



**BUSITEMA
UNIVERSITY**
Pursuing Excellence

P.O. Box 236, Tororo, Uganda
Gen: +256 - 45 444 8838
Fax: +256 - 45 4436517
Email: info@adm.busitema.ac.ug

www.busitema.ac.ug

FACULTY OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF ELECTRICAL ENGINEERING
FINAL YEAR PROJECT REPORT

**DESIGN AND DEVELOPMENT OF A TAMPER DETECTION SYSTEM FOR SINGLE PHASE
PREPAID METERS.**

SUPERVISORS: - PROF. RICHARH OKOU

: -MR. SOLOMON OJAGONLE

NAME	REGISTRATION NUMBER
EKIRAPA BRIAN	BU/UP/2022/1910

A final year Project report submitted to the Department of Electrical Engineering in Partial fulfillment of the Requirement for the award of a Bachelor of Science degree in Electrical Engineering of Busitema University.

May, 2026

DECLARATION

I do hereby declare that to the best of my knowledge and belief, this report is my original work and has never been submitted to any other institute of learning. It is therefore authentic, and where any references or secondary data have been used, they have been given due acknowledgement.

Name: EKIRAPA BRIAN

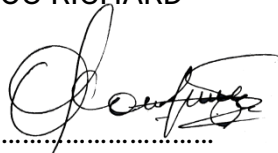
Signature.....

Date: 1/10/2026

APPROVAL

This final year project report titled "Design and Development of a Tamper Detection System for Single-Phase Prepaid Meters" has been submitted to the Department of Electrical Engineering, Faculty of Engineering and Technology, Busitema University, with my approval as a University Supervisor.

PROF. EKOu RICHARD

Signature.....

Date.....27.....06.....
2026

Mr. SOLOMON OJANGOLe.

Signature.....

Date.....28.....06.....
2026

ACKNOWLEDGEMENT

I extend our sincere gratitude to Mr. Solomon Ojangole and Professor Okou Richard, my project supervisors, for their invaluable guidance and support throughout this project. I also thank our lecturers and all others who have supported us along the way. Special appreciation to my parents and friends for their unwavering encouragement and assistance.

DEDICATION

I dedicate this work to my beloved parents, whose unwavering love, endless sacrifices, and steadfast encouragement have been the foundation upon which our dreams are built. To my cherished siblings, who stood by us with patience and understanding through every challenge and triumph. And to me, dear friends, whose companionship, laughter, and support made this journey not only bearable but truly memorable.

This achievement belongs as much to you as it does to me.

ABSTRACT.

Energy theft and meter tampering remain a significant challenge for electricity distribution companies in Uganda, resulting in substantial revenue losses annually. This project presents the design and development of a tamper detection system for single-phase prepaid (Yaka) meters, aimed at enabling real-time identification and reporting of unauthorized interference with electricity meters.

The proposed system employs an 8-bit RISC Atmel ATmega328P-PU microcontroller interfaced with a magnetic flux sensor, tilt sensor, current sensor, and voltage sensor to detect various tampering techniques, including the use of permanent magnets, physical tilting of the meter, exposure of internal components, and signal cable manipulation. Upon detection of any tampering event, the system triggers an alarm and transmits an SMS notification to the utility company's area manager via the GSM network, enabling prompt remote response.

The system design incorporates an independent Real-Time Clock (RTC) with battery backup to detect power interruption-based tampering, and anti-tamper switches to guard against physical intrusion. A prototype was constructed and tested using unit, integration, and system-level testing methodologies to verify functionality and reliability. The developed system offers a cost-effective, automated, and reliable alternative to existing monitoring approaches such as physical inspection and manual meter reading. It is expected to significantly reduce electricity theft, improve billing accuracy, and lower operational costs for UEDCL and similar utility companies in Uganda.

LIST OF ACRONYMS

PEMNS	Prepaid Energy Meter Notification System
ICT	Information and Communication Technology
PUB	Public Utility Board
RTC	Real Time Clock
AMR	Automatic Meter Reading
V _{DD}	Supply Voltage
GSM	Global System for Mobile Communication
RISC	Reduced Instruction Set Computer
SMS	Short Messaging Service
WAMR	Wireless Automatic Meter Reading
GPRS	General Packet Radio Service
CT	Current Transformer
ETSI	European Telecommunications Standard Institute
WAP	Wireless Application Protocol
LED	Light Emitting Diode
ID	Identification

TABLE OF CONTENTS

DECLARATION.....	i
APPROVAL.....	ii
ACKNOWLEDGEMENT.....	iii
DEDICATION.....	v
ABSTRACT.....	vi
LIST OF ACRONYMS.....	vii
TABLE OF CONTENTS.....	viii
CHAPTER ONE.....	1
1.0 Introduction.....	1
1.1 Background.....	1
1.2 Problem Statement.....	4
1.2.1 Formula Used For each district.....	5
1.3 Objectives:.....	8
1.4 Specific objectives:.....	8
1.5 Significance/Justification:.....	8
1.6 Scope:.....	8
CHAPTER II: LITERATURE REVIEW.....	9
2.0 Introduction.....	9
2.1 Types of Energy Meter Readers.....	9
2.1.1 Automatic Meter Reading (AMR) system.....	9
2.1.1.1 History of Automatic Meter Reading (AMR).....	9
2.1.2 Wireless Automatic Meter Reading System (WAMRS).....	10
2.2 Energy Theft and Meter Tampering Techniques.....	10
2.2.1 Global Scale and Economic Impact of Energy Theft.....	11
2.2.2 Historical Context and Evolution of Tampering Methods.....	12
2.2.3 Classification of Meter Tampering Techniques.....	13
2.2.3.1 Permanent magnet as a tamper:.....	13
2.2.3.2 Signal cable cutting.....	14
2.2.3.3 Tamper switch.....	15

2.2.3.3.1 Types and Construction of Tamper Switches.....	16
2.2.3.3.2 Integration with Microcontroller-Based Metering Systems.....	18
2.2.3.3.3 Importance of Tamper Switches in the Proposed System.....	19
2.2. 3.4 Inserting a foreign body.....	21
2.2.3.4.1 Types of Foreign Bodies Used and Their Characteristics.....	22
2.2.3.4.2 Electrical Effects of Conductive Foreign Body Insertion.....	23
2.2.3.4.3 Effects on Current Sensors and Metering Accuracy.....	25
2.2.3.4.4 Mechanical, Electrical, and Magnetic Disruption Effects.....	26
2.2.3.4.5 Implications for the Proposed Tamper Detection System.....	27
2.2.3.5 Other tamper techniques:.....	29
2.3 Related Projects and Experiments.....	29
2.4 The Existing Energy Metering Systems.....	30
2.4.1 Prepaid metering.....	30
2.4.2 Automatic meter reading.....	31
2.4.3 Personalized digital meter.....	31
2.4.4 Physical monitoring.....	31
2.5 The Proposed Project: Prepaid Energy Meter Tamper Detection System.....	31
2.6 Comparison between the existing system and the proposed system.....	33
2.7 The Technology in the Proposed System.....	33
2.7.1 The GSM Technology.....	33
2.7.2 The SMS Technology.....	36
2.7.3 Current sensor.....	38
2.7.3.1 Applications.....	40
2.7.4 Tilt Sensors (Inclinometers).....	42
CHAPTER III: METHODOLOGY.....	47
3.0 Introduction.....	47
3.1 System Study.....	47
3.1.1 Requirement Elicitation.....	47
3.1.2 Data collection methods.....	47
3.2 System Analysis.....	48
3.3 System Design.....	48
3.4 System Construction.....	49
3.4 Testing.....	49
3.4.1 Unit testing.....	49

3.4.2 Integration testing.....	49
3.4.3 System test.....	49
3.5 Validation.....	49
3.6 CODE FOR THE PROJECT.....	50
REFERENCES:.....	56
APPENDICES.....	59
Appendix E: Photographs of Prototype.....	59

LIST OF FIGURES:

Figure 1: Showing prepaid metering layout.....	3
Figure 2:Showing a graph of revenue loss.....	6
Figure 3:Showing Report from UEDCL.....	7
Figure 4:Showing report from UEDCL.....	7
Figure 5:showing the green, red, and yellow signal wires.....	15
Figure 6:showing a meter without a tamper cover.....	21
Figure 7:showing GSM Illustration.....	36
Figure 8:Showing the current sensor.....	41
Figure 9:Showing the tilt sensor.....	46
Figure 10:System block diagram.....	48

LIST OF TABLES

Table 1:Showing revenue loss.....	5
-----------------------------------	---

CHAPTER ONE

1.0 Introduction.

This chapter gives an introduction that led to the proposal of the design and construction of a tamper detector system for UEDCL meters. It is composed of the following subsections: the background of the project, problem statement, objectives of the proposed project, significance/justification, and the scope to be covered while designing the project.

1.1 Background.

Due to the increasing cost of electricity, energy theft is becoming a major concern for government agencies (Public Utility Boards) across the globe, this is according to a World Bank report 2009. In utility metering applications, the hacker might want to extract information and/or modify the internal settings. The common method used is to insert a permanent magnet into the meter without affecting any design in the electronics of the meter board. Many of these methods include tweaking the time so as to fool the system. Electricity distribution companies may have different billing rates depending on time of day, maximum demand, load, etc., thus requiring the real-time clock (RTC) to provide an accurate time reference. One may tamper with 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 [15,16], and a hacker may change the RTC crystal to slow it down so as to count less, thus introducing inaccuracies in measurement and billing. 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 [8]. 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 the developed world, utility companies will benefit by automatically knowing any tampering events that might happen remotely [6].

However, smart grid metering utilities have not been assumed yet in low-developed countries like Uganda.

In 2010, Uganda's largest electricity distribution company, UMEME, tendered out a Pre-Payment Metering to turnkey Business Solution, which led to the deployment of the Yaka smart electricity meters as we know them today [9,13].

As a company, UMEME expects to address some challenges, like poor payment of electricity bills, the current high cost of billing, and create an opportunity for easier monitoring of consumers' meters and energy consumption. It was also anticipated that this new system would 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 meter system, a number that is likely to have doubled by the close of 2014 [11].

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 [7].

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 [4]. Now hackers can carry out billing-related fraud and shut down electricity supplies at will. By accessing their memory chips, one can carry out some re-programming as well as exploit any flawed code therein to tamper with meter readings, transfer readings to other customers, and insert network worms that can potentially leave entire neighborhoods in a blackout [5]. 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 [3].

In IT security, physical access to the hardware is one of the loopholes that one can use to initiate any compromise. The fact that these meters are easily accessible to consumers means a lot. Access to the onboard software (firmware) of these meters can enable one to 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 are shared IDs like factory default passwords, and poor protection from tampering.

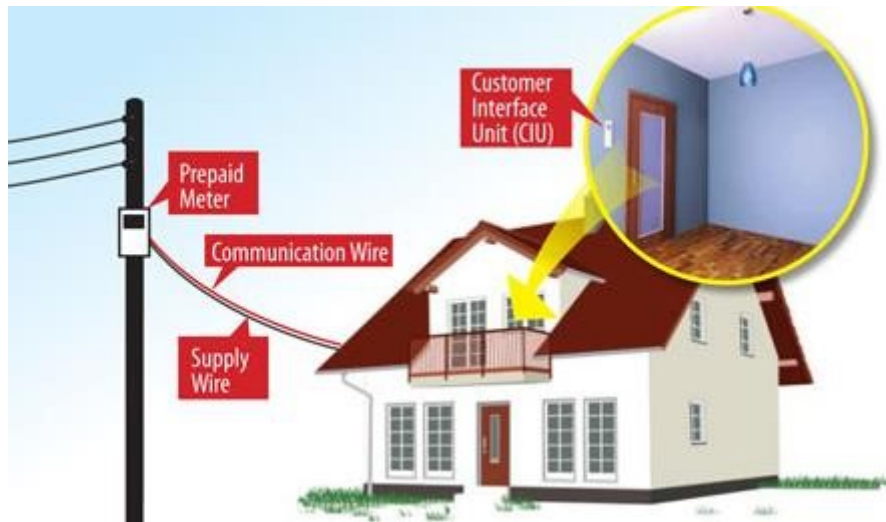


Figure 1: Showing prepaid metering layout

1.2 Problem Statement

Energy theft and meter tampering for Yaka-meter systems is a nationwide problem that contributes heavily to revenue losses [12]. Electricity theft has become an increasingly serious challenge for Uganda's power distribution network, directly undermining the financial sustainability of utility providers such as UEDCL. Consumers have been found manipulating their electric meters (Yaka meters) by inserting permanent magnets in the meter, bypassing the meter, cutting off the meter signal cables, using the neutral bypass, causing them to stop or under-register, hacking the meter to alter or stop the internal real-time clock, or even bypassing the meter, effectively using power without paying for it [1,2]. These fraudulent activities result in significant unaccounted-for energy, which translates directly into financial losses and places an unfair burden on honest consumers and the utility company alike.

The methods used to tamper with Yaka prepaid meters are varied and increasingly sophisticated. Physical tampering methods include the insertion of strong permanent magnets near the meter's sensing components, which interfere with the electromagnetic measurement mechanism and cause the meter to under-record actual energy consumption. In other cases, consumers have been found completely bypassing the meter by making illegal direct connections to the supply line, effectively consuming electricity without any form of measurement or payment. Additionally, some consumers cut off or interfere with the meter's signal cables, disrupting the communication between the meter's sensing elements and its processing unit, thereby causing inaccurate

readings or complete failure of the metering function [1,2].

More advanced forms of tampering involve logical or electronic attacks on the meter's internal systems. These include hacking the meter's firmware or internal real-time clock (RTC) to alter or completely stop the timekeeping function, which directly affects how energy consumption is recorded and billed. The neutral bypass technique, another commonly exploited method, involves rerouting the neutral conductor around the meter so that the meter only measures a fraction of the actual load current, causing significant under-registration of consumed energy [1,2].

Beyond these external manipulations, internal hardware-level attacks have also been documented. These include damage to the casing of the metering system, alteration of certain internal signals, removal of the battery while the system is actively powered (i.e., when VDD is powered ON), and removal of the battery while the system is in an inactive or off state (i.e., when VDD is powered OFF) [1,3]. Such actions can corrupt stored data, reset consumption records, or render the meter non-functional, all of which result in revenue loss for the utility provider.

Collectively, these tampering methods highlight a critical need for a reliable, automated, and real-time tamper detection system capable of identifying and reporting such fraudulent activities promptly. Without such a system in place, energy theft will continue to go undetected, further deepening the financial and operational challenges faced by Uganda's electricity distribution infrastructure.

Table 1: Showing revenue loss

Summary Table

District	Sept	Oct	Avg/Year	Energy Lost (kWh)	Revenue Loss (UGX)
Najjanakumbi	35	24	354	446,040	178,416,000
Natete	14	18	192	241,920	96,768,000
Kabalagala	30	23	318	400,680	160,272,000
Entebbe	25	19	264	332,640	133,056,000
Wandegeya	30	25	330	415,800	166,320,000
Lira	5	6	66	83,160	33,264,000
Masaka	10	9	114	143,640	57,456,000
Rubirizi	5	7	72	90,720	36,288,000
TOTAL	154	131	1710	2,154,600	861,840,000

1.2.1 Formula Used For each district,

$$\text{Avg/Year} = \frac{\text{Sept} + \text{Oct}}{2} \times 12$$

Average hidden energy per tampered meter = 105 kWh/month

Annual per meter:

$$E_{\text{per meter}} = 105 \times 12 = 1,260 \text{ kWh/year}$$

Tariff = 400 UGX/kWh

Energy loss:

$$E_{LOSS} = N \times 1260$$

Revenue loss:

$$R_{LOSS} = E_{LOSS} \times 400$$

Revenue Loss by District

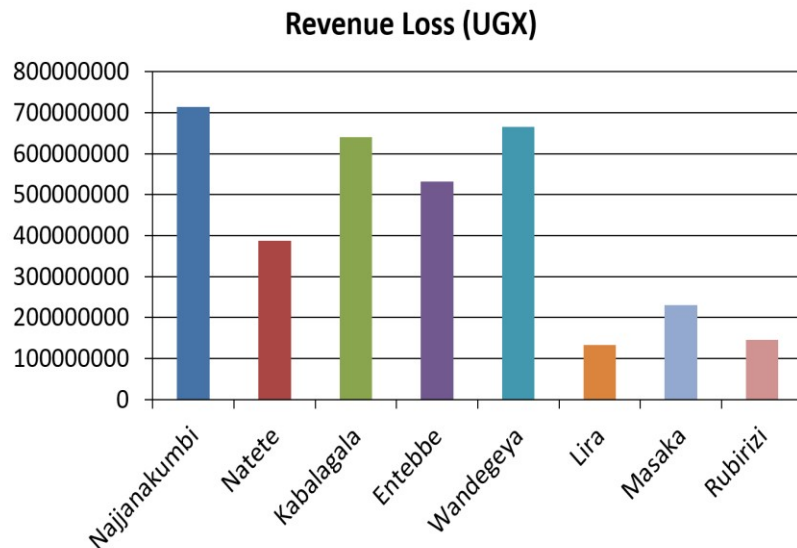


Figure 2: Showing a graph of revenue loss.



UGANDA ELECTRICITY DISTRIBUTION COMPANY LIMITED

TEST REPORT-SINGLE PHASE ELECTRONIC METER

METER PARTICULARS	District: NAJJANAKUMBI OFFICE			READINGS BEFORE TESTING	READINGS AFTER TESTING
				259.19kWh	259.17kWh
	Customer Name: NASSER MUSOKE				
	Meter Number: 14372037011			Meter Make: HEXING	W/O Number: 21478712
	Account Number: 102053994446			Date & Time brought: 05th /December/ 2025	
	Reason For Removal: SUSPECTED TAMPERED METER				
Brought by	Name: WALUSIMBI EDWINE			Check No: Not availed	
Report/Meter Taken by	Name:			N/A	
	Is meter taken?	NO		Date & Time taken	N/A
	Tick box				

GENERAL TESTS		REMARKS
External Visual Test	Seals	Not applicable
	Meter body	Plastic enclosure found partially opened and loosely connected.
	Current & Voltage Terminals	Both input and out terminals found ok.
Functional tests	LED pulsing output	Meter pulses normally when connected on supply and load
	Power ON indicator	Indicator LED is on when the meter is connected on supply and load
Communication tests	Communication indicator	Indicator LED flickers when the meter is connected to supply
	CIU display	CIU displays normally when paired with the meter.

DETAILED TESTS

TEST	TEST LOAD	ERROR VALUE	REMARKS
Accuracy Test	9.2A	-0.701%	PASSED; Meter accuracy is within the range of +/-1%
Internal visual examination	Foreign solder and glue were found added onto the circuit board.		
GENERAL REMARKS			CONCLUSION
Meter failed external and internal visual test.			Meter is Tampered with; Recommended for scrapping

Figure 3: Showing Report from UEDCL



Figure 4: Showing report from UEDCL

1.3 Objectives:

This document proposes the design and development of a prepaid energy meter tamper detector system for single-phase prepaid meter systems.

1.4 Specific objectives:

- To study the working principle of prepaid meters.
- To study the various techniques used by customers to tamper with prepaid meters
- To study and understand the available devices used for detecting tampered meters.
- To design and construct a proposed tamper detector prototype for pre-paid meters.
- To test the efficiency of the designed system.

1.5 Significance/Justification:

UEDCL-the utility company will benefit by making it simple to automatically know any tampering events that might happen remotely. The detector can also be used by field staff to check if magnets have been used for tampering without the hustle to open the meters. Also, the presence of an antitamper alarm will be a preventive approach to scare hackers from continuing with the bad act.

Consequently, the company will lower the losses due to electricity theft.

1.6 Scope:

The project seeks to design and construct a prepaid energy meter tamper detector system for prepaid systems. The device shall be based on an 8-bit RISC Atmel ATMEGA328P-PU microcontroller interfaced with a magnetic flux sensor, tilt sensor, current sensor, and voltage sensor. The LCD on the prototype will provide an alphanumeric display of the status of the meter subjected to a tamper test. The device shall be able to detect tampering by sensing meter tilt, touch, and light exposure of internal parts.

CHAPTER II: LITERATURE REVIEW.

2.0 Introduction.

This chapter analyses the existing literature and research relating to the project topic. It explains what the tamper-proof prepaid electricity energy meter system is and the need for embracing such a system as one of the key ways to ensure reduced losses in the energy sector due to illegal theft of electricity power in Uganda.

2.1 Types of Energy Meter Readers

2.1.1 Automatic Meter Reading (AMR) system

An Automatic Meter Reading (AMR) is the technology of automatically collecting data from water meters or energy metering devices (water, gas, and electric) and transferring that data to a central database for billing and analysis. This means billing can be based on actual consumption rather than an estimate of previous consumption, giving

customers better control over their use of electricity, gas, or water.

2.1.1.1 History of Automatic Meter Reading (AMR).

Automatic meter reading was first tested 30 years ago when AT&T conducted trials in cooperation with a group of utilities and Westinghouse, United States of America. After those successful experiments, AT&T offered to provide phone system-based AMR services at \$2 per meter. The price was four times more than the monthly cost of a person to read the meter, 50 cents. Thus, the program was considered economically unfeasible.

However, the modern era AMR began in 1985, when several major full-scale projects were implemented, which include;

Hackensack Water Co. and Equitable Gas Co. Were the first to commit to full-scale implementation of AMR on water and gas meters. In 1986, Minnegasco initiated a 450,000-point radio-based AMR system.

In 1987, Philadelphia Electric Co. was faced with a large number of inaccessible meters, and installed thousands of distribution line carrier AMR units to solve this problem. Thus, AMR is becoming more viable each day. Advances in solid-state electronics, microprocessor components, and low-cost surface-mount technology assembly techniques have been the catalyst to produce reliable, cost-effective products capable of providing the economic and human benefits that justify the use of AMR systems on a large, if not full-scale, basis. Originally, these devices just collected meter readings electronically and matched them with accounts. As technology advanced, additional data can now be captured, stored, and transmitted to the main computer [22]. (Tamarkin, September - October 1992)

2.1.2 Wireless Automatic Meter Reading System (WAMRS).

The main goal of the WAMRS project was to send periodical readings of an electricity meter wirelessly to a server in the billing office of the electricity supply company. Central points were covering each geographical area, since each premises unit would have a limited range of wireless coverage, while the central points would have long-

range wireless transmitters that could deliver the meter-reading data over long distances to the billing office. The server in the billing office had a highly secure database system, which enabled authorized staff members of the electricity supply company to read and print electricity bills. For premises out of the coverage area of any central point, the solution proposed was to make the nearest premises unit (covered by a central point) the central point for such remote premises. This added a constraint on the wireless device used for such a purpose because such a device should have the capability of both sending and receiving the data. (Tarik, July 2-4, 2008)

2.2 Energy Theft and Meter Tampering Techniques.

Meter tampering, in the broadest sense, is an illegal method employed by consumers to gain unauthorized entry into, break in to, or in some cases physically destroy an electricity meter in order to deplete its key functionalities, with the ultimate goal of reducing or completely eliminating the cost of energy usage. This fraudulent practice has grown into one of the most persistent, widespread, and financially devastating challenges confronting electricity utility providers across the globe. It directly undermines the revenue collection process upon which utility companies depend to fund their operational activities, maintain and expand their distribution infrastructure, and deliver reliable electricity services to all consumers within their service areas. The consequences of meter tampering extend far beyond the immediate financial losses suffered by the utility provider, affecting the broader economy, the quality and reliability of electricity supply, and the fairness of the energy billing system for all consumers, both honest and dishonest alike.

The act of meter tampering encompasses a remarkably wide spectrum of activities, ranging from crude and unsophisticated physical interference with the meter enclosure to highly technical and carefully planned electronic manipulation of the meter's internal measurement, recording, and communication systems. In some cases, tampering is carried out by individual consumers acting alone, motivated purely by the desire to reduce their personal electricity bills. In other cases, organized criminal networks have been found to be involved in systematic large-scale electricity theft operations, exploiting vulnerabilities in the distribution network across entire neighborhoods or industrial zones.

Regardless of the specific method employed or the scale at which it is practiced, the underlying objective of all forms of meter tampering remains fundamentally the same: to cause the electricity meter to record significantly less energy consumption than is actually being drawn from the network, or to bypass the metering process entirely, thereby allowing the consumer to use electricity without paying the correct amount or, in the most extreme cases, without making any payment whatsoever.

2.2.1 Global Scale and Economic Impact of Energy Theft.

The economic scale of the problem of energy theft at a global level is truly staggering and demands serious attention from governments, regulatory authorities, and utility providers alike. According to World Bank reports in 2009, annual electricity theft amounts to nearly \$90 billion worldwide, with well over half of that occurring in the world's emerging markets, including India, Brazil, and Russia. These figures, already alarming at the time of their publication, are widely believed to have increased significantly in the years since, as population growth, urbanization, and rising electricity demand have created new opportunities and incentives for energy theft in many parts of the developing world. The sheer magnitude of these losses underscores the fact that electricity theft is not merely a minor inconvenience or a localized problem but rather a systemic issue of global proportions that requires coordinated and technologically sophisticated responses from all stakeholders in the electricity supply chain.

In developing countries and emerging economies in particular, the financial losses attributable to electricity theft place an especially severe and disproportionate strain on the limited resources of utility companies and national governments. Unlike well-resourced utility providers in developed economies, which may be able to absorb a certain level of non-technical losses without immediate operational consequences, utility providers in developing nations such as Uganda often operate on thin financial margins and are heavily dependent on the efficient collection of revenue from all consumers to fund their day-to-day operations. When a significant proportion of the electricity delivered through the distribution network is stolen and goes unpaid for, the utility provider is forced to either absorb the resulting financial losses, which can threaten its long-term viability, or pass the costs on to paying consumers in the form of higher electricity tariffs.

Either outcome is deeply undesirable, as the former undermines the financial sustainability of the utility, while the latter places an unfair and regressive burden on honest consumers, many of whom may already be struggling with the high cost of electricity access.

Beyond the direct financial impact on utility providers, energy theft also has serious broader economic and social consequences. It discourages investment in the electricity sector by reducing the commercial attractiveness of utility operations and increasing the perceived risk for potential investors. It creates an uneven competitive playing field for businesses, as companies that steal electricity gain an unfair cost advantage over their law-abiding competitors who pay their electricity bills in full. It also contributes to the deterioration of power quality and supply reliability across the distribution network, as unauthorized connections and meter bypass arrangements can introduce additional loads and electrical disturbances that overload transformers, damage equipment, and cause voltage fluctuations and outages that affect all consumers in the vicinity. In extreme cases, illegal electrical connections made by untrained individuals can also create serious fire and electrocution hazards, posing a direct threat to public safety.

2.2.2 Historical Context and Evolution of Tampering Methods

Electricity theft is as old as the utility meter itself and draws on a variety of methods that alter the meter and its inputs in an attempt to influence the meter's energy measurements. From the very earliest days of commercial electricity supply in the late nineteenth and early twentieth centuries, a small but significant minority of consumers sought ways to manipulate the metering process for personal financial gain. The first electricity meters were relatively simple electromechanical devices, and the methods used to tamper with them were correspondingly straightforward, typically involving direct mechanical interference with the rotating disc or the meter's drive mechanism to slow or stop its rotation.

As metering technology evolved over the following decades, becoming progressively more sophisticated with the introduction of electronic components, digital processing, and ultimately smart metering systems with two-way communication capabilities, the techniques employed by fraudulent consumers evolved in parallel. Each new generation

of metering technology brought with it new vulnerabilities that could be exploited, and a new wave of tampering methods designed to take advantage of those vulnerabilities. This continuous technological arms race between meter manufacturers seeking to improve tamper resistance and fraudulent consumers or criminal networks developing new evasion methods has driven significant innovation in both metering technology and tamper detection systems, and continues to shape the development of modern electricity metering solutions to this day.

Understanding the full historical range and technical diversity of tampering techniques that have been documented across different metering technologies and geographic contexts is therefore an essential prerequisite for the design of an effective, comprehensive, and future-proof tamper detection solution. A detection system that addresses only a limited subset of known tampering methods, or that is designed without a thorough understanding of the adversarial context in which it must operate, will inevitably leave significant vulnerabilities unaddressed, reducing its overall effectiveness and allowing determined fraudsters to continue exploiting undetected loopholes.

2.2.3 Classification of Meter Tampering Techniques

The various methods of electricity theft and meter tampering documented in the technical literature and utility industry reports can be broadly organized into three major categories, namely physical tampering techniques, electrical bypass techniques, and electronic or logical attack techniques. Each of these categories exploits different aspects of the metering system's design and operational characteristics, and each presents distinct challenges for detection and prevention. A brief overview of each category is presented below, followed by a more detailed examination of the specific techniques within each.

2.2.3.1 Permanent magnet as a tamper:

In electronic meters, there are transformers, and hence, the placement of a magnet as close to this transformer as possible could cause overfluxing every half a cycle. This could cause a diode like affect in the meter electronics, and if the electronics are

designed to eliminate harmonics for calculating energy usage, then the magnet has let this person pay less for electricity, i.e., steal electricity.

Of course, good meters may also have a detection circuit for high harmonics and send a message back to the utility to say the harmonic level is too high, and a serviceman may then discover this magnet. However, this is not a feature in the current Yaka submeters.

Meters should offer compliance with the requirements of CBIP-304 and its amendments for tampering using external magnets. The meter should be immune to tampering using external magnets. The meters should be immune to 0.2T of A.C. magnetic fields and 0.5 T of D.C. magnetic fields, beyond which they should record as tamper if not immune."

2.2.3.2 Signal cable cutting.

Prepaid electricity meters rely on internal signal cables to connect critical components such as the sensing circuits, current transformers (CTs), voltage measurement circuits, token input module, relay switch, and communication modules. These internal signal cables carry electrical signals that allow the meter to correctly measure and record energy consumption.

Signal cable cutting is a tampering technique where a consumer intentionally cuts, disconnects, or interferes with these internal signal wires to manipulate meter operation.

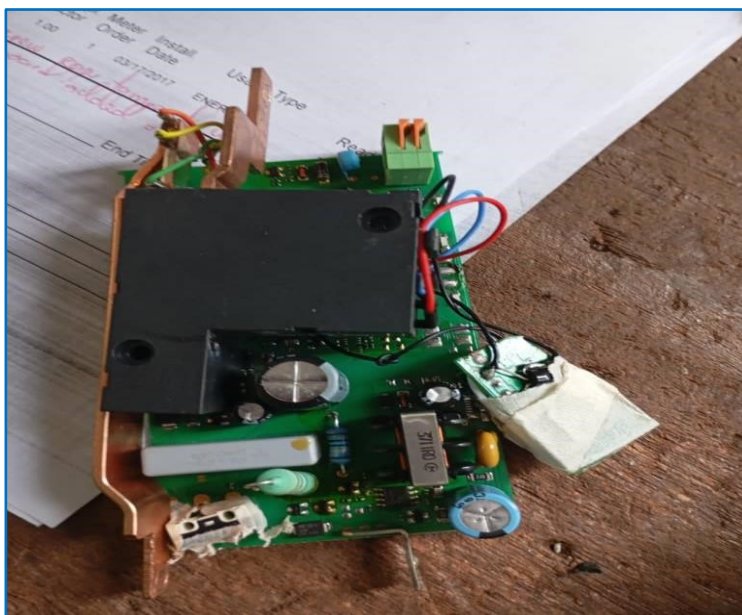


Figure 5: showing the green, red, and yellow signal wires

2.2.3.3 Tamper switch.

A tamper switch, also known as an anti-tamper switch, is a small sensor or electromechanical device installed inside prepaid electricity meters to detect unauthorized opening, physical interference, or manipulation of the meter enclosure. These devices represent one of the most fundamental and widely adopted hardware-level security mechanisms employed in modern electricity metering systems, serving as the first line of defense against physical tampering attempts that seek to gain unauthorized access to the internal components of the meter. By providing an immediate and reliable electrical signal in response to any unauthorized opening or physical disturbance of the meter enclosure, the tamper switch enables the metering system to detect, record, and report physical tampering events in real time, without relying on periodic manual

inspection or consumer self-reporting. The integration of tamper switches into prepaid electricity meters such as the Yaka meter is therefore a critical element of any comprehensive anti-tamper strategy, complementing other detection technologies to provide a robust and multi-layered defense against the full spectrum of physical interference techniques employed by fraudulent consumers.

The fundamental operating principle of a tamper switch is based on the detection of a change in the physical state of the meter enclosure, specifically the opening or displacement of the meter cover or casing. In its normal, undisturbed state, the tamper switch is held in a defined position by the closed meter enclosure, maintaining a specific electrical circuit condition, either normally open or normally closed, that represents the secure and uncompromised state of the meter. When the meter enclosure is opened or physically disturbed, the tamper switch is released from its compressed or engaged position, causing a change in the state of the internal electrical circuit. This state change produces an electrical signal that is detected by the meter's internal microcontroller or monitoring circuit, which interprets it as an indication that the meter enclosure has been opened or interfered with and responds accordingly by logging a tamper event, triggering an alarm, or initiating a communication sequence to notify the utility provider of the detected incident.

The main purpose of the tamper switch is to signal the utility company or log an internal event whenever someone attempts to open or interfere with the meter. This dual function of external notification and internal event logging is critically important for ensuring that tampering incidents are both recorded for future reference and reported to the utility provider in a timely manner, enabling an appropriate operational response. The internal logging function ensures that a permanent record of all detected tampering events is maintained within the meter's non-volatile memory, even in situations where real-time communication with the utility provider is temporarily unavailable due to network outages or signal disruptions. The external notification function, implemented in the proposed system through the GSM communication module, ensures that utility personnel are alerted to tampering incidents promptly, enabling them to dispatch field teams to investigate and address the identified meter within the shortest possible time.

2.2.3.3.1 Types and Construction of Tamper Switches

Tamper switches are available in a variety of designs and configurations, each suited to different installation environments, enclosure geometries, and performance requirements. The most commonly used types in electricity metering applications include mechanical push-button or plunger-type switches, microswitch-based tamper detectors, reed switches, and optical tamper detection systems. Understanding the construction and operating characteristics of each type is important for selecting the most appropriate tamper switch technology for a given metering application.

Mechanical plunger-type tamper switches are among the most widely used and straightforward tamper detection devices in prepaid electricity meters. These switches consist of a spring-loaded plunger mechanism housed within a compact body that is mounted on the interior surface of the meter enclosure. When the meter cover is in its closed and secured position, it presses against the plunger, compressing the internal spring and holding the switch in its actuated state. In this actuated state, the switch maintains a defined electrical circuit condition, typically a closed circuit in the case of a normally closed switch, that represents the secure state of the meter. When the meter cover is opened or removed, the mechanical pressure on the plunger is released, and the compressed spring pushes the plunger back to its resting position, causing the switch to transition to its unactuated state and changing the electrical circuit condition accordingly. This transition from the actuated to the unactuated state produces the tamper detection signal that is monitored by the meter's microcontroller. The simplicity, reliability, and low cost of mechanical plunger-type tamper switches make them the most commonly adopted solution in mass-produced prepaid electricity meters, including those used in Uganda's Yaka metering system.

Microswitch-based tamper detectors operate on a similar principle to plunger-type switches but use a precision snap-action microswitch mechanism that provides a highly reliable and repeatable switching action with a very small actuation force and displacement. Microswitches are characterized by their extremely long mechanical life, typically rated for millions of switching cycles, and their precise and consistent switching point, which ensures that the tamper detection signal is generated reliably and at a well-

defined point in the opening motion of the meter cover. These characteristics make microswitch-based tamper detectors particularly suitable for applications where high reliability and consistent performance over a long operational lifetime are required.

Reed switches represent an alternative tamper detection technology that uses magnetic actuation rather than direct mechanical contact to detect the opening of the meter enclosure. A reed switch consists of two thin ferromagnetic contact blades sealed within a glass or plastic tube, positioned in close proximity to each other but not in contact under normal conditions. When a permanent magnet is placed near the reed switch, the magnetic field causes the ferromagnetic blades to be attracted to each other, making electrical contact and closing the circuit. In a reed switch-based tamper detection arrangement, a small permanent magnet is attached to the removable meter cover, and the reed switch is mounted on the interior of the meter body in alignment with the magnet. When the cover is in its closed position, the magnet holds the reed switch in its actuated state. When the cover is opened and the magnet moves away from the reed switch, the magnetic field weakens, causing the contact blades to spring apart and opening the circuit, thereby generating the tamper detection signal. Reed switch-based tamper detectors offer the advantage of contactless actuation, which eliminates the mechanical wear associated with direct-contact switches and can extend the operational lifetime of the tamper detection mechanism significantly.

Optical tamper detection systems represent a more advanced approach to enclosure tamper detection, using a light source and a photodetector to sense the opening of the meter cover. In a typical optical tamper detection arrangement, an infrared LED and a photodetector are mounted within the meter enclosure in such a way that the meter cover blocks the light path between them when closed. When the cover is in place, the photodetector receives no light from the LED and produces a corresponding output signal indicating the secure state. When the cover is opened or removed, the blocked light path is restored, the photodetector receives the infrared light from the LED, and the resulting change in its output signal is detected by the meter's microcontroller as a tamper event. Optical tamper detection systems are completely non-contact in their operation, immune to mechanical wear, and capable of detecting even very small

openings of the meter cover, making them highly sensitive and reliable. However, their greater complexity and higher cost compared to mechanical switch solutions mean that they are typically reserved for higher-specification metering applications where the enhanced performance justifies the additional expense.

2.2.3.3.2 Integration with Microcontroller-Based Metering Systems

The integration of a tamper switch with a microcontroller-based metering system, such as the ATmega328P platform used in the proposed Yaka meter tamper detection system, is a relatively straightforward process that leverages the digital input capabilities of the microcontroller to monitor the state of the tamper switch output in real time. The tamper switch is connected between a general-purpose input/output (GPIO) pin of the microcontroller and either the supply voltage or ground, with an appropriate pull-up or pull-down resistor used to define the logic level at the GPIO pin when the switch is in its open state. When the tamper switch changes state in response to the opening of the meter enclosure, the voltage level at the connected GPIO pin changes accordingly, transitioning from a logic high to a logic low or vice versa depending on the specific switch configuration and circuit design.

The microcontroller can be configured to detect this change in GPIO pin state through two primary methods: software polling and hardware interrupt-driven detection. In the polling approach, the microcontroller periodically reads the state of the tamper switch GPIO pin within its main program loop and compares the current reading with the expected secure state value. If a discrepancy is detected, the microcontroller identifies this as a tamper event and initiates the appropriate response sequence. While simple to implement, the polling approach introduces a latency in tamper event detection that is determined by the polling interval, which may be unacceptable in applications requiring very rapid response to tampering attempts.

The interrupt-driven approach offers a superior alternative in which the tamper switch GPIO pin is configured as an external interrupt input on the ATmega328P microcontroller. When the state of the pin changes due to a tamper switch actuation, the microcontroller's hardware interrupt system immediately suspends the current program execution and transfers control to a dedicated interrupt service routine (ISR) that handles the tamper

event response. This approach ensures that tamper events are detected and responded to with the minimum possible latency, regardless of what other tasks the microcontroller may be performing at the time of the tampering event. The use of interrupt-driven tamper detection is therefore the preferred implementation approach in the proposed system, as it maximizes the responsiveness and reliability of the tamper detection function without imposing a significant additional burden on the microcontroller's processing resources.

Upon detection of a tamper switch actuation event, the ATmega328P microcontroller in the proposed system initiates a predefined response sequence that includes logging the tamper event with a timestamp to the meter's internal non-volatile memory, activating any local alarm indicators such as LEDs or buzzers that may be incorporated into the system design, and initiating a GSM communication sequence through the SIM800L module to transmit an SMS alert notification to the designated utility provider contact number at UEDCL. This multi-stage response ensures that the tampering event is both permanently recorded within the meter and promptly communicated to the utility provider, enabling a timely and informed operational response to the detected incident.

2.2.3.3.3 Importance of Tamper Switches in the Proposed System

In the context of the proposed Yaka meter tamper detection system, the tamper switch serves as a dedicated and highly reliable sensor specifically designed to detect the most fundamental form of physical meter tampering, namely the unauthorized opening or removal of the meter enclosure. While other sensors integrated into the system, such as the current sensor, tilt sensor, and magnetic field sensor, provide detection coverage for specific types of tampering activity, the tamper switch provides direct and unambiguous detection of any attempt to physically access the interior of the meter, which is a prerequisite for many of the more sophisticated tampering techniques described in Section 2.2. By detecting enclosure opening events immediately and reliably, the tamper switch effectively serves as a gatekeeper that can identify tampering attempts at the earliest possible stage, before any further manipulation of the meter's internal components has the opportunity to occur.

Furthermore, the tamper switch provides detection coverage for tampering scenarios that might not be captured by the other sensors in the system. For example, a consumer who

opens the meter enclosure to inspect its internal components, without yet making any modifications that would be detectable by the current or magnetic field sensors, would be immediately identified by the tamper switch as having made an unauthorized access attempt. Similarly, a consumer who attempts to disable or bypass the other tamper detection sensors by physically disconnecting them from the microcontroller would first need to open the meter enclosure, an action that would be immediately detected and reported by the tamper switch before any further interference could take place. This layered detection capability, in which the tamper switch provides an overarching physical access detection function that complements the more specific detection functions of the other sensors, is a key factor in the overall effectiveness and robustness of the proposed tamper detection system.

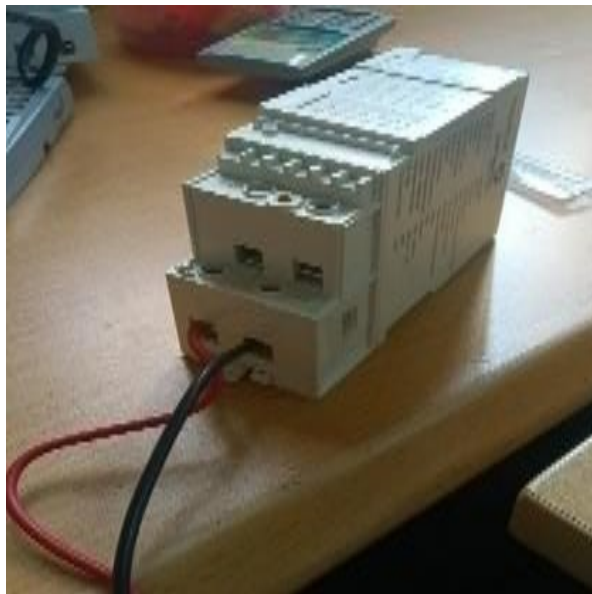


Figure 6: showing a meter without a tamper cover

2.2. 3.4 Inserting a foreign body.

Inserting foreign bodies into prepaid electricity meters is a deliberate and calculated tampering method in which physical objects such as metal wires, needles, paper clips, blades, conductive foils, or plastic strips are intentionally pushed, inserted, or forced into the internal cavities of the meter through available external openings. These openings may include ventilation slots cut into the meter enclosure to allow heat dissipation from internal electronic components, gaps around the keypad or token entry interface, spaces around the terminal block where the supply and load conductors enter and exit the meter, or any other aperture or clearance that provides a pathway from the external surface of the meter to its internal electronic circuitry. The primary objective of this tampering technique is to physically interfere with the internal components of the meter in a manner that disrupts its normal measurement, recording, or communication functions, ultimately causing the meter to under-register actual energy consumption or to cease functioning as a metering device entirely, thereby allowing the consumer to use electricity without paying the correct amount.

This method of tampering is particularly concerning from a utility provider's perspective because it can be carried out without requiring the complete removal or forced opening of the meter enclosure, making it significantly harder to detect through routine visual inspection than tampering methods that involve obvious physical damage to the meter casing or seals. A consumer employing this technique can insert a foreign object through an existing ventilation slot or keypad gap in a matter of seconds, without leaving any immediately obvious external evidence of interference, and the resulting internal damage or disruption may not become apparent until a detailed technical inspection of the meter's internal components is carried out. Furthermore, in some cases, the inserted object may be deliberately chosen to be thin enough to pass through the available openings without causing any visible deformation of the meter enclosure, making the tampering even more difficult to identify through external examination alone.

2.2.3.4.1 Types of Foreign Bodies Used and Their Characteristics

The specific types of foreign bodies used in this tampering method vary widely depending on the availability of materials, the physical dimensions of the accessible openings in the meter enclosure, and the specific interference effect that the individual carrying out the tampering intends to achieve. However, the most commonly reported foreign objects used in this type of meter tampering can be broadly categorized into conductive metallic objects and non-conductive or semi-conductive objects, each of which interacts with the meter's internal components in different ways to produce different types of disruption.

Conductive metallic objects represent the most commonly used and potentially most damaging category of foreign bodies employed in meter tampering. Objects in this category include thin metal wires stripped from electrical cables, sewing needles, steel paper clips that have been straightened to form thin probes, razor blades or blade fragments, metal foil strips cut from food packaging or capacitor materials, and thin metallic rods or pins of various dimensions. The defining characteristic shared by all metallic foreign bodies is their high electrical conductivity, which gives them a very low electrical resistance. This low resistance property is the key to understanding the electrical damage mechanism associated with the insertion of metallic foreign bodies into the meter's internal circuitry, as explained in detail in the following subsection.

Non-conductive or semi-conductive foreign bodies, such as plastic strips, thin cardboard, or rubber fragments, may also be inserted into prepaid meters with the intention of causing mechanical interference rather than electrical disruption. These objects can be used to physically obstruct the movement of mechanical components within the meter, to wedge open or hold shut internal switching contacts, to block ventilation pathways and cause thermal overloading of internal components, or to physically displace sensors or circuit board components from their correct positions. While non-conductive foreign bodies cannot cause the electrical short circuit effects associated with metallic objects, they can still produce significant disruption to the meter's mechanical and thermal

operating environment, potentially causing measurement errors, component failures, or complete meter malfunction.

2.2.3.4.2 Electrical Effects of Conductive Foreign Body Insertion

The insertion of a conductive metallic object into the internal circuitry of a prepaid electricity meter can produce a range of harmful electrical effects, the most significant and immediately damaging of which is the creation of an unintended short circuit between conductors or circuit nodes that are normally electrically isolated from one another. The relationship between the resistance of the inserted metallic object and the resulting electrical effects can be understood through the fundamental principles of electrical circuit theory, specifically Ohm's Law, which states that the current flowing through a conductor is inversely proportional to its resistance for a given applied voltage. This relationship is expressed mathematically as:

$$I = \frac{V}{R}$$

Where I represents the current flowing through the conductor in Amperes, V represents the voltage applied across the conductor in Volts, and R represents the electrical resistance of the conductor in Ohms. From this relationship, it is immediately apparent that:

Low Resistance (R) → High Current (I)

When a metallic foreign body with very low electrical resistance is inserted into the meter and makes contact with two or more conductors or circuit nodes that are normally at different electrical potentials, it creates a low-resistance pathway between

those nodes through which a very large current can flow. This excessive current flow, driven by the voltage difference between the shorted nodes and limited only by the very low resistance of the metallic foreign body and the internal impedance of the supply source, can produce several serious and potentially irreversible electrical effects within the meter's internal circuitry.

The most immediate consequence of a short circuit created by a metallic foreign body is the generation of a large amount of heat within the shorted pathway, in accordance with Joule's Law of electrical heating, which states that the power dissipated as heat in a conductor is proportional to the product of the resistance of the conductor and the square of the current flowing through it, expressed as $P = I^2R$. Even though the resistance of the metallic foreign body may be very low, the extremely large short circuit current that flows through it can generate sufficient heat to cause thermal damage to adjacent components, melt insulation on nearby conductors, or in extreme cases initiate a fire within the meter enclosure. Beyond the immediate thermal effects, the large short circuit current can also stress and permanently damage sensitive electronic components connected to the affected nodes, including integrated circuits, transistors, capacitors, and other semiconductor devices that form part of the meter's measurement and processing circuitry.

The current sensing elements of the prepaid meter are particularly vulnerable to damage from the electrical effects of conductive foreign body insertion. Current sensors, including both current transformer-based and Hall Effect-based sensing elements, are precision devices designed to operate within specific current and magnetic flux ranges that correspond to the expected range of load currents in the metering application. When a short circuit caused by a metallic foreign body drives an excessively large current through the current sensing element or its associated circuitry, the resulting overcurrent condition can saturate the magnetic core of a current transformer, driving it into a nonlinear operating region where its output no longer accurately represents the actual current being measured. In the case of Hall Effect sensors, the extremely large

magnetic field associated with the short circuit current can exceed the linear operating range of the Hall sensing element, causing it to produce a saturated or distorted output signal that does not correctly represent the measured current. In more severe cases, the overcurrent condition can physically damage the current sensing element itself, causing it to produce no output signal at all or to generate a permanently incorrect output that causes the meter to systematically under-read or completely fail to register energy consumption.

2.2.3.4.3 Effects on Current Sensors and Metering Accuracy

The damage or disruption caused to the current sensing elements of the prepaid meter by the insertion of conductive foreign bodies has a direct and immediate impact on the accuracy of the meter's energy consumption measurements. Since the current sensor is the primary element responsible for measuring the magnitude of the electrical current being drawn by the consumer's load, any impairment of the sensor's accuracy or functionality directly translates into errors in the meter's calculated energy consumption values. These errors can manifest in several distinct ways depending on the nature and severity of the damage inflicted on the current sensing element.

In cases where the foreign body insertion causes partial damage or saturation of the current sensing element, the sensor may continue to produce an output signal but with a significantly reduced sensitivity or a shifted zero reference point. This means that the sensor will underestimate the actual current being drawn by the consumer's load, causing the meter to calculate and record an energy consumption value that is systematically lower than the true value. From the consumer's perspective, this results in lower electricity bills that do not accurately reflect their actual energy usage, effectively allowing them to consume more electricity than they are paying for. From the utility provider's perspective, this represents a direct and ongoing revenue loss that may go undetected for extended periods if the meter's recorded consumption values are not compared against expected consumption profiles or physically verified through independent measurement.

In the most severe cases, where the foreign body insertion causes complete failure or destruction of the current sensing element, the sensor may cease to produce any output signal at all. In this scenario, the meter's processing unit receives no current measurement data and may respond by displaying a zero consumption reading, generating an error code, or reverting to a default fault state. Depending on the specific firmware implementation of the meter, a complete current sensor failure may cause the meter to stop registering any energy consumption entirely, effectively providing the consumer with free electricity for as long as the sensor failure remains undetected and unrepaired. This represents the most financially damaging possible outcome of the foreign body insertion tampering technique and underscores the critical importance of implementing robust tamper detection mechanisms that can identify current sensor failures and other anomalous meter conditions in real time.

2.2.3.4.4 Mechanical, Electrical, and Magnetic Disruption Effects

Beyond the specific effects on current sensing accuracy described above, the insertion of foreign bodies into prepaid electricity meters can produce a broader range of mechanical, electrical, and magnetic disruption effects that collectively compromise the meter's overall measurement integrity and operational reliability. Understanding these broader disruption mechanisms is important for appreciating the full scope of the threat posed by this tampering technique and for designing detection and prevention measures that address all of its potential consequences.

From a mechanical perspective, the physical presence of a foreign object within the meter enclosure can interfere with the normal operation of any mechanical components present within the meter, including switches, relay contacts, token entry mechanisms, and display assemblies. A foreign object that becomes lodged between moving mechanical parts can prevent them from operating correctly, causing switches to remain permanently open or closed regardless of the intended control signal, relay contacts to fail to make or break the circuit as required, or the token entry mechanism to jam and prevent the legitimate entry of prepayment tokens. Any of these mechanical

interference effects can disrupt the normal operation of the meter in ways that may be exploited by the fraudulent consumer to avoid correct registration of energy consumption or to prevent the disconnection of supply when the prepaid credit is exhausted.

From an electrical perspective, in addition to the short circuit effects described earlier, the insertion of a conductive foreign body can also cause unintended connections between signal lines within the meter's processing circuitry, introducing unwanted electrical noise, interference, or signal corruption that degrades the accuracy of the meter's measurements. Even in cases where the inserted foreign body does not create a direct short circuit between power supply nodes, its presence near sensitive signal processing circuitry can introduce capacitive or resistive coupling effects that distort the measurement signals being processed by the meter's microcontroller, leading to systematic measurement errors that cause the meter to under-register consumption without any obvious indication of malfunction.

From a magnetic perspective, the insertion of certain types of metallic foreign bodies, particularly those made from ferromagnetic materials such as iron or steel, can distort the magnetic field environment within the meter enclosure in ways that affect the accuracy of any magnetic field-sensitive measurement components present within the meter. Hall Effect current sensors and current transformers are both sensitive to the magnetic field environment in their vicinity, and the presence of a ferromagnetic foreign body near these components can alter the distribution of the magnetic flux that they rely on for accurate current measurement, introducing systematic errors that cause the meter to under-read or over-read the actual current. The combination of these mechanical, electrical, and magnetic disruption mechanisms means that the insertion of foreign bodies into prepaid electricity meters has the potential to compromise virtually every aspect of the meter's measurement and control functions, making it one of the most broadly damaging tampering techniques in terms of its impact on metering accuracy and system integrity.

2.2.3.4.5 Implications for the Proposed Tamper Detection System

The foreign body insertion tampering technique presents specific and important implications for the design and implementation of the proposed Yaka meter tamper detection system. Since this tampering method does not necessarily require the complete removal or forced opening of the meter enclosure, it may not always be detected by the tamper switch alone, particularly if the foreign body is inserted through an existing ventilation slot or other aperture without disturbing the meter cover. This means that the detection of foreign body insertion events requires additional sensing capabilities that can identify the downstream effects of the tampering on the meter's electrical and measurement systems, rather than relying solely on the detection of physical enclosure access.

The current sensor integrated into the proposed tamper detection system plays a particularly important role in detecting the effects of foreign body insertion, as the disruption of the meter's internal current sensing elements caused by this tampering technique will typically produce abnormal current measurement readings that deviate significantly from the expected values for the connected load. By continuously monitoring the output of the current sensor and comparing it against predefined normal operating thresholds, the ATmega328P microcontroller can detect anomalous current measurement conditions that may be indicative of sensor damage or disruption caused by foreign body insertion, and respond by logging a tamper event and transmitting an alert to UEDCL via the GSM module.

Furthermore, the physical disturbance caused by the insertion of a foreign object through the meter enclosure may also produce a detectable change in the meter's orientation or vibration profile, which could be captured by the tilt sensor integrated into the proposed system. While the tilt sensor is primarily designed to detect deliberate repositioning or displacement of the entire meter unit, it may also respond to the mechanical disturbance associated with the forceful insertion of a foreign object, providing an additional layer of detection coverage for this tampering technique. The

combination of current sensor monitoring, tilt detection, and tamper switch-based enclosure access detection within the proposed multi-sensor detection architecture therefore provides a comprehensive and overlapping detection capability that maximizes the probability of identifying foreign body insertion tampering events across the full range of scenarios in which they may occur.

2.2.3.5 Other tamper techniques:

Attacking its memory through hardware, with insufficient protective features, all that one needs is to insert a needle on each side of the device's memory chip. The needle intercepts the electrical signals in the memory chip. From these signals, a device's programming can be determined.

Using a digital radio to hack a Smart Meter, the two-way radio chip in a smart meter allows the device to be read remotely and receive commands over the network. A hacker, who has cracked the smart meter's programming, can use security codes from the software in the chip to get on the network and issue commands.

Accessing the meter; another method of hacking the smart meter is through a wireless device. Using a software radio programmed to mimic a variety of communication devices, a hacker can listen in on wireless communications in the network and, over time, guess how to communicate with the meter. Another method is to steal a smart meter and reverse-engineer it; although inexpensive, the process would require a good knowledge of integrated circuits.

Measuring the Smart Meter's electrical consumption; Inside smart meters are sensors that measure energy consumption. Under the old mechanical meters, interfering with the meter's ability to report accurately has been the means of many unscrupulous individuals to save money on electricity, such as by the use of magnets. The old method used with analog meters may not be difficult to use in fooling the old meters, but the

new generation of smart meters was designed to protect against such automated methods.

2.3 Related Projects and Experiments.

In the last few decades, with the development of embedded systems involving wireless and sensor technologies, several works have focused on the automation of power and energy systems. Amongst these works are: Mr. Nazir Bin Abdullah [18] developed an automatic meter reading system (Automation of Residential Electricity Cut off using Embedded controller) in 2012 for domestic users. In this project, he used a GSM modem for transmitting and receiving information, both sides mean the user side and the energy side.

Recently, a system entitled “Design and implementation of SMS based control for monitoring systems” was developed, and it presents three modules involving a sensing unit for monitoring the complex applications, a processing unit that is a microcontroller, and a communication module that uses a GPRS modem or cell phone via serial port RS-232. The SMS is used for status reporting, such as power failure [17].

Mr. Hung Cheng Chen [23] proposed a wireless automatic meter reading system in 2012. In this project, he used a ZigBee module on both sides. This technology is cheap and low-cost.

In 2010, Mr. H.G.Rodney Tan and Mr. Mejbau Haque [19, 20] developed an automatic power meter reading system using GSM network infrastructure in 2007. In this system, a GSM digital power meter was installed in every consumer unit and an electricity e-billing system on the energy provider side. This project was based on a single-phase digital prepaid energy meter for an improved meter and billing system.

One of the sophisticated ways of stealing electricity is tampering with the secondary side of the current transformers (CT) of the energy meter. If CT is tampered with, then it will not be able to measure the correct current passing from the energy meter to the consumer, or it will record slow readings. This kind of theft is easily detected in smart meters by the option of “EL” glowing. EL is an option in a smart meter, whose Light

Emitting Diode (LED), when it flashes, shows certain points, such as when the mismatch between the phase and neutral current is detected. (Anas et al., 2012)

2.4 The Existing Energy Metering Systems.

2.4.1 Prepaid metering

This is a digital metering system in which payments for the bills are made either by using prepaid cards or scratch numbers. These systems have algorithms for reading cards and determining the right scratched number. They operate in such a way that when the prepaid amount is used up, an automatic disconnection is performed in the meter. UMEME advanced to this system to allow clients to monitor their electricity usage in their houses/premises, give customers complete control of their electricity budget, and promote convenience in paying for their electricity bills since customers will be able to purchase electricity from more than one outlet, such as supermarkets and shops [9].

2.4.2 Automatic meter reading.

This is a digital system that is employed to automate the reading of the power units from the clients' side, and billing is also done automatically by the billing server. This method has some security features in that when a request to the metering system is made from the central system, and the system happens to be off, then suspicious action will have been anticipated on the distributor side, after which follow-ups can be made.

This AMR system consists of three main parts: an accurate digital meter, a transmission facility, and the billing server. To make an affordable AMR system, low-cost off-the-shelf materials are used [14]. (Al-Omary et al., 2011)

2.4.3 Personalized digital meter.

This system came as an improvement in the analog meters. It reads digital values of current and voltage. This system has solved some of the problems that were in analog meters, like reversal of current in the meter, easy opening of the meter's internal system while altering its architecture, and disconnection of the meter's neutral wire, among

others.

2.4.4 Physical monitoring.

Here, UEDCL Company sends the technical teams of employees to investigate the problems with the metering in the different households of the customers. In case of misuse of electricity, the customer is denied the right to use power by disconnecting their supply lines. In this way, the victims of power theft have been partially captured, and therefore, the power theft issue is being partially resolved.

2.5 The Proposed Project: Prepaid Energy Meter Tamper Detection System.

The proposed system shall be in a position to detect tampering with the energy meters in real time and send notifications to the area manager about what happens at the site. It consists of a microcontroller, which includes an independent RTC that has its own power domain and is thus decoupled from the rest of the system. The independent RTC is enabled at all times by running on the main supply, V_{DD} , when the main supply is available, and automatically switches to battery supply V_{BAT} in the event of main power failure.

The independent RTC is capable of detecting a fall in the main supply, V_{DD} , at a certain threshold, below which it automatically switches to a battery supply, and only the RTC and its oscillation are kept working, with the rest of the microcontroller powered off.

Protection against battery removal: Removal of the battery when power is unavailable allows the hacker to manipulate the system and then reconnect the battery as if nothing had happened. The independence of RTC includes its reset, clock, and power sources. On removal of this independent power source while the device is powered off, the independent RTC is reset when the battery is reconnected and defaults to a tampered state. The independent RTC detects the removal of the battery and then generates the internal tamper interrupts to the microcontroller.

Protection against external tampering to the system: Several attacks, including alteration of certain signals, damaging of the casing, etc., the independent RTC monitors and detects these intrusions by having support for off-chip anti-tamper switches that can be connected to the microcontroller dedicated anti-tamper pins, and since these switches needs to be monitored all time, they are powered by battery, V_{BAT} and incorporating sensors like touch and tilt to detect the harsh and sensitive handling of the system. Therefore, the notifications are sent to the area manager in realtime about what is happening on the site, and the alarm system is also initialized upon detection of such tampering.

2.6 Comparison between the existing system and the proposed system.

Parameters considered	Existing systems	A system with PEMNS as a subsystem
The cost of running	Expensive since they require physical manpower in monitoring theft and misuse cases	Cheap since, after deployment, the system controls itself
Level of automation	Some existing systems, such as the physical monitoring, and others have a low level of automation, like AMR, where theft is detected only when the meter is OFF	The level of automation is high since, after the detection of electricity misuse, it will perform switching without anybody's

		intervention
Time at which theft or misuse is realized	In most of these systems, theft or misuse of power is realized after a long time, due to frequent auditing of these meters	Theft or misuse of power is realized early.
Reliability	These systems are unreliable since the stakeholders, especially the workers, are corrupted by taking bribes from the victims of power theft or misuse	The system is reliable since the operation(s) are hardware automated

2.7 The Technology in the Proposed System.

2.7.1 The GSM Technology.

Global System for Mobile Communications (GSM) is a standard developed by the European Telecommunication Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices, first deployed in Finland in July 1991. As of 2014, it has become the default global standard for mobile communication, operating in over 219 countries and territories worldwide. The development of GSM marked a significant milestone in the evolution of wireless communication, transitioning the telecommunications industry from first-generation (1G) analog systems to a more robust, efficient, and standardized digital framework. This transition brought with it greatly improved voice quality, enhanced security features, and the ability to support data services, fundamentally transforming the way devices communicate over cellular networks.

The GSM standard operates on several frequency bands, most commonly the 850 MHz,

900 MHz, 1800 MHz, and 1900 MHz bands, allowing it to function across a wide range of geographic and regulatory environments. The use of Time Division Multiple Access (TDMA) technology enables multiple users to share the same frequency channel by dividing the signal into different time slots, thereby making efficient use of the available radio spectrum. This architectural design was a key factor behind GSM's rapid global adoption, as it allowed network operators to serve large numbers of subscribers simultaneously without significant degradation in service quality.

GSM network provides global coverage across countries, thus enabling communication to every nook and corner without the need to implement a new communication infrastructure solely for this purpose. This is a particularly important advantage in the context of the proposed tamper detection system for Yaka prepaid meters. Rather than investing in the design and deployment of a dedicated proprietary communication network – which would be both costly and time-consuming – the proposed system leverages the already existing and well-established GSM infrastructure. This means that tamper alerts and notifications generated by the metering system can be transmitted instantly to the utility provider, UEDCL, through the same cellular network that is already operational and widely accessible across Uganda. This significantly reduces the overall cost and complexity of the system deployment, while at the same time ensuring reliable and wide-reaching communication coverage, even in remote or rural areas where other forms of communication infrastructure may be limited or entirely unavailable.

Apart from seamless coverage, the GSM technology also provides services like SMS (Short Message Service) and GPRS (General Packet Radio Service) for requesting and retrieving readings from individual houses back to the energy provider wirelessly. SMS is a lightweight, low-bandwidth communication service that allows short text messages to be transmitted between devices over the GSM network. In the context of the proposed system, SMS serves as the primary medium through which tamper alert notifications are sent from the metering unit to the utility provider or designated personnel whenever a tampering event is detected. The simplicity and reliability of SMS make it an ideal choice for this application, as it does not require an active internet connection, functions effectively even on low signal strength, and is supported by virtually all GSM-enabled

devices and modules, including the SIM800L GSM module employed in this project.

GPRS, on the other hand, is a packet-oriented mobile data service available on GSM networks that enables devices to transmit data over the internet at moderate speeds. GPRS extends the capabilities of the GSM network beyond simple voice calls and text messages, allowing for the wireless transmission of larger volumes of data, such as energy consumption logs, meter status reports, and historical tamper event records, from individual meters back to the utility provider's central monitoring system. This makes it possible for UEDCL to not only receive real-time tamper alerts but also to remotely monitor the operational status of meters across its distribution network, thereby improving the overall efficiency and responsiveness of the energy management process. The combination of SMS and GPRS services within a single GSM framework therefore provides a flexible and scalable communication solution for the proposed tamper detection system.

Moreover, the GSM network is a more efficient, reliable, and secure communication standard that has been widely used for more than several decades without any significant technical issues. The security features inherent in the GSM standard, including subscriber authentication using a SIM (Subscriber Identity Module) card and encryption of transmitted data over the air interface, help to protect the integrity and confidentiality of the information exchanged between the metering unit and the utility provider. This is especially important in a tamper detection application, where the authenticity and accuracy of transmitted alerts are critical to ensuring an appropriate and timely response from the utility company. Any unauthorized interception or manipulation of the communication channel could otherwise compromise the effectiveness of the entire detection system.

The low cost, simple setup, wide operating distance, and minimal human intervention required are some of the other salient features of this GSM-based system. GSM modules such as the SIM800L, which is used in the proposed design, are commercially available at relatively low prices, making them accessible for integration into low-cost metering solutions without significantly increasing the overall system budget. The setup process for a GSM-based communication link is straightforward, typically requiring only the

insertion of an active SIM card and the configuration of a few software parameters within the microcontroller firmware to establish a functional communication link. Furthermore, once the system is deployed and operational, it requires very little ongoing human intervention, as the transmission of tamper alerts is fully automated and triggered directly by the detection logic embedded within the ATmega328P microcontroller. This autonomous operation reduces the dependence on manual monitoring and ensures that tamper events are reported promptly and consistently, regardless of the time of day or the availability of on-site personnel.



Figure 7:showing GSM Illustration

2.7.2 The SMS Technology.

The Short Message Service (SMS) allows text messages to be sent and received to and

from mobile telephones. The text can comprise words, numbers, or an alphanumeric combination. SMS was created as part of the GSM Phase 1 standard. The first short message is believed to have been sent in December 1992 from a PC to a mobile phone on the Vodafone GSM network in the UK. Each short message is up to 160 characters in length when the Latin alphabet is used and 70 characters in length when non-Latin alphabets such as Arabic and Chinese are used.

There is no doubting the success of SMS. The market in Europe alone had reached over three billion short messages per month as of December 1999, despite little proactive marketing by network operators and phone manufacturers. Key market drivers over the next two years, such as the Wireless Application Protocol (WAP), will continue this growth path.

Typical uses of SMS include notifying a mobile phone owner of a voicemail message, alerting a salesperson of an inquiry, and telling a driver the address of the next pickup. (short message systems, 2010)

SMS is essentially similar to paging, but SMS messages do not require the mobile phone to be active and within range, as they will be held for many days until the phone is active and within range. SMS messages are transmitted within the same cell or to anyone with roaming capability. They can also be sent to digital phones from a website equipped with a PC Link or from one digital phone to another. An SMS gateway is a website that lets you enter an SMS message to someone within the cell served by that gateway or acts as an international gateway for users with roaming capability.

The SMS is a store-and-forward service. In other words, short messages are not sent directly from sender to recipient, but via an SMS Center. Each mobile telephone network that supports SMS has one or more messaging centers to handle and manage the short messages.

The SMS features confirmation of message delivery. This means that, unlike paging, users do not simply send a short message and trust and hope that it gets delivered. Instead, the sender of the short message can receive a return message notifying them whether the short message has been delivered or not.

Short messages can be sent and received simultaneously with GSM (Global System for Mobile Communications) voice, data, and fax calls. This is possible because, whereas voice, data, and fax calls take over a dedicated radio channel for the duration of the call, short messages travel over and above the radio channel using the signaling path. As such, users of SMS rarely, if ever, get a busy or engaged signal as they can during peak network usage times. (Cretkovic, June 2005)

Ways of sending multiple short messages are available. SMS concatenation (stringing several short messages together) and SMS compression (getting more than 160 characters of information within a single short message) have been defined and incorporated in the GSM SMS standards.

The network operator needs to purchase its first-generation SMS Center as part of the network commissioning plan. The initial SMS Center may simply be a voice mail platform module or a stand-alone SMS Center. It is not possible to make the SMS available without an SMS Center, since all short messages pass through the SMS Center

2.7.3 Current sensor.

A current sensor is an electronic device designed to detect and measure the flow of electrical current, expressed in Amperes, through a wire or electrical circuit. These devices play a fundamental role in a wide range of electrical and electronic systems by providing accurate, real-time information about the magnitude and behavior of current flowing through a conductor. By monitoring current flow, these sensors enable systems to detect anomalies, protect equipment from damage, and ensure that electrical networks operate within their intended parameters. In the context of the proposed Yaka meter tamper detection system, the current sensor serves as a critical component for identifying irregular current flow patterns that may be indicative of tampering or unauthorized manipulation of the metering unit.

The operating principle of most modern current sensors is based on the Hall Effect, a phenomenon discovered by physicist Edwin Hall in 1879. The Hall Effect describes the production of a voltage difference, known as the Hall voltage, across an electrical

conductor or semiconductor when a magnetic field is applied perpendicular to the direction of current flow. When electrical current flows through a conductor, it generates a surrounding magnetic field whose strength is directly proportional to the magnitude of the current. A Hall Effect current sensor exploits this relationship by positioning a Hall Effect sensing element in proximity to the current-carrying conductor, where it detects the induced magnetic field and produces a corresponding output voltage or signal that is proportional to the current being measured. This output signal can then be read and processed by a microcontroller or signal processing unit to determine the actual current value in the circuit.

One of the most significant advantages of Hall Effect-based current sensors is that they provide galvanic isolation between the current-carrying conductor and the measurement circuit. This means that the sensor can measure current without making any direct electrical contact with the high-current conductor, thereby protecting the sensitive measurement electronics and the connected microcontroller from potentially dangerous voltages. This non-contact measurement approach also eliminates the risk of introducing additional resistance or impedance into the measured circuit, ensuring that the presence of the sensor does not interfere with the normal operation of the electrical system being monitored. This characteristic makes Hall Effect current sensors particularly well-suited for use in metering applications, where measurement accuracy and circuit integrity are of paramount importance.

Current sensors are broadly classified into two main categories based on their measurement approach: open-loop and closed-loop sensors. Open-loop Hall Effect sensors directly measure the magnetic field produced by the current and convert it into a proportional output voltage using a Hall Element and a signal conditioning circuit. These sensors are generally simpler in design, more compact, and less expensive, making them suitable for applications where moderate accuracy is sufficient. Closed-loop sensors, on the other hand, employ a feedback mechanism in which a compensation coil generates an opposing magnetic field to null the field produced by the primary current, achieving a higher degree of measurement accuracy and linearity. While closed-loop sensors offer superior performance, their increased complexity and cost make open-loop sensors the

more practical choice for cost-sensitive applications such as the proposed tamper detection system.

In addition to Hall Effect technology, current sensors may also be implemented using other principles, including current transformers (CTs), shunt resistors, and Rogowski coils. Current transformers operate on the principle of electromagnetic induction and are widely used in power system metering and protection applications. They step down the primary current to a lower, measurable secondary current that is proportional to the original value. Shunt resistors, also known as current shunts, measure current by sensing the small voltage drop produced across a precision low-resistance element connected in series with the load, applying Ohm's Law to calculate the current. Rogowski coils are air-core toroidal coils used to measure alternating currents and are valued for their wide bandwidth and ability to measure very high currents without saturation. However, despite the availability of these alternative technologies, Hall Effect sensors remain the most commonly adopted solution in modern embedded metering and monitoring systems due to their combination of accuracy, isolation, compact size, and ease of integration with microcontroller-based platforms.

The output characteristics of current sensors vary depending on the design and intended application. Analog output sensors produce a continuous voltage signal that varies linearly with the measured current, typically centered around a midpoint reference voltage representing zero current. This type of output is directly compatible with the analog-to-digital converter (ADC) inputs available on most microcontrollers, including the ATmega328P used in the proposed system, allowing the microcontroller to sample and digitize the sensor output for further processing. Digital output sensors, on the other hand, provide a discrete high or low output signal when the measured current exceeds a predefined threshold, making them suitable for simple overcurrent detection and protection applications where a binary response is sufficient.

2.7.3.1 Applications.

Current sensors find application across a broad spectrum of industries and systems due

to their versatility, reliability, and ease of integration. Some of the most notable applications include the following:

In **power systems and energy metering**, current sensors are used to measure the amount of electrical energy consumed by residential, commercial, and industrial loads. They form the core sensing element of energy meters, including prepaid meters such as the Yaka meter, where accurate current measurement is essential for correct billing and revenue collection. Any deviation in the measured current from the expected value can signal a fault condition or, as is relevant to this project, a deliberate act of tampering intended to manipulate the meter's readings.

In **motor control and drive systems**, current sensors are employed to monitor the current drawn by electric motors and variable frequency drives (VFDs). By continuously tracking motor current, control systems can detect overload conditions, phase imbalances, rotor faults, and other abnormalities that could lead to equipment damage or failure. The sensor feedback is used by the drive controller to regulate torque, speed, and power consumption, ensuring efficient and safe motor operation across varying load conditions.

In **renewable energy systems**, such as solar photovoltaic (PV) installations and wind turbines, current sensors are used to monitor the output current of energy generation sources and storage systems. They play a critical role in maximum power point tracking (MPPT) algorithms, battery charge controllers, and grid-tie inverters, where accurate current measurement is essential for optimizing energy harvest and ensuring safe operation within the limits of the connected equipment.

In **battery management systems (BMS)** for electric vehicles and energy storage applications, current sensors are used to monitor the charge and discharge currents of battery packs. Accurate current measurement is essential for calculating the state of charge (SOC), state of health (SOH), and remaining capacity of the battery, enabling the BMS to protect the cells from overcharging, deep discharging, and excessive current draw, all of which can significantly reduce battery lifespan and pose safety risks.

In **overcurrent protection and circuit breakers**, current sensors are integrated into protective relay systems and electronic circuit breakers to detect fault currents caused by

short circuits or overloads. When the measured current exceeds a safe threshold, the protection system triggers a trip signal to isolate the faulty section of the network, preventing damage to equipment and reducing the risk of electrical fires or injuries.

In the context of the **proposed tamper detection system**, the current sensor is used to monitor the current flowing through the Yaka meter circuit in real time. Any sudden or unexplained change in the current profile, such as a sharp drop caused by a bypass connection or an unexpected interruption caused by the cutting of signal cables, is detected by the sensor and reported to the ATmega328P microcontroller for analysis. If the detected anomaly meets the predefined criteria for a tampering event, the microcontroller triggers an alert that is communicated to UEDCL via the GSM module, enabling a prompt and informed response to the identified incident.



Figure 8: Showing the current sensor

2.7.4 Tilt Sensors (Inclinometers)

Tilt sensors, also commonly referred to as tilt switches or inclinometers, are electromechanical devices designed to detect the orientation or inclination of an object relative to the force of gravity. These sensors are capable of determining whether an object has been displaced, rotated, or tilted beyond a specified angular threshold from its

original or reference position. By providing a measurable electrical response to changes in physical orientation, tilt sensors serve as a simple yet highly effective means of detecting unauthorized physical interference with equipment, machinery, or enclosures. In the context of the proposed Yaka meter tamper detection system, tilt sensors play a vital role in identifying instances where the meter unit has been physically disturbed, repositioned, or tilted in a manner consistent with deliberate tampering activity.

The fundamental operating principle of a tilt sensor is rooted in the effect of gravitational force on a movable conductive element contained within the sensor's housing. When the sensor is in its normal, upright orientation, the conductive element rests in a position that either completes or breaks an internal electrical circuit, producing a defined output state. When the sensor is tilted or inclined beyond a predetermined angular limit, the gravitational force acting on the conductive element causes it to shift from its resting position, thereby changing the state of the internal circuit and generating a corresponding output signal. This output signal is then read by a connected microcontroller or control circuit, which interprets the change in state as an indication that the sensor, and by extension the object to which it is attached, has been physically displaced or tilted.

Common tilt sensor modules, such as the widely used SW-520D, employ a simple and robust internal mechanism consisting of a small metal ball housed within a cylindrical or conical cavity. The interior of the cavity contains two conductive contact pins positioned at one end of the housing. Under normal operating conditions, when the sensor is held in its upright or near-upright position, the metal ball rests away from the contact pins due to gravity, leaving the internal circuit open and producing a high or inactive output signal. When the sensor is tilted beyond its designed angular threshold, typically in the range of 10 to 45 degrees depending on the specific module, gravity causes the metal ball to roll toward the contact pins. Upon reaching the pins, the metal ball bridges the gap between them, completing the electrical circuit and producing a low or active output signal that indicates a tilt event has occurred. This mechanical simplicity makes the SW-520D and similar ball-type tilt sensors extremely reliable, low-cost, and easy to integrate into embedded systems such as the ATmega328P-based tamper detection platform used in this project.

In addition to the metal ball mechanism, some tilt sensors employ conductive fluid, typically a small amount of mercury or a non-toxic conductive liquid, enclosed within a sealed glass or plastic capsule. In mercury-based tilt switches, the liquid mercury rests at the lower end of the capsule under the influence of gravity when the sensor is in its normal orientation. When the sensor is tilted sufficiently, the mercury flows toward the opposite end of the capsule, making contact with embedded electrodes and completing the circuit. Although mercury tilt switches offer excellent conductivity and long operational life, their use has become increasingly restricted due to environmental and health concerns associated with mercury toxicity. As a result, non-toxic conductive fluid alternatives and solid-state tilt sensing technologies have been developed to replace mercury-based devices in modern applications.

Beyond the basic mechanical tilt switch, more advanced inclinometer technologies have been developed to provide precise angular measurements rather than simple binary tilt detection. Electrolytic tilt sensors, for example, use a partially filled electrolytic fluid cell with multiple electrodes. As the sensor tilts, the distribution of the conductive fluid between the electrodes changes, altering the resistance or impedance between electrode pairs and producing an analog output that is directly proportional to the angle of inclination. This allows for continuous and accurate measurement of tilt angle across a defined range, making electrolytic sensors suitable for applications requiring precise angular data rather than simple threshold detection.

Microelectromechanical systems (MEMS)-based accelerometers represent another category of advanced tilt sensing technology that is increasingly used in modern electronic devices. MEMS accelerometers measure the acceleration forces acting on a microscopic proof mass suspended within a silicon structure. When the device is tilted, the component of gravitational acceleration acting along the sensor's sensitive axis changes in proportion to the angle of inclination, allowing the tilt angle to be calculated mathematically from the measured acceleration values. MEMS-based tilt sensors offer significant advantages over mechanical tilt switches in terms of accuracy, resolution, small form factor, and the ability to measure tilt in multiple axes simultaneously. However, their higher cost and greater complexity compared to simple ball-type tilt switches make

mechanical sensors such as the SW-520D the more practical and cost-effective choice for the binary tilt detection function required in the proposed tamper detection system.

The electrical interface of tilt sensors is generally straightforward and highly compatible with microcontroller-based systems. The SW-520D module, for instance, produces a simple digital output signal that transitions between a logic high and a logic low state in response to tilt events. This digital output can be connected directly to a general-purpose input/output (GPIO) pin of the ATmega328P microcontroller, which can be configured to detect the change in signal state through either polling or interrupt-driven techniques. The use of external interrupt pins on the microcontroller allows the system to respond to tilt events immediately and in real time, without the need for continuous polling of the sensor output, thereby improving the overall responsiveness and efficiency of the tamper detection system.

The sensitivity of a tilt sensor, defined as the minimum angle of inclination required to trigger a state change, is an important parameter that must be considered during system design. For the proposed tamper detection application, the sensitivity of the tilt sensor must be carefully selected to ensure that the system can reliably detect deliberate physical manipulation of the Yaka meter while remaining insensitive to minor vibrations or environmental disturbances that might otherwise cause false alarms. The SW-520D offers a fixed angular sensitivity determined by its mechanical design, which has been found to be well-suited for detecting the degree of physical disturbance typically associated with meter tampering activities such as removal, repositioning, or forceful displacement of the meter enclosure.

Applications

Tilt sensors find application across a diverse range of industries and systems where the detection of angular displacement, orientation change, or physical disturbance is required. Some of the most significant and widely recognized applications are described as follows:

In **anti-tamper and security systems**, tilt sensors are used to detect unauthorized physical interference with protected equipment, enclosures, or assets. When attached to

a device such as an electricity meter, a vending machine, an ATM, or a security cabinet, the tilt sensor can immediately detect if the device is being moved, rotated, or forcefully displaced from its installed position. Upon detection, the sensor triggers an alarm or alert notification, enabling security personnel or utility operators to respond promptly to the suspected tampering activity. This is the primary application of the tilt sensor in the proposed Yaka meter tamper detection system, where it is used to detect physical disturbance of the meter unit consistent with deliberate tampering.

In **consumer electronics**, tilt sensors and MEMS accelerometers are widely integrated into smartphones, tablets, gaming controllers, and digital cameras to enable orientation-aware functionality. These devices use tilt sensing to automatically rotate the display between portrait and landscape modes, to detect shaking gestures for interface navigation, and to stabilize camera images by compensating for hand movement during photography. The intuitive and responsive user experience offered by modern mobile devices is largely made possible by the precise tilt and motion sensing capabilities provided by embedded MEMS accelerometers.

In **automotive safety systems**, tilt sensors are employed in vehicle rollover detection and electronic stability control (ESC) systems. By continuously monitoring the angular orientation of the vehicle, these sensors can detect the onset of a rollover event and trigger protective measures such as the deployment of side curtain airbags, the application of selective braking to individual wheels, and the adjustment of engine torque to help the driver regain control. Accurate and fast-responding tilt sensing is therefore a critical component of modern vehicle safety architecture, contributing directly to the prevention of serious road accidents and fatalities.

In **industrial machinery and equipment monitoring**, tilt sensors are used to ensure that heavy machinery, cranes, lifting platforms, and construction equipment remain within safe operating angles during use. Exceeding the permissible tilt angle for such equipment can lead to structural instability, loss of load control, or catastrophic equipment failure. Tilt sensors provide continuous real-time monitoring of equipment orientation and trigger audible alarms or automatic shutdown sequences when unsafe inclination levels are detected, thereby protecting both equipment and personnel from injury or damage.

In **robotics and autonomous systems**, tilt sensors and inertial measurement units (IMUs) incorporating accelerometers and gyroscopes are used to provide orientation feedback to control algorithms. Mobile robots and unmanned aerial vehicles (UAVs) rely on this feedback to maintain balance, navigate uneven terrain, and execute precise maneuvers. Accurate tilt sensing is essential for the stability and control of such systems, particularly in dynamic environments where rapid changes in orientation must be detected and compensated for in real time.

In **agricultural and civil engineering applications**, inclinometers are used to monitor the stability and structural integrity of slopes, embankments, retaining walls, dams, and foundations. By measuring changes in the angle of inclination of these structures over time, engineers can detect early signs of ground movement, soil creep, or structural settlement that may indicate potential failure risks. This enables timely intervention and remediation measures to be implemented before catastrophic structural failure occurs, protecting both infrastructure and human life.

In **medical and rehabilitation devices**, tilt sensors are incorporated into patient monitoring systems, prosthetic limbs, and physical therapy equipment to track body posture, limb orientation, and movement patterns. This information assists healthcare professionals in assessing patient mobility, monitoring recovery progress, and designing personalized rehabilitation programs. Wearable tilt sensing devices also enable the detection of falls in elderly or mobility-impaired patients, triggering automatic alerts to caregivers or emergency services when a fall event is detected.



Figure 9: Showing the tilt sensor

CHAPTER III: METHODOLOGY

3.0 Introduction.

This chapter describes the different techniques and tools that shall be used to achieve the objectives stated and eventually lead to the design and construction of an energy meter tamper detector system for Yaka systems. The techniques include: Data collection techniques, System design and implementation, and many others that will be achieved in the following phases.

3.1 System Study.

3.1.1 Requirement Elicitation

The requirements will be based on the useful literature that will be obtained from relevant sources. The understanding of the system deployment environment greatly contributes to the elicitation of the system requirements, which in my case will be the energy meter.

3.1.2 Data collection methods

- i. Literature Review. This will include the use of relevant textbooks contained in the university library, and the different data from the web pages, journals, research papers, and newspapers obtained from the internet will also be used to review the existing literature on the related system. These will be used to obtain some of the requirements of the system.
- ii. Consultations. This method will be aimed at acquiring and seeking advice from experienced people and experts in the field, like lecturers, engineers, and the UEDCL Company consultative team, who are faced with these challenges.
- iii. Observation. The method involves collecting data through various visits to technicians and UEDCL customers who are enrolled on the prepaid meters, so as to establish what is actually on the ground. It is from these observations that I can draw a conclusive work on the project. In other words, it involves visiting and examining the existing security features of the pre-paid (Yaka) systems.

3.2 System Analysis.

Systems analysis is the process of looking at and summarizing data with the intention of extracting useful information and developing conclusions. This shall aim at extracting requirements from all the collected data for designing the system. The data collected shall be analyzed based on the objectives of the study. This shall be done qualitatively by giving meaning to findings to be able to make effective recommendations. Data will be cross-checked for consistency based on the concepts of the different data collection methods and interpreted to provide requirements for the design and construction of a

magnetic energy meter tamper detector subsystem for Yaka systems. The strength of the existing systems will be incorporated into the new design, whereas their weaknesses will be clearly studied to be solved.

3.3 System Design.

This is a process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. The design of the proposed design and construction of an energy meter tamper detector system for Yaka systems shall be composed of both the hardware and software components.

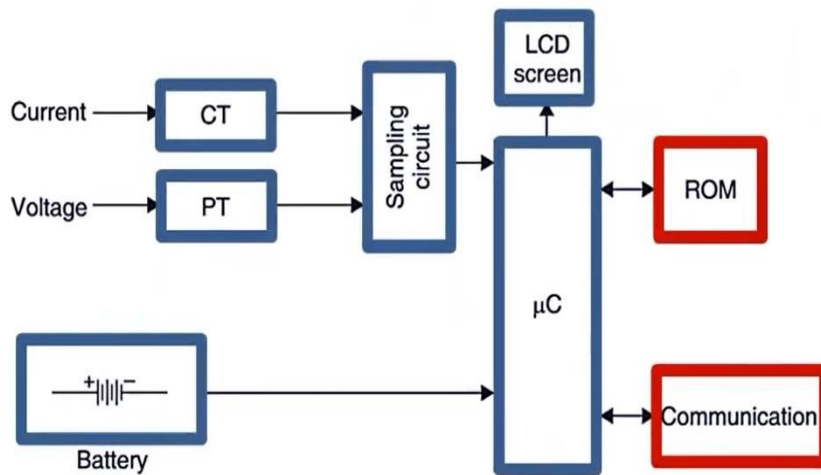


Figure 10: System block diagram.

3.4 System Construction

The implementation of the proposed system will begin by designing the appropriate circuit using Proteus. The different components will then be interconnected on a breadboard to give an overall system overview. They will then be soldered on the Vero board. The coding for the microcontroller will be in an embedded C language program, which will then be downloaded onto the microcontroller using AVR Studio/Atmel Studio and the AVR In-System Programmer.

The proposed system will be implemented in an electrical environment with the energy meter reader connected.

3.4 Testing

This is the process of executing application programs with the intention of finding errors, using careful and planned test strategies and realistic conditions. The developed system will be tested using different techniques, which will include;

3.4.1 Unit testing

The goal of this method will be to test each component that will be used before integrating them on board. This will be done to ensure that the right components with the desired functionality are chosen.

3.4.2 Integration testing

This involves testing the components according to their functionalities, and at each stage of development, before reaching the final stage, testing will be done. This helps to know how the combined units work and their functionality status. It is done on the different modules.

3.4.3 System test

This will be conducted on a complete, integrated system to evaluate its compliance with specified requirements. The aim will be to uncover faults in the algorithms used in the system so as to achieve the main objective of the study.

3.5 Validation

The validation process for a magnetic energy meter tamper detector subsystem for Yaka systems will provide a high degree of assurance that specific processes consistently provide products that meet predetermined specifications and quality attributes. It will involve identifying compliance with quality management procedures, life cycle definition and specifications, for example, user requirements specification and functional specification, documentation controls, and testing procedures.

3.6 CODE FOR THE PROJECT.

```
#include <LiquidCrystal_I2C.h>
#include <SoftwareSerial.h>
#include <EEPROM.h>
#include <math.h>
// ----- LCD -----
LiquidCrystal_I2C lcd(0x27, 16, 2);
// ----- mySerial ----- SoftwareSerial
mySerial(2, 3); // RX, TX
const char phoneNumber[] = "+256782509318";//put in small
board const int hes=5; const int tilt=9; const int ldr=A3; const
int green=6; const int red=7;
// ----- voltage -----
String readMSG()
{
String    ret    =    "";
while( mySerial.available()
)
{
```

```

char ccc
=mySerial.read(); ret =
ret + ccc; }ret.trim();
return ret;
}

// =====

// SEND SMS

// ===== void
sendSMS(String message)
{
mySerial.println("AT+CMGF=1");
delay(500);
mySerial.print("AT+CMGS=\"");
mySerial.print(phoneNumber);
mySerial.println("\");
delay(500);
mySerial.print(message);
delay(500);
mySerial.write(26);    //    CTRL+Z
delay(3000);
}

// =====

// READ SMS

// =====String
readSMS()
{
String msg = ""; while
(mySerial.available())
{

```

```

char c =
mySerial.read(); msg
+= c; } msg.trim();
return msg;
}

// =====

// SETUP

// ===== void
setup()
{ lcd.begin();
  lcd.backlight()
;
  pinMode(hes,
  INPUT);
  pinMode(tilt,I
  NPUT);
  pinMode(gre
  en,OUTPUT);
  pinMode(red,
  OUTPUT);
  lcd.print("TA
  MPER
  DETECTION");
  lcd.setCursor(0, 1);
  lcd.print("SYSTEM");Serial.begin(9600)
; delay(3000); mySerial.begin(4800);
delay(1000); mySerial.println("AT");
delay(1000);
mySerial.println("AT+CMGF=1"); // set SMS mode to text
delay(100);

```

```

mySerial.println("AT+CNMI=2,2,0,0,0");
delay(500);
mySerial.println("AT+CREG?");
delay(500); while
(!mySerial.available())
{ lcd.clear();
digitalWrite(red,HIGH);
digitalWrite(green,LOW);
lcd.print("CHECK MODEM and ");
lcd.setCursor(0,1);
lcd.print("retry...."); delay(1000);
}

String response=mySerial.readString();
while(!(response.indexOf("+CREG: 0,1")>-1))
{
digitalWrite(red,HIGH);digitalWrite(green,HIGH); mySerial.println("AT+CREG?");
response=mySerial.readString(); lcd.clear(); lcd.print("Connecting....."); delay(3000); }
if(response.indexOf("+CREG: 0,1")>-1)
{
mySerial.println("AT+CREG?");
digitalWrite(green,HIGH);
digitalWrite(red,LOW);
response=mySerial.readString();
lcd.clear();
lcd.print(" CONNECTED");
delay(1000); }
mySerial.println("AT");
delay(1000);
mySerial.println("AT+CMGF=1"); // set SMS mode to text
delay(100);

```

```

mySerial.println("AT+CNMI=2,2,0,0,0");
delay(2000);sendSMS("Connection
OK"); delay(5000); } void loop() { float
Vcc = 4.12; float max_v = 0; float Veff
= 0; for (int i = 0; i < 100; i++) { int
sensorValue = analogRead(A2);
// Find the peak value in the 100ms window
if (sensorValue > max_v)
{ max_v = sensorValue;
} delay(1);
}
if (max_v > 511) {
// 1. Convert ADC peak to Volts based on 4.12V
reference float Vpeak_ADC = ((max_v - 511) * Vcc) /
1024.0;
// 2. Convert to RMS
float Vrms_ADC = Vpeak_ADC / 1.4142;
// 3. Apply your specific hardware mapping// If your old formula was: (((VeffD - 420.76)
/ -90.24) * -210.2) + 210.2
// You must re-calibrate these constants using a multimeter.
// For now, use a simple multiplier (Slope) if you don't have new
constants: float slope = 250.0; // Example: Adjust this until Veff
matches your multimeter Veff = Vrms_ADC * slope; if(Veff<20)
{
mySerial.println("AT+CMGF=1");
delay(500);
mySerial.print("AT+CMGS=
\\");
mySerial.print(phoneNumb

```

```

er); mySerial.println("\n");
delay(500);
mySerial.print("Meter power
outage: "); mySerial.print(Veff);
mySerial.print("V"); delay(500);
mySerial.write(26); // CTRL+Z
delay(3000);
}
} else {
Veff = 0;
}
int N=analogRead(ldr);
Serial.println();
Serial.print(N);Serial.print("
");Serial.print(Veff);
if(digitalRead(hes)==LOW){ sendSMS("
Magnetic tamper alert!");
}
else if(digitalRead(tilt)==LOW)
{
sendSMS("Tilt tamper alert!");
} else
if(N<300)
{
sendSMS("Open tamper alert!");
}
delay(5000)
;

```

}

REFERENCES:

- [1] J. Wire, 'Is UMEME's pre-paid Smart Metering a time bomb?', The New Vision, 2014.
[Online]. Available: <http://newvision.com>. [Accessed: 11- Nov- 2014].

- [2] FBI, 'Smart Electric Energy meters altered to steal electricity', 2010. [Online]. Available:
<http://fbi.gov/cybercrime>. [Accessed: 27- May- 2010].
- [3] Patriot & Paulies (Editors), '5 Hacks that render Smart Meters dumb', 2012. [Online]. Available: <http://patriotandpaulies.wordpress.com>. [Accessed: 16- Aug- 2012].
- [4] T. Leautier, 'Is Mandating "Smart Meters" Smart?', *EJ*, vol. 35, no. 4, 2014.
- [5] D. Baker, 'Malware-based Smart meters' attack', *ioactive.com*. Available: <http://www.ioactive.com/>. [Accessed: 08- Oct- 2013].
- [6] H. M. Zahid Iqbal, M. Waseem, and Dr. Tahir Mahmood, *Automatic Energy Meter Reading using Smart Energy Meter*.
- [7] S. Arun and Dr. Sidappa Naidu, 'Hybrid Automatic Meter Reading System', ISSN: 2277 128X, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 7, pp. 361-365, 2012.
- [8] Depuru, S .S, Wang, L., Devabhaktuni, V.: Electricity theft: Overview, issues, prevention, and a smart meter-based approach to control theft. *Energy Policy*. 39, 1007–1015 (2011)
- [9] Kasita, I.: UMEME starts pre-paid power billing. *The New Vision*, Kampala (2011). <http://www.newvision.co.ug>
- [10] Muneza, S.: Umeme Seeks Help To Cut Electricity Theft. *The Red Pepper*, Kampala, Uganda, (2014). <http://www.redpepper.co.ug>
- [11] LADU, I. M.: Umeme to install 16,000 pre-paid meters. *Daily Monitor*, Kampala (2014). <http://www.monitor.co.ug>
- [12] Ssekika, E.: Uganda loses Shs 76bn annually to power theft: *The Observer*, Kampala, Uganda, (2013). <http://observer.ug>
- [13] N. Wesonga, "Umeme in bid to reduce power distribution losses," *Daily Monitor*, Kampala, Uganda, Dec 2012.
- [14] Ashna. K, Sudhish N George, "GSM Based Automatic Energy Meter Reading System with Instant Billing", 978-1-4673-5090-7/13©2013 IEEE, pp. 65-71.

- [15] Marvin E. Ferking, "*Crystal Oscillator Design and Temperature Compensation*", Van Nostrand Reinhold Company, New York, 1978.
- [16] Benjamin Parzen, "*Design of Crystal and other Harmonic Oscillators*", John Wiley and Sons, Inc., New York, 1983.
- [17] Jawarkar, N. P., Ahmed, V., Ladhake, S. A. & Thakare, R. D. (2008). "Microcontroller-based Remote Monitoring Using Mobile through Spoken Commands", *Journal of Networks*, 3(2), 5863. Retrieved from <http://www.academypublisher.com/jnw/vol03/no02/jnw03025863.pdf>
- [18] Jubi. K, MareenaJohn, "Prepaid Energy Meter with GSM Technology", *AIJRSTEM*, pp. 195- 98, June-August, 2013.
- [19] Dr. K. Sheelasobanarani¹, S. Dinesh Raja², B. Dhanaraj³, K. Manickam⁴, K. KarthickRaja⁵. "A Prepaid Energy meter for efficient Power Management", *International Journal of Emerging Technology and Advanced Engineering*, Volume 4, Issue 3, March 2014
- [20] Bharat Indorey, M.Lokhande, "ZigBee-Based Advanced Energy Prepaid Meter", *International Journal of Innovations in Engineering and Technology (IJJET)*, Volume 3, Issue 3, February 2014
- [21] www.mobilecomms-technology.com/protects/sms, Retrieved November 13th 2011
- [22] D. Tom Tamarkin, 'Automatic Meter Reading', *Public Power Magazine*, vol. 50, pp. 5. SeptOct 1992
- [23] Dr.Boyina S. Rao, B. Gnanasekaranathan, M. Raguram, S. Pravinkumar, P. Kamalesh, "Domestic Prepaid Energy Distribution System for Saving of Power Consumption", *IJAET/Vol.III/ Issue II/April- June, 2012/26-29*.
- [24] Anton A.Huurdemann, 'The worldwide history of telecommunication', John Wiley & Sons, pp. 529, 31 Jul 2003
- [25] "GSM Global System for Mobile Communications", 4G Americas, retrieved 2014-03-22

APPENDICES

Appendix E: Photographs of Prototype.

