with the conventional mesh network.

The LoRa network consists of four basic elements which include a LoRa node or End Points, a gateway, a network Server, and an application Server as illustrated below. [10]

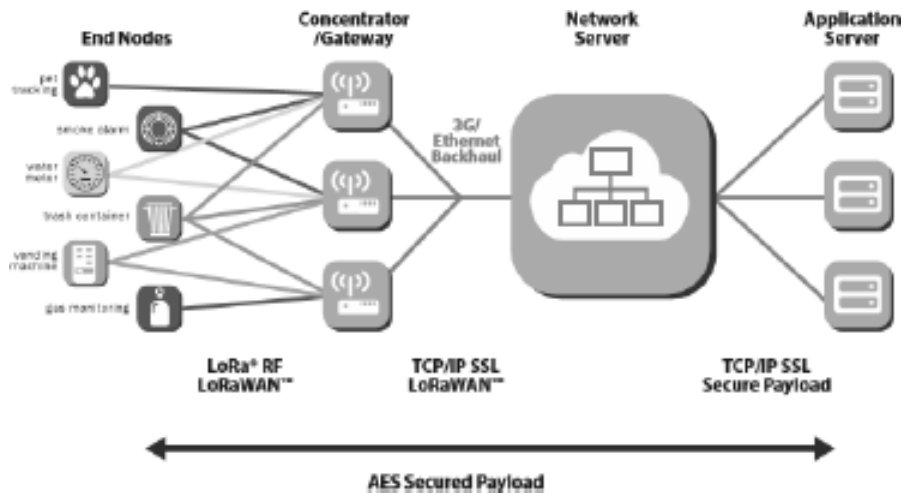


Figure 4: Lora Architecture

2.1.2 Why LoRa

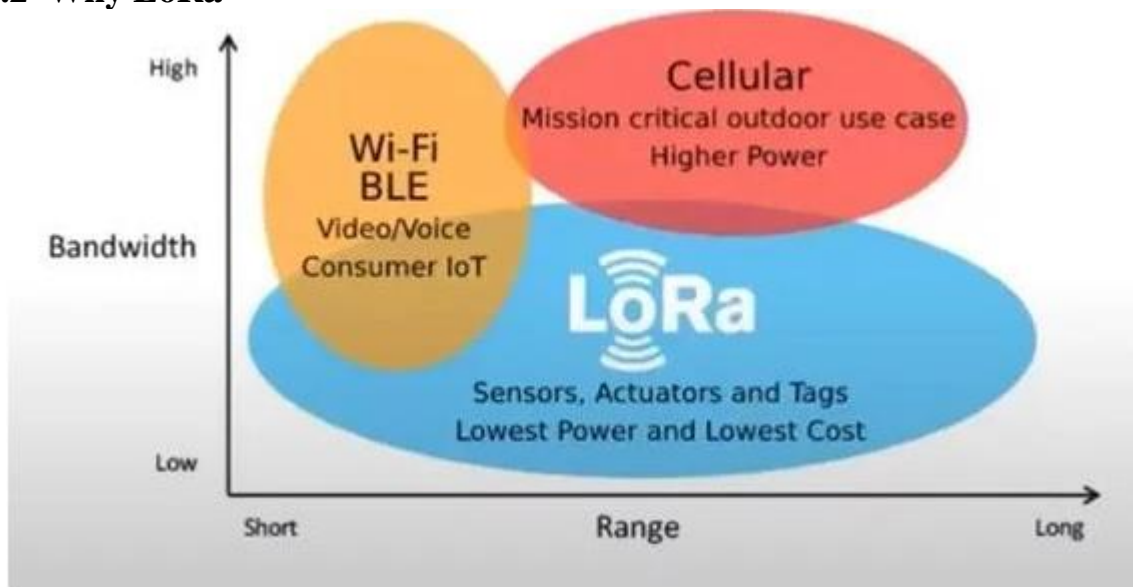


Figure 5: Comparison of LoRa technology and other technologies

LoRa compares with other technologies in several ways as illustrated in the graph above. Cellular data transmission (i.e., 4G and 5G) has no range restrictions, providing high bandwidth communications over large distances, they have extremely high-power requirements.

Wi-Fi offers high bandwidth wireless communication but is limited to very short ranges, limiting its use in industrial IoT applications.

LoRa offers low bandwidth communication over short and long ranges with low power

requirements, which makes it well-suited to IoT applications where, generally, battery-powered devices must be able to relay small amounts of data over large distances. This makes the application of LoRa suitable for this project. [11]

2.1.3 LoRa Technology in Uganda.

Several gateways are being set up with Research and Education Network for Uganda (RENU) as one of the organizations fronting the deployment and setting up of LoRa architecture. For example, WIMEA-ICT pushed RENU to deploy the first LoRa gateway in Uganda, and RENU pledged to support the AdEMNEA project.

Clouds have been set up to store the information that will be processed to ensure the project work goes on well. RENU will provide linkages to similar projects for benchmarking as they are supporting some IoT-based projects and providing connectivity for them.

This makes the deployment of projects based on LoRa technology feasible since the technology is already being deployed in the country. [12]

2.2 Meter tampering.

Several configurations are used in measuring energy consumption one is by measuring the voltage between line in and neutral in, and the current sent across a shunt connected between line in and line out. The sum of the voltage-current product is used to calculate the active power. This is equivalent to the r-miss current and r-miss voltage, multiplied by the cosine of the angle between the voltage and current. [13]

With the numerous configurations used in the billing process based on the active power measurement, utility meters are still tampered with making the power consumption non-proportional to the amount billed.

2.2.1 Ways of meter tampering

2.2.1.1 Internal tampers

Phase and neutral interchange

Phase and neutral of the meter are interchanged then reverse current flows through the meter, the meter may read the reverse energy which takes off the kWh reading from total reading

Partially or Fully Earth Condition

In partial earth conditions, one of the loads is connected to the earth and the other is returned to the neutral of the meter. In fully earth condition the total load is earthed. In both cases the current in the neutral wire I_N is less than that in the Phase wire (I_P)

Missing Neutral

The missing neutral tampering condition occurs when the neutral is disconnected from the meter. In this condition, there is no voltage input and thus no output would be generated by the power supply. However, when the load is applied, there would be a valid input signal on the current circuit, hence power will be consumed. Since the voltage on Neutral is zero, Power $P = V \times I = 0$. This condition is also known as single-wire operation. [13]

Bypassing Meter

There are many ways to bypass an energy meter. The most common way is by putting a jumper in the meter terminal such that the connection is bypassed and the energy consumption is not registered.

Double Feeding the Meter

"Double Feeding" to bypass the meter where additional feeding is connected directly to the line so that the consumption for additional feeding is not registered. Here one would have legal service but the meter will not register the consumption for bypass load. Usually, the additional feeding is done to connect an appliance that requires more electricity load (like the Air Conditioner). The other loads like lights still go through legal connection so that the electric company will not get suspicious.

Magnetic Interference

Meters use magnetic material in voltage and current measurement circuits and thus are affected by abnormal external magnetic influences, that in turn affect the proper functioning of the meter. [13]

2.2.1.2 External Tamperers

External tampering may include breaking the meter case, chemical injection, or even burning the meter. All of these result in changing the electrical characteristics of the components thereby recording less or no energy usage. One may want to open the meter case to change the settings or even remove the backup battery so that the meter will reset when the main power goes off. [13]

It was noted that a large number of the tamper methods are internal tamperers and require accessing the internal components of the meter case. This is addressed by the choice of sensors selected for this project specifically the Light Detecting Resistor (LDR) sensor which signals once the internal parts of the meter are exposed to light.

For external tamper methods like magnetic interference and vandalizing the meter, the Hall effect sensor and the tilt sensor are used to detect these kinds of tamperers.

2.3 Related works.

Several works have been done on meter tampering and reporting techniques as discussed below:

2.3.1 LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid.

José Luis Gallardo, Mohamed A. Ahmed, and Nicolás Jara a member of IEEE developed a LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid. This paper proposed an IoT-based architecture for AMI networks, which is a key component for deploying the future smart grid concept. A particular case of LoRa communication technology is considered a promising candidate for deploying the proposed architecture. A simulation scenario of the AMI system was considered for a suburban neighborhood. Several aspects are discussed and evaluated to determine if LoRa technology can be operated under different circumstances. The simulation results were compared considering two different operation scenarios of LoRa networks under various metrics, such as delivery ratio, energy consumption, throughput, collisions, and SF

distribution. The proposed solution was used to deploy the smart meters in an AMI network and enables the network to be dynamic and solve scalability issues in future configurations (adding more smart meters). [14]

The works entirely focused on the simulation of LoRa's performance and hence there was no physical deployment of Lora on the ground. Works didn't include prepaid meter tamper monitoring and reporting as was in their initial objectives.

2.3.2 Development of an SMS-Based Prepayment Energy Meter Monitoring System for Consumers and Utility Companies.

Henry Erialuode Amhenrior developed a meter that uses SMS for communication through the GSM modem. It is made SMS capable by interfacing Atmega2560 with SIM900 Global System for Mobile Communications (GSM) module. The system also has a server consisting of Atmega328P and SIM900 GSM module that enables the utility company to access the meter. The server is interfaced to a PC which is used for management and administrative Platform. Several commands are used for communication with the meter for monitoring and some of the information the communications seek to include, unit balance, unit consumed time of power failure, and time of power restoration. Other monitoring communications capabilities of the meter are checking the tokenrecharge into the meter, credit warning alert, wireless meter disconnection, and connection. SMS communication is a two-way communication and this enables the activities of the meter to be monitored wirelessly. The results obtained show that SMS is very efficient, effective, and successful in achieving the monitoring aspects of this work as proposed distribution companies can communicate with the meter to obtain information through the GSM SMS platform at will [15].

However, GSM SMS-based monitoring requires a continuous subscription for the cellular service and this is one reason why prepaid meters are not on-net for real-time monitoring as the case with LPU meters.

2.3.3 Web-based Prepaid Energy Meter with theft control.

The idea behind this project is to construct the web-based Prepaid Energy Meter with theft control, which eliminates manual meter reading so that the bills can be paid in advance by which the

consumers can plan their electricity bills well in advance. In this system, anyone can recharge their electricity need, like our mobile phones. This proposed system helps the users with real-time information about the peak loads (max energy consumption), energy theft, effective usage of power consumption, billing status, etc. This automated system is built by using an Arduino controller, different sensors & IoT. It continuously reads the energy meter readings and the real-time information is available to the user with IoT. Whenever the energy consumption reaches its limit, the power supply connection will be disconnected and alert information is given to the consumer during minimum balance and null balance. Power theft information is given to both the user and the electricity board; hence it is helpful to identify the exact power theft location. To avoid unnecessary usage of power consumption, load based automatic switch system is used which can build up a home automation system. [16] This energy-saving system replaces the conventional meter reading and offers consumers user-friendly access to energy meters from remote locations.

2.3.4 IoT-Based Energy Meter Reading, Theft Detection, and Disconnection.

Ajeeba A A1, Anna Thomas, and Risa Rasheed proposed a PIC16F877A microcontroller-based design and implementation of an energy meter using the IoT (Internet of Things) concept. The design was to eliminate human involvement in electricity maintenance. The energy meters were to be connected to the PIC microcontroller through an interfacing circuit. The opt coupler sensor was to give an interrupt each time the meter LED flashes to the programmed PIC microcontroller. The readings of the main energy meter and sub-energy meters were compared to identify the theft status. Whenever there was a discrepancy in the two values, a message that theft has occurred was displayed on the LCD as well as on the web page. Consumers could easily track their energy usage so that effective monitoring of power consumption is possible. The hardware interface circuit consisted of a PIC16F877A micro controller, MAX232, LCD, and opt coupler. [17]

However, the system application is unrealistic in our setting as it requires more infrastructure to run web services. The cost of the internet and its limited access makes it impossible still as an ideal solution in the Ugandan setting.

Chapter 3: Methodology

This section discusses in detail the description of the work done, the modeling, and the design of the proposed system.

Quantitative and qualitative research, review of articles, and consultations from UMEME as the main distribution company about the numerous Yaka-meter tampering techniques.

Literature review through textbooks, journals, review articles, reports, and other relevant information from reliable sources about Lora Technology.

The design of the system prototype for a Yaka-meter tamper notification system was based on standalone long-range wireless communication. This device was based on an 8-bit RISC Atmel ATMEGA328P-PU microcontroller interfaced with 8km E32- 433T30D LoRa modules to provide localized communication to the local service provider. The device can detect tampers by sensing meter tilt, magnetic exposure, and light exposure of internal parts. [18]

3.1 Work package, deliverable, and tools

MILESTONE	WORK PACKAGE	DELIVERABLE	TOOLS
Design of the tamper proof prototype.	<ul style="list-style-type: none">• Designing a circuit diagram for the system prototype.• Obtaining a Deeper understanding of Lora technology.	Circuit design	Proteus software
Construct the tamper proof and monitoring device.	To build the tamper proof and monitoring device.	Device Prototype	<ul style="list-style-type: none">• Arduino/Atmel Studio• Circuit board, circuit components.

Table 1: Methodology

MILESTONE	WORK PACKAGE	DELIVERABLE	TOOLS
To design and develop the service provider Web interface.	Back end development. Front end development Integration of the two ends	Web application	XAMPP/MySQL
Integration of the device and developed interface	Linking the matched Lora pair (receiver and transmitter)	Web interface can connect to the prototype	Putty
Report Writing	Writing a detailed technical report	Project Report	Paper, Computer

Table 2: Methodology

3.2 Proposed system architecture

The figure depicts the proposed functional block diagram of the Lora-based tamper monitoring system for Yaka utility meters. This shows how the various components are interlinked.

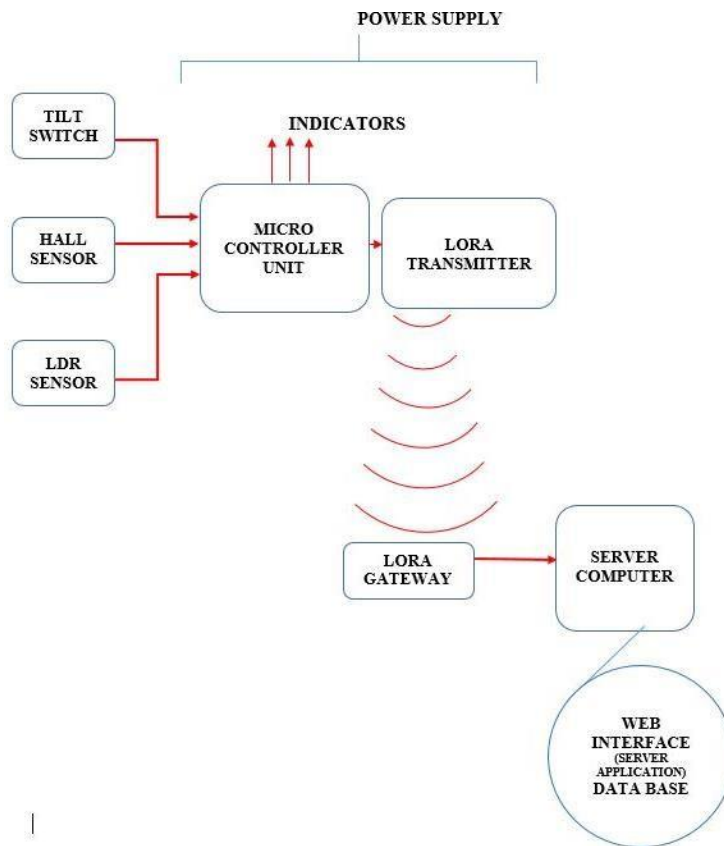


Figure 6: Proposed System Architecture

3.2.1 Control System

Hall sensor

This sensor mainly will detect Magnetic Interference. Hall sensors devices are activated by an external magnetic field. Since Meters use magnetic material in voltage and current measurement circuits and thus are affected by abnormal external magnetic influences that in turn affect the proper functioning of the meter, and also the output signal from a Hall Effect sensor is the function of magnetic field density around the device. Hence when the magnetic flux density around the sensor exceeds a certain pre-set threshold, the sensor detects it and generates an output voltage. [19]

Tilt sensor

The tilt sensor will help in detecting any change in the position of the meter. One may want to open the meter case to change the settings or even remove the backup battery so that the meter will reset when the main power goes off. A tilt sensor is an instrument that is used for measuring the tilt in multiple axes of a reference plane. Tilt sensors measure the tilting position with reference to gravity. The tilt sensor has a metallic ball that is designed to move the two pins of the instrument from the 'on' to the 'off' position, and vice versa, if the sensor reaches a pre-determined angle. [20]

LDR sensor

An LDR is a component that has a (variable) resistance that changes with the light intensity that falls upon it. This will be used as a light sensing device to detect exposure of the internal components to light. [21]

Microcontroller unit

A microcontroller (sometimes called an MCU or Microcontroller Unit) is a single Integrated Circuit (IC) that is typically used for a specific application and designed to implement certain tasks. This chip will intake instructions from the sensors and operate the respective indicator then trigger the Lora transmitter to operate. [22]

3.2.2 Communication Layer.

Lora transmitter and receiver.

This will send and receive the tamper signals from the meter to the receiver at the central monitoring location respectively.

3.3.3 User Interface Layer.

Server PC

This will contain the graphic user interface with the Web application where the operator will be notified about the tamper method and location of the tamper.

Application Layer

The application layer is in charge of all the tasks related to data processing, display, and disposition of data to the utilities for the different applications that are intended. For utility, business-side tasks include business model applications, graphs, flowcharts, and big data analysis of meter tampering cases and the specific tampering method for the perceived data from the perception layer.

Under this domain, the following applications may coexist user dashboard and meter tampering data including the location of any meter tampering occurrence and the method of tamper displayed.

3.4 Steps to accomplish the project.

The steps we used to accomplish the project are ideation, design, build, integration and test as illustrated in the block diagram below.

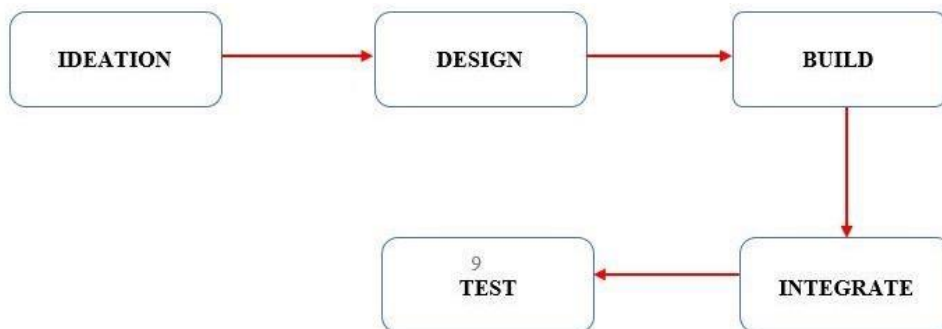


Figure 7:Steps to accomplish the project

The ideation stage

Is the initial stage and involves the formation of the idea or the concept.

The design stage

At this stage, we shall produce a sketch showing the schematic drawing and the simulation shall be developed. This information will be used to research the equipment needed and the materials to be used.

The build stage

This is the project execution phase and the design is delivered. The prototype hardware shall be developed with several components brought together as per the design.

The integration stage

This shall involve coordinating all the resources that are the prototype and the web application and also managing any conflicts between the different aspects of the project. We shall focus on the requirements for adding this external circuit to the already existing Yaka meter.

Test stage

Unit testing, integration testing, system testing, and acceptance testing shall be executed and results shall be analyzed. This shall involve a test for both the hardware and the software.

Chapter 4: Results and Discussion

4.1 Circuit design

The circuit design was designed in proteus software as per the proposed system architecture and contained several sections including the power supply, control system, communication system, and relaying circuit.

4.1.1 Schematic design.

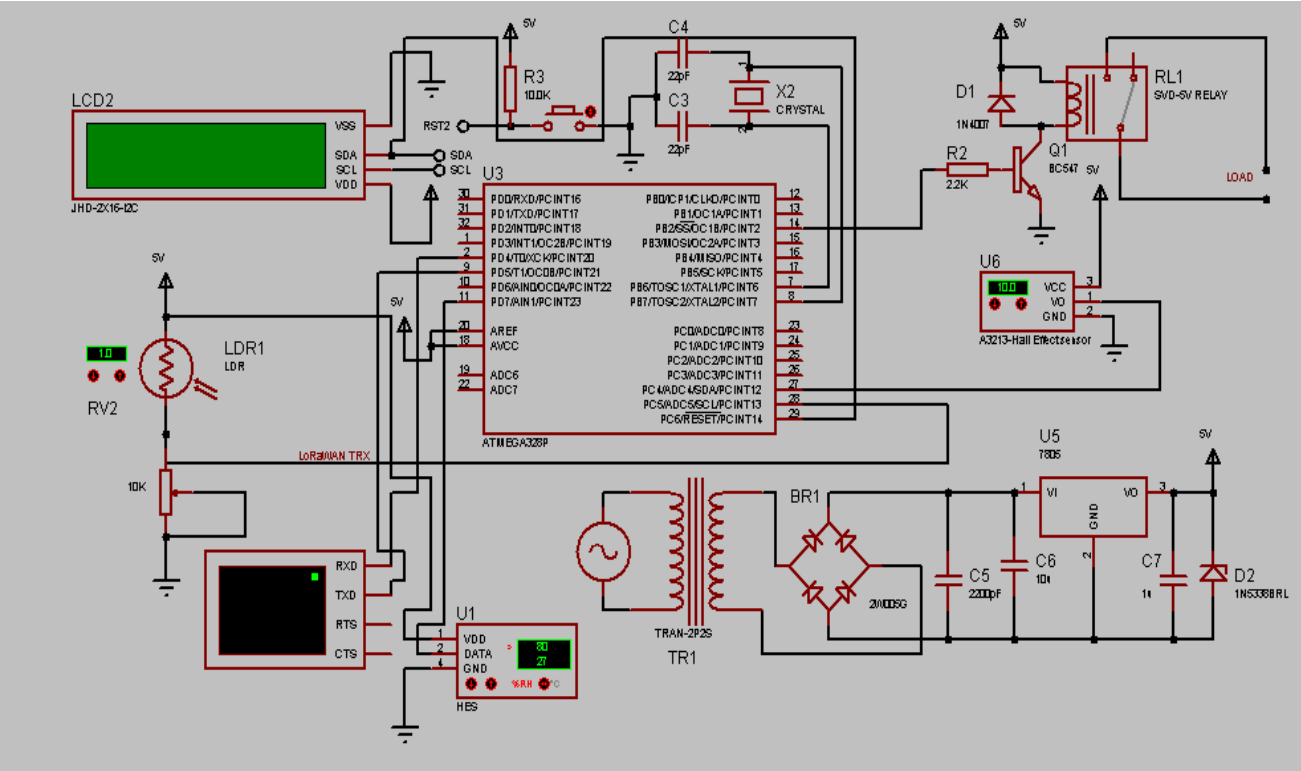


Figure 8: System schematic design

4.2 Construction of the tamper-proof and monitoring device.

The circuit components were soldered together on a Vero board. To make the necessary connections as per the schematic design, current flow paths were created and the electronic components were fitted onto the board by soldering.

Some of the equipment used included a soldering gun and iron, Vero board, resistors, capacitors, relay module, diodes, BJTs, LED, LCD, LoRa module, jumper wires, and multimeter among others.

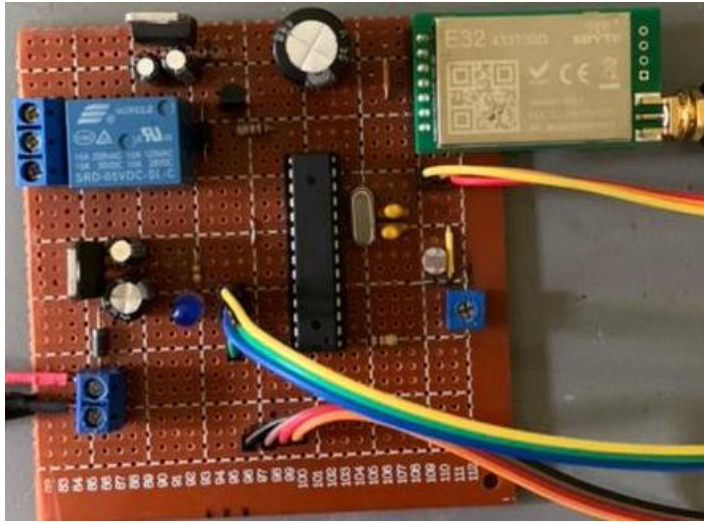


Figure 10: Device prototype

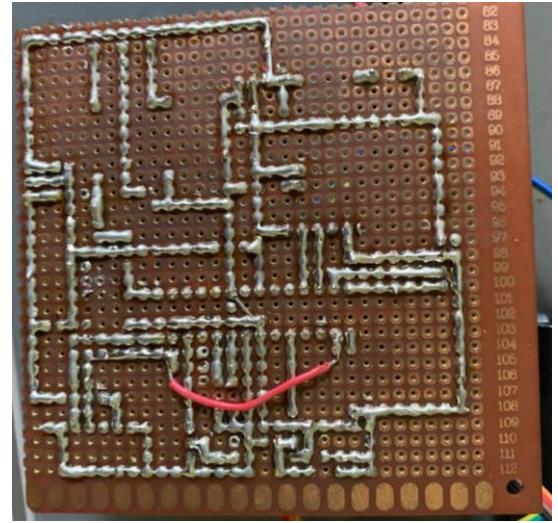


Figure 9: Back view of the device prototype.

4.2.1 Power supply.

The circuit was powered by a 240VAC supply at the primary side of the step-down transformer which steps the voltage down to 12VAC. The voltage was then rectified using a full bridge rectifier circuit to output a 12VDC power supply which powered up the system components.

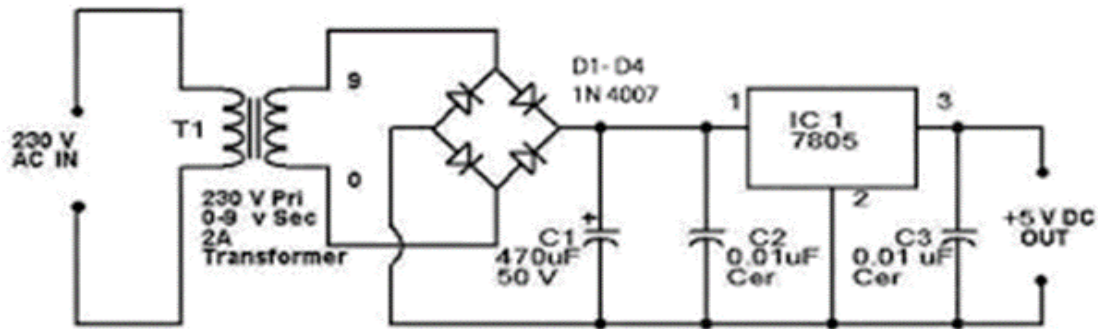


Figure 11: 5V power supply circuit diagram

The 12VDC power supply was then stepped down using a potential divider circuit to 5V which is regulated using a voltage regulation circuit. This circuit consists of the T0-220 package, 7805 1.5A, 5V DC voltage regulator chip, a 10 microfarad reservoir capacitor at the input side, and a 1 micro farad decoupling capacitor at the output side of the regulator. A Schottky diode was also connected across the output voltage.

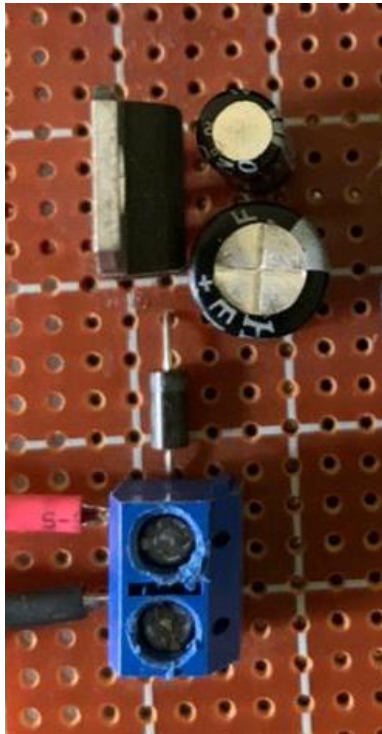


Figure 12: Power supply section of the device

For this system, the voltage regulation circuit was replicated and a second circuit was connected to power up the LoRa transmitter since the LoRa module has a higher power consumption. At the output, a 25V 2200 microfarad capacitor is connected to store charge and is a voltage source to the LoRa transmitter module. This is done due to the power consumption rate of the LoRa transmitter that would cause excessive heating up of the voltage regulator if the output was directly connected.

4.2.2 The Control System.

At the center of the control system is a microcontroller unit. A microcontroller is a computer on a single chip. Therefore, it consists of the main parts of a computer that is the Central Processing Unit, storage (memory), Input/ Output pins, power supply, clock, and an Analogue Digital Convertor (ADC).

An n-DIP (28- dual inline package) chip that is the Atmega 328 was used. ATmega328P is a high-performance yet low power consumption 8-bit AVR microcontroller that's able to achieve the most single clock cycle execution of 131 powerful due to its advanced RISC architecture.

Below are some of the chip's important specifications.

- 8-Bit AVR Microcontroller

- Modified Harvard RISC Architecture
- Storage
- 32KB Flash Memory
- 1KB EEPROM
- 2KB SRAM
- Two 8-bit Timer/Counters
- One 16-bit Timer/Counter
- Six 10-Bit ADC Channels in 28-pin DIP
- USART, SPI and I2C Interfaces
- Watchdog Timer, Pin Change Interrupt, and Wake-up
- Power-on Reset, Internal and External Interrupts
- Operating Voltage: 1.8V to 5.5V for 0 – 4MHz, 2.7V to 5.5V for 0 – 10MHz and 4.5V to 5.5V for 0 – 20MHz speed grades.
- Active Mode Power Consumption of 0.2mA at 1.8V and 1MHz
- Power Down Mode Consumption of 0.1µA at 1.8V and 1MHz

An illustration of the chip;

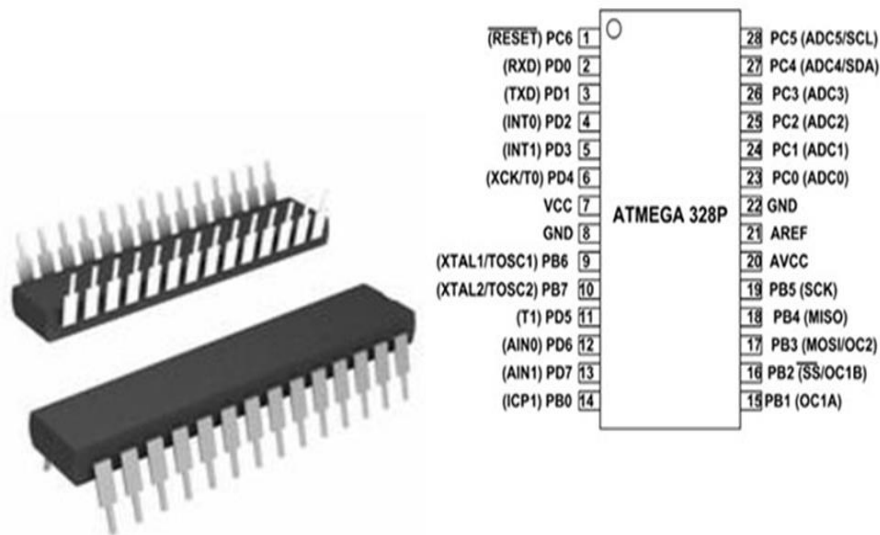


Figure 13: Illustration of the Atmega microcontroller Unit.

4.2.2.1 Programming the microcontroller.

The microcontroller unit was inserted into a programming board and programmed using Arduino software. Several steps were followed;

4.2.2.2 A detailed explanation of the pins used.

Pin 1 is a reset pin. The AVR chip is active low on reset and therefore must be kept high to avoid unwanted system resets. A pull-up resistor is recommended of not less than 10k ohm to disable reset. It was noted that connecting the reset pin directly to VCC could damage the chip.

The schematic diagram is shown below;

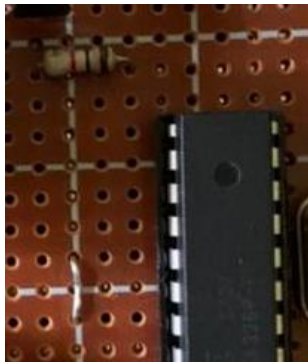


Figure 14: Pull-up resistor connected to pin 1

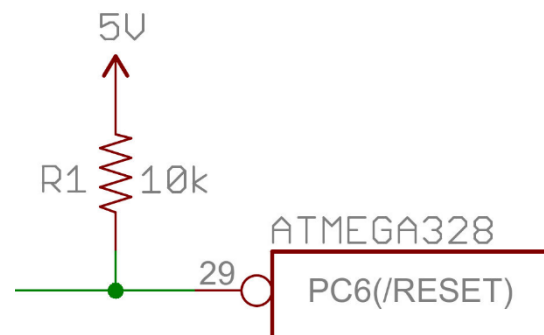


Figure 15: Schematic diagram of pull-up resistor circuit connected to MCU

In case of a manual reset, an electronic switch is applied that is connected to the ground which turns the chip active low when pressed.

4.2.2.3 The clock.

The Atmega 328 has an inbuilt clock that is tuned to 8MHz. This AVR chip can be run to higher speeds up to 20MHz and where faster performance is desired, an external clock source can be used. For this system, an external oscillator was connected to pins 9 and 10 labeled as XTAL1 and XTAL2 from which the chip was sourcing an external clock.

The 16MHz crystal oscillator required two ceramic capacitors of similar capacitance that is 22pF as recommended from the device datasheet to operate. These were connected in parallel and then grounded as shown in the schematic.

Oscillator hookup;

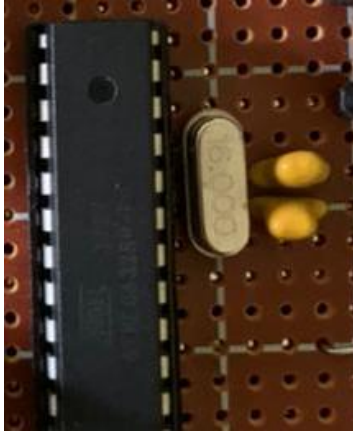


Figure 17: Crystal oscillator connected to the MCU

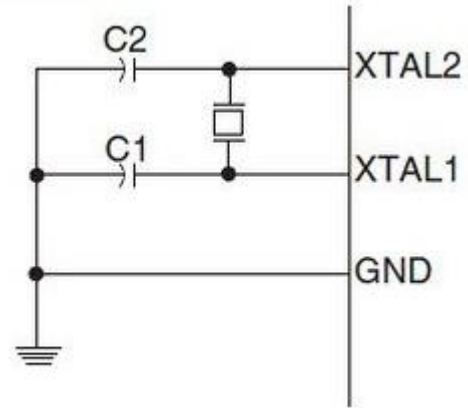


Figure 16: Schematic diagram of Oscillator connection to MCU

4.2.2.4 Light Detecting Resistor (LDR) sensor.

This is a variable resistor for which the resistance value changes based on the light intensity. Its resistance is directly proportional to darkness and inversely proportional to light therefore it conducts or has a very low resistance once the light intensity is high.

It was connected using a potential divider circuit in which a potentiometer was set to a given voltage across a resistor R1 and the voltage across the LDR sensor (R2) is connected as an input to the microcontroller unit.

As the resistance R2 of the LDR varies in response to the light intensity, a given voltage is output.

From voltage division,

$$V_o = \frac{R_2}{R_1 + R_2} V_{cc}$$

When R1 is much greater than R2 in high light intensity conditions, Vout tends towards 0V and when R2 is much greater than R1 in low light intensity conditions or darkness, the Vout tends towards Vin. The LDR sensor output is connected to pin 5 which is pin 3 of port D (external interrupt source 1) of the microcontroller

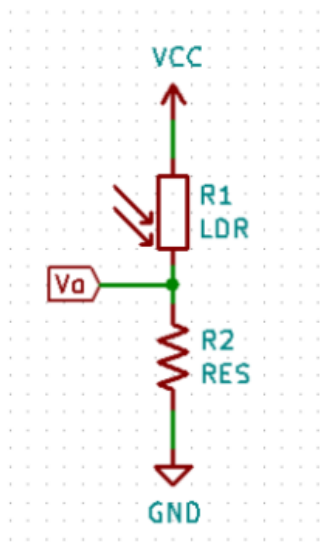


Figure 19: Schematic diagram showing the connection of the LDR sensor

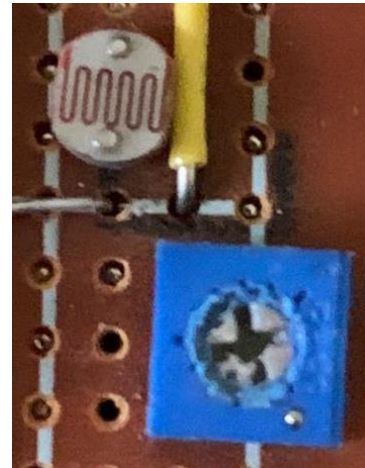


Figure 18: LDR sensor and potentiometer on device

Using the potentiometer, a threshold can easily be set regarding the environment in which the system has been deployed.

4.2.2.5 Hall Effect Sensor.

This works on the principle of the hall effect where there is the production of a voltage difference (the Hall voltage) across an electrical conductor, transverse to an electric current in the conductor, and an applied magnetic field perpendicular to the current. It offers an analog input.

In this system, this sensor was used to detect magnetic interference in the vicinity of the circuit. It is connected to pin of the microcontroller and once the magnetic field is detected, a signal is sent to the microcontroller unit with triggers the relay cutting off power from the customer. A tamper notification is also sent to the Web interface.

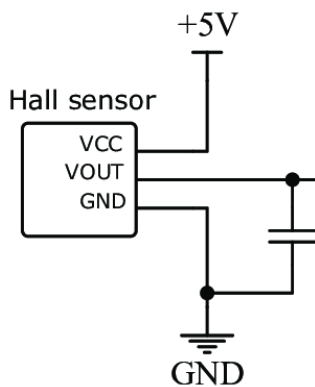


Figure 21: Schematic diagram of HES connection to MCU

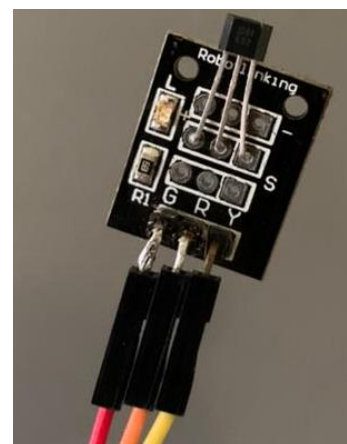


Figure 20: Hall effect sensor

4.2.2.6 The tilt sensor.

A tilt sensor is an instrument that is used for measuring the tilt in multiple axes of a reference plane. Tilt sensors measure the tilting position with reference to gravity. The tilt sensor has a metallic ball that is designed to move the two pins of the instrument from the 'on' to the 'off' position, and vice versa, if the sensor reaches a pre-determined angle.

It is used to detect any change in the position of the meter for example in cases where customers relocate and carry their meters along among other scenarios.

The tilt sensor was connected to the microcontroller unit at pin ... and offers an input signal. Once the system (meter) has been tilted beyond the threshold, a signal is sent to the web interface but unlike the response to tampers from the LDR and HES, this does not trigger the relaying system to cut off supply from the customer. This was due to the numerous environmental factors that could cause the meter to tilt other than meter tampering therefore room for investigation exists and this reduces the undesired cutting off of supply from customers due to false signals.



Figure 23: Tilt Sensor

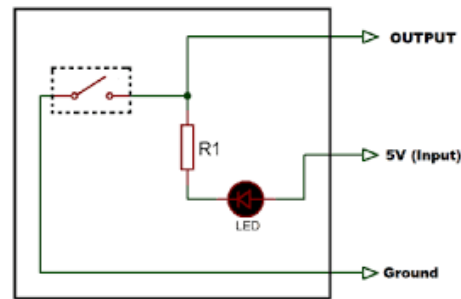


Figure 22: Tilt sensor connection to MCU

4.2.3 Communication layer

This is made up of a matched pair of 433Hz, E32- 433T30D, 8km Lora modules interfaced with the microcontroller unit to offer localized communication to the local service provider. A LoRa transmitter exists as part of the device in the customer meter and a receiver node is a gateway inserted into the computer on which the web interface is locally hosted.



Figure 24: E32 433T30D LoRa module

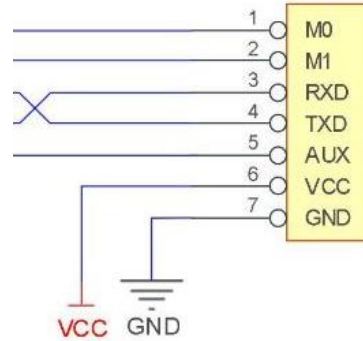


Figure 25: LoRa module pin configuration

The module was powered using 5V DC source pins 6 and 7 for VCC and Ground respectively.

Pin 1 and 2 were connected and grounded to enable transmission mode since the module transmits when M0 and M1 are active low.

Pin 3 and pin 4 are the receiver and transmitter pins respectively of the module and were connected to pin 14 and pin 2 respectively of the microcontroller unit.

The baud rate for the communication was configured to 9600 in the code running on the microcontroller unit.

The LoRa module communicates with the microcontroller unit using serial communication (UART). Serial communication is the transfer of data bit by bit over a single line in every direction.

The Universal Asynchronous Receiver Transmitter provides the computer with the interface necessary for communication with modems and other serial devices.

At the utility side, a receiver module that is the gateway for this setup is plugged into a web local host computer.



Figure 27: LoRa module on the device (Yaka meter side)

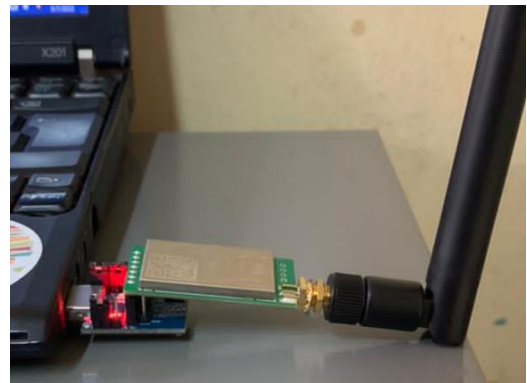


Figure 26: LoRa module plugged into a computer on the Utility side

The Liquid Crystal Display

This was used to aid in the programming and configuration of the device. The LCD communicates with the microcontroller using the I2C communication protocol. The LCD was powered using a 5V supply and connected to pins 27(SDA) and 28(SCL) of the microcontroller. It was then programmed using a programming board to show the output status of the microcontroller unit as per the program running.



Figure 28: Liquid Crystal Display

4.2.4 The relaying system

The supply cables from the meter are meant to be passed through the relay system before termination at the customer's premises. Once a tamper is detected, the relay is triggered to cut off supply from the customer. The triggering signal is forwarded from the microcontroller unit.

The relay is connected to pin 15 of the microcontroller unit.

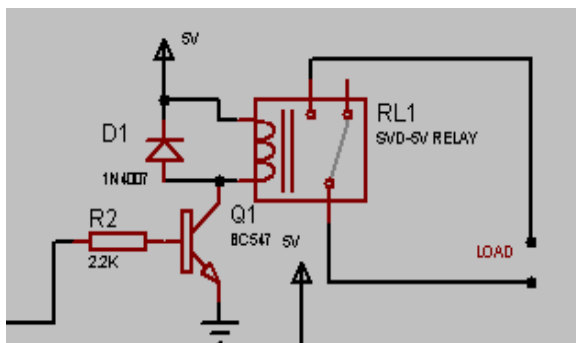


Figure 30: Schematic diagram of the relaying system



Figure 29: Relaying system on the device

4.3 Web interface.

The web interface was developed using several tools like python, XAMPP, and MySQL as the database and contains a login page. Accounts are created by the monitoring team and login credentials are required before accessing the home page of the web interface.

The interface contains a homepage, records page, graphs page, users page, and notification page.

The system was designed and the appearance on the interface for a single customer “KIMERA” was as follows.

4.3.1 Home page

contains three tiles colored green, red, and blue with green for light exposure, red for tamper due to magnetic field exposure, and blue for tamper due to tilt.

Each tile contains a value that is either a one or a zero and under normal operation (without any tamper occasion), the tiles display active low values. In the case of a tamper, the respective tile value goes active high showing a one on the tile, and a record is stored on the notification page.

4.3.2 Records page

shows a per-second status of the system with or without any tamper case. A timestamp is recorded at each record that is taken. The record shows "0" shows no tamper due to a given method at a given time stamp while a "1" shows tamper.

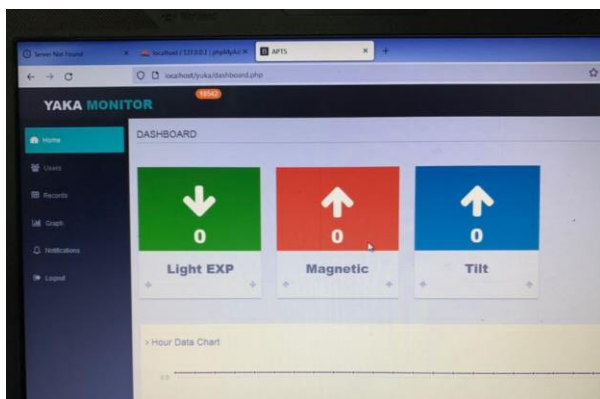


Figure 32: Web-interface home page

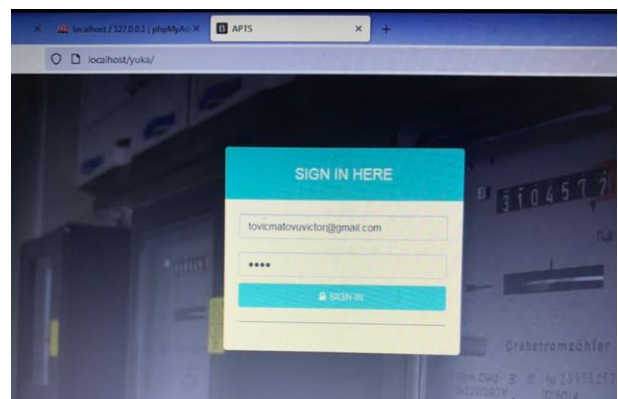


Figure 31: Web- interface login page

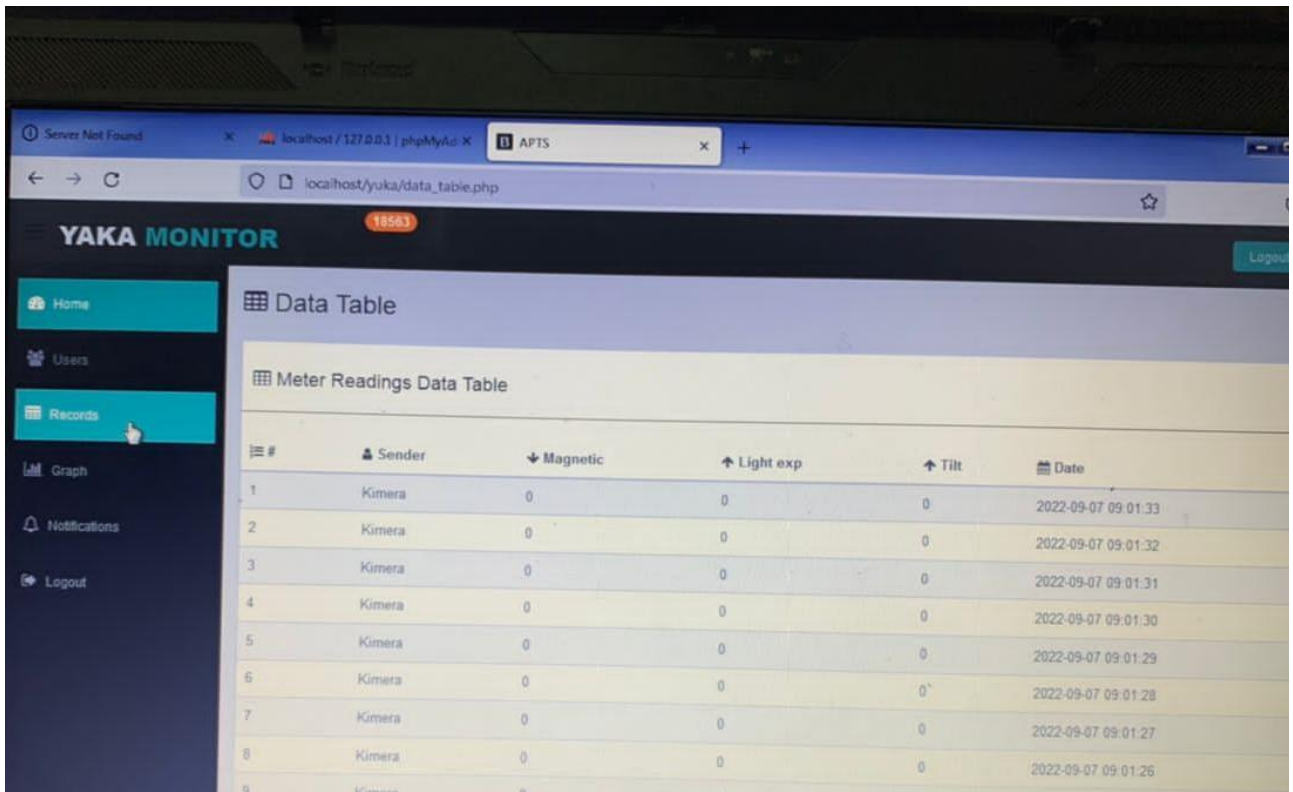


Figure 33: Web interface records page

4.3.3 Users page

shows the details of registered users whose credentials can be used to log onto the web interface system.

4.4 Tamper scenarios

A scenario for tamper due to magnetic interference is demonstrated below. Here, a magnet was placed in the vicinity of the system and was detected by the hall effect sensor.

The relay system was immediately triggered and a notification was forwarded to the web interface via Lora.

At the web interface, a one was observed on the tile for the tamper due to the magnetic interface, and on the records page, the value in the column for magnetic immediately changed to a one with a time stamp was also noted.

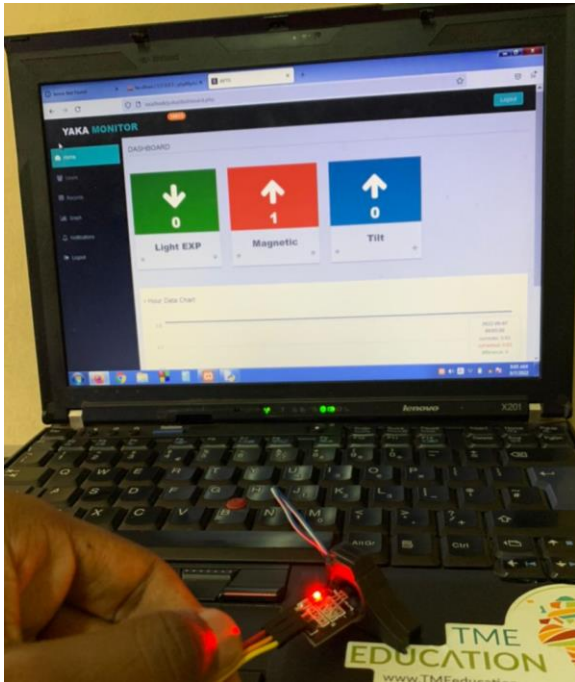


Figure 34: Home page during a tamper due to magnetic interference

Data Table

Meter Readings Data Table

#	Sender	Magnetic	Light exp
0	Kimera	0	1
1	Kimera	0	1
2	Kimera	0	1
3	Kimera	0	1
4	Kimera	0	1
5	Kimera	1	0
6	Kimera	1	0
7	Kimera	1	0
8	Kimera	1	0
9	Kimera	1	0
10	Kimera	1	0
11	Kimera	1	0
12	Kimera	1	0
13	Kimera	1	0

Figure 35:Records page during a tamper due to magnetic interference

Similarly, for tamper due to tilting the meter.

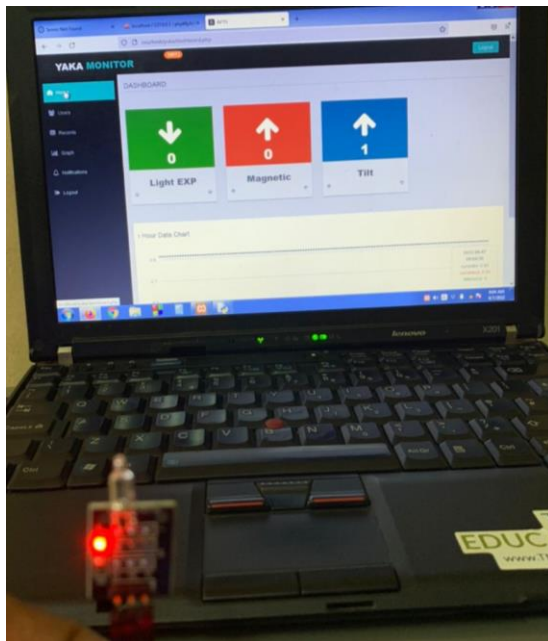


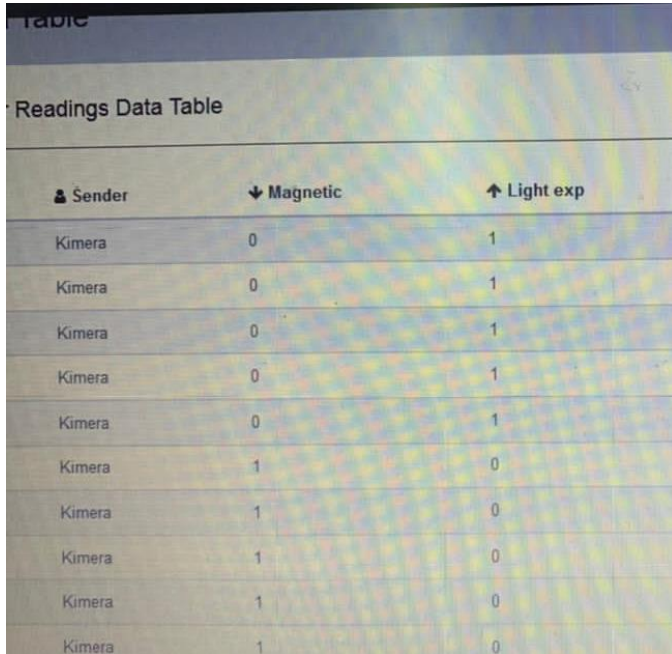
Figure 37: Home page during a tamper due to meter-tilt

Meter Readings Data Table

Light exp	Tilt	Date
1	1	2022-09-07 09:08:08
1	1	2022-09-07 09:08:07
1	1	2022-09-07 09:08:06
1	1	2022-09-07 09:08:05
1	1	2022-09-07 09:08:04
0	0	2022-09-07 09:08:03
0	0	2022-09-07 09:08:02
0	0	2022-09-07 09:08:01
0	0	2022-09-07 09:08:00
0	0	2022-09-07 09:07:59
0	0	2022-09-07 09:07:58

Figure 36:Records page during a tamper due to meter-tilt

Similarly, for tampers due to light exposure.



Sender	Magnetic	Light exp
Kimera	0	1
Kimera	0	1
Kimera	0	1
Kimera	0	1
Kimera	0	1
Kimera	1	0
Kimera	1	0
Kimera	1	0
Kimera	1	0
Kimera	1	0

Figure 38: Records page for a tamper due to light exposure.

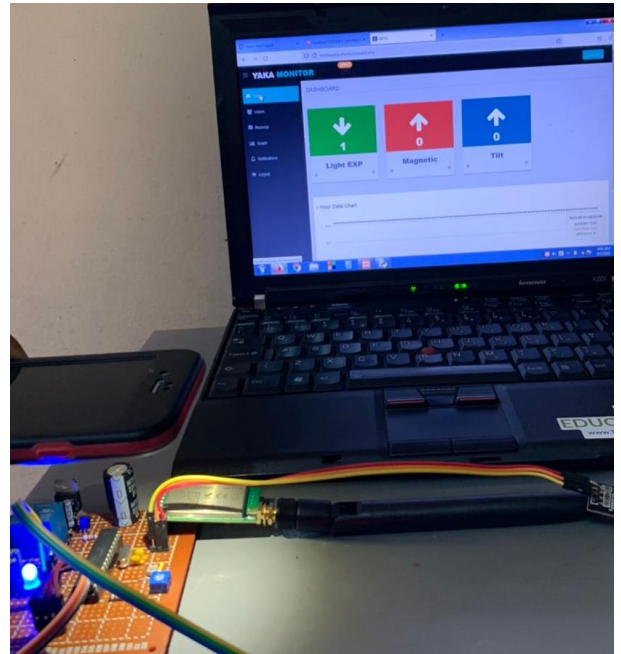


Figure 39: Home page for a tamper due to light exposure

4.5 Cost-benefit analysis.

The constructed prototype design shall be installed and deployed at a suitable point within the meter casing at the pole. A single-circuit design shall work for a single customer.

For the communication infrastructure, a single Lora transmitter module is installed on each prototype setup at the meter side (customer side) and a single receiver is inserted into a personal computer hosting the web interface. This is a gateway and a single module can be connected to multiple nodes (multiple device prototypes) to act as a reception point for data from the numerous nodes.

4.5.1 Objective

This is aimed at determining the feasibility of the project considering the costs of implementation and the magnitude of financial impacts caused by the effects of the problem being solved which is power theft.

4.5.2 Costs

The costs include;

Development costs.	Operational costs
Acquisition of circuit components and building prototypes.	Maintenance costs
Acquisition of Lora transmitter	Investigation of tamper signals due to tilt sensor.
Development and management of the utility service web interface	Costs incurred due to power consumed by device prototype
Deployment and installation of the prototype at the customer end.	
Setting up of the gateway (LoRa receiver)	
Non-recurring costs	Recurring costs
Recurring payment for use of communication technology since LoRa does not require recurrent payments as compared to GSM	Costs incurred due to power consumed by device prototype

Table 3: Costs incurred

4.5.3 Benefits

- Cost reductions in costs incurred by the utility since the available real-time monitoring methods apply the use of GSM technology which requires recurrent payment. When applied for use to monitor single-phase prepaid meters, a cost may be incurred in monitoring dormant meters. [23]
- LoRa technology can be deployed in remote areas without a cellular network or in basements for storage buildings and shall provide seamless communication with the utility during monitoring.

- It shall reduce costs incurred by the utility company during the numerous power anti-theft drives carried out to curb power theft.
- It offers a remote monitoring capability, data acquisition, and profitable use of tamper data stored to forge better ways of mitigating meter tampering by the utility company.
- The system shall make meter tampering undesirable to the end-user or customer since power is cut off once a tamper is detected.
- The communication technology is a low-power technology that reduces the power consumption rate as compared to earlier applied GSM technology.

4.5.4 Assessment and Comparative Cost-Benefit Analysis.

A large sum of financial resources is lost by the utility company due to power theft. For example, from the UMEME report, UMEME says it lost Shs98b in Jinja Sub-region, between January and March 2021.

John Baptist Nuwamanya, the metering sales manager at Umeme, said during the same period, the country lost 191 million units or about 18% of all the energy Umeme procures from Uganda Electricity Transmission Company Limited (UETCL), which translates into a loss of Shs97.7 billion. [24]

These losses are transferred to the other customers and reflects as an increase in the unit cost of electricity charged by the utility company. An investment in such a device would cost a large sum but have a positive long-term effect on both the utility and the end-user or customer.

Chapter 5: Conclusion, Challenges, and Recommendations.

5.1 Conclusion

There was a rampant increase in the power theft for single-phase prepaid meters which arouse the need for measures to curb this vice since it has several negative impacts on the utility as well as the end customers. This was aimed at making meter tampering entirely undesirable to the end users.

A LoRa-based tamper monitoring system for utility meters was presented in this project. The project contained the construction of a device prototype, the development of a web interface, and the integration of the interface and the prototype.

Light detecting Resistor, Hall effect sensor, and tilt sensor were connected to detect the various meter tampers. A working prototype was built which when exposed to light cuts off the supply from the end user and notifies the utility. When placed in a magnetic field cuts off supply and also notifies the utility and finally when tilted notifies the utility but does not cut off supply.

The data is transferred in real-time using LoRa technology.

The entire system is an important setup and allows for remote monitoring of single-phase prepaid utility meters in real-time.

5.2 Challenges

We faced a challenge when it came to the acquisition of the E32 433T30D LoRa modules from the stores around and resorted to shipping the devices from abroad.

A communication delay of about ten seconds was noticed between when a tamper occurs and when it is reflected on the home page as an active high on the respective tile.

5.3 Recommendation

Use of a computer with higher processing power to act as a local host for the web interface to easily process the data received to reduce the communication delay.

More still, the use of an online server to host the web interface enables access to the data from any point once one has an internet connection.

In future works, the device should be configured to function with setup gateways as this would improve the efficiency and ease deployment of a large number of device prototypes.

Lastly, in future works, more appropriate sensors can be added to fully curb any form of meter tampering based on the numerous methods of meter tampering.

References

- [1] Monday, 10 August 2015. [Online]. Available: <http://ethertek.blogspot.com/2015/08/how-to-hack-yaka-umeme-meter-get-free.html#.Yi8uInrMLrc..>
- [2] L. Hexing Electrical Co., 2013 march. [Online]. Available: http://www.inogate.org/documents/10.1_User_manual_of_Single_HXE12-KP.pdf..
- [3] [Online]. Available: <https://www.umeme.co.ug/stories/1358>.
- [4] November 11 2014 . [Online]. Available: b. J. Wire, "Is UMEME's Yaka Smart Metering a security time bomb?," New Vision article.
- [5] J. H. Awan, Pakistan Council for Science and Technology, 2017. [Online]. Available: https://www.academia.edu/35964903/Issues_and_Challenges_of_Existing_Electricity_Pre_Paid_Smart .
- [6] N. Wesonga, " umeme powering company," 16 09 2020. [Online]. Available: <https://www.umeme.co.ug/stories/1001..>
- [7] August 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2095809917306057..>
- [8] Friday 25 August 2017. [Online]. Available: [https://www.gsma.com/mobilefordevelopment/country/uganda/an-update-on-umemes-smart-energy-solutions-how-ugandas-electricity-utility-has-been-tackling-losses-in-the-last-3-years/..](https://www.gsma.com/mobilefordevelopment/country/uganda/an-update-on-umemes-smart-energy-solutions-how-ugandas-electricity-utility-has-been-tackling-losses-in-the-last-3-years/)
- [9] August 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2095809917306057..>
- [10] [Online]. Available: <https://lora-alliance.org/about-lorawan/>.
- [11] [Online]. Available: <https://www.azosensors.com/article.aspx?ArticleID=2440>.
- [12] [Online]. Available: <https://www.ademnea.net/article/14>.
- [13] [Online]. Available: <https://training.ti.com/anti-tamper-techniques-thwart-attacks-smart-meters-introduction-common-meter-tampering-techniques>.
- [14] M. A. A. a. N. J. J. L. Gallardo, "LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid 2021," IEEE Access, vol. 9, pp. 124295-124312.
- [15] H. E. Amhenrior., "Development of an SMS-Based Prepayment Energy Meter Monitoring System for Consumers and Utility," American Journal of Embedded Systems and Applications. Vol. 6, No. 1,pp. 37-45, , 2018.
- [16] S. e. a. ANANTH, "Web based Prepaid Energy Meter with theft control," European Journal of Molecular & Clinical Medicine 7.11, , 2021.
- [17] A. A. A. T. a. R. R. Ajeeba, "IoT Based Energy Meter Reading, Theft Detection and Disconnection," International Research Journal of Engineering and Technology, 2017.

- [18] The things network, 2020 . [Online]. Available: <https://www.thethingsnetwork.org/forum/t/butterfly-lora-node-based-on-atmega328-and-with-rtc/21846..>
- [19] [Online]. Available: <https://www.electronics-tutorials.ws/electromagnetism/hall-effect.html>.
- [20] [Online]. Available: <https://www.azosensors.com/article.aspx?ArticleID=318>.
- [21] [Online]. Available: <https://kitronik.co.uk/blogs/resources/how-an-ldr-light-dependent-resistor-works>.
- [22] "what-is-a-microcontroller," [Online]. Available: <https://www.arrow.com/en/research-and-events/articles/engineering-basics>.
- [23] [Online]. Available: <https://enterpriseiotinsights.com/20170612/internet-of-things/what-lowrawan-main-benefits-technology-tag23#:~:text=%E2%80%9CThe%20main%20benefits%20of%20LoRa,coverage%2C%20energy%20efficiency%20and%20location..>
- [24] [Online]. Available: <https://sun-connect.org/uganda-umeme-loses-billions-to-power-theft/>.
- [25] UMEME. [Online]. Available: <https://www.umeme.co.ug/stories/1001>.

Appendix



COLLEGE OF ENGINEERING, DESIGN, ART AND TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

DEVELOPMENT OF A LORA BASED TAMPER MONITORING SYSTEM FOR UTILITY METERS

CASE STUDY: UMEME YAKA METERS

By

NEKESA RACHEAL 18/U/36085/PS

MATOVU DERRICK VICTOR 18/U/22517/PSA

SUPERVISOR: MR. DAVID MARTIN AMITU

CO -SUPERVISOR: MR.INNOCENT OKETCH

Project proposal Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of Bachelor of Science in Electrical Engineering of Makerere University

JUNE 2022

Contents

List of Figures	ix
List of tables	x
Chapter 1: Introduction	1
1.1 Project background.	2
1.2 Problem statement.....	4
1.3 Justification.	6
1.4 Project objectives	7
1.4.1 Main Objective.....	7
1.4.2 Specific Objectives.....	7
Chapter 2: Literature review	8
2.1 Lora Technology.....	8
2.1.1 The Lora Architecture.....	8
2.1.2 Why LoRa.....	9
2.1.3 LoRa Technology in Uganda.....	10
2.2 Meter tampering.....	10
2.2.1 Ways of meter tampering.....	11
2.3 Related works.....	12
2.3.1 LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid.....	12
2.3.2 Development of an SMS-Based Prepayment Energy Meter Monitoring System for Consumers and Utility Companies.....	13
2.3.3 Web-based Prepaid Energy Meter with theft control.....	13
2.3.4 IoT-Based Energy Meter Reading, Theft Detection, and Disconnection.....	14
Chapter 3: Methodology	15
3.1 Work package, deliverable, and tools.....	15
3.2 Proposed system architecture	16
3.2.1 Control System.....	17
3.2.2 Communication Layer.....	18
3.3.3 User Interface Layer.....	18
3.4 Steps to accomplish the project.....	18
Test stage.....	19
Chapter 4: Results and Discussion	20
4.1 Circuit design.....	20
4.1.1 Schematic design.....	20
4.2 Construction of the tamper-proof and monitoring device.....	20
4.2.1 Power supply.....	21

4.2.2 The Control System.....	22
4.2.3 Communication layer.....	27
4.2.4 The relaying system.....	29
4.3 Web interface.....	30
4.3.1 Home page.....	30
4.3.2 Records page.....	30
4.3.3 Users page.....	31
4.4 Tamper scenarios.....	31
4.5 Cost-benefit analysis.....	33
4.5.1 Objective.....	33
4.5.2 Costs.....	34
4.5.3 Benefits.....	34
4.5.4 Assessment and Comparative Cost-Benefit Analysis.....	35
Chapter 5: Conclusion, Challenges, and Recommendations.	36
5.1 Conclusion.....	36
5.2 Challenges.....	36
5.3 Recommendation.....	37
References	38
Appendix.....	40

List of figures

Figure 1: three phase meters faulty due to tampering	5
Figure 2: single phase prepaid meters faulty due to tampering	5
Figure 3: Proposed system Architecture	13
Figure 4: steps to accomplish the project.....	15

Declaration

We MATOVU DERRICK VICTOR and NEKESA RECHEAL hereby declare that this is project proposal work entitled “Development of a Lora based tamper monitoring system for utility meters ” except where explicit citation in it has been presented to any institution of higher learning for any academic award.

Signature:

Date.....

Signature.....

Date.....

Approval

This is to certify that the project proposal under the title “Development of a Lora based tamper monitoring system for utility meters” has been done under my supervision and is now ready for examination.

Signed:

Date:

Mr. David Martin Amitu

Department of Electrical Engineering,

Makerere University.

Signed:

Date:

Mr. Innocent Oketch

Department of Electrical Engineering,

Makerere University.

Abstract.

Electricity crisis has become a serious issue, since the demand of power is increased over its production. One of the major challenges in electricity management is misuse of the power consumption due to electricity theft in the public areas. The project document proposes the technical development of a Lora based system for utility meters. The proposed solution seeks to develop a device prototype with ability to detect prepaid meter tampering scenarios including magnetic, opening and displacement among others and be able to report them to a centralized system via Lora. A 433 MHz E32-433T30D matched Lora pair is being proposed to be used with a maximum link distance of up to 24KM. The real time tamper detection and reporting system is meant for use in Yaka prepaid domestic meters case as subsequently termed by UMEME, the utility service provider. The acquired information is collected to a developed web application database and the Graphic user interface displays location and method of meter tampering.

Introduction.

Due to the increasing cost of electricity, energy theft is becoming a major concern for government agencies (Public Utility Boards) across the globe. In utility metering applications, the hacker might want to extract information and/or modify the internal settings. Many of these methods include tweaking the time so as to fool the system. [1] Electricity distribution companies may have different billing rates depending on time of the day, maximum demand, load, etc., thus requiring the real time clock (RTC) to provide accurate time reference. One may tamper the clock or manipulate the time to fool the system so as to charge differently, e.g. changing PM to AM such that metering firmware charges less due to nonpeak load tariff during the changed time. The RTC usually relies on a 32.768 kHz external crystal oscillator, and a hacker may change the RTC crystal to slow it down so as to count less, thus introducing inaccuracies in measurement and billing. [2] A large portion of these revenue losses can be recovered by installing electronic energy meters because they can detect tamper conditions and assure proper billing, unlike electromechanical meters. However, a delay in tamper awareness can also increase the magnitude of the loss in such meter settings. Additionally, as these meters become networked with the introduction of advanced metering technologies like AMR or smart grid in developed world, utility companies will benefit by automatically knowing any tampering events that might happen remotely. However, smart grid metering utilities have not been assumed yet in low developed countries like Uganda.

Background.

In 2010, Uganda's largest electricity distribution company UMEME put out a tender for a Pre-Payment Metering turnkey Business Solution which led to the deployment of the Yaka smart electricity meters as we know them today. As a company, 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 [3]

A good look at how Smart Meters operate shows a heavy reliance on ICT systems. A smart meter is 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. Governments globally are rooting for Smarter metering systems in order 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. [4]

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 to attacks. Now hackers have the ability to 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.

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. Other flaws these meters are likely to have been shared IDs like factory default passwords and poor protection from tampering. [5]

Problem statement.

Energy theft and meter tampering for Yaka-meter systems is a nation-wide problem that contributes heavily to revenue losses. In the six months to June 2020, UMEME registered an increase in losses to 17.4% (with meter tampering contributing 4.8%) compared to 16.9% for the same period in 2019. The rise was a result of a reduction in the number of anti-power theft drives during the COVID- 19 induced lockdown. The 3 per cent energy losses gap in 2020 to the target of 14.4% translated into Shs 27 billion negative impact on sales, the company noted in its half year interim financial statement. [6].

For the period of February and March 2022, the results from stress testing of the faulty meters that were retrieved by UMEME to identify the cause of the fault are shown below.

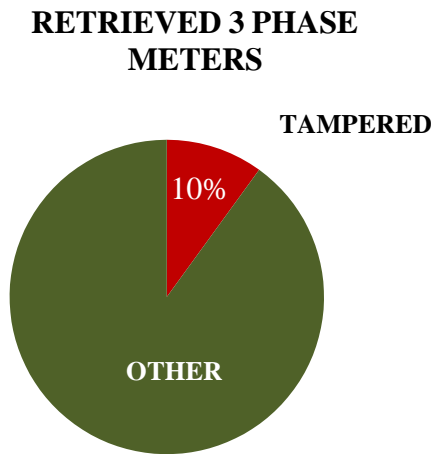


Figure 2: three phase meters faulty due to tampering

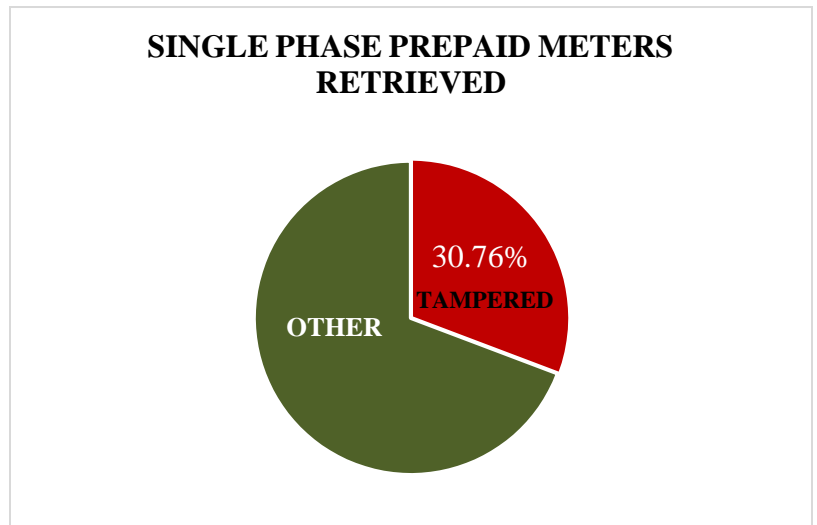


Figure 1: single phase prepaid meters faulty due to tampering

Figure two shows that 10% of the three phase meters that were retrieved were faulty due to tampering while figure one shows that 30.76% of the single-phase meters retrieved were faulty due to tampering.

As reported from an interview with the principal metering Engineer, Research and development of UMEME, he noted that the energy losses as of the end of March 2022 were at 17.6%. As energy losses, hence the need for ways of making meter tampering undesirable to the end customer and therefore the need for a low-cost real-time monitoring system to report these tampers.

Justification.

Whereas the majority of customers are households, the industrial and commercial customers (0.5 percent of total customer database) account for over 70 per cent of UMEME's sales and revenue. Tackling losses from this customer segment could drive significant revenue increases, which in turn can help UMEME connect more households [UMEME, 2017]. Particularly on the demand side, for example, communication infrastructure is incomplete at, low-power wide-area network (LPWAN) is a new solution in the context of a wireless breakthrough in the communication sector. Two representative technologies of LPWAN are the narrow-band Internet of Things (NB- IoT) and Long Range (LoRa) technology the power distribution level, and even less communication infrastructure is available for utilization systems at lower voltage levels. [7] UMEME had proposed Yaka meters with GSM connectivity to monitor and report meter tamper and vandalism activity. However, it was realized to be a non-cost-effective solution since it wasn't feasible to sustain connectivity as some prepaid meters are running dormant with no subscription over a long time. [8] To overcome this barrier. The NB-IoT is inherited from cellular communication, and seamlessly works on the existing global system for mobile (GSM) and long-term evolution (LTE) networks in licensed frequency bands. In contrast, LoRa technology operates in the unlicensed frequency band, so that end users are free to build up LoRa gateways that are similar to house-owned WIFI routers. Therefore, LoRa technology is perfect for outlying regions without cellular network coverage, or for establishing private networks with specific requirements for quality and security. [9]

This is a cost-effective solution as Lora will not require communication subscription costs as the case with the pre-tested GSM.

Objectives.

Main Objective.

This document proposes the design and construction of a regional centralized Yaka LoRa based tamper monitoring system for Yaka Utility meters.

Specific Objectives.

- ❖ To design the tamper proof prototype.
- ❖ To construct the tamper proof and monitoring device.
- ❖ To design and develop the service provider Web interface.
- ❖ Integration of the device and developed interface.

Literature review.

Internet of Things (IoT) technologies including Lora enable physical objects to see, hear, think and perform jobs by having them “talking “together in order to share information, and coordinate decisions. IoT technologies will transform static devices into smart devices by exploiting their underlying technologies, such as ubiquitous and pervasive computing, embedded devices, and communication technologies. In terms of dimensions, prepaid meters can communicate to remote monitoring infrastructure over a long distance. Several works have been done on meter tampering and reporting techniques as discussed below:

LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid.

José Luis Gallardo, Mohamed A. Ahmed and Nicolás Jara a member of IEEE developed a LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid. This paper proposed an IoT-based architecture for AMI networks, which is a key component for deploying the future smart grid concept. A particular case of LoRa communication technology is considered as a promising candidate for deploying the proposed architecture. A simulation scenario of the AMI system was considered for a suburban neighborhood. Several aspects are discussed and evaluated to determine if LoRa technology can be operated under different circumstances. The simulation results were compared considering two different operation scenarios of LoRa networks under various metrics, such as delivery ratio, energy consumption, throughput, collisions, and SF distribution. The proposed solution was used to deploy the smart meters in an AMI network and enables the network to be dynamic and solve scalability issues in future configurations (adding more smart meters).

The works entirely focused on simulation of Lora performance and hence there was no physical deployment of Lora on ground. Works didn't include prepaid meter tamper monitoring and reporting as was in their initial objectives. [10]

Development of an SMS-Based Prepayment Energy Meter Monitoring System for Consumers and Utility Companies.

Henry Erialuode Amhenrior developed a meter that uses SMS for communication through the GSM modem. It is made SMS capable by interfacing Atmega2560 with SIM900 Global System for Mobile Communications (GSM) module. The system also has a server consisting of Atmega328P and SIM900 GSM module that enables the utility company to access the meter. The server is interfaced to a PC which is used for management and administrative Platform. Several commands are used for communication with the meter for monitoring and some of the information the communications seek include, unit balance, unit consumed, time of power failure and time of power restore. Other monitoring communications capabilities of the meter are checking the token recharge into the meter, credit warning alert, wireless meter disconnection and connection. The SMS communication is a two-way communication and this enables the activities of the meter to be monitored wirelessly. The results obtained show that SMS is very efficient, effective and successful in achieving the monitoring aspects of this work as proposed distribution companies can communicate with the meter to obtain information through the GSM SMS platform at will.

[11]

However, GSM SMS based monitoring requires continuous subscription for the cellular service and this is one reason why prepaid meters are not on-net for real-time monitoring as the case with LPU meters.

Web based Prepaid Energy Meter with theft control.

The idea behind this project is to construct the web based Prepaid Energy Meter with theft control, which eliminates manual meter reading so that the bills can be paid in advance by which the consumers can plan their electricity bill well in advance. In this system anyone can recharge their electricity need, like our mobile phones. This proposed system helps the users with the real time information about the peak loads (max energy consumption), energy theft, effective usage of power consumption, billing status etc. This automated system is built by using Arduino controller, different sensors & IoT. It continuously reads the energy meter readings and the real time information is available to the user with IoT. Whenever the energy consumption reaches its limit,

the power supply connection will be disconnected and alert information is given to the consumer during minimum balance and null balance. Power theft information is given to both user and electricity board; hence it is helpful to identify the exact power theft location. To avoid unnecessary usage of power consumption, load based automatic switch system is used which can build up home automation system. [12] This energy saving system replaces the conventional meter reading and offers the consumers with user friendly access to energy meter from remote location.

IoT Based Energy Meter Reading, Theft Detection and Disconnection.

Ajeeba A A1, Anna Thomas, Risa Rasheed proposed a PIC16F877A micro controller-based design and implementation of energy meter using IoT (Internet of Things) concept. The design was to eliminate the human involvement in electricity maintenance. The energy meters were to be connected to the PIC micro controller through an interfacing circuit. The opt coupler sensor was to give an interrupt each time the meter LED ashes to the programmed PIC micro controller. The readings of the main energy meter and sub energy meters were compared so as to identify the theft status. Whenever there was discrepancy in the two values, a message that theft has occurred was displayed in the LCD display as well as in the web page. The consumers could easily track their energy usage so that effective monitoring of power consumption is possible. The hardware interface circuit consisted of PIC16F877A micro controller, MAX232, LCD display, and opt coupler. [13]

However, the system application is unrealistic in our setting as it requires more infrastructures to run web services. The cost of internet and its limited access make it impossible still as ideal solution in the Ugandan setting.

Project work plan

Methodology.

This section discusses in detail and the description of the work done, modelling and design of the proposed system.

Quantitative and qualitative research, review of articles and consultations from UMEME as the main distribution company about the numerous Yaka-meter tampering techniques.

Literature review through textbooks, journals, review articles and reports and other relevant information from reliable sources about Lora Technology.

The design of the system prototype for a Yaka-meter tamper notification system will be based on standalone long range wireless communication. This device shall be based on an 8-bit RISC Atmel ATMEGA328P-PU microcontroller interfaced with 24KM E32- 433T30D LoRa modules to provide localized communication to the local service provider. The device shall be able to detect tamper by sensing meter tilt, magnetic exposure and light exposure of internal parts. [14]

The table shows the work package, deliverable and tools that shall be used to achieve each particular objective.

MILESTONE	WORK PACKAGE	DELIVERABLE	TOOLS
Design of the tamper proof prototype.	<ul style="list-style-type: none">• Designing a circuit diagram for the system prototype.• Obtaining a Deeper understanding of Lora technology.	Circuit design	Proteus software
Construct the tamper proof and monitoring device.	To build the tamper proof and monitoring device.	Device Prototype	<ul style="list-style-type: none">• Arduino/Atmel Studio• Circuit board, circuit components.

MILESTONE	WORK PACKAGE	DELIVERABLE	TOOLS
To design and develop the service provider Web interface.	Back end development. Front end development Integration of the two ends	Web application	XAMPP/MySQL
Integration of the device and developed interface	Linking the matched Lora pair (receiver and transmitter)	Web interface can connect to the prototype	Putty
Report Writing	Writing a detailed technical report	Project Report	Paper, Computer

Proposed system architecture.

The figure depicts the proposed functional block diagram of the Lora based tamper monitoring system for Yaka utility meters. This shows how the various components are interlinked.

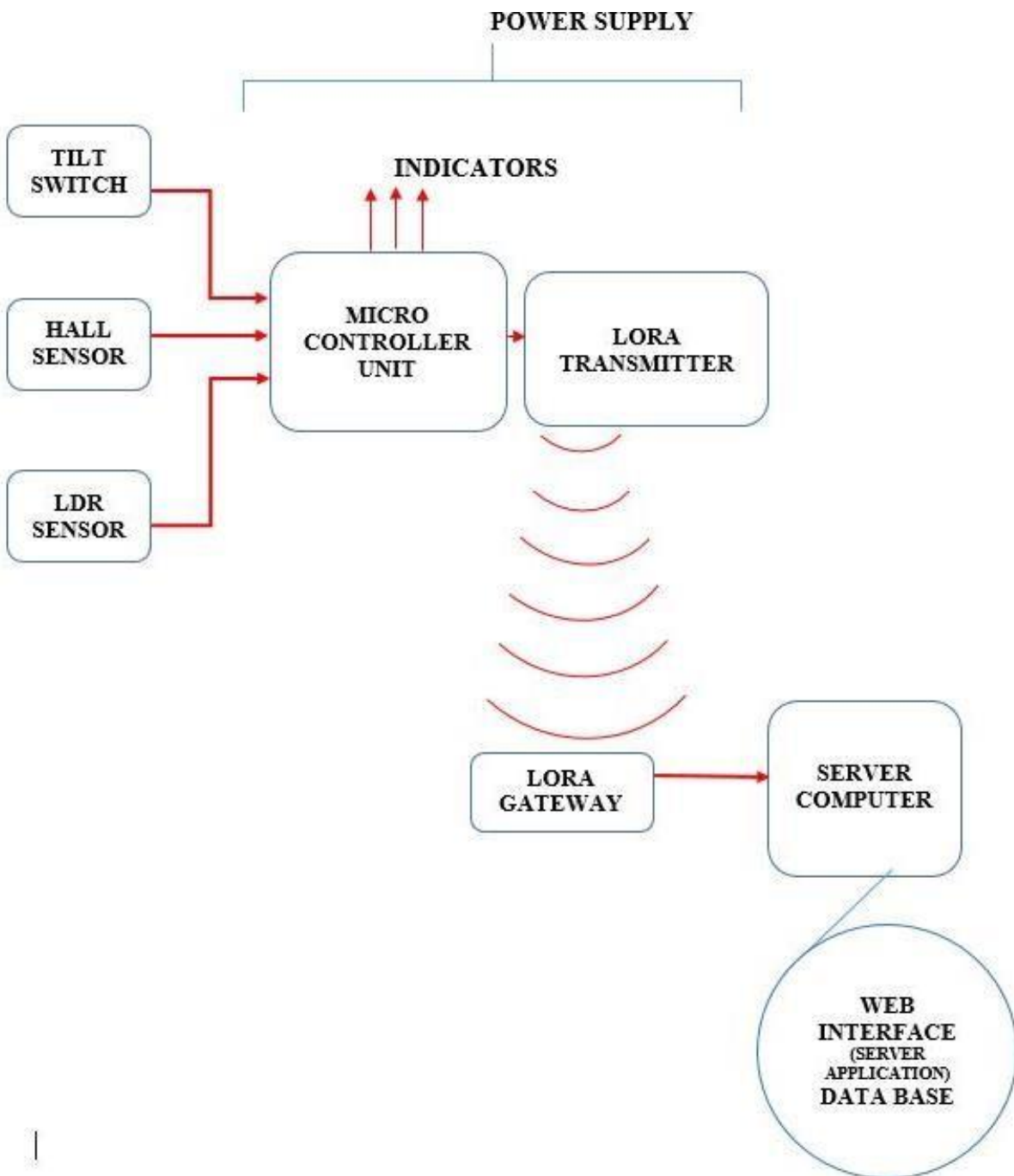


Figure 3: Proposed system Architecture

Control System

Hall sensor

This sensor mainly will detect Magnetic Interference. Hall sensors devices which are activated by an external magnetic field. Since Meters use magnetic material in voltage and current measurement circuits and thus are affected by abnormal external magnetic influences that in turn affect proper functioning of the meter, and also the output signal from a Hall Effect sensor is the function of magnetic field density around the device. Hence when the magnetic flux density around the sensor exceeds a certain pre-set threshold, the sensor detects it and generates an output voltage. [15]

Tilt sensor

The tilt sensor will help in detecting any change in the position of the meter. One may want to open the meter case to change the settings or even remove the backup battery so that the meter will reset when the main power goes off. A tilt sensor is an instrument that is used for measuring the tilt in multiple axes of a reference plane. Tilt sensors measure the tilting position with reference to gravity. tilt sensor has a metallic ball that is designed to move the two pins of the instrument from the 'on' to the 'off' position, and vice versa, if the sensor reaches a pre-determined angle. [16]

LDR sensor

An LDR is a component that has a (variable) resistance that changes with the light intensity that falls upon it. This will be used as a light sensing device to detect exposure of the internal components to light. [17]

Micro controller unit

A microcontroller (sometimes called an MCU or Microcontroller Unit) is a single Integrated Circuit (IC) that is typically used for a specific application and designed to implement certain tasks. This chip will in take instructions from the sensors and operate the respective indicator then trigger the Lora transmitter to operate. [18]

Communication Layer.

Lora transmitter and receiver.

This will send and receive the tamper signals from the meter to the receiver at the central monitoring location respectively.

User Interface Layer.

Server PC

This will contain the graphic user interface with the Web application where the operator will be notified about the tamper method and location of the tamper.

Steps to accomplish the project.

The steps we shall use to accomplish the project are ideation, design, build, integrate and test as illustrated in the block diagram below.

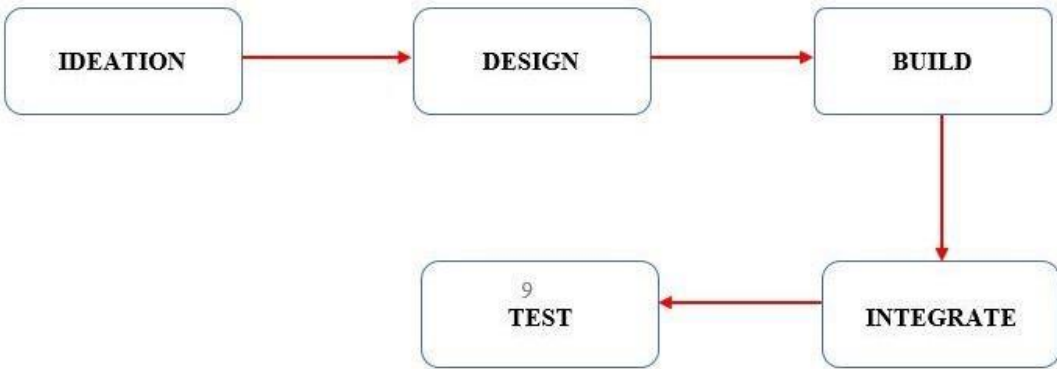


Figure 4: steps to accomplish the project

The ideation stage

Is the initial stage and involves the formation of the idea or the concept.

The design stage

At this stage we shall produce a sketch showing the schematic drawing and the simulation shall be

developed. This information will be used to research on the equipment needed and the materials to be used.

The build stage

This is the project execution phase and the design is delivered. The prototype hardware shall be developed with several components brought together as per the design.

The integration stage

This shall involve coordinating all the resources that is the prototype and the web application also managing any conflicts between the different aspects of the project. We shall focus on requirements for adding this external circuit to the already existent Yaka meter.

Test stage

Unit testing, integration testing, system testing and acceptance testing shall be executed and results shall be analyzed. This shall involve a test for both the hardware and the software.

Application Layer

The application layer is in charge of all the tasks related to data processing, display, and disposition of data to the utilities for the different applications that are intended. For utility, business-side tasks include business model applications, graphs, flowcharts, and big data analysis of meter tampering cases and the specific tampering method for the perceived data from the perception layer.

Under this domain, the following applications may coexist: user dashboard and meter tampering data including the location of any meter tampering occurrence and the method of tamper displayed.

Expected results.

- ❖ Functional tested prototype.
- ❖ Web application.
- ❖ Development report.

Proposed budget.

NO.	ITEM	UNIT PRICE
1.	Prototyping supplies	300,000/=
2.	Stationary	100,000/=
3	Miscellaneous	100,000/=
TOTAL		500,000

Timeline.

ACTIVITIES	DURATION 2022							
	FEB	MAR	APR	MAY	JUNE	JULY	AUG	SEPT
Literature review								
Abbreviated proposal writing and submission								
Midterm Presentations								
Final Proposal report writing and submission								
Data collection and analysis								
Prototyping								
Testing and accessing the performance of the prototype								
Final presentation								
Final report writing and submission								

References.

- [1] Monday, 10 August 2015. [Online]. Available: : <http://ethertek.blogspot.com/2015/08/how-to-hack-yaka-umeme-meter-get-free.html#.Yi8uInrMLrc..>
- [2] L. Hexing Electrical Co., 2013 march. [Online]. Available: http://www.inogate.org/documents/10.1_User_manual_of_Single_HXE12-KP.pdf..
- [3] [Online]. Available: <https://www.umeme.co.ug/stories/1358>.
- [4] November 11 2014... [Online]. Available: b. J. Wire, "Is UMEME's Yaka Smart Metering a security time bomb?," New vision article.
- [5] J. H. Awan, Pakistan Council for Science and Technology, 2017. [Online]. Available: https://www.academia.edu/35964903/Issues_and_Challenges_of_Existing_Electricity_Pre_Paid_Smart.
- [6] N. Wesonga, umeme powering company, 16 09 2020. [Online]. Available: <https://www.umeme.co.ug/stories/1001..>
- [7] August 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2095809917306057..>
- [8] Friday 25 August 2017. [Online]. Available: : <https://www.gsma.com/mobilefordevelopment/country/uganda/an-update-on-umemes-smart-energy-solutions-how-ugandas-electricity-utility-has-been-tackling-losses-in-the-last-3-years/..>
- [9] August 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2095809917306057..>
- [10] M. A. A. a. N. J. J. L. Gallardo, "LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid," IEEE Access, vol. 9, pp. 124295-124312, 2021.
- [11] H. E. Amhenrior., "Development of an SMS-Based Prepayment Energy Meter Monitoring System for Consumers and Utility," American Journal of Embedded Systems and Applications. Vol. 6, No. 1, pp. 37-45, 2018.
- [12] S. e. a. ANANTH, "Web based Prepaid Energy Meter with theft control," European Journal of Molecular & Clinical Medicine 7.11 , 2021.
- [13] A. A. A. T. a. R. R. Ajeeba, "IoT Based Energy Meter Reading, Theft Detection and Disconnection,," International Research Journal of Engineering and Technology , 2017.
- [14] The things network, 2020. [Online]. Available: <https://www.thethingsnetwork.org/forum/t/butterfly-lora-node-based-on-atmega328-and-with-rtc/21846..>
- [15] [Online]. Available: <https://www.electronics-tutorials.ws/electromagnetism/hall-effect.html>.
- [16] [Online]. Available: <https://www.azosensors.com/article.aspx?ArticleID=318>.
- [17] [Online]. Available: <https://kitronik.co.uk/blogs/resources/how-an-ldr-light-dependent-resistor-works>.
- [18] "what-is-a-microcontroller," [Online]. Available: <https://www.arrow.com/en/research-and-events/articles/engineering-basics>.