KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY, KUMASI

SCHOOL OF GRADUATE STUDIES

COLLEGE OF ENGINEERING

DEPARTMENT OF COMPUTER ENGINEERING

A LOW COST EARLY ADOPTION STRATEGY FOR IMPLEMENTING SECURED SMART ENERGY METERING SYSTEMS IN AFRICAN DEVELOPING COUNTRIES

Thesis submitted in partial fulfillment for the degree of

Doctor of Philosophy in Computer Engineering

By

Eliel Keelson (BSc.)

SUPERVISORS: (1) PROF. K.O. BOATENG

(2) PROF. ISAAC GHANSAH

MARCH, 2016

DECLARATION

I hereby declare that except for specific references which have been properly acknowledged, this work is the result of my own research and it has not been submitted in part or whole for any other degree elsewhere.

Signature …….. Date ……

Eliel Keelson (Candidate)

Signature …….. Date ……

Prof. Isaac Ghansah (Supervisor)

Signature …….. Date ……...

Prof. K. O. Boateng (Supervisor and Head, Computer Engineering Department)

ABSTRACT

Electricity continues to be a great power behind the world's industrial revolution and an indispensable asset in everyday living. Its significance has necessitated the extensive rollout of electrification projects. Despite these rollouts, the continent of Africa is yet to enjoy reliable supply of electric power and its associated benefits. Due to Africa's high population growth and economic development, it is ever so plagued with extensive seasons of power shortages – energy crises. The effect of these crises can be clearly seen in Africa's vicious cycle of poverty. This thesis links the nemesis of these crises to the inability of Africa's utilities to conduct effective demand analyses on day-to-day consumption of electricity. These analyses are a prerequisite in avoiding unprecedented demand. To mitigate these crises, it suggests the migration from standalone metering systems to smart metering systems. Bearing in mind that this migration has often come at a high expense to developed countries, it proposes a low cost early adoption strategy for implementing secured smart metering systems in African developing countries. A key aspect of this proposition is a secured low cost smart retrofit which furnishes existing standalone meters with smart metering capabilities. It also proposes a security protocol and a datagram format for secured information exchange in the proposed smart metering system. Finally, the proposed system is applied in providing a Smart Quota Policy, which is an effective power rationing alternative to rotational load shedding (blackouts).

Keywords: Smart Metering System; Power Crises; African developing countries; Smart Retrofit; Smart Quota System.

ACKNOWLEDGEMENT

I would like to use this medium to express my heartfelt gratitude to God almighty for His guidance and protection all through this programme. I am eternally grateful to the Vice Chancellor, Prof. W.O Ellis, for giving me this golden opportunity to pursue this degree. My sincere thanks go to Prof. K.O Boateng, Prof. Isaac Ghansah and Prof. William Ofosu for their unrelenting support and keen supervision during the course of this programme. Their constructive criticisms and high sense of objectivity always kept me on the right track. They unearthed in me the right attitude to stay focused and achieve the set high goals.

Special thanks to Mr. Okrah for his cordial assistance. *To my beloved wife, Ruth Naa Kai Keelson.* I also acknowledge Mr. Michael Wilson, Mr. Hubert Attah and Mr. Fabrice Jean Boyoro who assisted me during my research. I also extend my sincere thanks to Mr. Griffith Selorm Klogo and Mr. Eric Tutu Tchao for their immense encouragement and contributions. Last but not the least; I would like to express my profound gratitude to my parents, siblings, wife and son for their persistent prayers, unfailing love and support all through this hectic period.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

µA	Micro Amps
µΩ	Micro-Ohm
2G	Second Generation
3D	Three Dimensional
3G	Third Generation
4G	Fourth Generation
A	Amps
AC	Alternating Current
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructures
BPL	Broadband Over Power-Line
BSC	Base Station Controller
BTS	Base Transceiver Station
CA	Certificate Authority
CDMA	Code Division Multiple Access
CERR	Council Of European Energy Regulators
CIA	Confidentiality, Integrity And Availability
CIS	Customer Information System
Cm	Centimeter
CPP	Critical Peak Pricing
CT	Current Transformer
dBA	Decibels
DECC	Department Of Energy And Climate Change
DES	Data Encryption Standard
DH	Diffie-Hellman
DoS	Denial Of Service
DR	Demand Response
DSA	Digital Signature Algorithm
DSM	Demand Side Management
DSP	Digital Signal Processors

DTCP	Dynamic Traffic Class Prioritization
ECAES	Elliptic Curve Augmented Encryption Scheme
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECG	Electricity Company Of Ghana
EDGE	Enhanced Data GSM Environment
EEPROM	Electrically Erasable Programmable Read-Only Memory
EIA	Energy Information Administration
EMR	Electromechanical Relay
FAT	File Allocation Table
FeNi	Ferronickel
FeSi	Ferrosilicon
FTTH	Fiber To The Home
GDP	Gross Domestic Product
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System For Mobile Communications
HAN	Home Area Network
HFC	Hybrid Fiber Coax
HLR	Home Location Register
HSPA	High-Speed Packet Access
HSPA+	Evolved High-Speed Packet Access
HSPDA	High-Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
HTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilating And Air Conditioning
IC	Integrated Circuits
ICT	Information And Communications Technology
ID	Identification
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronic Engineers
IIS	Integrated Information System
IP	Internet Protocol
IPv4	Internet Protocol Version 4
ITU	International Telecommunication Union
kB	Kilobyte
Kbps	Kilobits Per Second
kWh	Kilowatt Hours
LCD	Liquid Crystal Display
LDR	Light Dependent Resistor
LED	Light Emitting Diode
LTE	Long Term Evolution

M2M	Machine-To-Machine
mA	Milliamps
mAh	Milliamp Hour
MAS	Multiple Address System Radio
MB	Megabyte
Mbps	Megabits Per Second
MCU	Microcontroller Unit
MDMS	Meter Data Management System
MHz	Megahertz
MITM	Man-In-The-Middle
MNO	Mobile Network Operator
MS	Mobile Subscriber
MVNO	Mobile Virtual Network Operator
MVPN	Mobile Virtual Private Network
MW	Megawatts
nH	Nano-Henries
NiMH	Nickel Metal Hydride
NSA	National Security Agency
NSS	Network Switching System
OS	Operating System
OSHAN	Open Source Home Area Network
PKC	Public Key Cryptographic
PLC	Power Line Carrier
QoS	Quality Of Service
RGB	Red Green Blue
RMS	Root Mean Squared
RoHS	Resistance Of Hazardous Substances
RTC	Real Time Clock
RTP	Real Time Pricing
SCADA	Supervisory Control And Data Acquisition
SD	Secure Digital
SEP	Smart Energy Profile
SGIG	Smart Grid Investment Grant
SGSN	GPRS Support Node
SHA	Secured Hash Algorithm
SIM	Subscriber Identity Module
SKC	Symmetric Key Cryptographic
SMS	Short Message Service
SSM	Supply Side Management
SSR	Solid-State Relay
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TMSI	Temporal Mobile Subscriber Identity

TOU	Time Of Use
TTL	Transistor-To-Transistor Logic
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol
V	Volts
VLR	Visitor Location Register
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
WiMAX	Worldwide Interoperability For Microwave Access
WLAN	Wireless Local Area Network

CHAPTER ONE: INTRODUCTION

1.0 NEMESIS OF POWER CRISES IN AFRICA

The significance of electricity in the world today cannot be overemphasized. It is the power behind the industrial revolution and the springboard for many inventions; bringing comfort and luxury into the lives of many [1.1]. Its importance has necessitated the increase in electrification projects all over the world including Africa; a task of providing every habitable area with access to electric power [1.2]. There is hardly any modern community that does not depend heavily on electric energy. Due to the overdependence on electricity coupled with population growth and economic development, its demand in Africa has been on a constant upsurge. Energy Information Administration (EIA) has forecasted that a large percentage of the world's demand of electric energy would emerge from developing countries, of which most African countries are a part [1.3].

This constant growth in electric energy demand calls for an equivalent increase in electricity generation – a feat, most developing countries in Africa fail to accomplish. These countries often attribute this failure entirely to the lack of readily available resources. A typical example is Ghana, which declared in October 2013, that its ever recurring energy crisis was due to the lack of financial resources and that the country needed USD 4 billion to end the crisis [1.4]. This failure to meet growing demand in a timely manner is the nemesis of most energy crises in Africa. Developing countries like Egypt, Ethiopia, Ghana, Nigeria, Uganda and Rwanda have been plunged into extended seasons of energy crises resulting in a disruption of economic growth as well as comfort in the lives of their people [1.5]. Such countries are helpless in meeting demand and can only address the problem by rationing power through the authorization of blackouts. Africa experiences an average of 56 days of power outages each

year causing businesses 6 to 20% losses in sales and productivity [1.6]. This is one plausible explanation of Africa's very low Gross Domestic Product (GDP).

One is tempted to think that developed countries hardly experience energy crisis because they have superabundant energy resources. On the contrary, most developed countries like Canada, Italy, Netherland, New Zealand, Spain and United States of America have effectively addressed the endless growth in electric energy demand by carefully studying the nature of the current demand, from which they forecast and plan to meet future demands in a timely fashion [1.7]. Without these finely tuned detailed analyses, these developed countries would also be overwhelmed at a point in time with unprecedented demands. These analyses also help them avoid generating more than what is needed for a particular period of time, thus preventing energy waste and reducing carbon emissions. Therefore the processes of electricity generation, transmission and distribution are kept in a right balance with energy demand [1.8]. This therefore connotes that the efficient supply of electricity to meet demand is primarily dependent on demand analyses and not necessarily the provision of abundant resources as stated earlier by some African developing countries.

The close monitoring of energy demand, as done by most developed countries, has been made possible by the adoption of Smart Metering Systems. In this system, smart meters are installed for every consumer of electricity. The smart meters record consumption data and transmit recorded data to utilities in real-time or near real-time. Utilities critically analyze the data to understand the nature of the prevailing demand. They then forecast and take appropriate measures to meet future demands thus avoiding energy crisis [1.9]. Ever since its introduction in 2009, the smart metering system has proven to be very useful in matching demand with supply [1.10]. Its two-way communication ability has also provided utilities with remote and accurate meter reading, remote connection and disconnection, remote energy theft detection

and remote detection of power outages or system faults. All of these have drastically reduced the operational cost of utilities [1.11]. With the provision of consumption data in real-time, consumers are capable of altering their consumption lifestyles thus contributing to energy conservation and reduction in bills [1.12].

Despite the many benefits associated with this system, many developing countries in Africa have not yet adopted this system [1.13]. One would have thought that for a continent so much plagued with energy crises, adopting this system would have been its first response to addressing the issue. A plausible explanation to the delay in adopting the smart metering system in African developing countries is the high initial cost associated with the massive rollout of this system. Developed countries that have adopted this system have had to make huge financial investments. For example, in February 2011, Connecticut Light and Power estimated the massive rollout in Connecticut to cost USD 500 million. Also the Department of Energy and Climate Change (DECC) of the United Kingdom Impact Assessment estimated the deployment to cost £10 billion [1.7] [1.14]. Going by these high figures, developing countries in Africa if adopting the same method of rolling out, would find this feat difficult to attain if not impossible.

1.1 PROBLEM STATEMENT AND MOTIVATION FOR THE RESEARCH

Historically, the continent of Africa has been entangled in a vicious cycle of poverty [1.15]. Its side effects on the African people are superfluously atrocious and very undesirable. Some of which are a high prevalence of negative health conditions, high mortality rate, low level of literacy and high unemployment rate [1.16]. The World Bank has suggested that through industrialization and technology, Africa can break out of this vicious cycle [1.17].

With the aid of domestic and foreign investments, most developing countries in Africa have taken initiatives to setup various industries while making an effort to adopt new technologies. Despite these efforts, one thing still stands in its path of fast reaching its goal – electric energy crisis. Bearing in mind that industrialization as well as most technological approaches to solving problems ride heavily on the backbone of electricity, the high presence of electric energy crisis would cripple their potential of helping these countries to break away from poverty. Most African developing countries are currently struggling with energy crisis and this possibly explains why the introduction of several industries has had little or no impact on their economies [1.18]. With unreliable power comes low productivity, high operational cost, high losses in sales and eventually low GDPs. In other words, reliable supply of electricity is pertinent to ending Africa's woeful plight of poverty. With the survival of the economy and its people heavily hinged on the power of electricity, the urgency of dealing with energy crisis cannot be overstated.

The traditional methods developing countries in Africa have employed in meeting the growing demand are increasing generation capacity as well as the energy resources required for electricity generation [1.19]. The capital intensive nature of these procedures has made it difficult, if not impossible, for such developing countries to carry them out in a timely fashion thus still causing an imbalance in demand and supply – unresolved energy crisis. In areas where there is shortage in supply, utilities ration power by legislating rotational load shedding programs, often called blackouts [1.6]. This is an inefficient way of rationing power since it is not carried out in a socially equitable way and it hardly ever prepares such countries for a future of little or no energy crisis [1.20]. A more effective way of dealing with this issue is matching the growing demand of electricity with supply.

A balance in demand and supply can be achieved with detailed demand analysis and forecasting, reduction in system losses and energy waste as well as effective demand side management. These are not options for most developing countries because their current infrastructures are standalone (non-smart) and heavily human dependent in nature. These measures, if implemented, would not necessarily wipe out the need to increase generation capacities or increase energy resources, but would lessen the rate at which these are done. They would also provide utilities with precise information that would help them plan and meet demand in a timely manner. These measures also hold the potential to reduce the operational cost of most utilities, minimize energy theft and effectively mobilize revenue to facilitate the smooth running of the energy sector [1.11]. To implement these measures in African developing countries would mean making ―smart‖ the current electric energy metering system. And this would have to be done at a cost that they can afford.

1.2 RESEARCH OBJECTIVES

The general objective of this research is to provide a plausible low cost early adoption strategy for the implementation of a secured smart metering system in Ghana. Due to the identical nature of electric metering infrastructure in most African developing countries, there is a strong possibility that this strategy can also be adopted for these countries. The four specific research objectives for this thesis are as follows:

1. To develop a simple low cost retrofit which would provide existing standalone electric meters with secured smart metering capabilities. This retrofit's design will provide measures to deal with physical tampering, energy theft and other security vulnerabilities that are likely to exist in its communication network.

2. To provide guidelines for the rollout of a plausible low cost early adoption strategy for the implementation of a secured smart metering system in Ghana. These guidelines can be tailored towards specific environment of any other African nation that chooses to adopt it.
3. To provide a secured smart metering architecture based on the suggested low cost early adoption strategy. This architecture will facilitate the provision of several services; for example, the implementation of a smart quota policy for rationing power in Ghana and other African developing countries as an efficient alternative to enforcing blackouts.

1.3 SIGNIFICANCE OF THE STUDY

Ever since its inception in 2009, the Smart Metering System has proven to be an effective system in matching electric demand with supply. With its provision of real-time or near realtime consumption data, utilities are now in a better position to critically analyze demand and efficiently and adequately meet it [1.10]. There is hardly ever any unprecedented demand therefore it is possible to keep the generation, transmission and distribution processes in balance with consumption. By attaining this balance consumer satisfaction is achieved and a platform for industrial productivity, which eventually would lead to economic growth, is established.

Also the Smart Metering System has become a valuable asset in most modern Demand Response (DR) programs. Since these programs are drawn with the main aim of encouraging consumers to reduce energy demand especially during peak hours, the smart meter's provision of consumption data, tariffs and price signals to consumers in real-time help trigger consumers to make these reductions. Consumers do not only receive incentives by adhering to these

programs but they also receive lower bills and help utilities reduce the cost of generation, transmission and distribution.

Despite the potential of the Smart Energy Metering System in dealing effectively with the issue of energy crisis, developing countries in Africa, most of which have been and are currently being hit by this predicament, have barely taken any steps to adopt this system. An arguable interpretation to their inaction is the high initial cost of deploying this system as experienced by most developed countries. The work in this research is targeted on bringing to light a plausible low cost early adoption strategy of establishing secured smart metering system in Ghana as an attempt to resolve the issue of energy crisis. This study may provide the foundation for the design and implementation of smart metering systems tailored for developing countries all over Africa.

1.4 ORGANISATION OF THESIS

The rest of the thesis is organized as follows:

In Chapter two, smart metering systems are introduced and existing literature on proposed and deployed low cost strategies of implementing smart metering systems in different parts of the world are reviewed. This review is done in an attempt to identify gaps in literature which need to be addressed.

Chapter Three presents guidelines of a Retrofit Design Science Research Methodology (RDSRM) which is adopted for this research. In Chapter four, the guidelines provided in the previous chapter are considered in the design of a simple low cost retrofit which would provide existing standalone meters with smart metering capabilities.

Chapter Five describes all the steps followed in implementing the smart retrofit design. These steps are guided by the retrofit design provided in the previous chapter. Chapter Six throws more light on the selected communication network for the deployment of the proposed smart metering system. It also suggests security protocols required to guard the system from known attacks.

In Chapter Seven the system is validated based on a set of functional requirements and research objectives. In addition cost benefit analyses are conducted to ascertain savings made by adopting the proposed system. In Chapter Eight, an implementation of a smart quota based scheme of effectively rationing power is provided for the proposed system. In addition, important attributes of this scheme that makes it more efficient than rotational load shedding exercises are presented.

Finally, Chapter Nine summarizes the thesis and provides recommendations for future work that will augment contributions made by the research.

REFERENCES

[1.1] Alan W. Hodges and Mohammad Rahmani, ―Economic Impacts of Generating Electricity‖, Wood to Energy, pp.1-8, September 2007.

[1.2] International Energy Agency, ―Energy and Poverty‖, World Energy Outlook, Chapter 13, June 2008.

[1.3] Catherine Wolfram, Orie Shelef, and Paul Gertler, ―How Will Energy Demand Develop in the Developing World?‖ pp. 1-5, January 2012.

[1.4] Edwin Appiah, ―Government needs $4bn to solve energy crisis‖, Myjoyonline, http://www.myjoyonline.com/business/2013/october-24th/government-needs-4bn-tosolve-energy-crisis.php, October 2013.

[1.5] Akin Iwayemi, Suleiman J. Al-Herbish and Roger M. Gaillard, ―Energy Poverty in Africa‖, Proceedings of a Workshop held by OFID in Abuja, Nigeria, Issue 39, pp. 17-56, June 2008.

[1.6] Chloë Oliver, Rahul Kitchlu,Elvira Morella, Jamal Saghir, Lucio Monari and Meike van Ginneken , ―Turning the Lights on Across Africa – An Action Agenda for Transformation‖, Sustainable Development Series, The World Bank, pp. 11-17, April 2013.

[1.7] ―Smart Meter‖, Wikipedia, http://www.en.wikipedia.org/wiki/Smart_meter, April 2015.

[1.8] Wes Frye, Cisco Internet Business Solutions Group, ―Transforming the Electricity System to Meet Future Demand and Reduce Greenhouse Gas Emissions‖, Cisco White Paper, November 2008.

[1.9] Armin Haghi, Oliver Toole, ―The Use of Smart Meter Data to Forecast Electricity Demand‖, CS229 Course project, Fall 2013.

[1.10] Tom Wilson, BSEE, Green and Healthy Homes, ―Smart Grid & Smart Meter Architecture‖, Wireless Safety Summit Washington DC, Oct. 5, 2011.

[1.11] Department of Energy, U.S.A., American Recovery and Reinvestment Act of 2009, ―Operations and Maintenance Savings from Advanced Metering Infrastructure – Initial Results‖, Smart Grid Investment Grant Program, December 2012.

[1.12] Henk van Elburg, ―Dutch Energy Savings Monitor for the Smart Meter‖, Rijksdienst voor Ondernemend Nederland, pp. 16-24, March 2014.

[1.13] Norman B. Ndaba, ―Smart metering — transforming Africa's energy future‖, EY, October 2012.

[1.14] Pablo Rámila and Hugh Rudnick, ―Assessment of the Introduction of Smart Metering in a Developing Country‖, IEEE, 2009.

[1.15] Pedro Olinto and Hiroki Uematsu, Poverty Reduction and Equity Department, ―The State of the Poor‖, The World Bank, 2010.

[1.16] International Economics, ―The Economics of Developing Countries‖, Bonus Web Chapter, 39W-2, Part Eleven, 2010.

[1.17] Punam Chuhan-Pole, Luc Christiaensen, Allen Dennis, Gerard Kambou, Manka Angwafo, ―An analysis of issues shaping Africa's economic future‖, Africa's Pulse, Volume 8, October 2013.

[1.18] Mbunwe Muncho Josephine, ―Analysis of Energy Crisis and How it Affects Production Sector and Economic Growth of Nigeria‖, Proceedings of the World Congress on Engineering and Computer Science 2014 Vol. I, WCECS 2014, October 2014.

[1.19] Energy Sector Management Assistance Program (ESMAP), ―Implementing Power Rationing in a Sensible Way - Lessons Learned and International Best Practices‖, Report 305/05, August 2005.

[1.20] Luiz T.A. Maurer, Luiz A Barroso, ―Electricity Auctions‖, An Overview of Efficient Practices, A World Bank Study, 2010.

CHAPTER TWO: LITERATURE REVIEW

2.0 INTRODUCTION

This chapter introduces smart metering systems and reviews existing literature on proposed and deployed low cost strategies of implementing smart metering systems in different parts of the world. Section 2.1 describes smart metering systems and throws more light on its potency in dealing effectively with power crises. Section 2.2 reviews relevant literature on low cost smart metering systems in an attempt to showcase current trends as well as identify a gap in literature that must be addressed. Section 2.3 discusses various communication options available for deploying smart metering systems in Africa.

2.1 SMART METERING SYSTEMS

A smart meter is an advanced metering device that records electrical consumption data and transmits the recorded data to a designated utility over short periods of time – typically 30 minutes or less [2.1]. These smart meters are installed on the premises of consumers to measure the amount of electrical energy consumed by the consumer over a period of time. Unlike traditional standalone meters, they are equipped with two-way communication ability that allows them to transmit consumption data to utilities as well as receive notifications and control

information from utilities [2.2] [2.3]. Figure 2.1 provides a brief explanation of the entire smart metering system.

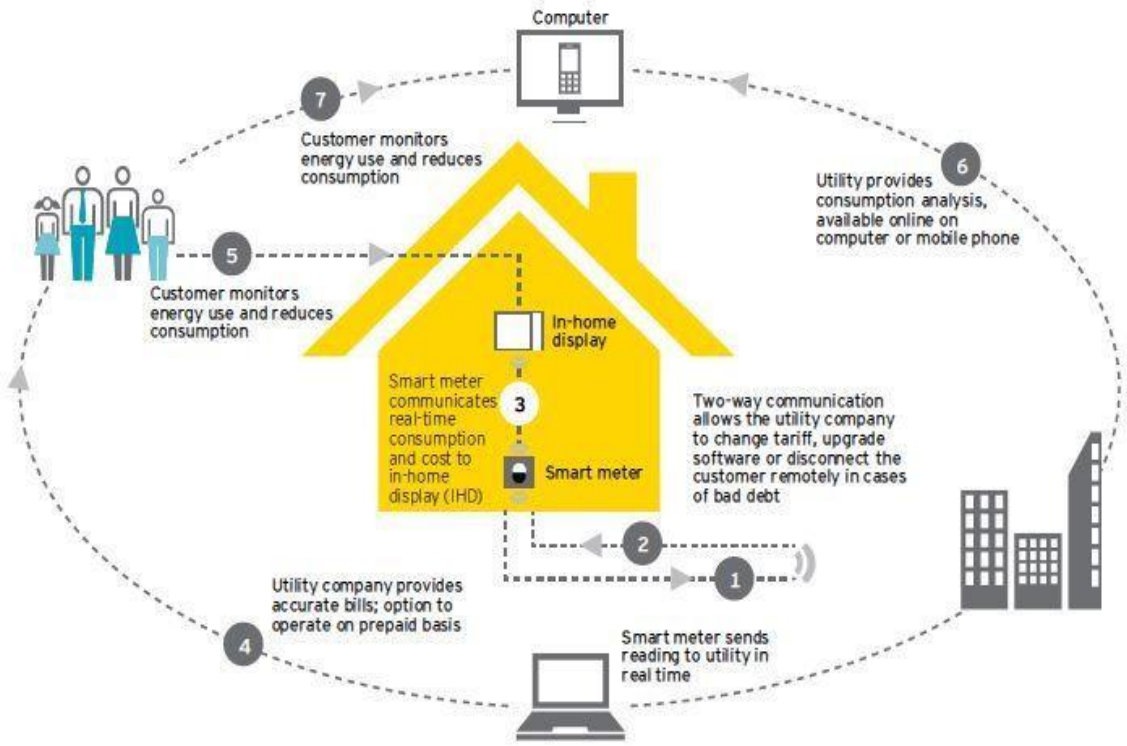


Figure 2.1 the Smart Metering System

In Figure 2.1, a smart meter installed for a household/office provides consumers with consumption data and utility notifications in real-time. The consumption data is transmitted in real-time via the two-way communication channel to a designated utility. Based on the consumption data the utility performs detailed demand analysis from which they forecast and plan to meet future demand in a timely manner. The utility also makes available the analysis of the user's consumption data accessible via mobile and web platforms. The consumer monitors his energy consumption via the data provided on these platforms as well as on the in-home display. By monitoring consumption the user is capable of making behavioural changes to reduce his consumption – thus conserving energy and minimizing his bills.

Based on the mode of operation of the smart metering system, utilities and consumers enjoy a wide range of benefits, some of which are discussed in the subsections below.

2.1.1 Providing Feedback That Facilitates Behavioural Change in Consumption

Research has proven that consumers are completely oblivious to how they consume energy; consumption still remains invisible to them. They consume at will without necessarily considering how much energy is consumed per activity [2.4]. This unawareness is the prime cause of energy waste – increase in energy demand [2.5]. Mari Martiskainen et al did comprehensive work in this area and explained that this oblivion is as a result of consumption patterns users have developed over time [2.6]. These consumption patterns or behaviours, such as when they turn off their lights, how long they use or regulate their heating, ventilating and air conditioning (HVAC) systems and the type of appliances they buy, are highly influenced by several complex factors. Some of these factors are beliefs, societal norms and external regulations [2.7]. Mari further explained that these behaviours though subconscious and well ingrained in an individual, may fade away when the consumer is provided with regular timely feedback on his consumption [2.6]. By alluding to the research by Young and Erdman et al that Information and Communications Technology (ICT) should be leveraged to advocate sustainable consumption patterns, Mari suggests the introduction of smart meters [2.8 – 2.9].

As depicted in Figure 2.1 above, smart meters have in-home digital displays which are designed to provide consumers with uncomplicated real-time direct feedback on their moment-by-moment consumption [2.10]. This consumption is displayed in both kilowatt hours and its equivalent monetary value based on the energy tariff. Figure 2.2 shows an example of a smart meter's in-home digital display/monitor.

Figure 2.2 A Smart Meter's In-Home Display/Monitor [2.11]

In addition to being displayed for the consumer, the consumption data is also transmitted to utilities in real-time, from which utilities provide consumers with indirect feedback accessible online via computers and mobile phones. This indirect feedback present consumers with detailed analysis of their consumption spanning over timeframes such as hours, days, weeks or months. Information presented here is often graphical in nature, clearly defined and may provide comparisons of consumptions of different periods of time [2.12]. Figure 2.3 shows a typical display of a consumer's smart meter dashboard accessible online.

Figure 2.3 A Smart Meter's Online Dashboard [2.13]

So unlike standalone credit based energy meters which provide only indirect feedback via monthly bills which are prepared, printed and manually distributed long after consumption has taken place, smart meters provide readily available feedback. Thus the feedback provided by smart meters is more likely to cause behavioural change in consumers as compared to that provided by standalone meters [2.6].

Results from Darby's research on the effectiveness of feedback on behavioural change affirm the statement above [2.12]. In this research, data gathered from Canada, Netherlands, Scandinavia, United Kingdom and United States of America, proved that in-home display monitors; providing direct feedback, contribute to 5-15% savings in energy. Darby also added that indirect feedbacks may contribute to 0-10% savings in energy on condition that they are accurate, frequent and provide additional information such as historical and comparative feedbacks as well as detailed periodic energy reports [2.12]. Smart metering systems are more likely to meet this condition since delivery of indirect feedbacks are automated and not manually prepared or distributed [2.6]. To buttress this point Figure 2.4 shows comparisons between the types of feedback and their relative tendencies of causing behavioural change.

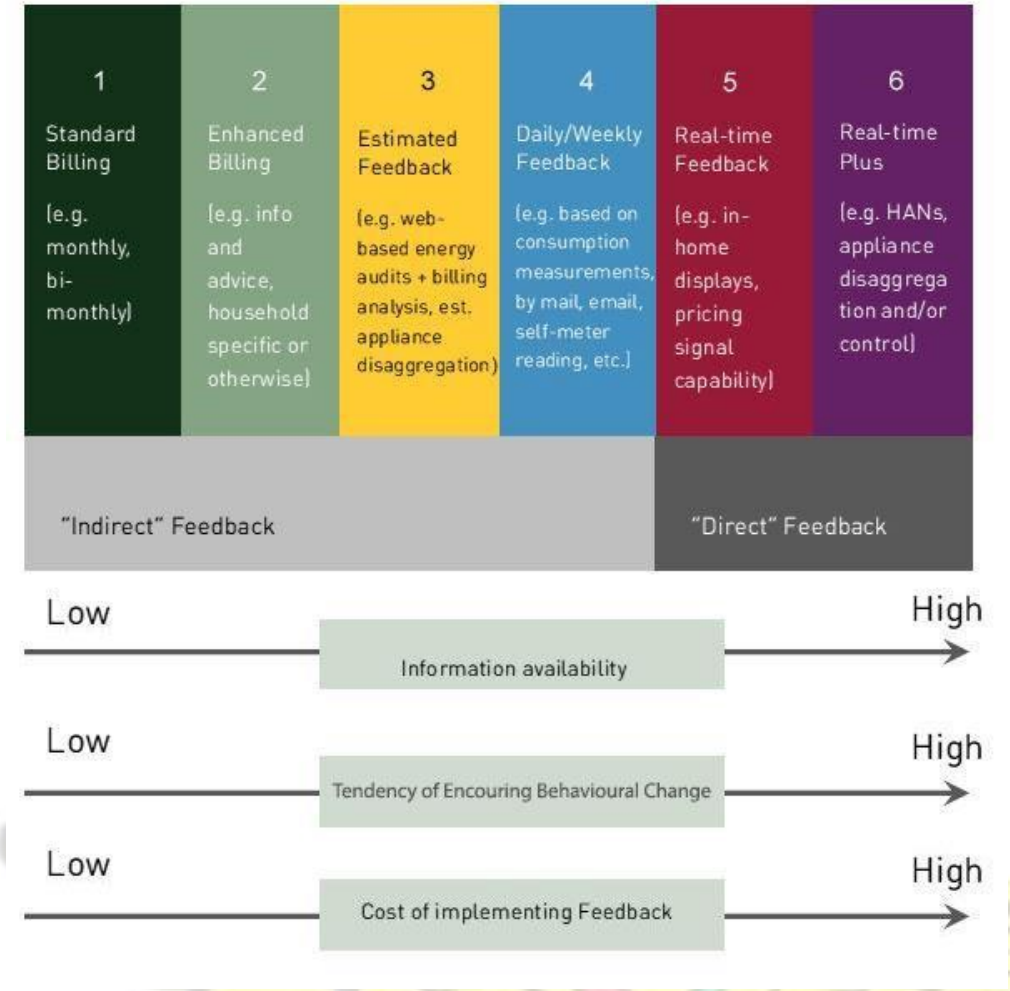


Figure 2.4 Comparisons between Direct and Indirect Feedback [2.14]

Also data analysis conducted by Dr. Karen Ehrhardt-Martinez on 36 feedback field reports supported Darby's results on the energy savings that are contributed by the various type of feedback [2.14]. Figure 2.5 shows a summary of the final results from the analysis.

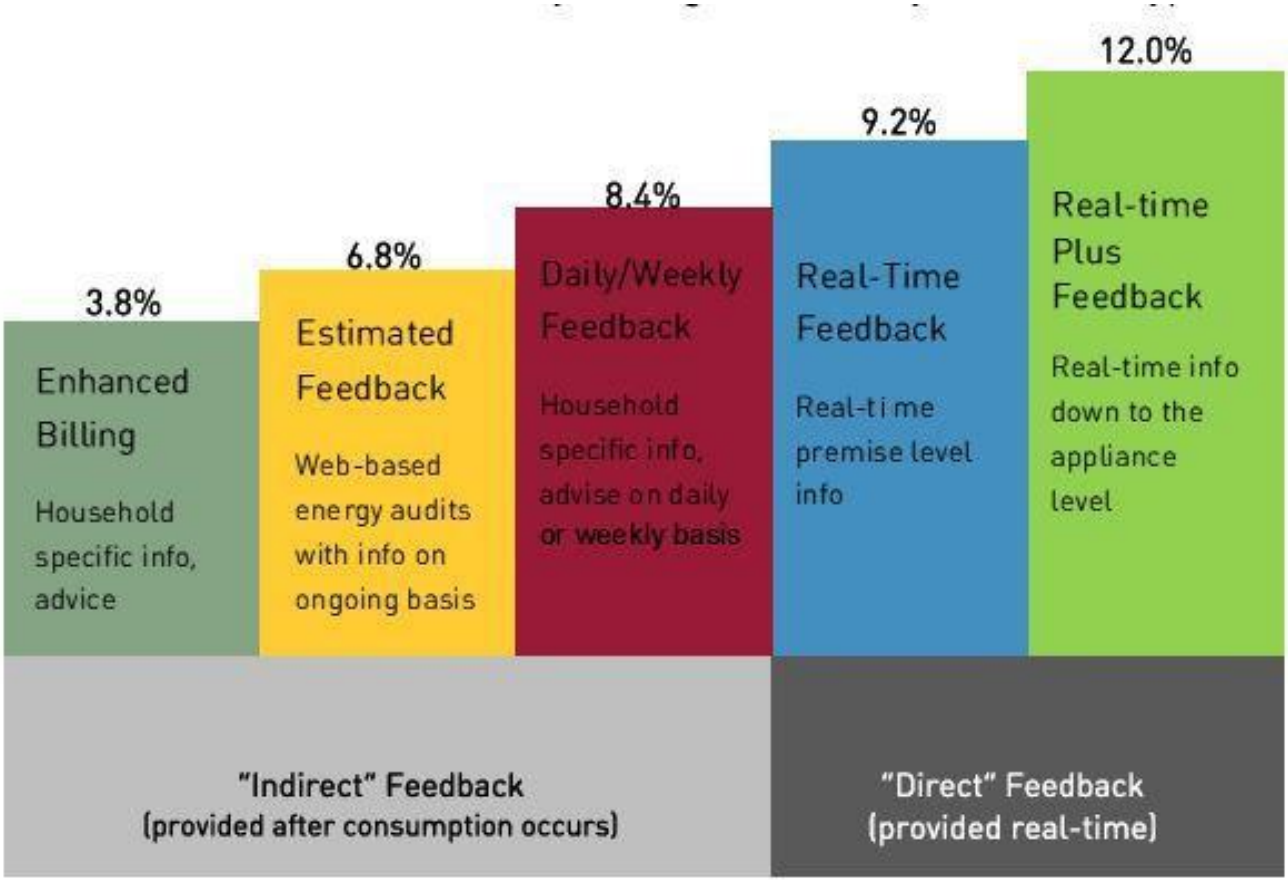


Figure 2.5 Energy Savings Potential of the different types of feedback [2.14]

So in short, smart meters which provide consumers with frequent, accurate and real-time feedback have a higher tendency of making consumers more aware of their energy consumption thus leading to behavioural change and energy conservation. This would eventually yield lower bills, lower energy demand and lower carbon emissions.

2.1.2 An Essential Tool for Demand Response Programs

Research has proven that the energy savings attained as a result of frequent and accurate feedback are often short-term in nature and would not persist over medium to long-term. These savings may not completely dwindle but may reduce with time [2.15]. Dr. Karen Ehrhardt-Martinez explained that this is because most of the behavioural changes, such as

turning off lighting systems when not needed, require considerable human conscious effort and as such may dim out with time. She added that if they were more technological in nature, such as the purchase and use of more energy efficient appliances, they would persist over longer periods of time [2.14]. Froehlich et al. and Abrahamse et al described these technological measures as efficiency behaviours and human conscious efforts as curtailment behaviours. They both alluded to the fact that the former persisted more than the latter [2.16 – 2.17].

As a consequence of this fact, Demand Response (DR) programs were introduced to achieve persistence [2.18]. In these programs consumers are provided with triggers that help them to voluntarily react in order to reduce peak demand. Customers who respond accordingly to these triggers are often incentivized and in some cases those who do not respond accordingly are charged extra for peak power [2.19]. These measures in addition to effective feedback help ensure persistence of energy savings among consumers.

Since the success of DR programs is founded on the premise of consumers' voluntary reaction to economic signals such as energy prices, incentives and punitive measures, it is important that utilities communicate these dynamic signals to consumers in real-time [2.19]. Such real-time notifications are achievable via smart metering systems. With its two-way communication ability, utilities are capable of notifying consumers via their smart meter's inhome display and online dashboard thus making smart meters an essential tool for carrying out DR programs [2.20]. This is however difficult to attain with standalone meters since they have no communication ability.

Through the implementation of dynamic energy prices such as Time of Use (TOU) rates, Real Time Pricing (RTP) rates and Critical Peak Pricing (CPP) rates, most utilities in developed countries have realized some level of persistence in energy conservation and a reduction in

peak demand [2.21]. Ahmad Faruqui et al provided analytical data to assert the potential of DR programs in reducing peak demand. They described how the success of DR programs is highly dependent on the clarity and accuracy of price signals conveyed to consumers in good time. Once this is done, consumers are capable of deciding, far before time, how they would respond to price signals [2.22]. Table 2.1 shows peak reductions from DR programs rolled out in different parts of the world, measured between 2004 and 2009. **Table 2.1 Peak Reductions from DR Programs [2.22]**

Location	**Reduction in Peak Power**
Ontario, Canada	5.7 - 25.4%
California, USA	32 - 51%
Florida, USA	41%
Illinois, USA	15%
Missouri, USA	24 - 35%
Washington, USA	15 - 20%
New South Wales, Australia	20 - 30%
Norway	8 - 9%

2.1.3 Reduction in Cost of Running Utilities

The world's largest deployment of smart meters was carried out in Italy by Enel Automated Meter Management Solution. In this project approximately 30 million smart meters were deployed in all their customers' premises [2.23]. What precipitated the massive rollout of these smart meters were the huge cost savings estimated by the company. Some of these estimates are summarized in Table 2.2.

Table 2.2 Estimated Cost Savings after Smart Meter Deployment [2.22]

Item	Percentage Reduction
Customer Services Cost	20%
Purchasing and Logistics Cost	70%
Revenue Losses from Energy theft and payment defaults	80%
Field Operations Cost	90%

The above estimates connotes that the implementation of smart metering systems creates several avenues for utilities to reduce their cost of operations as well as minimize losses in revenue. Apart from the earlier mentioned ones in the subsections above, which involve reduction of peak demand leading to reduction in cost of energy generation, there are a lot more that utilities would benefit from smart meters. How these other savings are realized is explained in the paragraphs below.

Migrating from credit based standalone meters to smart meters relieves utilities from the need to manually read meters, prepare and distribute energy bills. This is because smart meters automatically transmit consumption data to utilities in real-time and utilities notify users of outstanding bills using the meter's in-home display and online dashboard. These processes are fully automated and require little or no human effort, thus significantly reducing operational cost, ensuring consumer privacy and eliminating human errors [2.24].

Another significant reduction in field operational cost is in the area of disconnection and reconnection activities. After smart meters are deployed utilities no longer have to visit the premises of defaulting customers before disconnecting or reconnecting them after payments are made. Smart meters allow for automatic remote disconnection and reconnection. Before this, utilities had to transport both logistics and human resources in order to carry out these

activities, thus requiring detailed planning and prioritization. The ease of carrying out these activities with smart meters also facilitates minimizing losses in revenue caused by payment defaults [2.21 – 2.24].

It is worth noting that the smart meter is an effective tool in mitigating energy theft. Energy theft is the illegal act of stealing and using electricity. Perpetuators of this act often accomplish this by bypassing the electric meter or modifying its functionality. By doing so the energy consumed by the user is either not recorded or not accurately recorded [2.25]. Equipped with tamper detection mechanism, the smart meter alerts utilities when criminals attempt to tamper with the meter. Also a Meter Data Management System (MDMS), which is responsible for collating transmitted meter data, is capable of detecting energy theft by using consumption patterns [2.26]. Utilities can respond to these detected felonious activities by remotely disconnecting the meter and follow up with the police to carry out further investigations and possibly make an arrest. This feature is very essential for most utilities in Africa because of the high rate of energy theft. Some examples of notable losses as a result of energy theft include: the annual average loss recorded by South Africa and Zimbabwe is estimated at $450 million and $120 million respectively [2.27 – 2.28]. Also it has been reported by Ghana's Minister of Energy and Petroleum that the Electricity Company of Ghana (ECG) experiences 30% losses in revenue each year [2.29]. If these humongous losses are prevented, utilities stand a better chance of minimizing energy demand and revenue deficits.

One more significant benefit utilities derive from deploying smart meters is reduction in the cost customer service. As a result of the extensive analyses conducted by utilities on consumption data and load profiles, they are able to detect anomalies such as power outages and system faults in real-time. These early detection mechanisms help utilities to recover quickly from anomalies, thus leading to higher customer satisfaction and reduction in the cost

of customer services [2.24] [2.30]. In other words, customers do not have to report the problem before the necessary corrective action is carried out. Also results from these analyses help utilities to efficiently plan to meet future demand thus avoiding power waste and shortages – energy crises [2.31 – 2.32].

From the above sections, the benefits of the smart metering system can be summarized as follows:

1. Provision of direct and indirect feedback to customers in real-time promotes energy savings, leading to reduction in demand, lower cost of electricity generation, lower energy bills and lower carbon emissions.

2. Provision of real-time notifications facilitates the rollout of DR programs which lead to persistence in energy savings.

3. Automatic and remote (dis)connection, power outage detection, energy theft detection, accurate meter reading and bills distribution drastically reduce a utility's field operational cost, customer service cost, revenue losses and purchasing and logistic cost.

From the above descriptions, it can be thus said that the features of the smart metering system make it an effective system for implementing demand side management strategies of dealing with energy crisis. It has the potential of achieving far more desirable results than the current measures implemented in African developing countries [2.33]. These measures are usually associated with campaigns, consumer sensitization and implementation of laws and policies to deter consumers from practicing energy theft, energy waste and payment defaults [2.34 – 2.36]. These measures are only successful when consumers cooperate with the utility. Most of these measures have turned out to be expensive, long winding and highly dependent on human efforts

thus making them ineffective [2.35]. On the other hand, smart metering systems are automatic, operate in real-time and are not human-dependent. They also have features which allow for the implementation of a smart quota policy for rationing power which is more efficient and ensures social equitability as compared to blackouts. Details of this policy are provided in Chapter Eight.

2.2 LITERATURE REVIEW

As clearly stated in the previous chapter, massive rollout of smart meters in most developed countries has often come at a humongous cost. Despite the high potential these meters have in curtailing perpetual energy crises in African developing countries, the initial cost of deployment may be hard to realize – alluding to Figure 2.6. With estimated deployment costs such as USD 500 million and £10 billion for Connecticut State and the United Kingdom respectively [2.37][2.38], African developing countries would need a low cost deployment strategy for implementing smart metering systems.

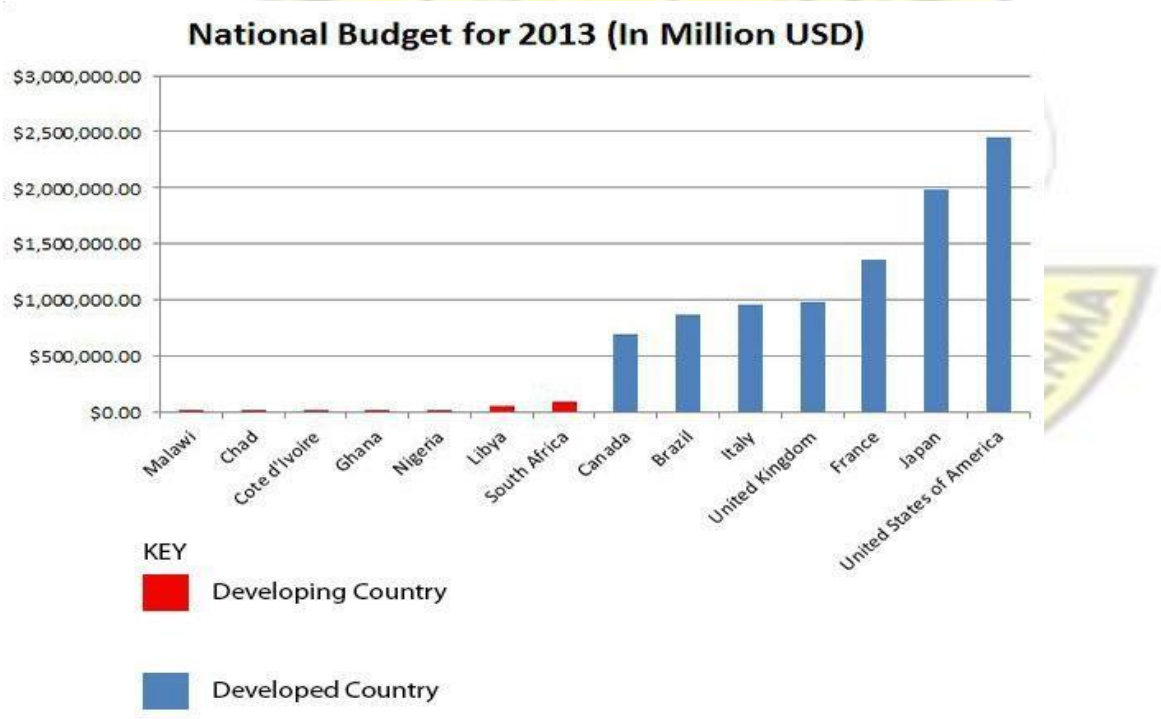


Figure 2.6 2013 national budgets of some developed and developing countries [2.39]

In [2.40], Gianluca Aurilio et al emphasized on the need for the manufacture of low cost smart meters in the near future. It was added that a key feature of these meters would be a reduction in component make up, while maintaining its primary function. Based on this premise a low cost combined voltage and current transducer was developed. This transducer worked in conjunction with a low cost microcontroller board (Arduino) in recording power quality measurements – a basic function of modern smart meters. Various time and frequency domain simulations were conducted to verify the variability of the transduction ratio with the amplitude of the input. Experimental results revealed that the combined low cost transducer was of good performance and accurate at reading power quality measurements. However cost-benefit analysis was not conducted to ascertain the savings made by adopting this low cost module.

In [2.41], Haroldo Amaral and André Souza developed a low cost smart meter for data collection and in-place tests. This meter had a flexible structure which made it easy to modify whenever other field parameters, such as harmonic distortions, were to be considered while taking meter readings. The latest 16-bit MSP430 microcontrollers developed by Texas Instruments were used for carrying out control and logical operations. The MSP430F2013 handled voltage and current signal sampling coming from the mains while the MSP430G2955 stored the waveforms and carried out further signal processing in order to ascertain consumption. Based on experimental results, this low cost smart meter's voltage and current readings had an accuracy of at least 99.1%. Detailed cost-benefit analysis were not conducted, however the cost of components was stated to be USD 41.00. It was also observed that this design did not consider energy theft as an issue to be tackled. Therefore it lacked the necessary anti-tamper and intrusion detection mechanisms and algorithms in its makeup. Also the only

means of communicating recorded data was via a Serial Peripheral Interface (SPI), thus requiring one to connect the meter to an external device before accessing logged meter data.

In [2.42], the authors presented a low-cost strategy to implementing smart meters. The mode of implementation was based on the principle of retrofitting. Standalone electromechanical energy meters were retrofitted with repurposed mobile devices which used image processing to extract energy information. With the aid of tables, this scheme was compared with Internet Protocol (IP) based Smart Meters in terms of cost, frequency of data collection, system components, deployment effort and data reliability. The proposed scheme was argued to be less costly since the only components provided were the mobile device, wall mount and charger as compared to the latter which required a complete replacement of the existing standalone meter – consisting of a lot more components. The cost of the proposed scheme was estimated at USD 140 while that of the IP-based Smart Meters was priced between USD 200 and 800. Backed by efficient digital image processing algorithms, snapshots of analog meter readings taken periodically by the mobile device were further processed after transmission via a wireless communication channel. The cost of wireless communication and power to continuously charge the mobile handset were however not considered. Also this low cost scheme focused only on analog meters and not digital meters. Furthermore, security of the retrofit was not considered. In addition, alluding to the design presented, it was thus judged that communication was one-way; from meter to the utility. The utility therefore had no way of instructing the retrofit (mobile device) to carry out specific operations.

A similar concept is presented in [2.43] by Potuganti Prudhvi et al. In this publication, a low cost add-on device was proposed for existing standalone electromechanical energy meters in India. This add-on was capable of detecting the black/red strip on the magnetic rotary disc of the meter. This made it possible to determine the total number of revolutions made by the disc

which is essential in calculating energy consumption. This add-on comprised basically of an Infra-red (IR) sensor, a comparator, a counter and a real-time clock. Focusing on the Indian context, the proposed communication architecture utilized ZigBee, Global System for Mobile Communication (GSM) and Power Line Carrier (PLC) for data transmission. Despite the allusion of the proposed smart add-on being of low cost, no cost-benefit analysis was provided. Also the add-on was made specifically for analog meters hence would not work with digital energy meters. Finally, no considerations were made for anti-tamper and intrusion mechanisms hence they were not included in the design.

The principle of retrofitting standalone energy meters as a method of producing low-cost smart add-ons/retrofits has not only been limited to the above reviewed publications but has also been implemented extensively by companies such as Connode AB, Cyan Technology Limited, RIO Tronics, Wilson Energy Limited and Xemtec Smart Energy Saving Solutions [2.44 – 2.49]. These companies have developed and deployed smart add-ons/retrofits which furnish existing standalone energy meters with smart meter functionalities. Some of these retrofits are discussed in the paragraphs below.

Connode AB's retrofit, known as the Connode 4, promises to be a cost effective way of upgrading existing standalone energy meters with smart capabilities. By upgrading meters with this retrofit, there is the high possibility of increasing efficiency with low operational and maintenance costs. This retrofit also has features that allow trusted third parties to access data transmitted from the system. Despite these benefits, this retrofit's current design limits it to work with only the Landis+Gyr E350 (ZMF 120/ZCF 120) standalone meter. This meter has an existing communication interface that the retrofit is capable of talking to and retrieving data from. Therefore this retrofit is not guaranteed to work with any other meter [2.44].

Driven by the motivation to provide a cost effective smart metering solution for utilities in emerging countries, Cyan Technology Limited launched the CyLec retrofit in December 2013. Ever since its launch there have been extensive deployments in India and Brazil [2.45]. The retrofit is packaged in a small box which measures 75mm×50mm×50mm. It connects to the existing standalone meter via a cable which is plugged into the meter's communication interface. Similar to the Connode 4 this retrofit is limited to meters of some particular standards. Some of which include IEC 62052-11, IEC 62053-21, IEC62056 DLMS/COSEM, DLT-645-2007 (China) and IEEE1377-2012 PIMA (Brazil) [2.46].

RIO Tronics' *RegistRead* retrofit also provides legacy standalone electromechanical meters with smart meter capabilities. Unlike the Connode 4 and CyLec retrofits which are obtained by utilities and installed by trained professionals, this retrofit is advertised for sale to energy consumers. Detailed instructions are provided to consumers on how the retrofit is to be installed. The method of installation is quite invasive and requires some high level of precision since it involves getting access to the dials of the electromechanical meter. It is also limited to analog energy meters of some particular form factor usually produced by companies such as General Electric, Landis+Gyr, Sangamo and ABB [2.47].

Wilson Energy Limited's CometXPR60 is a low cost retrofit which collects meter data from legacy non-pulsed meters and transmits it via local radio networks to the closest central data concentrator. They are produced for the European market since local radio networks such as ZigBee and Wi-Fi are highly available. Such radio networks are far from ubiquitous in most communities in African developing countries. This retrofit is also limited to analog energy meters; hence would not work with digital meters [2.48].

Xemtec has developed retrofits which furnish both analog and digital standalone meters with smart meter functionalities. These retrofits are carefully integrated into the existing meter in

order to capture images of meter readings. These images are captured using a unique optical lens system. Xemtec uses its patented Optical Character Recognition (OCR) algorithm to make out meter readings from captured images. Similar to RIO Tronics' RegistRead, the method of installation is quite invasive and requires some level of technical expertise. The amount of illumination in the surrounding environment must be considered during the installation process. Also the retrofit for digital meters requires that the meter's display is always turned on. This option considerably decreases the meter's battery life [2.49].

Based on the review of the above publications and deployed retrofits, it has been identified that there is a gap in the search for a low cost strategy for implementing secured smart metering systems in African developing countries. A great deal of the reviewed literature focused on standalone analog electromechanical meters. Over the past decade most of these electromechanical meters have been replaced by solid state digital pulsed meters, therefore there is the need to give ample attention to these new meters [2.50]. Also the method of retrofitting as presented by most of the above mentioned companies are usually invasive and requires some degree of technical expertise. It was also observed that the reviewed low cost designs did not consider anti-tamper and intrusion mechanisms as a measure of mitigating energy theft. In addition, detailed cost-benefit analysis was not conducted to ascertain the amount of savings made.

This research therefore attempts to address this gap by providing a low cost strategy for implementing secured smart metering systems in African developing countries. This strategy would seek to furnish a wide range of digital pulse standalone energy meters with smart meter functionality. It would seek to provide a non-invasive method of interfacing existing energy meters. This strategy would also attempt to incorporate ample anti-tamper and intrusion

mechanisms in order to deal with the issue of energy theft. Finally copious costbenefit analysis would be conducted in order to determine the cost-effectiveness of the proposed strategy.

From the above literature review it was observed that varying communication technologies were adopted for the various deployed and proposed low cost smart modules. In the following section a review of plausible communication technologies is provided in an attempt to highlight option(s) that would be preferable in the development of a low cost solution for African developing countries.

2.3 COMMUNICATION TECHNOLOGIES

The main feature that distinguishes smart meters from standalone meters is its two-way communication ability [2.51]. Most of the benefits associated with smart meters, as discussed earlier in this chapter, exist because of this ability. This implies that the most important feature of the smart meter is its ability to communicate to utilities as well as receive control information and notifications from utilities [2.52]. Therefore it is essential that the means of communication is established before smart meters are designed, manufactured and deployed.

There are a wide range of wired and wireless communication technologies that are currently used for smart metering systems; each having its advantages and disadvantages. It is important to understand these, before making a choice for a particular application area. Table 2.3 summarizes some notable communication technologies available for use in smart meter applications or Advanced Metering Infrastructures (AMI). They are placed under four categories; Landlines, Power Line Carrier (PLC), Wireless and Private Radio [2.53]. Communication technologies which use varying media channels are placed in the ―other‖ category.

Table 2.3 Notable Smart Meter Communication Technologies [2.53]

No.	Category	Technology	Advantages	Disadvantages
1.	Landline	Copper UTP	• Offers DSL, Analog Modem and T1 Speed; • Widely Available.	• Lack of control; • Continuing expenditure.
2.		Optical Fiber	• High Speed; • Secure.	• Expensive; • Point to Point.
3.		Fiber to the home (FTTH)	• Extremely Fast; • Unlimited Bandwidth	• Very Expensive; • Limited Availability.
4.		Hybrid Fiber Coax (HFC)	• Fiber to the neighborhood or group of homes; • Coax into homes.	• Lack of Control.

5.	Power-Line	Power Line Carrier (PLC)	• Long distance communication at slow speed possible; • Low cost and reliable, ready infrastructure; • Communication over power • Supports grid control function (SCADA) and substation; • Good for HAN	• Point-to-point communication; • Low to medium speed; • Can cause disturbances on transmission lines especially in developing countries; • Concerns for Data Security.
6.		Broadband over Power-Line (BPL)	• Supports specific needs of DA, AMI and DR; • Communicates over MV and LV lines; • Next generation of products may not cause interference.	• Lack of interoperability and standards; • Limited deployment; • Can cause electromagnetic interference; • Poor tolerance for noise.

7.	Power-Line	Home-Grid Forum	• Meets need for AMI & DR (SEP v2.0) • Communicates over power-lines, telephone lines and coaxial lines; • Amateur bands are notched in the HomeGrid Forum G.hn specification; • Dual-mode devices interoperate with Home-Plug.	• Cost; • Amateur bands may be only optionally notched in non-Home-Grid Forum G.hn devices; • Single-mode devices interoperate poorly with Home-Plug.
8.		Home-Plug	• Meets needs for AMI and DR; • Communicates over power-line; • Installation quick, easy, and inexpensive; • Good for in-premise communication.	• Interoperability a concern; • FECs adds cost and complexities; • Security can be concern; • Limited deployment.

9.	Radio	Multiple Address System Radio (MAS)	• Flexible, compact and reliable; • SCADA and DA application utilizing it now; • Point to multipoint.	• Poor market penetration; • Limited bandwidth.

10.		Frequency-Hopping Spread Spectrum Radio	• Useful for last mile connection; • Point to multipoint; • Unlicensed Spectrum 902-928MHZ.	• Continuous frequency hopping required; • Line of sight required.
11.	Wireless	3G Cellular	• Less expensive for monitoring substation performance; • Cost effective; • Ready infrastructure, Quick implementation.	• Unsuitable for online substation control; • Coverage area incomplete; • Suitable for short burst of data.
12.		Wi-Fi	• 5 -54 mbps achievable; • Office/Home penetration high; • Open standards to IEEE 802.11g and 802.11b.	• Short range less than 100m; • Poor building reception.
13.		Wi-MAX	• Can gain 75mbps over 10-30 miles; • Backhaul media for in-premise BPL, WiFi, and Zigbee; • Adheres to IEEE802.16d communication standards.	• Poor market penetration; • Currently expensive.

14.		Zigbee	• Unlicensed spectrum 2.4 GHz is used; • Low cost and requires less power; • IEEE 802.15.4 is standards; • Smart Energy Profile (SEP v2.0) available for interoperability with home appliances	• Limited range (lineof-sight); • Concrete walls penetration is weak.
15.		VSAT	• Widely used for remote monitoring and control of transmission and sub-station; • Broad Coverage; • Quick Implementation.	• Severe weather can affect service; • High cost.
16.	Wireless .	Paging Networks	• Short messages to small mobile terminals; • One-way is cost effective; • Some Standards exist.	• Not owned by the power company (lack of control) • Two-way messaging costly; • Most systems proprietary.

17.		OSHAN	• Low cost; • Low power consumption; • IEEE 802.15.4 Standard; • Unlicensed 900MHz spectrum used.	• Medium range inside buildings; • Poor market penetration; • Limited product availability.
18.	Wireless	CDMA Wireless	• Current 2G system uses IS-95 Standard; • Widely available; • 3G Cellularuses IS2000 Standard.	• Only suitable for short bursts of data; • Not suitable for online substation control; • Coverage area incomplete.
19.		TDMA Wireless (Cellular)	• Open IS-136 Standard; • Unique time slots for each user; • Widely available.	• 3G systems use CDMA; • Network capacity limits number of active radios.
20.	Other	Internet Protocol (IP)	• Universal availability; • Low cost; • Multi-vendor functionality; • Open Standards.	• Security; • Latency; • Bandwidth.

21.		Internet2	• High-speed next generation backbone; • 200 Universities working on network applications.	• Not Available

Judging from the information presented in Table 2.3, all the communication technology options have their strengths and weaknesses. Therefore the selection of one or more of them for the design of a low cost secured smart metering system ought to have strengths that are highly desirable and weaknesses that have little or no effect in this application area. In addition, the choice of communication technology must be guided by the following factors:

1. Availability: Leveraging the pervasiveness of technology for quick implementation
2. Reliability: Assurance of data delivery
3. Cost: Price associated with deploying and utilizing the technology

2.3.1 Wireless Communication Technologies in Africa

Among the categories mentioned, the most ubiquitous communication technologies in Africa fall in the Wireless Category [2.54]. This category encompasses the following technologies:

1. Code Division Multiple Access (CDMA)
2. Global System for Mobile Communications (GSM)
3. Open Source Home Area Network (OSHAN)
4. Very Small Aperture Terminal (VSAT)

5. Wireless Local Area Network (WLAN) based on IEEE 802.11 standard also known as Wi-Fi.
6. Worldwide Interoperability for Microwave Access (WiMAX)
7. ZigBee (Based on IEEE 802.15.4 standard)

Figure 2.7 presents a relative comparison analysis of these wireless communication technologies deployed in Africa under the aforementioned guidelines; Availability, Reliability and Cost. Based on these guidelines, plausible communication technologies for a low cost smart metering system for African developing countries should be highly available, highly reliable and of low cost.

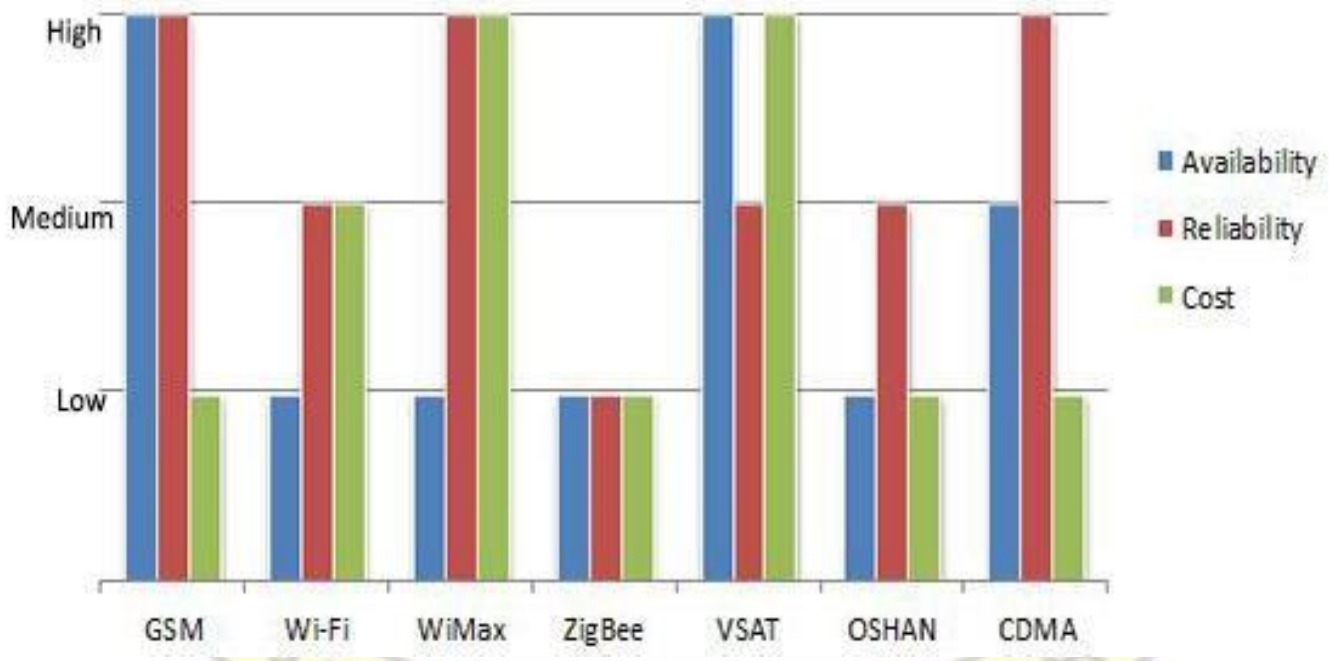


Figure 2.7 Relative Comparisons of Wireless Communication Technologies in Africa [2.53]

From the relative comparisons in Figure 2.7, GSM appears to be highly available, highly reliable and of low cost. Details of these attributes are discussed in the next section.

2.4 GLOBAL SYSTEM FOR MOBILE (GSM) COMMUNICATION

GSM is the most pervasive communication technology in Africa [2.55]. Its wide coverage implies that the necessary infrastructure has already been installed thus making it a suitable early adoption technology for establishing low cost smart metering communication – requiring little or no setup cost. As shown in Figure 2.8, GSM covers a large percentage of the population in most African developing countries. Averagely it covers 70% of the continent's population [2.55].

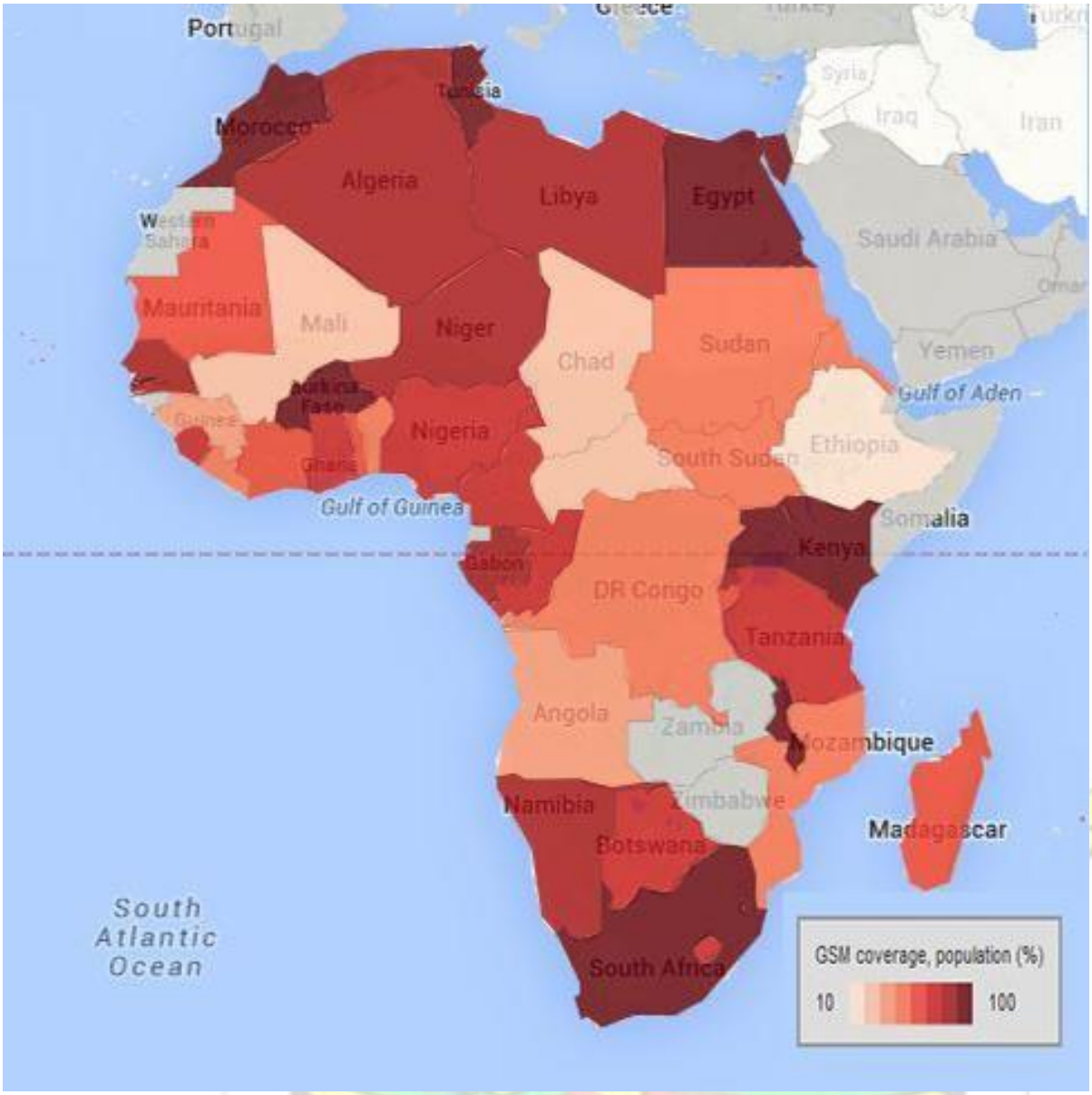


Figure 2.8 Percentage of the population of African Countries covered by GSM [2.55]

GSM has also been tested and tried over decades to reliably deliver data over long distances. As compared to other wireless communication technologies, it has a high propensity of penetrating through concrete walls. Figure 2.9 presents a comparison between GSM and other wireless technologies in terms of data rate and range [2.56].

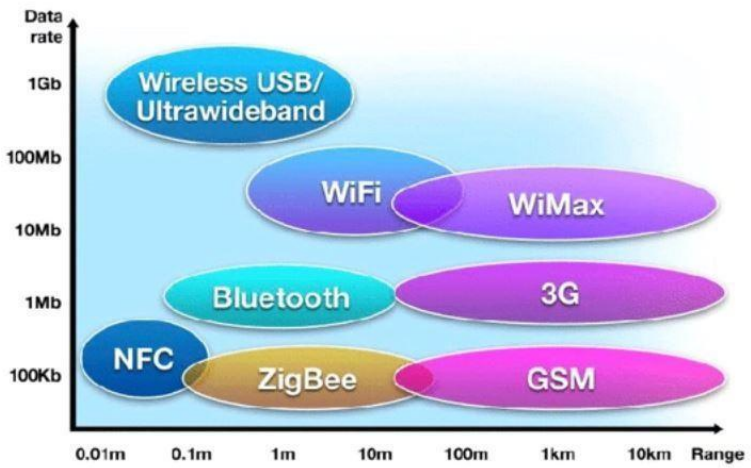


Figure 2.9 Comparisons of Wireless Communication Technologies [2.56]

As pointed out in Table 2.3 and Figure 2.7, subscribers of GSM networks pay lower rates as compared to communication technologies like WiMax, VSAT and Wi-Fi. As a consequence of keen competition among Mobile Network Operators (MNO) in African developing countries, the rates for voice, short message service (SMS) and data via GSM keep subsiding. For example, the cheapest bundle (prepayment) for 60 SMS in Africa dropped from USD 3.1 in 2010 to USD 1.1 in 2014, representing a reduction of 31.4% [2.57]. This is illustrated in Figure 2.10.

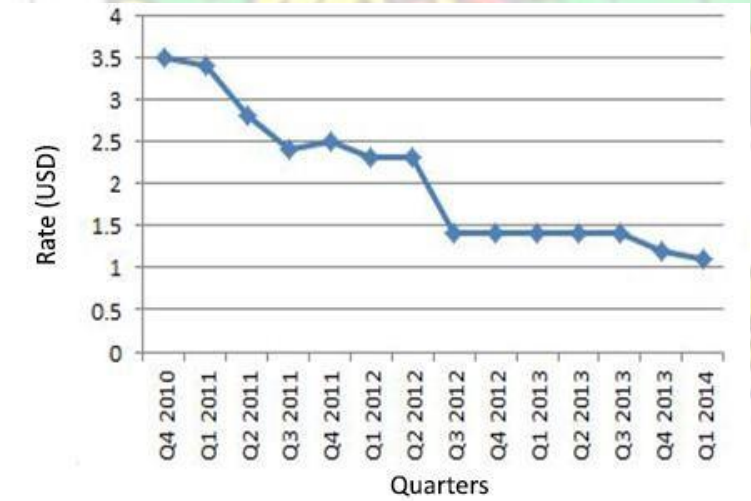


Figure 2.10 Cheapest Bundle Rate in Africa for 60 SMS [2.57]

High-speed transmission of data via GSM is made possible by Packet Switching Services, also known as Mobile Broadband Services [2.58]. These services, unlike Circuit Switching Services, do not require a dedicated communication channel before streaming data; rather, they break the data into packets before transmitting. Each packet can take a different path to the designated destination. This makes these services network efficient, reliable, resilient and cost effective [2.59]. Table 2.4 presents a list of well-known Mobile Broadband Services [2.60].

Table 2.4 Mobile Broadband Services and their maximum data rates [2.60]

Mobile Broadband Services	Maximum Data Rate
Second Generation (2G)	
General Packet Radio Service (GPRS)	114 Kbps
Enhanced Data GSM Environment (EDGE)	368 Kbps
Third Generation (3G)	
High-Speed Downlink Packet Access (HSPDA)	14 Mbps
High-Speed Uplink Packet Access (HSUPA)	34.5 Mbps
High-Speed Packet Access (HSPA)	168 Mbps
Fourth Generation (4G)	
Long Term Evolution (LTE)	299.6 Mbps

Second Generation Mobile Broadband Services (GPRS and EDGE) are the most prevalent services in Sub-Saharan Africa. As at December 2013, 85% of the deployed Mobile Broadband Services were 2G. 3G and 4G services have been predicted to take quite a while before catching up. Figure 2.11 illustrates the predicted growth of Mobile Broadband Services in the Sub-Saharan Region [2.61].

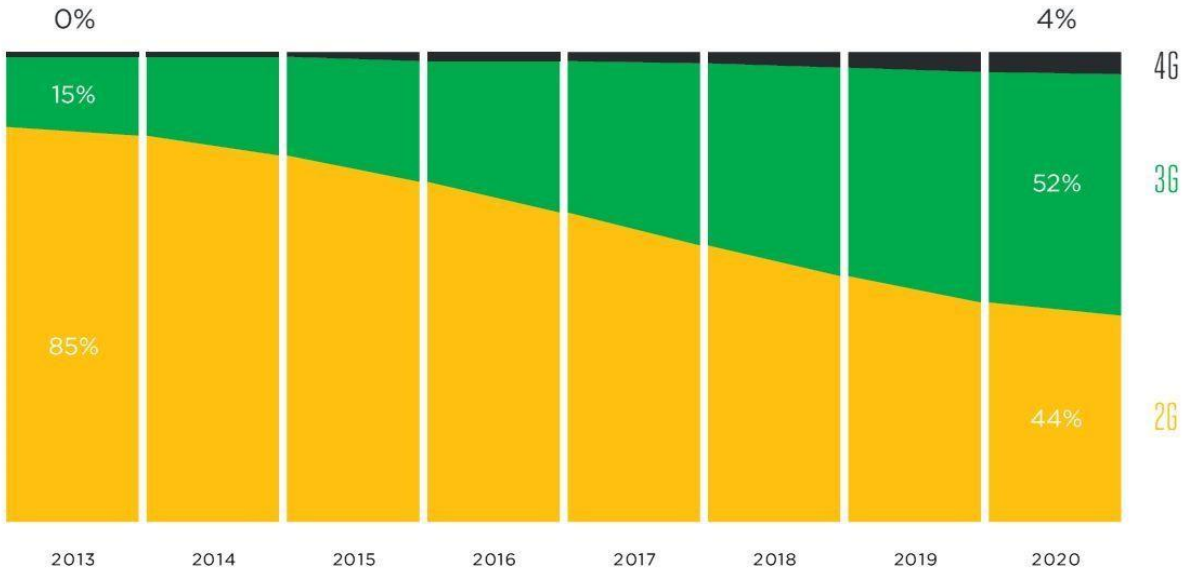


Figure 2.11 Predicted growth of Mobile Broadband in Sub-Saharan Africa [2.61]

Alluding to the high availability and slow decline rate of 2G services in the region, it would not be far from right if smart metering systems deployed in this region transmit data via this service. There should however be support for upcoming 3G services such as Evolved HighSpeed Packet Access (HSPA+).

2.5 ENERGY THEFT

The prime aim of installing an energy meter on a customer's premises is to allow the customer to easily access the meter to know his consumption. Based on this fact utilities do not hide meters or install meters in cramp locations but carefully place them within the customer's reach. It is this ease of access that has facilitated meter tampering by some consumers. This is done with the motive of reducing or totally eliminating the cost of energy consumption; a criminal act often termed as energy theft [2.62].

One of the main purposes for rolling out smart meters is to mitigate energy theft [2.63]. These non-technical losses have been identified as the largest contributor to revenue losses in distributing companies (discos) in African developing countries [2.64]. As stated earlier, Enel

Automated Meter Management Solution estimated that the massive rollout of 30 million smart meters in Italy would result in 80% reduction in these losses [2.65]. It has been reported that ever since this rollout, Enel makes an annual savings of $750 million [2.66].

This confirms their predictions, thus reasserting the smart meter's ability to effectively mitigate energy theft.

Designing a secured low cost smart metering system to effectively combat energy theft in African developing countries requires a thorough understanding of how these felonious acts are carried out. This would suggest the necessary features and systems to be included in the design. The following subsections describe some of the ways in which these acts are carried out and suggest methods of detecting them.

2.5.1 Types of Energy Theft

2.5.1.1 Tampering with Internal Mechanism

This method is aimed at slowing down the meter's kilowatt-hour counter. This is often targeted at electromechanical meters which use the movement of an Aluminium rotor disc to register consumption [2.67]. As depicted in Figure 2.12 the basic components of an electromechanical meter are a rotor disc, a stator, retarding magnets and dials to register consumption.

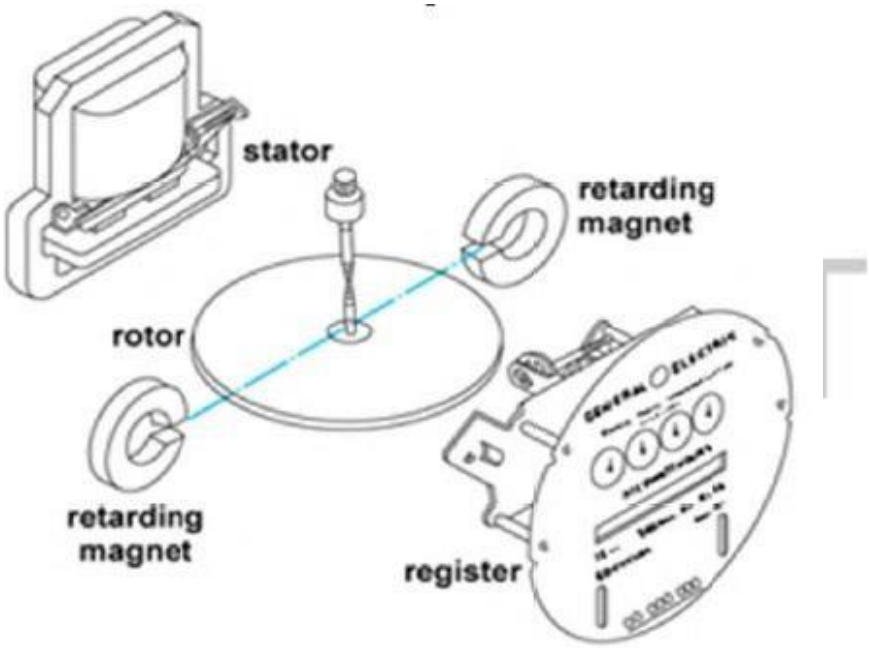


Figure 2.12 Basic parts of an electromechanical meter [2.68]

Criminals tamper with the internal mechanisms of this meter by either breaking off the meter's seal and opening it up or drilling holes into the meter's casing. After getting access, they find ways of resisting the free movement of the rotating disc. This may be done by pouring a coarse material, such as sand, over the disc or placing Neodymium magnets around the rotating disc [2.69]. This strong permanent earth magnet increases the braking torque of the rotating disc, thus slowing it down.

In electronic meters where there are no moving parts, magnetic interference can still be used to destabilize the proper operation of the meter. This is done by using these strong magnets or strong alternating current fields to saturate the meter's magnetic components [2.70]. Current transformers and power supplies are typical examples of such components. By interfering with these components, accurate meter reading is affected.

2.5.1.2 Bypassing the Meter

This is the most common way energy theft is carried out. It is done by connecting a fraction or the entire consumer's load directly to the mains; the cables coming directly from the utility. By doing so, the consumed power is not recorded by the meter. In most cases the perpetrators are not caught because they either carefully conceal the bypass or they take them off right before the meter readers visit their premises [2.71]. Figure 2.13 shows a typical example of a meter bypass.

Figure 2.13 Bypassing a meter [2.72]

2.5.1.3 Inverting the Meter

This method is also targeted at electromechanical meters. Since this meter measures energy consumption through the forward rotation of an Aluminium disc mounted on a motor, its backward rotation would rather reduce the measured value. This backward rotation can be achieved by simply inverting the meter which would reverse the polarity of the connections to the rotating motor as depicted in Figure 2.14 [2.73].

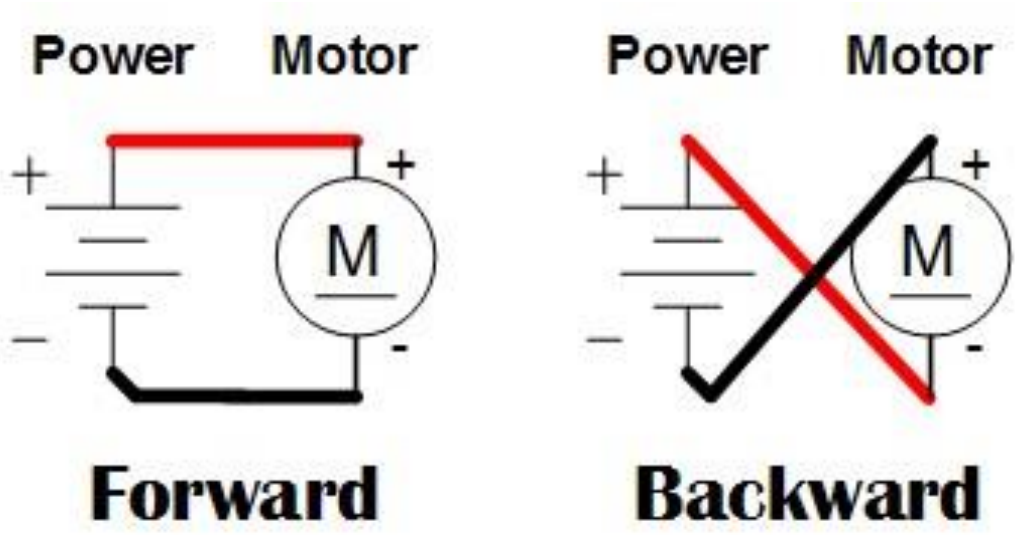


Figure 2.14 Achieving forward and backward rotation of a motor [2.74]

2.5.1.4 Installing a Spare Meter

This is another way energy theft is carried out. Criminals unplug the utility installed meter and install a spare meter in its place to record the bulk of the consumed energy. They are careful to reinstall the meter provided by the utility before meter readers visit their premises [2.67]. This practice has become so easy to carry out considering the fact that visits from meter readers are so predictable; usually at the end of the month. Also these meters are being made available for purchase, especially from online stores [2.75].

2.5.1.5 Corrupt Officials from Utilities

Another plausible way energy theft is carried out is through the help of corrupt officials from utilities. These officials, for a price, may help perpetrators of these acts go undetected by not reporting them or even helping in the pilferage by sending reduced meter readings to the utility for billing [2.76].

2.5.1.6 Faulty Meters

Even though most utilities thoroughly test meters before installing them on the premises of consumers, there are cases where meters have gone faulty. Such meters are likely to give anomalous readings and as such need replacement upon detection. However, criminals who detect these anomalies, especially when readings are far below the expected, would intentionally not report such faults [2.77].

The above methods of energy theft are to be considered when designing the proposed smart retrofit to enhance standalone energy meters with smart meter functions. These felonious activities can be mitigated when the right energy theft detection mechanisms are incorporated into the system design.

2.5 SUMMARY

In this chapter, smart metering systems are introduced as an effective system for dealing with power crises. In addition proposed and deployed low cost smart modules and retrofits are reviewed in an attempt to bring to light current trends in smart metering systems and identify a gap in literature. Also a discussion is made on plausible communication technologies for deploying a low cost secured smart metering system for African developing countries. Finally, common methods of energy theft are briefly described with the aim of including ample detection mechanisms to mitigate these acts.

REFERENCES

[2.1] A Joint Project of the EEI and AEIC Meter Committees, ―Smart Meters and Smart Meter Systems: A Metering Industry Perspective‖, An EEI-AEIC-UTC White Paper, pp. 5-10 March 2011.

[2.2] Silver Spring Networks, ―Smart Metering - The foundation of the Smart Grid‖, Silver Spring Networks Whitepaper, June 2013.

[2.3] Norman B. Ndaba, ―Smart Metering – Transforming Africa's Energy Future‖, EY GM Limited, 2013.

[2.4] Faruqui A., Sergici S. and Sharif A., ―The Impact of Informational Feedback on Energy Consumption – A Survey of the Experimental Evidence‖, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1407701, 2009.

[2.5] Dobbyn J. and Thomas G., ―Seeing the light: the impact of microgeneration on the way we use energy.‖, Qualitative research findings. Hub Research Consultants, London, on behalf of the Sustainable Consumption Roundtable, pp. 5 – 6, 2005.

[2.6] Mari Martiskainen and Josie Ellis, ―The role of smart meters in encouraging behavioural change - prospects for the UK‖, Sussex Energy Group, SPRU (Science and Technology Policy Research), University of Sussex, 2013.

[2.7] Jackson, T., ―Motivating Sustainable Consumption, a review of evidence on consumer behaviour and behavioural change‖, Sustainable Development Research Network, 2005.

[2.8] Young, S., ―Climate Change and ICT‖, Ovum Comments, 2006.

[2.9] Erdmann, L., Hilty, L., Goodman, J. and Arnfalk, P., ―The Future Impact of ICTs on Environmental Sustainability‖, Institute for Prospective Technological Studies, European Commission Joint Research Centre, 2004.

[2.10] SMWG, ―Report of Smart Metering Working Group‖ http://www.ofgem.gov.uk/temp/ofgem/cache/cmsattach/1721_SmartReport.pdf, 2001.

[2.11] Environmental Health Services, ―Smart Monitor Loan Service‖, Exeter City Council, http://www.exeter.gov.uk/index.aspx?articleid=10545, June 2015.

[2.12] Darby S., ―The Effectiveness of Feedback on Energy Consumption - A Review for DEFRA of the Literature on Metering, Billing and Direct Displays‖, Environmental Change Institute, Oxford University. http://www.defra.gov.uk/environment/energy/research/, 2006.

[2.13] Jon Fakuda, ―Smart Meters: Power to the People – The New Energy Experience‖, Limina, http://limina-ao.com/blog/tag/smart-meters/, May 2009.

[2.14] Karen Ehrhardt-Martinez, ―The Persistence of Feedback-Induced Energy Savings‖, http://www.stanford.edu/group/peec/cgi-bin/docs/behavior/research/Ehrhardt-Martinez%202011%20-%20Feedback%20and%20Persistence%20Paper.pdf, 2011.

[2.15] Van Dam S., Bakker C. and Van Hal J., ―Home energy monitors: impact over the medium-term‖, Building Research & Information 38 (5), 458-469, 2010.

[2.16] Froehlich J., Larson E., Gupta S., Cohn G., Reynolds M. and Patel S., ―Disaggregated End-Use Energy Sensing for the Smart Grid. Pervasive Computing‖, http://homes.cs.washington.edu/~sidhant/docs/ElectriSense_Journal.pdf, 2011.

[2.17] Abrahamse W., Steg L., Vlek C. and Rothengatter T., ―A review of intervention studies aimed at household energy conservation‖, Journal of Environmental Psychology, 25, 273–291, 2005.

[2.18] U.S. Department of Energy, ―Benefits of Demand Response in Electricity Markets and Recommendations for Achieving Them‖, A Report to the United States Congress Pursuant to Section 1252 of the Energy Policy Act of 2005, February 2006.

[2.19] IndEco Strategic Consulting Incorporated, ―Demand side management and demand response in municipalities‖, Clean Air Partnership, 2003.

[2.20] United States Federal Energy Regulatory Commission, ―Demand Response and Advanced Metering‖, Staff Report, December 2014.

[2.21] Barbara Alexander, ―Smart Meters, Real Time Pricing, and Demand Response Programs: Implications for Low Income Electric Customers‖, Consumer Affairs Consultant, May 2007.

[2.22] Ahmad Faruqui, Dan Harris and Ryan Hledik, ―Unlocking the €53 Billion Savings from Smart Meters in the EU: How increasing the adoption of dynamic tariffs could make or break the EU's smart grid investment‖, The Brattle Group, October 2009.

[2.23] ―Energy in Africa‖, Wikipedia, http://www.en.wikipedia.org/wiki/Energy_in_Africa, March 2015.

[2.24] United States Department of Energy, ―Operations and Maintenance Savings from Advanced Metering Infrastructure – Initial Results‖, American Recovery and Reinvestment Act of 2009, Smart Grid Investment Grant Program, December 2012.

[2.25] Thomas B.Smith, ―Electricity theft: a comparative analysis‖, Energy Policy 32 (2004) 2067–2076, pp. 1-4, December 2004.

[2.26] Sharelynn Moore, ―Key Features of Meter Data Management Systems‖, Itron White Paper, Meter Data Management, 2008.

[2.27] Africa Energy Indaba, Press Release ,―Africa Energy Indaba ups the ante with new side events for 2015‖, Solutions for Africa Conference and Exhibition, August 2014.

[2.28] ESI Africa, ―Zimbabwe cancels pre-paid meters with immediate effect‖, http://www.esi-africa.com/zimbabwe-cancels-pre-paid-meters-with-immediateeffect/, October 30, 2014.

[2.29] Buzztrick, ―ECG loses 12.4% revenue due to non-payment of bills‖, Ghana Web, http://buzztrick.com/buzz/2014/09/11/ecg-loses-124-revenue-due-non-payment-bills, September 2014.

[2.30] Silver Spring Networks, ―How the Smart Grid Makes Restoration Faster and Easier for Utilities‖, Silver Spring Networks Whitepaper, July 2013.

[2.31] Armin Haghi and Oliver Toole, ―The Use of Smart Meter Data to Forecast Electricity Demand‖, CS229 Course project, Fall 2013.

[2.32] Wes Frye, ―Smart Grid: Transforming the Electricity System to Meet Future Demand and Reduce Greenhouse Gas Emissions‖, Cisco Internet Business Solutions Group, Cisco Whitepaper, November 2008.

[2.33] Hanna Svahnström, ―Demand Side Management in Smart Grids: A review of selected research and demonstration projects and identification of success factors and research needs‖, Göteborgs Universitet, May 2013.

[2.34] Martin Fitch and Cosmo Graham, ―Electricity and Gas Theft‖, Centre for Utility Consumer Law, University of Leicester, January 2010.

[2.35] Sara Bryan PaSquier, ―Saving Electricity in a Hurry‖, Energy Efficiency Series, International Energy Agency, pp. 4-20, June 2011.

[2.36] Saurabh Amin, Galina A. Schwartz and Hamidou Tembine, ―Incentives and Security in Electricity Distribution Networks‖,Gamesec, pp. 264-280, November 2012.

[2.37] ―Smart Meter‖, Wikipedia, http://www.en.wikipedia.org/wiki/Smart_meter, April 2015.

[2.38] Pablo Rámila and Hugh Rudnick, ―Assessment of the Introduction of Smart Metering in a Developing Country‖, IEEE, 2009.

[2.39] International Statistics, ―Countries Compared by Economy > Budget > Revenue‖, Nation Master,

http://www.nationmaster.com/countryinfo/stats/Economy/Budget/Revenues, July 2015.

[2.40] Gianluca Aurilio, Daniele Gallo, Carmine Landi, Mario Luiso, Vivianna Cigolotti and Giorgio Graditi, ―Low Cost Combined Voltage and Current Transducer for Smart Meters‖, Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, 2014 IEEE International Conference, Pages: 1459 - 1464, DOI: 10.1109/I2MTC.2014.6860987, 2014.

[2.41] Haroldo L. M. do Amaral and André N. de Souza, ―Development of a Low Cost Smart Meter to Collecting Data and In-Place Tests‖, Industry Applications (INDUSCON), 2014 11th IEEE/IAS International Conference, Pages: 1 - 7, DOI: 10.1109/INDUSCON.2014.7059422, 2014.

[2.42] Yachen Tang, Chee-Wooi Ten, Chaoli Wang and Gordon Parker, ―Extraction of Energy Information from Analog Meters Using Image Processing‖, IEEE Transactions on Smart Grid, Volume: 6, Issue: 4, Pages: 2032 - 2040, DOI: 10.1109/TSG.2015.2388586, 2015.

[2.43] Potuganti Prudhvi, Dhruv Bhalodi, Manikant Manohar, Vamshi Padidela and Sudarshan Adapa, ―A Smart Energy Meter Architecture in Indian Context‖, 2012 2nd Iranian Conference on Smart Grids (ICSG), Pages: 1 – 6, 2012.

[2.44] Connode AB, ―Solutions - Connode‖, http://www.connode.com/solutions/, January 2016.

[2.45] Cyan Technology Limited, ―Cyan Provides Retrofit Upgrade to Enable Smart Upgrade of Existing Meter Deployments‖, http://www.cyantechnology.com/articles/cyan-provides-retrofit-upgrade-enablesmart-upgrade-existing-meter-deployments/, December 2013.

[2.46] Cyan Technology Limited, ―Smart electricity metering‖, http://www.cyantechnology.com/smart-electricity-metering/, November 2015

[2.47] Rio Tronics', ―Electric Submetering‖, http://www.riotronics.com/submeteringsystems/electric-submetering/, January 2016.

[2.48] Wilson Energy Limited, ―New Products, Smart Metering – Retrofit Meter Solution‖, http://www.wilsonenergy.co.uk/?page_id=137, January 2016.

[2.49] Xemtec SA, ―Automated Readings‖, http://www.xemtec.com/index.php/solutionsen/automated-readings-en, February 2016.

[2.50] Brian Seal and Mark McGranaghan, ―Accuracy of Digital Electricity Meters‖, Electric Power Research Institute, May 2010.

[2.51] A Joint Project of the EEI and AEIC Meter Committees, ―Smart Meters and Smart Meter Systems: A Metering Industry Perspective‖, EEI-AEIC-UTC White Paper, pp. 5-10 March 2011.

[2.52] Silver Spring Networks, ―Smart Metering - The foundation of the Smart Grid‖, Silver Spring Networks Whitepaper, June 2013.

[2.53] The Energy and Resource Institute, ―Smart Grid Communication Technologies Getting Smarter‖, Shakti Sustainable Energy Foundation, http://regisindia.com/wpcontent/uploads/2013/10/Smart-Grid-Communication-Technologies_12112013_F.pdf, July 2015.

[2.54] Mirjam De Bruijn, ―Communication technologies in Latin America and Africa: A multidisciplinary perspective‖, African Studies Centre, Leiden University, October 2009.

[2.55] ―GSM Coverage Population‖, Mobile for Development Impact, https://mobiledevelopmentintelligence.com/statistics/67-gsm-coverage-population, January 2015.

[2.56] Future Electronics, ―Comparison of Wireless Technologies, (NFC - WIFI - Zigbee - Bluetooth - GSM)‖, Future Electronics Limited, Egypt, http://www.futelectronics.com/wpcontent/plugins/fe_downloads/Uploads/Comparison%20of%20Wi reless%20Technologies.pdf, June 2015.

[2.57] Enrico Calandro, Chenai Chair and Alison Gillwald, ―Shift from just voice services: African markets gearing for internet‖, Research ICT Africa, 2014.

[2.58] Brahim Ghribi and Luigi Logrippo, ―Understanding GPRS: The GSM Packet Radio Service‖, School of Information Technology and Engineering, University of Ottawa, 2000.

[2.59] Heino Hameleers and Christer Johansson, ―IP Technology in WCDMA/GSM core networks‖, Ericsson Review, No. 1, 2002.

[2.60] Qualcomm, ―The Evolution of Mobile Technologies‖, Qualcomm Technologies Incorporated, June 2014.

[2.61] Groupe Spéciale Mobile Association (GSMA), ―The Mobile Economy: Sub-Saharan Africa 2014‖, GSMA Intelligence, 2014.

[2.62] Thomas B.Smith, ―Electricity theft: a comparative analysis‖, Energy Policy 32 (2004) 2067–2076, pp. 1-4, December 2004.

[2.63] M. Anas, N. Javaid, A. Mahmood, S. M. Raza, U. Qasim and Z. A. Khan, ―Minimizing Electricity Theft using Smart Meters in AMI‖, University of Alberta, Alberta, Canada, August 2012.

[2.64] Africa Energy Indaba, Press Release ,―Africa Energy Indaba ups the ante with new side events for 2015‖, Solutions for Africa Conference and Exhibition, August 2014.

[2.65] Ahmad Faruqui, Dan Harris and Ryan Hledik, ―Unlocking the €53 Billion Savings from Smart Meters in the EU: How increasing the adoption of dynamic tariffs could make or break the EU's smart grid investment‖, The Brattle Group, October 2009.

[2.66] KEMA Laboratories, ―Combatting Energy Theft with the Smart Grid‖, DNV GL, http://smartgridsherpa.com/wp-content/uploads/2013/02/Energy-Theft-D1V4.pdf, June 2015.

[2.67] Karl A. Seger and David J. Icove, ―Power Theft – The Silent Crime‖, FBI Law Enforcement Bulletin, March 1988.

[2.68] Power Systems Lost, ―Construction of an Electro-Mechanical Meter and Basic Parts‖, http://powersystemsloss.blogspot.com/2011/11/construction-of-electromechanical.html, January 2012.

[2.69] Roman Targosz, ―Electricity Theft – A Complex Problem‖, Leonardo Energy, http://www.leonardo-energy.org/blog/electricity-theft-complex-problem, July 2009.

[2.70] Steve Eckles and Skip Clark, ―Pulling the Plug on Energy Theft‖, Electric Light and Power, http://www.elp.com/articles/powergrid_international/print/volume-12/issue9/features/pulling-the-plug-on-energy-theft.html, January 2007.

[2.71] Sahoo S, Nikovski D.N., Muso T. and Tsuru K, ―Electricity Theft Detection Using Smart Meter Data‖, Mitsubishi Electric Research Laboratories, Tr2015-005, January 2015.

[2.72] Katherine Tweed, ―Hack Your Meter While You Can‖, Green Tech Grid, https://www.greentechmedia.com/articles/read/hack-your-meter-while-you-can, April 2010.

[2.73] Rick A. Schmidt, ―Steps to Reducing Power Theft Overview: State of the Industry‖, Power System Engineering Incorporated, Tech Advantage Conference and Expo, February 2013.

[2.74] Robot Room, ―Simplest Method to Make a Motor Turn Off, Turn On, Go Forwards, and Go Backwards‖, http://www.robotroom.com/DPDT-Bidirectional-MotorSwitch.html, July 2015.

[2.75] Peter Kelly-Detwiler, ―Electricity Theft: A Bigger Issue than You Think‖, Forbes, http://www.forbes.com/sites/peterdetwiler/2013/04/23/electricity-theft-a-bigger-issuethan-you-think/, April 2013.

[2.76] Roohi Ahmed, ―Corruption and Inefficiency in the Delivery of Public Utilities: Case Study of Electricity Services‖, Public Policy and Administration Research, ISSN 2224-5731(Paper), ISSN 2225-0972(Online), Vol.2, No.4, 2012.

[2.77] Money Web, ―Electricity theft in Joburg cripples power supply‖, http://savemoney.co.za/articles/electricity-theft-in-joburg-cripples-power-supply/, March 2015.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 INTRODUCTION

This chapter presents guidelines of a Retrofit Design Science Research Methodology (RDSRM) which is adopted for this research. Section 3.1 discusses two principles of low cost design which are derived from the reviewed literature. Section 3.2 introduces the prescribed steps of RDSRM.

3.1 PRINCIPLES OF LOW COST DESIGN

From the literature reviewed in the previous chapter, it was observed that two principles of low cost smart meter design were followed. These principles include:

1. Reduction in system component makeup by making a single low cost unit to accurately perform multiple functions; originally performed by several units.
2. Retrofitting existing standalone meters with smart modules to furnish them with smart meter functions.

The first principle required that existing standalone energy meters be completely replaced by new smart meters while the second suggested otherwise. The first principle was adhered by only [3.1] and [3.2] while the rest [3.3 – 3.10] followed the second principle. In other words, a great deal of the reviewed literature subscribed to the principle of retrofitting as a low cost strategy for implementing smart meters. The following are plausible reasons why this was so:

1. To avoid the complete replacement of existing standalone meters which over the years have proven to reliably and accurately measure consumption

2. To minimize time, cost and effort required to design and develop smart energy meters.

Based on these reasons, this research adopts this principle of retrofitting in providing a low cost early adoption strategy for implementing secured smart metering systems in African developing countries.

3.2 DESIGN METHODOLOGY

In adhering to the principle of retrofitting, it is imperative that the existing standalone energy meter be studied critically in order to develop an effective retrofit design. A research methodology that is potentially suitable for the design of system retrofits is the Retrofit Design Science Research Methodology (RDSRM) [3.11]. This methodology is a modification of the Design Science Research Methodology (DSRM) [3.12]. The latter focuses on creating innovative artifacts while the former focuses on transforming existing functional artifacts into other existing products. Therefore in RDSRM, even though the final products are not entirely innovative, they were not originally achieved through the process of retrofitting.

The prescribed guidelines of RDSRM are outlined below:

1. Relevance Identification
2. Comparative System Analysis
3. Design and Development
4. Comparative Evaluation
5. Communication

A brief introduction of how each of these guidelines is followed in this research is provided in the following subsections.

3.2.1 Relevance Identification

In identifying the relevance of this research, sufficient justification has been provided in the preceding chapters. These chapters covered the significance of the study by identifying the gap

in literature that the research attempts to address. Also the benefits African developing countries stand to achieve from this research have been clearly established.

3.2.2 Comparative System Analysis

This guideline requires that the existing system to be retrofitted be studied and juxtaposed to the final product to be produced. This is done in order to identify the missing sub-units, functions and algorithms in the existing system. Going by this guideline, a wide range of existing standalone digital pulse energy meters that are currently deployed in Ghana would be requested from a utility and studied. The functions and sub-units of these meters would be compiled and compared with those of standardized smart meters.

3.2.3 Design and Development

In this step, a retrofit is designed comprising the identified sub-units and functions that are missing in the existing standalone meter. A critical process which greatly influences the design of the retrofit is the method of interfacing – how the retrofit communicates with the existing meter. As stated earlier, this research seeks to provide a non-invasive method of interfacing the existing standalone meter. Therefore it is important this method is different from those presented earlier in the literature review. However, this method should not significantly increase the cost of producing the smart retrofit or limit its functionality or accuracy. Based on the design a prototype is developed and tested.

3.2.4 Comparative Evaluation

This guideline suggests that the newly retrofitted system be compared with a standardized smart meter in terms of performance. This is to verify if the design and development processes achieved the set objectives. In this research, it is important that these tests are done in the light

of the identified gaps in literature in order to ascertain if these gaps have been sufficiently addressed.

3.2.5 Communication

In this step, the problem the retrofitted system solves, its significance, design and development process and results from comparative evaluation must be communicated to a relevant audience.

3.3 SUMMARY

In this chapter guidelines are suggested for the design and development of a secured low cost smart metering system for African developing countries.

REFERENCES

[3.1] Gianluca Aurilio, Daniele Gallo, Carmine Landi, Mario Luiso, Vivianna Cigolotti and Giorgio Graditi, ―Low Cost Combined Voltage and Current Transducer for Smart Meters‖, Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, 2014 IEEE International Conference, Pages: 1459 - 1464, DOI: 10.1109/I2MTC.2014.6860987, 2014.

[3.2] Haroldo L. M. do Amaral and André N. de Souza, ―Development of a Low Cost Smart Meter to Collecting Data and In-Place Tests‖, Industry Applications (INDUSCON), 2014 11th IEEE/IAS International Conference, Pages: 1 - 7, DOI: 10.1109/INDUSCON.2014.7059422, 2014.

[3.3] Yachen Tang, Chee-Wooi Ten, Chaoli Wang and Gordon Parker, ―Extraction of Energy Information from Analog Meters Using Image Processing‖, IEEE Transactions on Smart Grid, Volume: 6, Issue: 4, Pages: 2032 - 2040, DOI: 10.1109/TSG.2015.2388586, 2015.

[3.4] Potuganti Prudhvi, Dhruv Bhalodi, Manikant Manohar, Vamshi Padidela and Sudarshan Adapa, ―A Smart Energy Meter Architecture in Indian Context‖, 2012 2nd Iranian Conference on Smart Grids (ICSG), Pages: 1 – 6, 2012.

[3.5] Connode AB, ―Solutions - Connode‖, http://www.connode.com/solutions/, January 2016.

[3.6] Cyan Technology Limited, ―Cyan Provides Retrofit Upgrade to Enable Smart Upgrade of Existing Meter Deployments‖, http://www.cyantechnology.com/articles/cyan-provides-retrofit-upgrade-enablesmart-upgrade-existing-meter-deployments/, December 2013.

[3.7] Cyan Technology Limited, ―Smart electricity metering‖, http://www.cyantechnology.com/smart-electricity-metering/, November 2015.

[3.8] Rio Tronics', ―Electric Submetering‖, http://www.riotronics.com/submeteringsystems/electric-submetering/, January 2016.

[3.9] Wilson Energy Limited, ―New Products, Smart Metering – Retrofit Meter Solution‖, http://www.wilsonenergy.co.uk/?page_id=137, January 2016.

[3.10] Xemtec SA, ―Automated Readings‖, http://www.xemtec.com/index.php/solutionsen/automated-readings-en, February 2016.

[3.11] J. Q. Azasoo and K. O. Boateng, ―Retrofit Design Science Methodology for Smart Metering Design in Developing Countries‖, Computational Science and Its Applications (ICCSA), IEEE, 2015 15th International Conference, 2015.

[3.12] Ken Peffers, Tuure Tuunanen, Charles E. Gengler, Matti Rossi, Wendy Hui, Ville Virtanen And Johanna Bragge, ―The Design Science Research Process: A Model For Producing and Presenting Information Systems Research‖, Proceedings of the First International Conference On Design Science Research In Information Systems And Technology (DESRIST 2006), Pages 83 – 106, February 2006.

CHAPTER FOUR: RETROFIT DESIGN

4.0 INTRODUCTION

Guided by the adopted research methodology, this chapter discusses the entire design process of the proposed smart retrofit. It begins with a recap of the objectives and significance of the research in Section 4.1. In Section 4.2 comparative analysis is conducted in order to ascertain the missing units in non-smart energy meters. Section 4.3 specifies the functional requirements of the smart retrofit to be designed. In Sections 4.4 and 4.5 discussions and experiments are conducted to determine a suitable non-invasive method of interfacing the existing meter. In Section 4.6 essential components for the smart retrofit design are elicited.

Finally in Section 4.7 engineering tools are used to model the system's important processes.

4.1 RELEVANCE IDENTIFICATION

As presented in Chapter Two, after having identified a gap in research for the search of a low cost early adoption strategy for the implementation of secured smart metering systems in African developing countries, this research attempts to do the following:

1. Provide a retrofit design which furnishes a wide range of existing digital pulse standalone energy meters with smart meter functionality.
2. Provide a non-invasive method of interfacing existing digital pulse standalone energy meters with the proposed smart retrofit design.
3. Incorporate ample anti-tamper and intrusion detection mechanisms into the proposed design in order to sufficiently deal with common methods of energy theft.
4. Provide detailed cost-benefit analysis to ascertain savings made by adopting the proposed smart retrofit design.

As stated earlier in Chapter One, after achieving the above mentioned objectives, African developing countries stand the chance of eliminating unprecedented energy demand through the provision of detailed demand analyses; thus dealing effectively with the bane of energy crises. Other associated benefits include the following:

4. An increase in energy conservation through the provision of direct and indirect feedback to customers in real-time. This would also lead to reduction in energy demand, lower cost of electricity generation, lower energy bills and lower carbon emissions.

5. Persistence in energy savings through the rollout of DR programs which are heavily dependent on real-time notifications.

6. A reduction in a utility's field operational cost, customer service cost, revenue losses and purchasing and logistic cost through the provision of automatic and remote

(dis)connection, power outage detection, energy theft detection, accurate meter reading and bills distribution.

The following sections cover the design of the smart retrofit intended to equip existing digital pulse standalone energy meters with smart meter functionality.

4.2 COMPARATIVE SYSTEM ANALYSIS

In order to determine the functional requirements of the smart retrofit there was the need to conduct comparative system analysis between existing digital pulse standalone energy meters and smart energy meters. A request was made to Electricity Company of Ghana (ECG), the main electricity distribution company for southern Ghana, to provide sample energy meters for this comparative analysis. They provided twelve different meters, which are samples of their most deployed energy meters. Their functions and features were juxtaposed to two Siemens smart energy meters – IM100 and IM300. These two smart meters comply with DLMS/IEC 62056 standards. Table 4.1 summarizes the results of this comparison.

Table 4.1 Comparative System Analysis between Non-Smart and Smart Energy Meters

Function/Feature	Non-Smart	Smart
In-home Display	✓	✓
Measuring of energy consumption in Kilowatt-hours	✓	✓
Measuring of energy consumption in Currency	✘	✓
Power Quality Measurements	✓	✓
Load Profiling	✘	✓
Consumer Notifications	✘	✓
Outage Notifications	✘	✓
Hourly/ On-demand Reads	✘	✓

Dynamic Energy Prices (Multiple Tariffs)	✘	✓
Two-Way Communication Ability	✘	✓
Anti-tamper and Intrusion Detection Mechanism	✘	✓

Alluding to Table 4.1, it can be thus said that both meter types are capable of performing the basic functionality of measuring and displaying consumption in kilowatt-hours. However, all other functions/features which are dependent on two-way communication ability such as consumer notifications, outage notifications, measuring of energy consumption in currency and load profiling are not present in these standalone (non-smart) meters. Also these standalone meters are incapable of providing ample anti-tamper and intrusion detection mechanisms against common methods of energy theft. Therefore Table 4.1 can be further summarized as Table 4.2.

Table 4.2 Summarized Comparative Analysis between Non-Smart and Smart Meters

Function/Feature	Non-Smart	Smart
Measuring/Display of energy consumption in kWh	✓	✓
Two-Way Communication Ability	✘	✓
Anti-tamper and Intrusion Detection Mechanism	✘	✓

Based on the summarization in Table 4.2, the smart meter can thus be seen as an ordinary standalone meter enhanced with communication and tamper detection mechanisms as depicted in Figure 4.1.

Figure 4.1 Basic Constituents of a Smart Meter

Therefore the retrofit to be designed must have these missing units in order to equip existing digital pulse standalone energy meters with the full functions of a standardized smart energy meter.

4.3 REQUIREMENTS SPECIFICATION

To have a clearer definition of the retrofit's basic functional requirements, use cases are employed in eliciting these requirements. These help to present in natural language (unambiguous terms) the expectations, goals and benefits of the system to the major actors/stakeholders, namely consumers and utilities (Distributing Companies and Power Generating Stations). These use cases are presented in Figures 4.2 and 4.3.

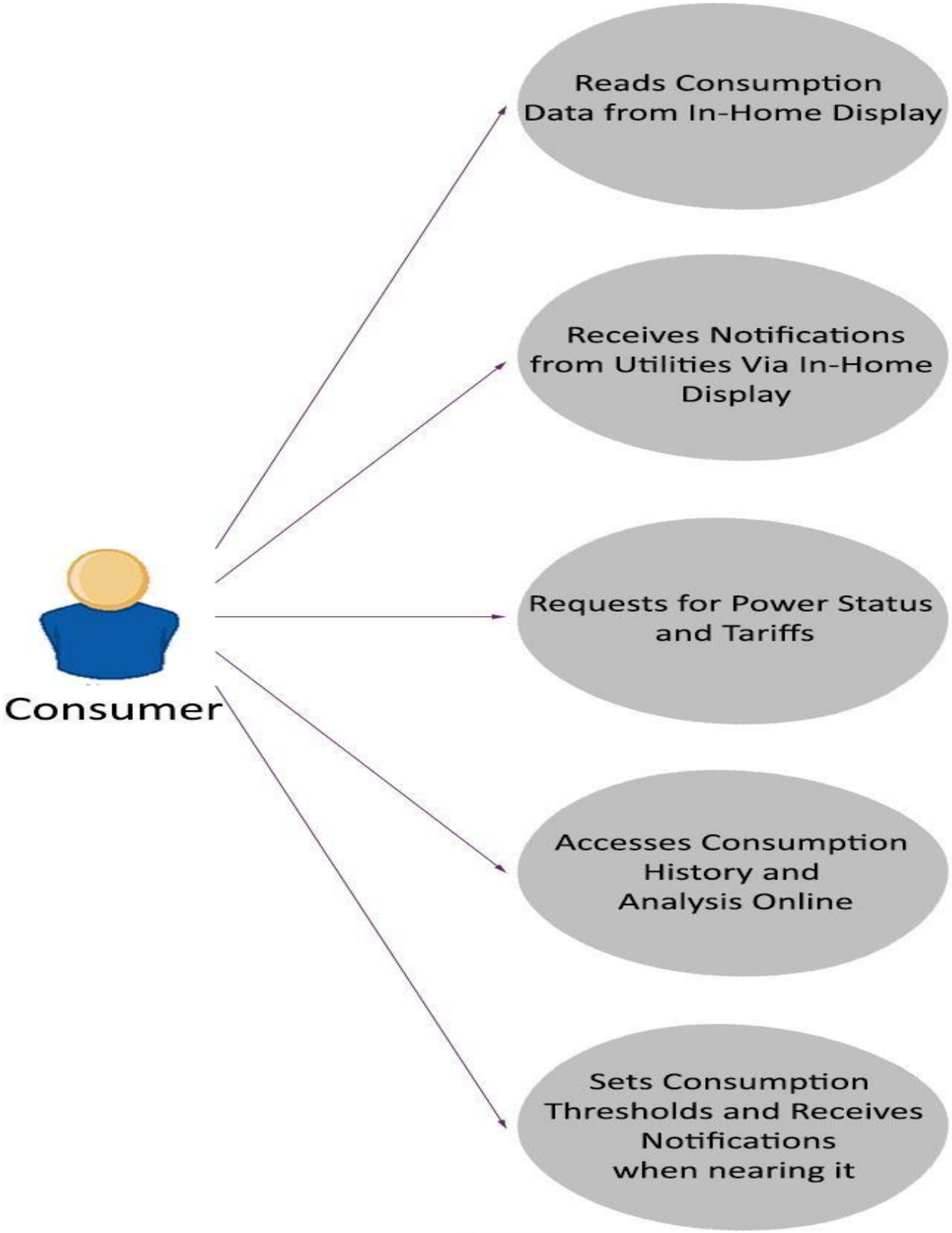

Reads Consumption Data from In-Home Display
Receives Notifications from Utilities Via In-Home Display
Requests for Power Status and Tariffs
Accesses Consumption History and Analysis Online
Sets Consumption Thresholds and Receives Notifications when nearing it
Consumer

Figure 4.2 Consumer Use Case

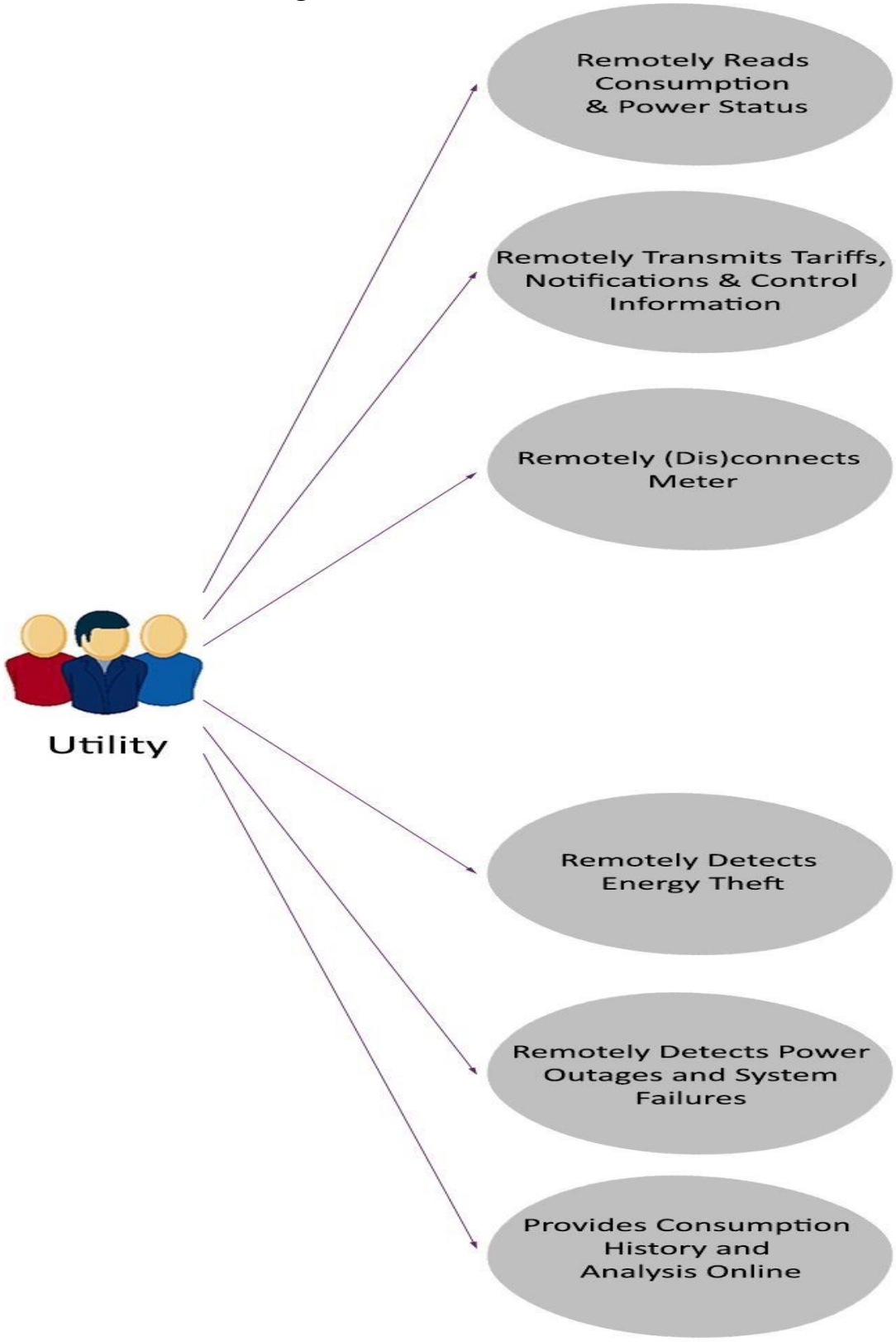


Figure 4.3 Utility Use Case

Based on the use cases provided above, the functional requirements of the retrofit can be summarized as follows:

1. Display of accurate consumption data in kWh and currency via in-home display.
2. Reception and display of utility transmitted notifications and control information.
3. Real-time transmission of accurate consumption data and power quality measurements to utilities.
4. Real-time detection and remote reporting of meter tamper.
5. Remote disconnection and reconnection of power supply.

The requirements provided above give an idea of the necessary building blocks of the retrofit. However, the retrofit's design and architecture is highly dependent on the manner in which the existing standalone meter would be retrofitted. Therefore there is the need to establish how the retrofit would interface the existing meter to enhance it with smart meter functions. From the requirements, it is evident that this interface is needed primarily to enable the retrofit collect and transmit recorded consumption data from the existing meter.

4.4 INTERFACE DESIGN

To rightly design this interface, a research was conducted to find out how metering is done in deployed standalone energy meters. The twelve standalone meters which were received from ECG were further studied for this purpose. These meters were of varying types; commercial and residential, single phase and three phase meters. Samples of these meters are provided in Figure 4.4.

Figure 4.4 Sample Energy Meters

After careful analysis of these meters it was observed that all the meters provided for the research were digital pulsed standalone energy meters of varying architectures. This suggested

that the utility had a higher preference for digital electronic meters than conventional electromechanical meters. These electronic meters are made of non-moving parts – solid-state components. Designed primarily on the principle of electromagnetism, these components were observed to be capable of generating an output frequency which is directly proportional to the alternating current (AC) drawn by a consumer's connected load. The output frequency is then accurately computed to produce the consumption reading in kilowatt-hours which is then presented on the meter's display.

It was observed that for all these solid-state meters the process of electromagnetic transduction was carried out mainly by current sensors. These current detectable components are responsible for determining consumption. This therefore suggested that by tapping the output signals of these sensors, there is a possibility that the retrofit would know how much consumption has been recorded by the existing meter. The following subsection examines the feasibility of doing so in the light of the research's objectives.

4.4.1 Interfacing via the Output of Current Sensors

In order to ascertain the feasibility and accuracy of this method of determining consumption from the existing meter, further research was conducted on the makeup and mode of operation of the various current sensing technologies used in these meters. The following current sensors were identified:

1. Low Resistance Current Shunt
2. Ferrosilicon (FeSi) Split Core Current Transformer (CT)
3. Ferronickel (FeNi) Split Core CT
4. Ferrite Split Core CT
5. Solid Core CT

6. Rogowski Coil

Alluding to experimental results from reviewed literature, the above listed sensors are enumerated in order of increasing accuracy, with the Low Resistance Current Shunt being the least accurate [4.10]. Their levels of accuracy are highly dependent on their structure, composition and mode of operation. For example comparing the Low Resistance Current Shunt and the Solid Core CT, they vary in their mode of operation. The operation of the former requires contact with the conductor while the latter does not. As a result the former introduces some inductance, in the order of a few nanohenries (nH). This inductance, though small, is responsible for causing high phase shift errors in the output current even at its operational frequency, thus affecting the accuracy of its current reading. Figure 4.6 presents simulation results of phase shifts caused by the introduction of an inductance of 2 nH from a 200 micro-ohm (μΩ) Riedon RS Low Resistance Current Shunt.

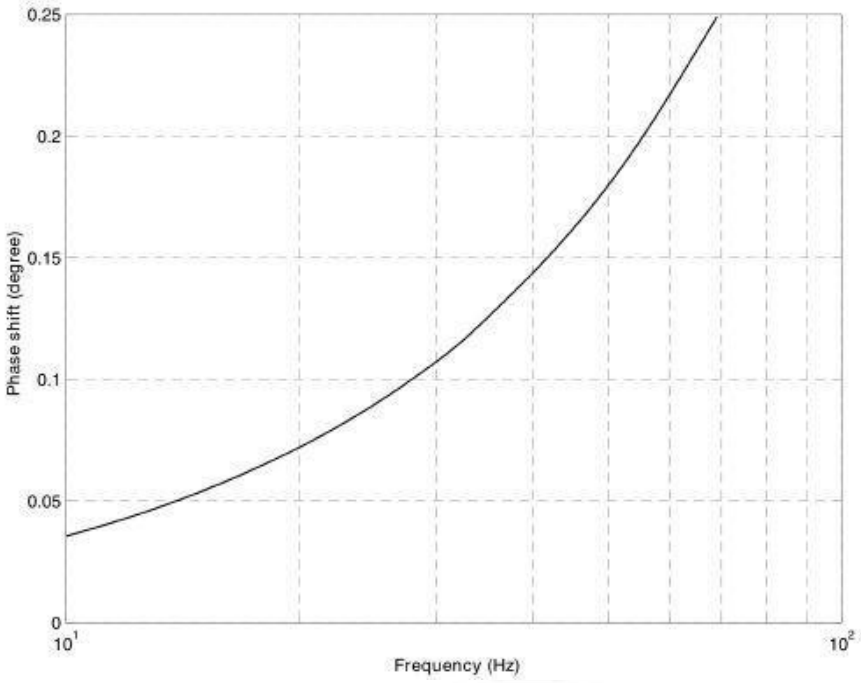


Figure 4.5 Phase Shift as a result of an introduction of 2nH in a 200 μΩ shunt

The effects of the power shift can be ascertained using the error measurement equation presented in equation 4.1

$$\_ \quad , \qquad 4.1$$

Where P is Power factor expressed as $P = \cos\theta$

P′ is the Apparent Power factor expressed as $P = \cos(\theta + \emptyset)$

θ is the phase angle

ø is the phase shift

$$E \quad \frac{\cos(\theta + \emptyset)}{\cos\theta} \qquad 4.2$$

Therefore for a power factor of 0.1 and a phase shift of 0.175 (which is the phase shift at 50Hz in Figure 4.5), the error is an unacceptable 3.04%.

Also the structure of the above mentioned split core CTs, namely FeSi, FeNi and Ferrite, introduces some quantum of inaccuracy in their output signals. Their magnetic core is split into two halves, thus weakening the contact between the two as well as making an inconsistent distribution of the secondary winding across the two halves. Also the research revealed that the material composition of these split core CTs necessitated the creation of some amount of air gaps in order to slenderize the effect of saturation – a state where the magnet cannot be magnetized any further. The allowable air gaps in FeSi and FeNi exceed that of Ferrite. The more the air gaps the higher the phase shift; thus increasing the percentage of inaccuracy. Thus making the Ferrite split core CT more accurate than the other two. Figure 4.6 presents simulation results of phase shifts in 5 amps (A) FeSi, FeNi and

Ferrite split core CTs.

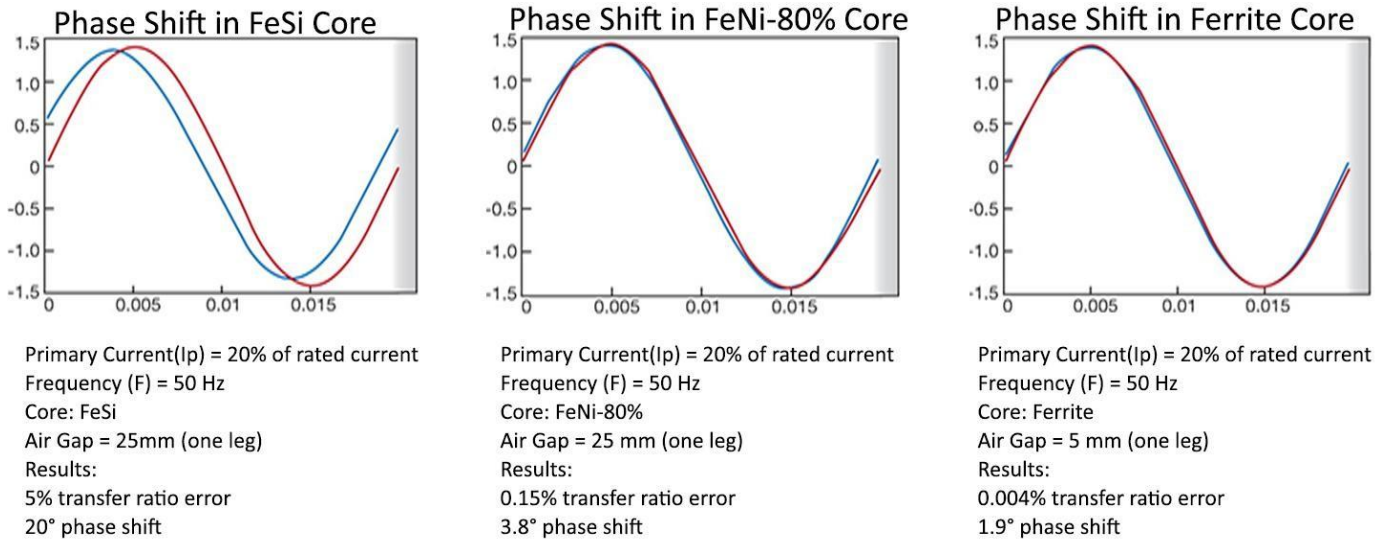


Figure 4.6 Simulation results of phase shifts in 5A CTs.

Current sensors made from Rogowski Coils do not require contact in their mode of operation and have very high accuracies. Experimental results from reviewed literature have proven that they are the best in measuring quick changing currents [4.11]. Rogowski Coils which are open ended are flexible and can easily be made to wrap around conductors of different shapes and sizes. However, the manner in which they are curved and twisted could lessen their accuracy by 1-3%. Also they require high powered integrators or digital signal processors (DSP) to integrate their output signal before obtaining the current reading. This is because their output signal is a voltage relative to the derivative of the current drawn by the connected load.

From the discussion above, it is clear that all these current sensing devices, under certain conditions, have some level of inaccuracy. A critical study of the circuitry of these sample meters revealed that, based on the knowledge of the susceptibility of these sensors to inaccuracies; metrology engineers have carefully designed these meters to lessen the effect of these errors on meter readings. The output signals of their current sensors are provided with the necessary processing and correction to cater for errors stemming from operating conditions, material compositions and ageing effects on the sensor. These compensations and error

handling mechanisms are better provided for in electronic meters than in electromechanical meters. This is a plausible reason why electronic meters are more accurate than electromechanical meters and are the preference of most utilities [4.14]. In the electronic meters obtained from ECG, it was observed that there were a number of specially designed integrated circuits (IC) which provided various error correction techniques to the output signal of the current sensors. A typical one is DRV401, a Sensor Signal Conditioning IC, which has been incorporated in some of these electronic meters which measure consumption using closed loop magnetic sensors. This IC processes and provides error detection and correction to the sensor's output signal.

It is therefore evident that interfacing the existing meter by merely tapping the output signals of the current sensors would provide inaccurate readings. To mitigate these inaccuracies would require gathering information of all the various current sensors employed in energy meters and their specific error correction schemes. Merging all these schemes into one unit, to provide a single interface that would work with all the different energy meters, would be a difficult task. Even after having known all there is to know, there is still the possibility that the results of the error correction scheme employed in the retrofit may be of a higher or a lower degree of accuracy than the manufacturer's scheme. This would mean that the consumption data recorded by the existing meter and retrofit would be different. Consumers and utilities would not take these differences lightly.

In addition, this method of interfacing would require that the existing standalone meter be opened during installation of the smart retrofit. This goes against the set objective of the research which seeks to provide a non-invasive method of interfacing the smart retrofit. There is therefore the need to find some other method of interfacing the existing meter with the retrofit.

4.4.2 Interfacing via the EEPROM

As a consequence of the identified challenges in the previous method of interfacing, an alternative was sought for. A research was conducted to assay the feasibility of the retrofit getting access to stored consumption data in the existing meter. This was done in an attempt to avoid having differences between the consumption data recorded by the existing meter and that of the retrofit.

The study revealed that these electronic meters obtained from ECG are equipped with nonvolatile storage media called Electrically Erasable Programmable Read-Only Memory (EEPROM). These memories store various configurations, calibrations and consumption data. Each EEPROM has a specified storage capacity and is segmented into several chunks identified by addresses. Access to data stored in these chunks requires knowledge of the specific address of the data's location. Bearing in mind that these storage media are from different manufacturers, having different storage capacities, architectures and addressing systems, it would be difficult, if not impossible, to have a generalized method of accessing consumption data stored in these varying media. Also this method of interfacing, even if feasible, would require opening up the existing meter which is in contrast with the set objectives. These challenges make this method of interfacing the existing meter impractical. Figure 4.7 presents a sample of EEPROMs found in electronic meters having different form factors and design.

Figure 4.7 Sample EEPROMs of varying form factors

4.4.3 Interfacing via the Light Emitting Diode (LED)

After further critical inspections of the standalone energy meter samples, it was discovered that each of these meters have a Light Emitting Diode (LED) on the outer casing. This bi-lead semiconductor light source has been engineered to pulsate brightly each time a specific quantity of energy is consumed. Metrology engineers have legibly stated on each meter the number of pulses that represents a kilowatt hour – the impulse rate. Figure 4.8 shows a sample of these energy meters indicating clearly their LEDs and impulse specification.

Figure 4.8 Sample Energy Meters showing LED's with impulse specification

Based on the function of these LEDs, another method of interfacing the existing standalone meter was discovered. In this method, pulses from these meters' LEDs are detected and counted in order to determine the amount of energy that has been read by the energy meter.

By dividing the total number of impulses by the impulse rate, one is capable of telling the magnitude of energy that has been consumed over a particular period of time. For example, the energy meter on the far right of Figure 4.8 has an impulse rate of 200 impulses per kilowatt hour (imp/kWh). So if 1000 impulses are detected over a particular time frame, it can be calculated that 5 kilowatt hours of energy has been consumed.

As compared to previously discussed methods, this does not require opening the meter's casing or tampering with its circuitry. The existing meter is still kept intact and the interfacing is done from the outside. Also unlike the other methods which require gathering information of the mode of operation of different components, this requires only knowing the impulse rate which is readily, accurately and legibly provided on the meter's casing by the manufacturer. Furthermore, in this method, computation of consumption only requires a simple division operation. Finally the form factor and mode of operation of all these LEDs are the same; thus allowing for the use of a single design to cater for all the different types of energy meters. This is a more practical approach to interfacing the existing meter with the proposed retrofit than the previously discussed methods. It is however important to establish how light pulses from the LED are accurately detected.

Having established that this method is a practical and non-invasive method, various light sensors are discussed in the next section in an attempt to select the most appropriate sensor(s) to be incorporated in the smart retrofit design.

4.5 LIGHT SENSORS

Based on the earlier discussions, the approved method of interfacing the existing standalone energy meter is via its pulsating LED. Light pulses from this LED are to be detected, processed, recorded and transmitted by the smart retrofit. There are various light sensors which are capable of detecting light pulses. A primary factor to be considered in the selection of light sensor(s) is the wavelength of the light to be detected. Figure 4.9 presents a wavelength chart of various commonly used coloured LED lights in nanometers (nM).

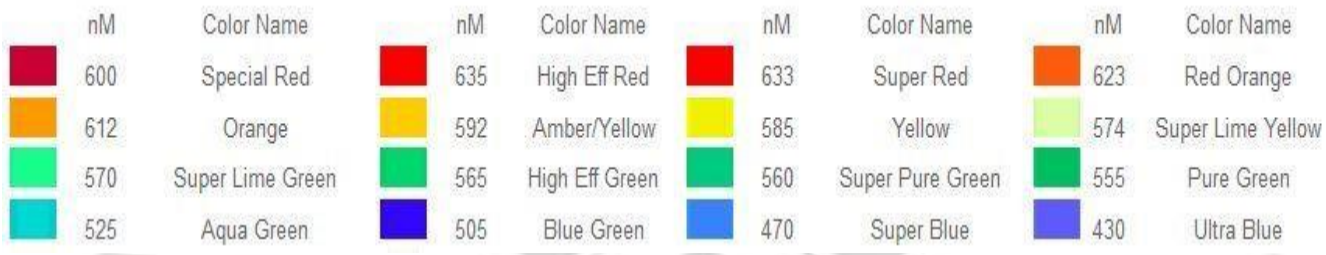


Figure 4.9 LED Wavelength Chart

From the chart, it can be thus said that the wavelength of LEDs range approximately between 400 and 650 nM. Therefore any light sensor which is capable of detecting lights within this range is a plausible option. It is however important to mention that the LEDs on all the ECG meters under study were bright red in colour; thus having their wavelengths between 600 and 650 nM. Notwithstanding, considering the possibility of change in future, the research seeks for a light sensor which can detect all the possible wavelengths of LEDs. Table 4.3 presents a comparison of a list of popular light sensors which are capable of detecting lights within this range.

Table 4.3 Comparison of Light Sensors [4.18]

	Photo-multiplier Tubes	Photo-diodes	Phototransistors	Photocells	Light-to-frequency converter (hybrid)

Description	A unique vacuum tube which has a photocathode which imbibes light photons.	A photojunction semiconductor device that reacts to light	Similar to the photo-diode but amplifies its output signal	A photoconductive cell which decreases its resistance when exposed to light	A light sensor which outputs a square wave with a frequency proportional to irradiance
Wavelengths (nM)	200 - 900	200 - 2,000	400 - 1,100	400 - 700	400 - 1,050
Performanceto-cost ratio	Fair	Good	Excellent	Excellent	Fair
Cost	High	Low	Very Low	Very Low	Low
Sensitivity	Excellent	Very Good	Very Good	Very Good	Very Good

The selection of a light sensor for the smart retrofit should be done in the light of the earlier mentioned research objectives – to provide a low cost smart retrofit for African developing countries. Alluding to Table 4.3, Photo-multiplier tubes are the best at sensing light pulses, however they are the most expensive. They are currently priced between USD 750 and 1,700 [4.19]. This high cost makes it an impracticable option for this application area. Photomultiplier tubes also require a high input voltage in order to detect light photons and produce several secondary electrons. This voltage; which is often greater than 15 volts, cannot be supplied by a connected microcontroller hence there is the need to provide an additional regulated power supply; thus increasing the cost of the smart retrofit.

All the other four sensors have relatively good levels of sensitivity and therefore are viable options. However, the performance-to-cost ratio ratings of the photo-diode and light-tofrequency converter are relatively lower than that of the photocell and phototransistor. Also their costs are relatively higher than that of the photocell and the phototransistor. The photodiode also requires the inclusion of a suitable operational amplifier to amply its output signal; this introduces an additional cost to the retrofit design. For these reasons, the photo-diode and light-to-frequency converter are dropped. The research narrows its study on the feasibility of using the other two sensors – photocell and phototransistor.

The photocell and the phototransistor have very similar ratings in Table 4.3; as such it is important to consider some additional significant factors that would help guide the selection for a suitable light sensor for the retrofit design. One key factor to be considered is how close the light sensor should be to the LED before detecting a light pulse. This is important because, as depicted in Figure 4.8, each meter's LED is covered with the meter's transparent casing. This means that there is no direct access to the LED. The measured distance between the LED and the casing of the twelve different standalone energy meters ranged between 2mm and 10mm. It is therefore important that the light sensor to be selected for the retrofit design must be capable of detecting light pulses, at least, 10mm away from the pulsating LED.

Two phototransistors, GP2S40J0000F and GP1L53VJ000F and a GL5528 Mini Photocell were tested for LED pulse detection from various distances. For each of these tests adequate isolation was provided in order to reduce noise from external light sources. This was done using an empty opaque barrel of a ball pen. A bright red pulsating LED of 450 lumens was placed at one end of the barrel and each of these light sensors with connection to a programmed microcontroller – Arduino Uno Revision 3 board, were lowered through the other end of the barrel in turns. They were lowered in at different depth proximities from the pulsating LED using a calibrated rod. The basic components of the experimental setup are presented in Figure 4.10.

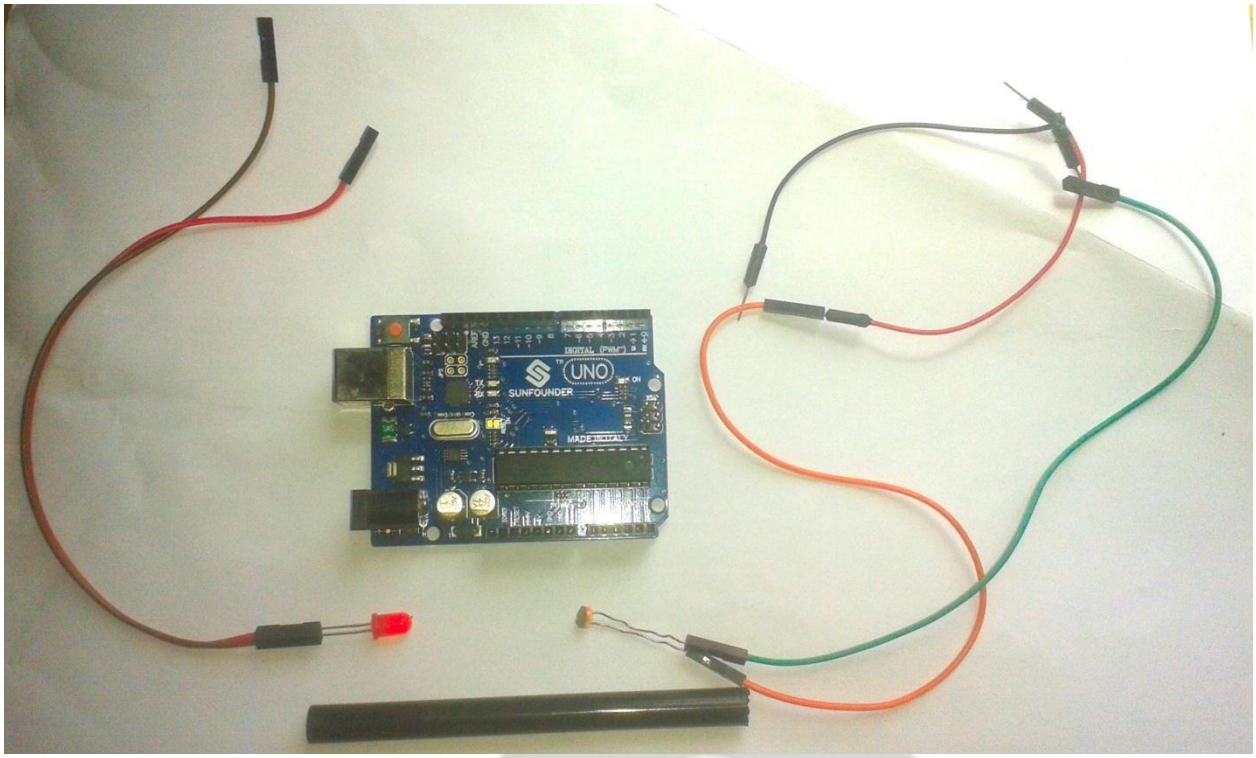


Figure 4.10: Basic Components of Light Sensor Depth Proximity Experiment

Accurate detection for this experiment is defined as the ability of the sensor to output an analog signal immediately the LED emits a pulse. Based on this definition it was observed that the GP2S40J0000F phototransistor could only accurately detect pulses when it was 0 – 5mm away from the LED. The GP1L53VJ000F phototransistor was also able to accurately sense light pulses when it was 0 – 7mm away from the LED. The GL5528 Mini Photocell was able to accurately detect LED pulses 0 – 35mm away from the LED. These results are summarized in Table 4.4.

Table 4.4 Proximity Distance for LED pulse detection

LIGHT SENSOR	DETECTABLE DISTANCE FROM LED (mm)
GP2S40J0000F phototransistor	≤ 5
GP1L53VJ000F phototransistor	≤ 7
GL5528 Mini Photocell	≤ 35

From the above results it was concluded that the GL5528 Mini Photocell has a higher detectable distance from the LED than the two phototransistors. Its maximum detectable distance covers the gap created by the meter's transparent casing. This therefore makes it a suitable light sensor for detecting LED pulses from standalone energy meters.

Despite these desirable characteristics of the photocell, before concluding on the selection of this light detector, it was important to ascertain if this photocell is capable of detecting a fast pulsating LED; a case where energy is consumed at a fast rate. To do so, an experiment was conducted using a red pulsating LED of 450 lumens. This LED was connected to an Arduino Nano microcontroller. The microcontroller was programmed to blink the LED steadily at specific frequencies, ranging between 10Hz and 80Hz. All the programs for this experiment were written in C++ using an Arduino Integrated Development Environment version 1.64, which is an open source software for programming Arduino boards. Figure 4.11 presents a snippet of the program written for pulsating the LED at specific frequencies.

```
/*
  LDR Responsivity test
  Turns on an LED on and off repeatedly.
 */

// Pin 13 has an LED connected on most Arduino boards.

int led = 13;
int howManySecHasToRun = 0;  //initialize how many seconds it has to run
int y = 20;
int z = 10;

// the setup routine runs once when you press reset:
void setup() {
  // initialize the digital pin as an output.
  pinMode(led, OUTPUT);
}

// the loop routine runs over and over again forever:
void loop() {

  delay(10000);
  for(howManySecHasToRun = 1; howManySecHasToRun <=y ; howManySecHasToRun++)
  {
    blinkRate(z);

    if((y%20)==0 && (howManySecHasToRun==y) && (y<301))
    {
      delay(10000);
      y += 20;
      howManySecHasToRun = 0;

      if(y == 320 && z<100)
      {

        y = 20;

        z += 10;
      }
      }
    }

  }

}

void blinkRate (int howManyPerSec)     //function to blink LED for a certain number of times per second
{
  int count = 0;
  unsigned long interval = 1000/howManyPerSec;

  while (count < howManyPerSec)
  {
    digitalWrite(led, HIGH);   // turn the LED on (HIGH is the voltage level)
    delay(50);                 // wait for a 50 milliseconds
    digitalWrite(led, LOW);    // turn the LED off by making the voltage LOW
    delay(interval);               // wait for the specified interval
    count++;
  }

}
```

Figure 4.11 C++ Code on Arduino Nano for Blinking LED at different frequencies

To ensure that detection of the light pulses was completely not affected by the computational power of the microcontroller, a different microcontroller was used for the photocell. The GL5528 Mini Photocell was connected to a programmed Arduino Uno Revision 3 board, an NE555 timer integrated circuit (IC) and a 10 kilo-ohm (kΩ) pull-down resistor, as presented in a simulation schematic in Figure 4.12.

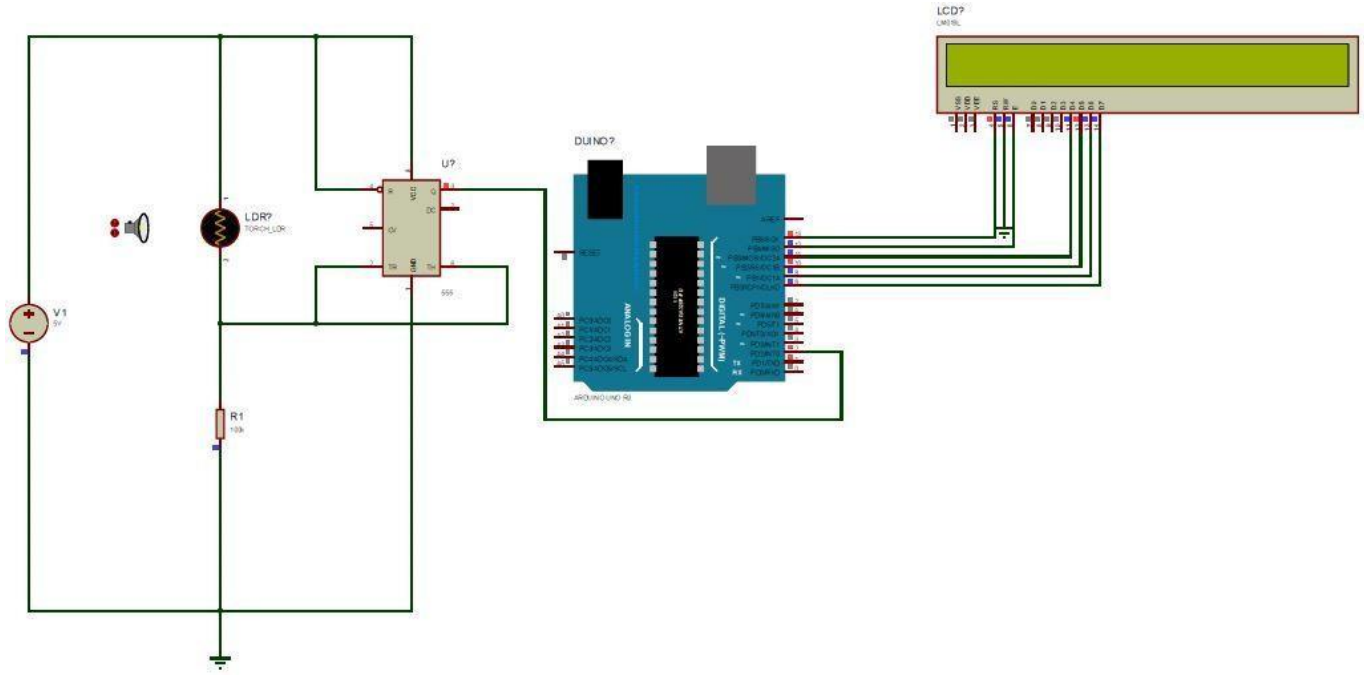


Figure 4.12 Simulation Schematic of LED Pulse Detection

The simulation schematic was constructed and ran using ISIS Professional Software version 7.9 SP 1; a software which offers virtual system modeling for circuit designs. The microcontroller connected to the photocell was programmed to interrupt the microcontroller each time a light pulse was detected by the photocell. The interrupt function increased, recorded and displayed the pulse count on a serial monitor. Figure 4.13 presents a snippet of the written code in C++.

```ino
#include <LiquidCrystal.h>

LiquidCrystal lcd (13,12,11,10,9,8);
int count = 0;
unsigned long interval = 9000; // interval in milliseconds to detect change in pulsating frequency
unsigned long currentMicros = 0;
unsigned long previousMicros = 0;

void setup() {
  // put your setup code here, to run once:
  Serial.begin(9600);
  attachInterrupt(0,countBlink, RISING);  //interrupt on rising edge
  lcd.begin (40,2);
}

void loop() {
  // put your main code here, to run repeatedly:
}

void countBlink()
{
  previousMicros = currentMicros;
  currentMicros = millis();
  if(currentMicros - previousMicros > interval)  // detecting if the pulsating LED has paused and is changing frequency
  {
    Serial.println();
    Serial.println();
    Serial.println("New Sequence");
    count = 0;
  }

  count++;
  Serial.println("detected");
  Serial.println(count);
  lcd.clear();
  lcd.setCursor(0,0);
  lcd.print(count);
}
```

Figure 4.13 C++ Code on Arduino Uno for detecting LED pulses at different frequencies

So in summary the Arduino Nano was programmed to pulsate an LED like an existing standalone pulsed energy meter and the Arduino Uno was programmed to detect and record LED pulses like a smart retrofit. It is important to note that the GL5528 Mini Photocell was placed 35mm from the pulsating LED. As stated earlier, this is the maximum detection distance for this photocell. The final experimental setup involving both microcontrollers is also presented in Figure 4.14.

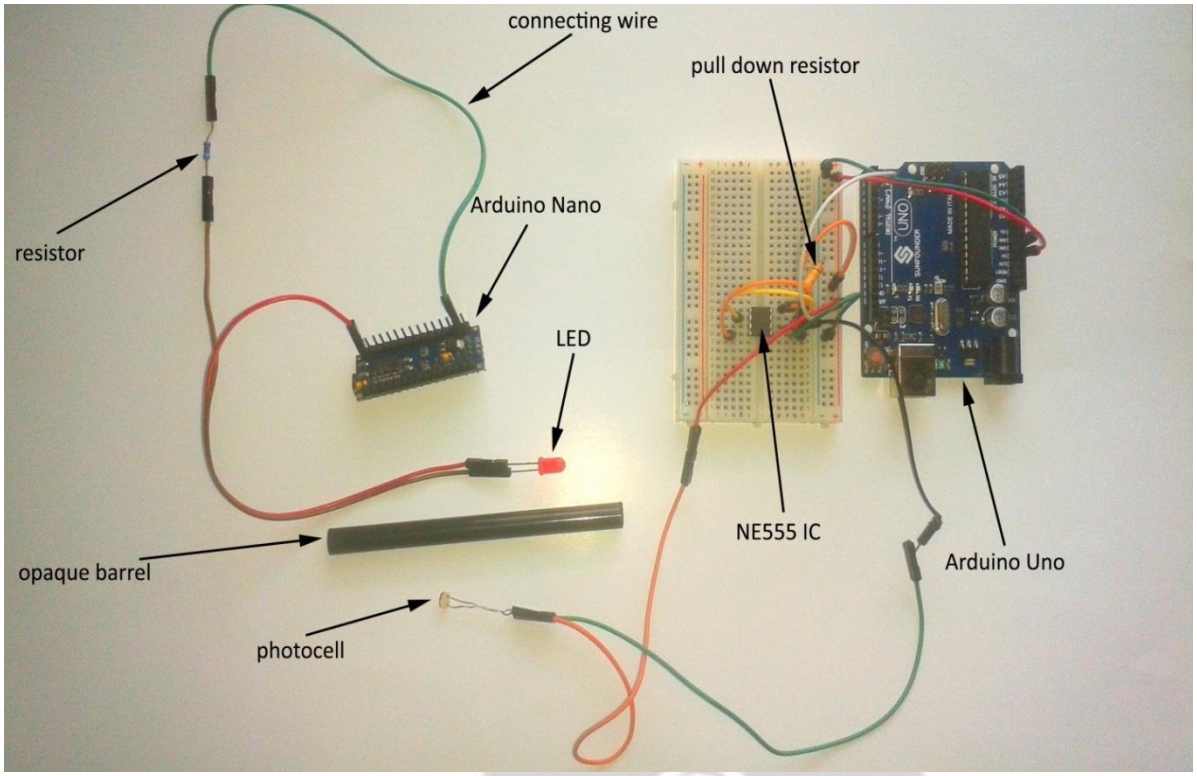


Figure 4.14 Experimental Setup for Photocell Response Test

From the code snippet in Figure 4.13 it is evident that the microcontroller outputs results to a serial monitor at a baud rate of 9600. Using a suitable open source serial terminal application called CoolTerm (version 1.4.6), a connection is made to the reporting communication port of the Arduino Uno and results from the LED detection program are gathered and stored to a text file. The results are tabulated and presented in Table 4.5.

Table 4.5: Experimental Results of LED Pulse Detection

Frequency (Hz)	Number of Pulses Detected in								
	20sec	40sec	60sec	80sec	100sec	120sec	140sec	160sec	180sec
10	200	400	600	800	1000	1200	1400	1600	1800
20	400	800	1200	1600	2000	2400	2800	3200	3600
30	600	1200	1800	2400	3000	3600	4200	4800	5400
40	800	1600	2400	3200	4000	4800	5600	6400	7200
50	1000	2000	3000	4000	5000	6000	7000	8000	9000
60	1200	2400	3600	4800	6000	7200	8400	9600	10800
70	1	1	1	1	1	1	1	1	1
80	1	1	1	1	1	1	1	1	1

In Table 4.5 all accurately detected pulses are in blue while inaccurately detected pulses are in red. It can be concluded that the GL5528 Mini Photocell was accurately able to detect light pulses for frequencies 10 to 60 Hz. For frequencies above 60 Hz, specifically 64 Hz, the photocell was only capable of detecting the very first LED pulse; all other pulses were not detected. The fast rate at which the LED was pulsating made it difficult for the photocell to uniquely identify each pulse. It sees all the fast blinking pulses as one pulse which lasts over a long period of time. It can be thus said that at frequencies beyond 60 Hz the photocell is flooded with LED pulses hence it does not respond linearly to its input. Therefore this photocell is only suitable for detecting LEDs which pulsate up to this frequency.

A 60 Hz pulsating LED, has a pulsating period of approximately 16.667 milliseconds (ms); thus it pulsates a total of 60 pulses every second. Having determined the minimum period between pulses that is detectable by the photocell, it is necessary to verify whether there would not be any periods smaller than this from an existing standalone energy meter. To do this, an assumption is made of a meter whose LED pulsates at this period of 16.667ms. This means that in an hour it would generate 216,000 pulses. From the sample meters presented in Figure 4.8, impulse rates of energy meters range between 200 and 1000 impulses/kWh.

Therefore assuming this meter has an impulse rate of 200 impulses/kWh, it would measure 1,080 kWh of energy every hour. Also assuming it has an impulse rate of 1000 impulses/kWh, it would measure 216 kWh of energy every hour. Thus energy consumption recorded in an hour by a meter which pulsates at a frequency of 60 Hz (period of ~16.667ms) ranges between 216 and 1,080 kWh.

The United States of America currently tops the list of the world's consumption of electricity. The current average hourly consumption of its residential consumers is 1.79 kWh and that for non-domestic (industrial and commercial) consumers is 8.45 kWh [4.6] [4.7]. These values are

far less than the range of energy consumption measured by the meter assumed to be pulsating at 60 Hz. This suggests that there would hardly ever be any meter that would pulsate at the maximum detectable frequency of 60 Hz. Therefore it can be concluded that the chosen photocell is capable of detecting all LED pulses pulsating at all possible frequencies.

Having dealt sufficiently with the objective of providing a non-invasive and effective method of interfacing the existing standalone energy meter, the other essential building blocks of the retrofit design are elicited in the following section.

4.6 BUILDING BLOCKS OF RETROFIT DESIGN

From the earlier discussed functional requirements and research objectives, the following components described in Table 4.6 have been identified as essential building blocks of the smart retrofit. They would furnish the existing standalone pulse energy meter with smart meter functions. Figure 4.14 shows a diagram of the basic interconnections between the selected components.

Table 4.6 Building Blocks of Smart Retrofit

No.	Name	Function
1.	Photocell	Detects LED pulses from existing meter.
2.	GSM/GPRS Communication Module	Provides reception and transmission of data messages to/from utilities.
3.	Liquid Crystal Display (LCD)	Displays consumption data, tariffs, power measurements, utility transmitted notifications and control information.
4.	Relay	Remote disconnection/reconnection of meter from/to power supply.
5.	Microcontroller	Programmed to handle all arithmetic and logical processes.
6.	Ball Rolling Switch (Tilt Sensor)	Energy Theft Detection Mechanism: Detects physical tamper of meter.
7.	Triple Axis Accelerometer	Energy Theft Detection Mechanism: Detects motion and shock.

8.	Hall Effect Sensor	Energy Theft Detection Mechanism: Detects external magnetic fields.
9	Current Sensor	Energy Theft Detection Mechanism: Detects meter bypass. Also required to carry out power quality measurements.
10.	Data Logger	Registers measurements from sensors at set intervals. Also keeps track of time.
11.	Speaker	Sounds an alarm to prompt user.
12.	Rechargeable Battery	Provides power to the retrofit even during power outages.

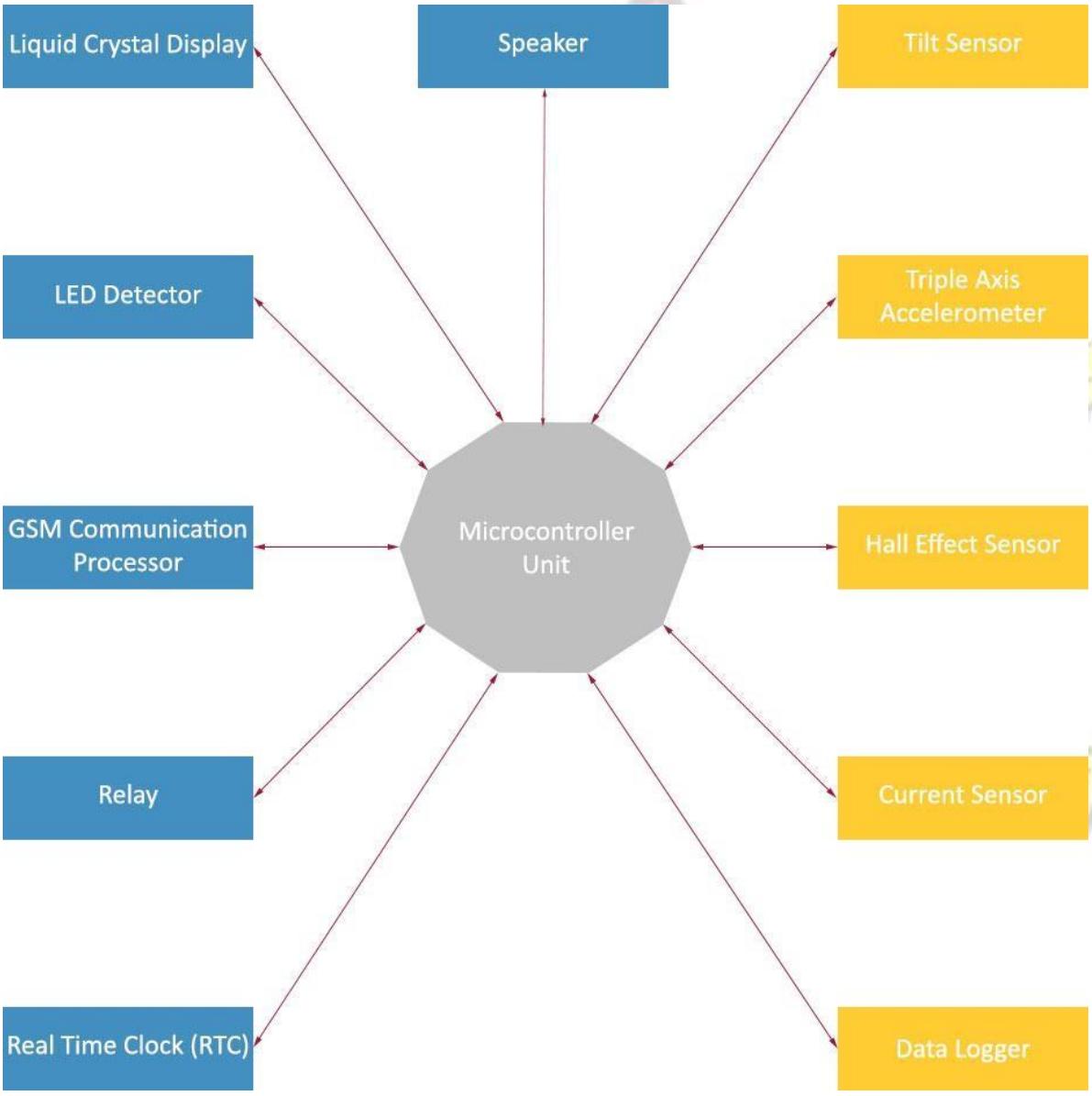


Figure 4.15 A Basic Block Diagram of Interconnecting Components

4.7 SYSTEM MODELING

This section focuses on modeling the smart retrofit using flow chart diagrams to provide a structured representation of the system's essential functions and features. These representations are used to elicit the workflow of important system processes/services. These processes have been categorized into two groups; non-preemptive and preemptive processes. The non-preemptive processes are high priority tasks which when scheduled to take place, execute without fail or interruption. If at the scheduled time of execution, a process of a low priority is being executed, it is interrupted briefly for the high priority task to execute. The only time a non-preemptive process is interrupted is when another non-preemptive process of a higher priority than the current process has been scheduled to run. In other words, nonpreemptive tasks have different classes of priority. Preemptive tasks on the other hand can always be interrupted and resumed later, where need be.

On most microcontrollers there are a number of digital pins that can be assigned to nonpreemptive tasks. It is important to identify the total number of non-preemptive functions in this application area in order to select a suitable microcontroller which allows for that number of interrupt service routines (ISR). After critical analysis of the smarts retrofit's functional requirements, detection of LED pulses and energy theft have been identified as essential nonpreemptive processes. Table 4.7 presents the list of identified non-preemptive functions and their level of priority.

Table 4.7 Interrupt Allocation Table

	Function	**Level of Priority**
1	Detection of LED pulses with Photocell	0
2	Detection of motion and shock with Triple Axis Accelerometer	1

3	Detection of external magnetic fields with Hall Effect Sensor	2
4	Detection of physical tamper of meter with Ball Rolling Switch	3

So from Table 4.7 it is evident that the detection of LED pulses in order to ascertain consumption is deemed the most important task of the smart retrofit. Three of the energy theft detection mechanisms are also assigned other interrupt pins. However, the fourth energy theft detection mechanism which uses the Current Sensors to detect meter bypass has not been included. This is because this mechanism requires some computation and comparison of current readings measured from the live and neutral lines before ascertaining if there has been a bypass or not. When the readings are approximately the same no bypass is detected, as such this mechanism cannot be assigned to interrupt each time readings are to be taken.

Power quality measurements and processing of received control information and notifications from the utility have been identified as preemptive tasks/processes. Figure 4.16 illustrates the basic workflow of the smart retrofit in performing these categorized tasks/processes.

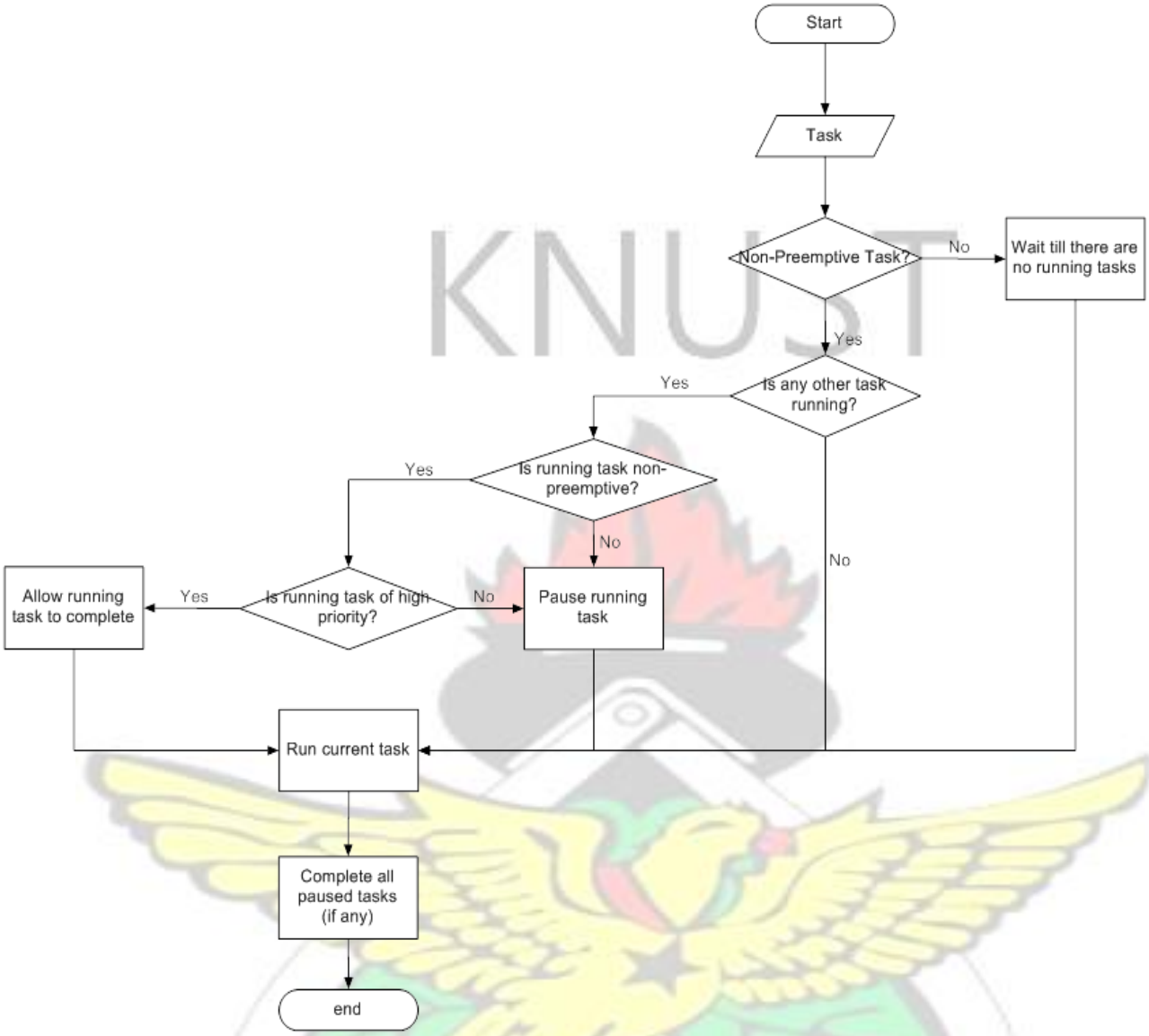


Figure 4.16: Task Execution Workflow

The workflow of each of these identified system functions are illustrated in Figures 4.17 to 4.20.

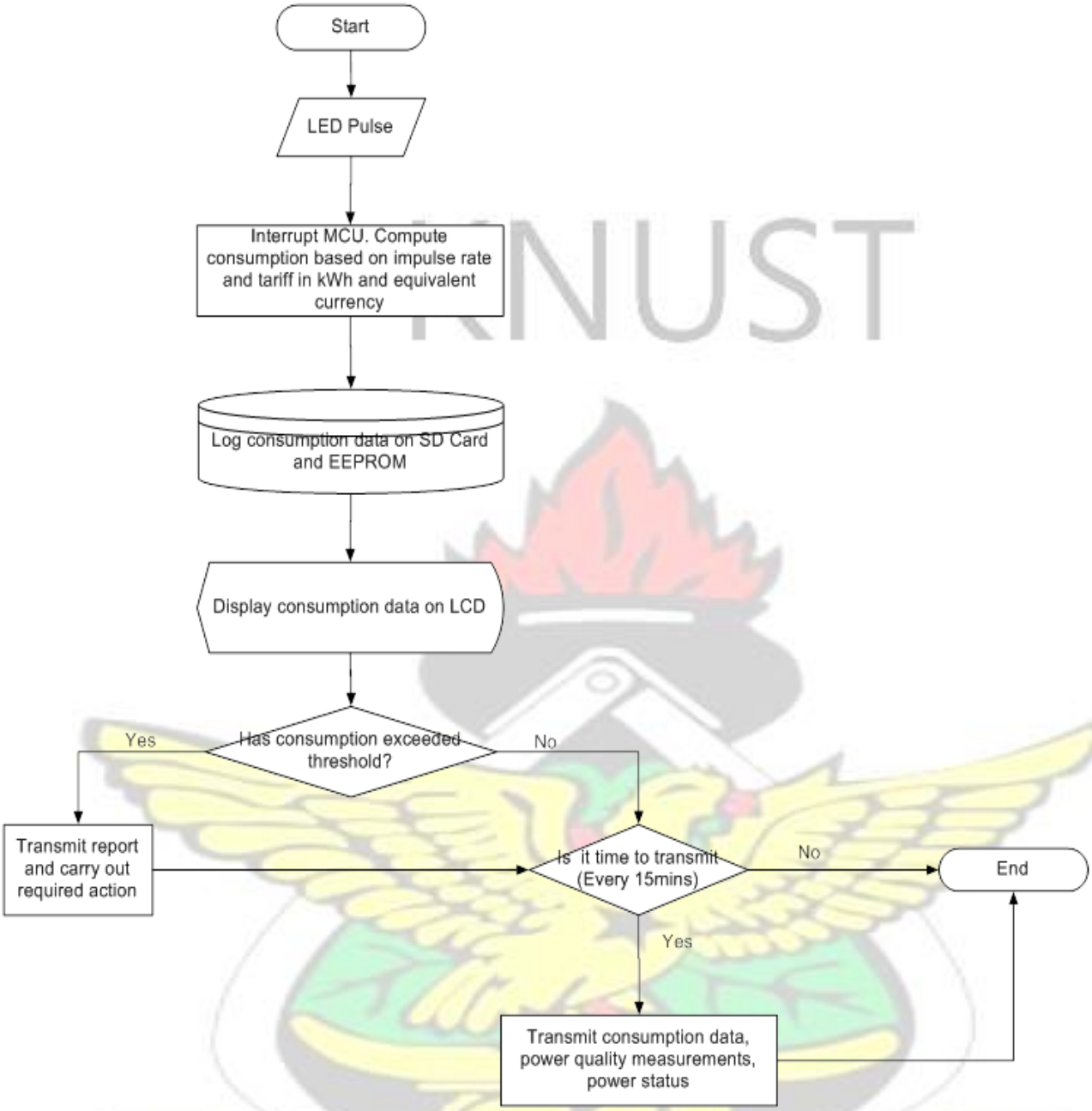


Figure 4.17: Determination of Consumption

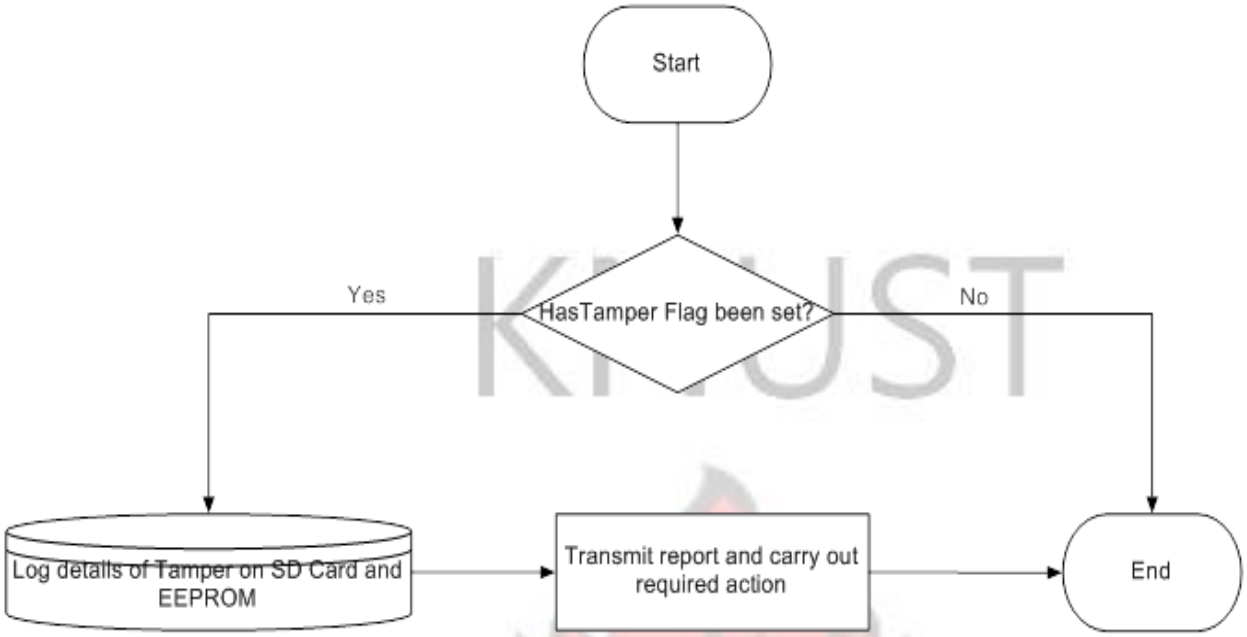


Figure 4.18: Energy Theft Detection

Figure 4.19 Processing of Utility Messages

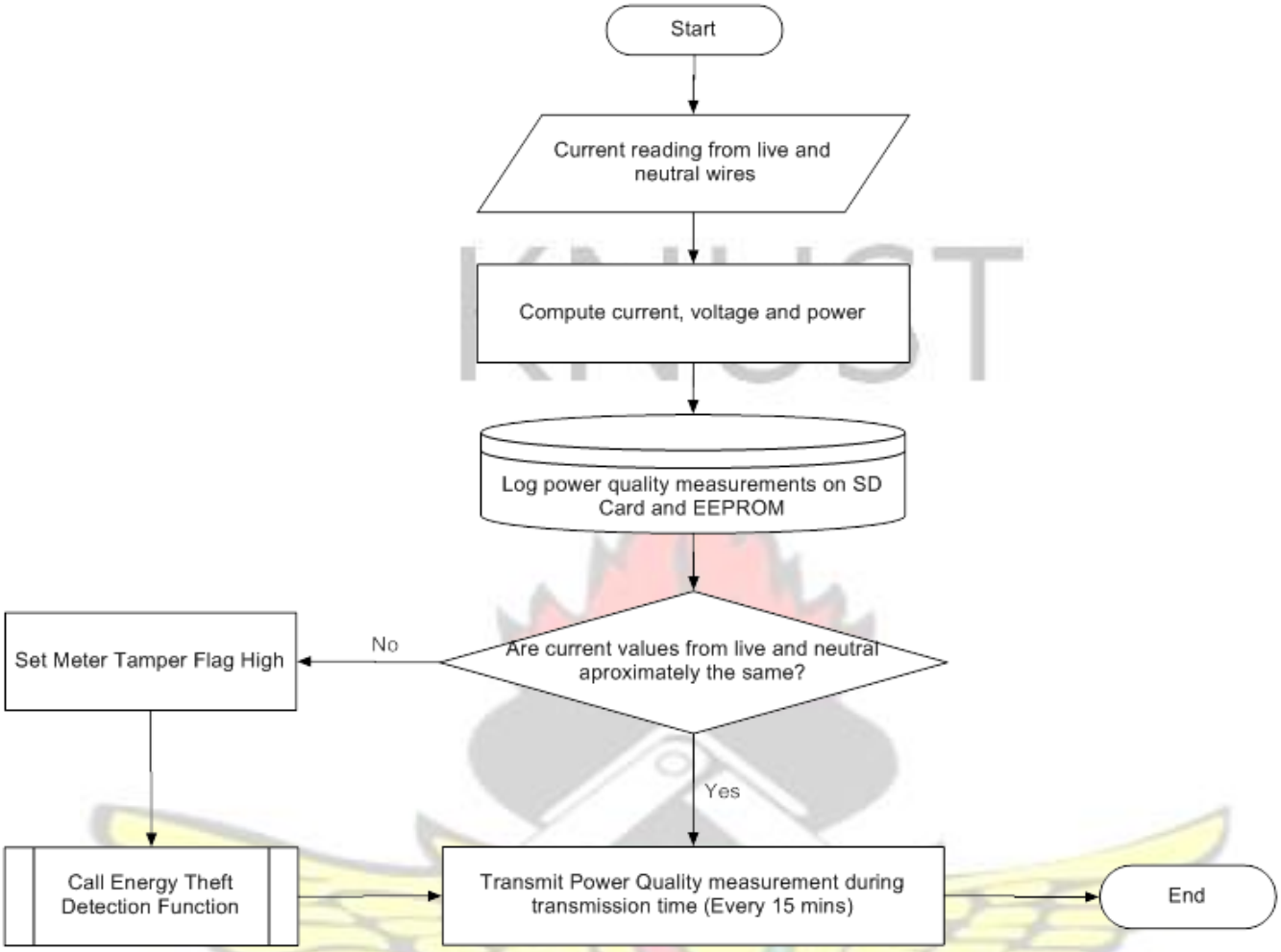


Figure 4.20: Power Quality Measurements

The above workflows serve as an essential guide in modeling the smart retrofit. Based on these workflows the appropriate system code, simulation and schematics are developed and presented in the next chapter.

4.8 SUMMARY

In this chapter, based on the adopted research methodology, the entire design of the proposed smart retrofit is provided. This smart retrofit is designed to provide existing non-smart standalone energy meters with smart meter functions. The functions, features and essential processes are elicited and modeled using effective engineering tools. A key aspect of this

chapter is the discovery and design of a non-invasive method of interfacing the existing standalone energy meter.

REFERENCES

[4.1] Bertrand Klaiber and Pierre Turpin, ―Sensing currents for maximum efficiency‖, LEM Energy & Automation Milwaukee, http://powerelectronics.com/alternativeenergy/sensing-currents-maximum-efficiency, October 2012.

[4.2] F. J. Arcega and J. A. Artero, ―Current sensor based on Rogowski coil‖, Department of Electrical Engineering, Universidad de Zaragoza, June 2004.

[4.3] CEA Task Group on Metering & Regulations, ―Industry Initiative: Electricity Measurement Accuracy Program (E-MAP) Proposal‖, Canadian Electricity Association, pp. 1-7, July 2001.

[4.4] ―Hamamatsu Photomultiplier Tube Modules‖, Edmund Optics Worldwide, http://www.edmundoptics.com/testing-detection/detectors/hamamatsuphotomultiplier-tube-modules/2512, March 2016.

[4.5] Larry Godfrey, ―Choosing the Detector for your Unique Light Sensing Application‖, www.johnloomis.org/ece445/topics/egginc/tp4.html, March 2016.

[4.6] Kent County Council, ―Non Domestic energy consumption 2013 Kent Local Authorities‖, Business Intelligence Statistical Bulletin, June 2015.

[4.7] Lindsay Wilson, ―Average Household Electricity Consumption‖, http://shrinkthatfootprint.com/average-household-electricity-consumption, June 2013.

CHAPTER FIVE: RETROFIT IMPLEMENTATION

5.0 INTRODUCTION

This chapter describes all the steps followed in implementing the smart retrofit design. These steps are guided by the retrofit design provided in the previous chapter. Section 5.1 highlights the essential components that have been selected to implement the smart retrofit. In Section 5.2, circuit simulations are conducted in order to verify system functional requirements. Finally in Section 5.3 the smart retrofit is constructed based on simulation results and developed circuit schematics.

5.1 COMPONENT SELECTION

The list of suggested components presented in the previous chapter for the implementation of the retrofit design, were more general than specific. In this section specific components are selected for the development of the smart retrofit. Similar to the selection process used during the interface design, these components have been carefully selected on the basis of performance-to-cost ratio, availability, mode of operation and robustness. Additional justification is provided in the subsections below to buttress their suitability.

5.1.1 GSM/GPRS Communication Module

A key function of the smart retrofit is the transmission of meter data and the reception of control information from its designated utility. Therefore there is the need to incorporate twoway communication ability into the system design. The choice of the communication technology to be used for the smart retrofit has been based on the comparisons made in Chapter Two on the various plausible communication technologies for smart meter deployment in African developing countries. From the comparisons, it was quite obvious that the features of GSM made it a more likely option for implementing the proposed smart retrofit. It is highly available,

highly reliable and cost effective. Details of a conducted technical evaluation of a sample GSM network would be presented in Chapter Six.

Based on these favourable features, a GSM/GPRS communication module is sought for in the implementation of the smart retrofit. A wide range of such modules exist. Common among these include: Sim300, Sim800 and Sim900 GSM/GPRS Communication modules. Of these three, Sim900 is the most recent module and has upgraded features which are superior to the other two modules. Some of these features include:

1. Support for GSM/GPRS/EDGE Quad band (850/900/1800/1900 MHz)
2. Low Power Consumption (1mA during sleep mode)
3. GPRS (data) downlink rate of 85.6 Kbps
4. Support for Packet Broadcast Control Channel (PBCCH)

Based on these desirable features, a GSM/GPRS TTL UART Sim900 Communication module was selected for the retrofit implementation. To further justify the selection of this component, diagnostic tests were carried out on this module using an online browser based AT Command Tester, accessible via the uniform resource locater http://m2msupport.net/m2msupport/module-tester/. Using standard AT commands, various tests were carried out with the module to ascertain the following:

1. Network Registration status
2. Signal Strength
3. Hypertext Transfer Protocol (HTTP) GET and POST

All conducted tests were successful and produced desirable results. These results are presented Figures 5.1 – 5.2.

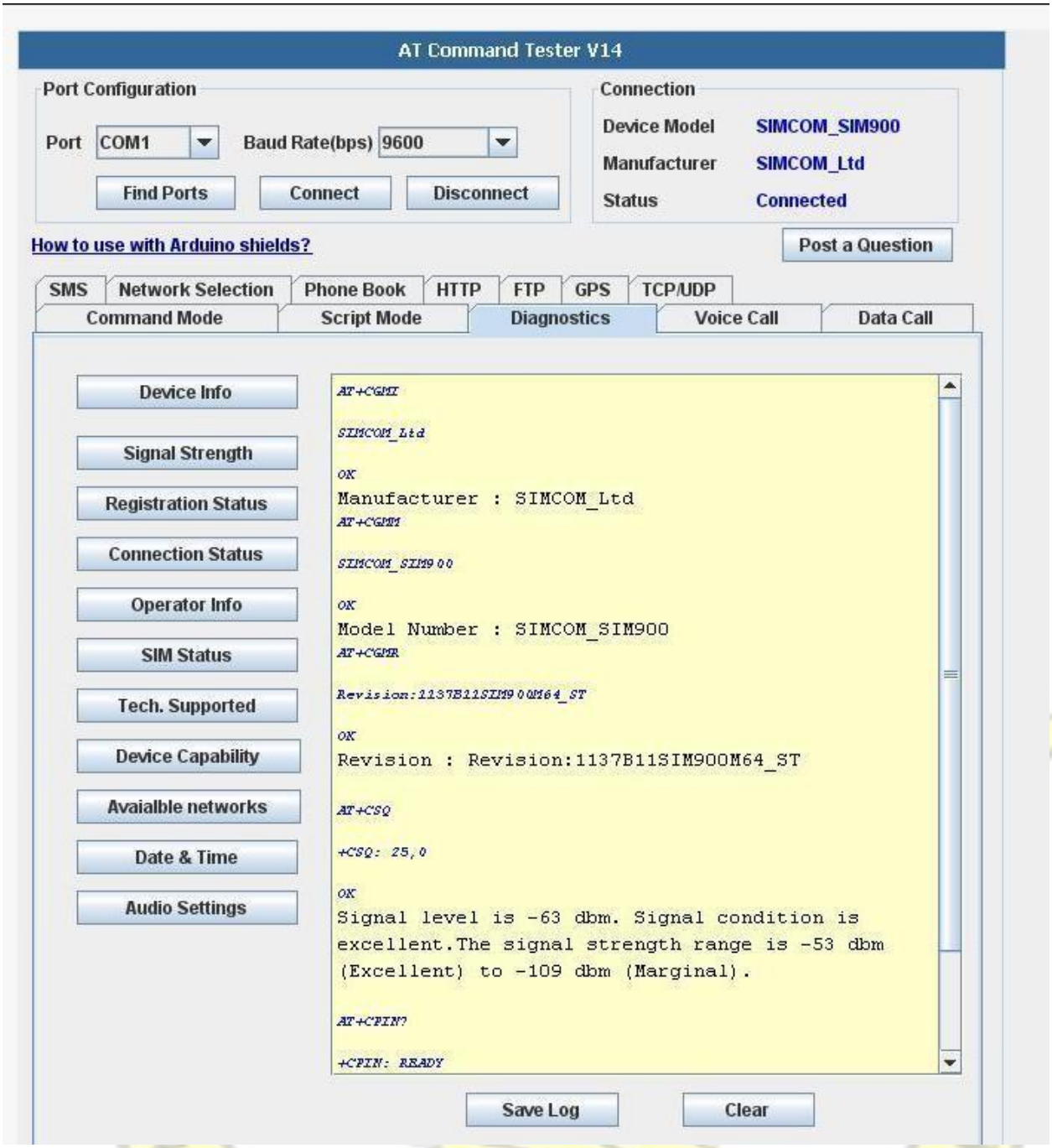

AT Command Tester V14
Port Configuration
Port COM1
Baud Rate(bps) 9600
Find Ports
Connect
Disconnect
Connection
Device Model SIMCOM_SIM900
Manufacturer SIMCOM_Ltd
Status Connected
How to use with Arduino shields?
Post a Question
SMS
Network Selection
Phone Book
HTTP
FTP
GPS
TCP/UDP
Command Mode
Script Mode
Diagnostics
Voice Call
Data Call
Device Info
Signal Strength
Registration Status
Connection Status
Operator Info
SIM Status
Tech. Supported
Device Capability
Avaialble networks
Date & Time
Audio Settings
AT+CGMI
SIMCOM_Ltd
OK
Manufacturer : SIMCOM_Ltd
AT+CGMM
SIMCOM_SIM900
OK
Model Number : SIMCOM_SIM900
AT+CGMR
Revision:1137B11SIM900M64_ST
OK
Revision : Revision:1137B11SIM900M64_ST
AT+CSQ
+CSQ: 25,0
OK
Signal level is -63 dbm. Signal condition is excellent.The signal strength range is -53 dbm (Excellent) to -109 dbm (Marginal).
AT+CPIN?
+CPIN: READY
Save Log
Clear

Figure 5.1 Diagnostic Test to Ascertain Signal Strength and Registration Status

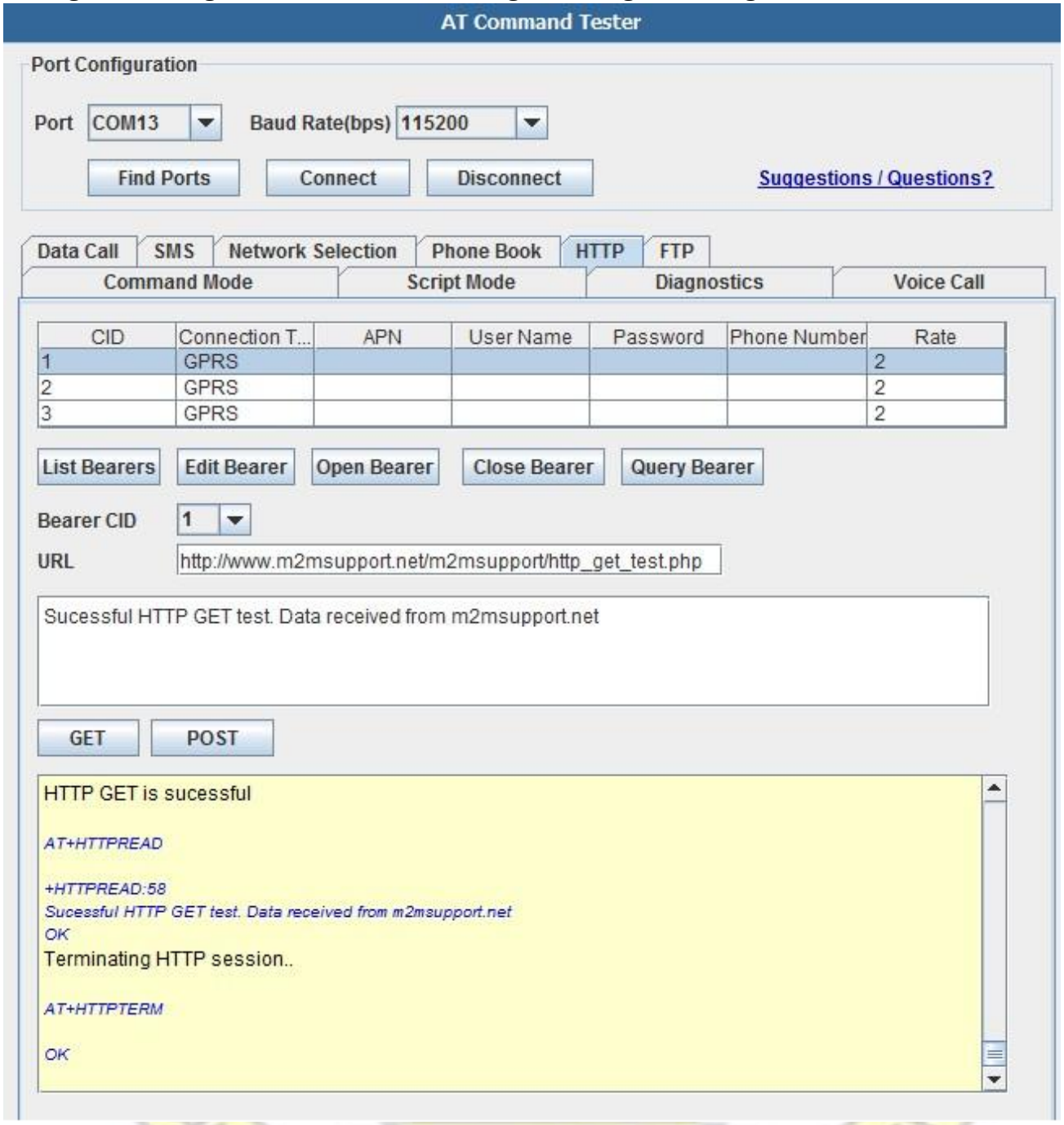


Figure 5.2 Diagnostic Test to Test for HTTP functionality

These results justify the selection of this Sim900 module for the implementation of two-way communication in the smart retrofit.

5.1.2 Liquid Crystal Display (LCD)

This component is responsible for displaying consumption data both in kWh and currency as well as tariffs, utility transmitted notifications and power quality measurements. This inhome display is essential in providing the consumer with direct feedback necessary for consumption behavioural change. The following LCDs are options for the provision of this function in the retrofit:

1. 16x2 Character Display
2. 20x4 Character Display
3. 128x64 Graphic Display

The above mentioned displays are listed in order of increasing size (display area) and cost. Among the three, it is only the 128x64 Graphic Display which is capable of displaying graphics of sizes greater than 5x7 pixels. The other two displays are more suitable for displaying text and small icons. Considering the nature of information presented here, displaying of graphics is not a priority; as such a Character Display would do. The 16x2 Character display can only present 32 characters at any point in time while the 20x4 displays a maximum of 80 characters. Thus the latter can present more information at a go than the former. Since it is more convenient to present consumer notifications on a single page than in multiple pages the 20x4 is preferred for the retrofit design.

The specific 20x4 Character Display selected for the design is the Xiamen Ocular GDM2004D LCD model. It has the following features:

1. LED Backlight to illuminate screen especially in darkness
2. +5 volts power supply

3. Expected lifetime of ~50,000 hours
4. Adjustable contrast
5. Operational Temperature range of 0~+50 ºC

Its low input voltage can be supplied by a microcontroller; thus not requiring the addition of any external power source. Also it illuminates brightly in the dark which makes its displayed characters legible for consumers. These features justify the selection of this LCD for the implementation of the smart retrofit in-home display.

5.1.3 Relay

In the retrofit design a relay is included to handle remote requests from the utility to either disconnect or reconnect the meter to power supply. Utilities could also allow consumers to request such services. Two types of relays are capable of this function. They are

1. Solid-State Relays (SSRs) and
2. Electromechanical Relays (EMRs).

SSRs are made of non-moving electronic parts and as such usually have longer lifespans than EMRs; hence they are mostly preferred in applications where switching would be done often – more than 10,000 times. Unlike EMRs, they are silent in their operation and consume very small power. Also they do not produce any sparks when they switch; thus making them ideal in highly flammable applications. Despite their several advantages, they suffer the disadvantage of not being able to completely switch off or on. In either state there is always some amount of resistance present in the semiconductor. This makes them to easily heat up thus requiring the addition of active or passive heat sinks. The on-state resistance can cause some measure of voltage drops, which is highly undesirable in voltage critical applications.

Also the off-state resistance causes more current than required, also known as leakage current, to flow to the connected load. This would add to the user's consumption; which is very undesirable in this application area.

For EMRs, their contacts would get stuck together or get oxidized if they are connected to loads higher than their power requirement. This can be avoided if the right EMR is selected to match the connected load. Based on their mode of operation, EMRs may cause some little electromagnetic interference if there are any perforations in their casing. This is however not a major problem if these devices are properly covered and distanced from likely affected components.

From the comparisons made above, EMRs are more ideal in this application area hence are included in the retrofit design. The specific EMR model used in the design is the Songle Single Channel 5V 30A High Power Relay Module. It has the following key features:

1. Can switch 220 volts AC loads
2. 5 - 12 V transistor-to-transistor logic (TTL) control
3. Maximum Switching Current of 30A

This component also has a low input voltage hence can be easily connected directly to the centralized microcontroller. Its ability to switch high power AC loads makes it a viable choice for switching the power mains connected to either a single-phase or three-phase energy meter.

5.1.4 Microcontroller Unit (MCU)

As described in previous chapter, the microcontroller unit is the centralized hub for all logic and arithmetic operations. It serves primarily as the main processing engine of the smart retrofit; processing all data that comes from the interconnecting components. Therefore the

selection of a microcontroller was influenced mainly by the anticipated processing power requirements, number of interconnecting digital and analog components, total number of nonpreemptive processes and memory requirements. The following MCUs were identified as plausible options for the design of the retrofit:

1. PICAXE
2. Arduino
3. Raspberry Pi
4. BeagleBone

The list provided above is in increasing order of cost, computation power and size. Although PICAXE is the least expensive it is limited in so many areas. For example, of all the MCUs presented it requires the inclusion of a lot more hardware for any basic setup. It also has the least online support and libraries; thus requiring more effort from the user and reducing its versatility.

Arduino and Raspberry Pi have the largest online support and libraries. They are also the most used because they are relatively cheaper than BeagleBone which is 3 times the price of an Arduino. Raspberry Pi and BeagleBone run on Linux Operating System (OS) and are equipped with a 700 Megahertz (MHz) processor; these make them fully fledged computers.

Arduino's Integrated Development Environment (IDE) and 16MHz processor however do not give it such functionality. However, its low computational speed implies that low power is required; which is highly desirable for battery powered systems such as the retrofit. In addition, unlike Raspberry Pi, Arduino has analogue input ports which are a basic requirement for operating some of the energy theft detection sensors. So in short, Arduino is the most ideal

MCU for the retrofit design. The Arduino board used in the retrofit design is the Arduino Mega 2560 Revision 3 model. It has the following features:

1. 54 digital input/output ports
2. 16 analog input ports
3. 4 Universal Asynchronous Receiver/Transmitter (UART) ports
4. 16 MHz Crystal Oscillator
5. Operating Voltage of 5V
6. 4 kilobyte EEPROM
7. 6 External Interrupt
8. Resistance Of Hazardous Substances (RoHS) Compliant

These features are copious enough to facilitate the implementation of the smart retrofit. The four earlier identified non-preemptive processes can be assigned to any of the six external interrupt pins. The remaining two unassigned interrupt pins as well as all other unused digital and analog pins are available for future upgrades. Table 5.1 presents a list of the available interrupt pins, their assigned non-preemptive processes and level of priority.

Table 5.1 Interrupt Allocation Table

Function	Pin Number	Level of Priority
Detection of LED pulses with Photocell	2	0
Not Assigned	3	1
Detection of motion and shock with Accelerometer	21	2
Detection of external magnetic fields with Hall Effect Sensor	20	3
Detection of physical tamper of meter with Tilt Sensor	19	4
Not Assigned	18	5

Alluding to the identified methods of energy theft in Chapter Two, the next few subsections describe sensors which have been carefully selected to detect these felonious activities whenever they occur.

5.1.5 Tilt Sensor

The tilt sensor's main function is to detect energy theft by physical tamper of the meter. It triggers the MCU when an attempt is made to move a part or the whole meter. The MCU would then transmit a tamper report to the utility via the GSM/GPRS communication module.

It was discovered that a simple ball rolling switches can implement this function. This switch contains a steel coated ball which closes a switch whenever it is tilted. An AT407 Ball Rolling Switch was therefore incorporated into the retrofit's design. It was selected because it has very low input voltage of 5V and low operating current of 6mA; hence can be connected directly to the MCU.

5.1.6 Triple Axis Accelerometer

Magnetometers, Gyroscopes and Triple Axis Accelerometers are all capable of detecting changes in acceleration or shock, hence can be used to detect meter tamper. However, the gyroscope and magnetometer have some inherent flaws or limitations. Since the magnetometer detects motion based on its relative position from the earth's true magnetic north its readings are susceptible to errors when magnets are brought into its field. Also gyroscopes are only accurate when used over very short periods of time. The Triple Axis Accelerometer is however not affected by these limitations. As such, the ADXL337 Triple
Axis Accelerometer was included in the smart retrofit's design to also detect physical meter tamper. It has the following attributes:

1. Ultralow Power

2. Operating Current of 300 micro amps (µA)
3. High Resolution
4. Wide voltage range (1.6~3.5 V)

These features, which are similar to the earlier selected components, are desirable for MCU applications. They can be easily attached to the MCU without the addition of external power sources or processors.

5.1.7 Hall Effect Sensor

This sensor is needed to detect energy theft caused by criminals who use strong earth magnets to cause electromagnetic devices in the meter to malfunction. It detects the presence of such strong magnets, triggers the MCU which in turn report to the utility via the communication module. A reed sensor is also capable of providing this functionality. However, it is often limited by its glass container and miniature size. The Hall Effect Sensor selected for the retrofit design is the US1881 Hall Effect Sensor. It has the following features:

1. Ultralow power consumption
2. Reverse polarity protection
3. Wide Range Operational voltage (3.5~24 V)
4. Temperature compensation

5.1.8 Current Sensor

This sensor is required to measure the current in the live and neutral wires. Any significant difference in their values indicates the possibility of a meter bypass. Also current measurements are necessary to evaluate the quality of supplied power. An ACS715 Hall Effect Based Linear

Current Sensor is employed for this purpose in the retrofit design. It has the following key features

1. 2100 V root mean squared (VRMS) isolation voltage
2. Operates at 5V
3. Capable of measuring up to 30A of current
4. Operational temperature of -40~150 ºC
5. Little or no magnetic hysteresis

This current sensor is a viable current measuring component for the smart retrofit because it is capable of measuring high currents even at high voltages while operating at a low input voltage.

5.1.9 Data Logger

This electronic device records data such as consumption data, meter tamper data, power quality measurement and tariffs unto a local storage medium. Equipped with a real time clock (RTC), each data entry is time stamped. This serves as a contingency plan for utilities; in case there is a communication failure meter data is stored locally and retransmitted later after the problem has been resolved. The following electronic devices are capable of providing this function:

1. SparkFun OpenLog
2. Adafruit Data Logging Shield

Although they are both capable of performing the same function, the latter is less expensive and requires addition of less hardware. It is also easier to assemble and customize to meet different installation requirements. Unlike the former, it has a slot for Secure Digital (SD) storage card as well as a battery which keeps the RTC running even after power is disconnected.

These are the reasons why the Adafruit Data Logging Shield was included in the retrofit's design. It has the following key attributes:

1. Saves data to a formatted File Allocation Table 16/32 (FAT16/32) storage SD card
2. Support for a majority of the Arduino boards
3. Onboard 3.3 V regulator safeguards SD cards from power surges

5.1.10 Speaker

This alerts a consumer by sounding an alarm when new notifications have been received from the utility, measured power quality is below standard or a user is about reaching his set threshold. There are a wide range of speakers that could be used in the retrofit design. However, a Piezo Speaker was incorporated in the retrofit design because of its compact size, low cost and ultralow power requirements. It has the following features:

1. Operational voltage: 3.5-5 V
2. Maximum current rating: 35 mA
3. Diameter: 12 millimeters
4. Operates in 2.048 kHz audible range
5. Sound output: 95 A-weighted decibels (dBA)

5.1.11 Backup Battery and Charger

A rechargeable backup battery is needed to supply the retrofit with power at all times; especially during power outages. Without this battery the retrofit would fail to perform its function during such periods. Critical functions such as meter tamper and outage detections are to be recognized

and reported in real-time to the utility and as such require perpetual supply of power to the retrofit.

The following battery options are considered for the retrofit design:

1. Lithium Polymer Ion (LiPo/ LiIon)
2. Nickel Metal Hydride (NiMH)
3. Coin Cell
4. Alkaline

From the list of batteries presented, LiPo batteries have the highest energy densities; most compact and having the highest capacity. They last longer than the others because they have an ultralow discharge rate. They are the most available and most used battery supply for electronic devices. Most LiPos are equipped with an internal circuitry to safeguard the battery from depleting below a certain threshold. They can be recharged with several low cost chargers.

Based on these attributes a 6,600 milliamp hour (mAh) Lithium Polymer Ion Battery fitted with a charger is included in the retrofit design. This unit has the following features:

1. Nominal Voltage of 3.7 V
2. Maximum charging rate of 3A
3. Maximum depletion rate of 6A

After having described and justified the above components, Table 5.2 summarizes the selected components and their basic performing functions.

Table 5.2 Major Components for Smart Retrofit Implementation

No.	Name	Function

1.	GL5528 Mini Photocell	Detects LED pulses from existing meter.
2.	Sim900 GSM/GPRS Communication Module	Provides reception and transmission of data messages to/from utilities.
3.	Xiamen Ocular GDM2004D 20x4 Liquid Crystal Display (LCD)	Displays consumption data, tariffs, power measurements, utility transmitted notifications and control information.
4.	Keyes 5V Electromechanical Relay Module	Remote disconnection/reconnection of meter from/to power supply.
5.	Arduino Mega 2560 Revision 3 model	Programmed Microcontroller to handle all arithmetic and logical processes.
6.	AT407 Ball Rolling Switch (Tilt Sensor)	Energy Theft Detection Mechanism: Detects physical tamper of meter.
7.	ADXL337 Triple Axis Accelerometer	Energy Theft Detection Mechanism: Detects motion and shock.
8.	US1881 Hall Effect Sensor	Energy Theft Detection Mechanism: Detects external magnetic fields.
9	ACS715 Hall Effect Based Linear Current Sensor	Energy Theft Detection Mechanism: Detects meter bypass. Also required to carry out power quality measurements.
10.	Adafruit Data Logging Shield	Registers measurements from sensors at set intervals. Also keeps track of time.
11.	Piezo Speaker	Sounds an alarm to prompt user.
12.	6,600 milliamp hour (mAh) Lithium Polymer Ion Rechargeable Battery	Provides power to the retrofit even during power outages.

Detailed datasheet specifications of each of these components are obtainable from trusted online stores such as Adafruit, Digikey, Mouser and SparkFun.

5.2 SIMULATION OF SMART RETROFIT

After having keyed out the specific components required for the implementation of the smart retrofit, the research progressed with circuit simulations. These simulations were done using ISIS Professional Software version 7.9 Service Pack 1. These simulations were carried out primarily to imitate the functions of the selected interconnecting components. This step is important in verifying the established functional requirements of the smart retrofit. It is

however important to note that a few of the specified components were not available in the chosen circuit simulator. As such, suitable replacements were used to achieve the same functionality. The schematic of the circuit simulation is presented in Figure 5.3.

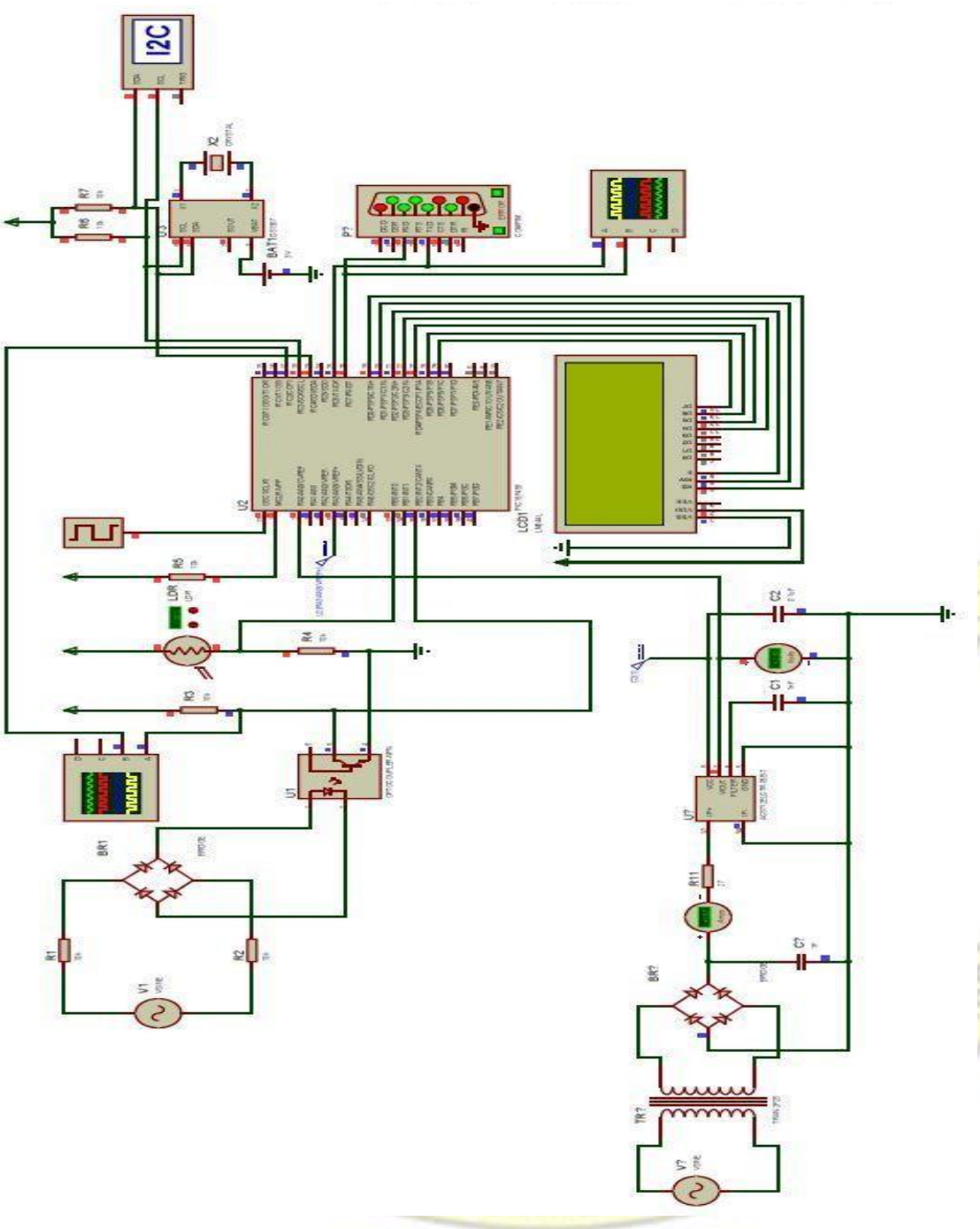


Figure 5.3 Schematic of Smart Retrofit Circuit Simulation

During the circuit simulation, a program was written for the centralized microcontroller unit (MCU) to perform the required system processes. This program was written in C and compiled

using a CCS C Compiler, Version 4.093. After compiling the code, a hex file was generated and loaded unto the centralized MCU. The written program is presented in Appendix A.

The simulation environment was designed to mimic features that pertain to the current electrical grid in Ghana. Key among the features includes:

1. A voltage supply of AC220 volts ±10%
2. Voltage signal supplied at a frequency of 50Hz
3. Power factor ranging between 0 and 0.9

The key performance indicators (KPIs) for this simulation are implicitly given as the basic functional requirements of the smart retrofit. These requirements were elicited in the previous chapter and are summarized below.

1. Display of accurate consumption data in kWh and currency via in-home display.
2. Reception and display of utility transmitted notifications and control information.
3. Real-time transmission of accurate consumption data and power quality measurements to utilities.
4. Real-time detection and remote reporting of meter tamper.
5. Remote disconnection and reconnection of power supply.

After having run the simulation over a period of time; providing it with input from the various connected components, the following observations were made:

1. The retrofit gathers consumption data from the existing standalone meter by detecting light pulses from the LED using the photocell (LDR)

2. Upon the detection of a light pulse, the LDR interrupts the MCU to increase the count of pulses detected.

3. Based on the impulse rate of the meter and the pulse count, energy consumption is computed in kWh and stored in the MCU's EEPROM and logged on the SD Card

4. At the end of specific time periods; such as hour, day, week, month and year, the MCU computes the average consumption over the period and stores results in its EEPROM

5. Power quality measurements (voltage, current and active power) are taken using the ACS715 Hall Effect Based Linear Current Sensor.

6. The MCU stores the measured value and does various checks to find out if power supplied to the meter is of good quality. The MCU also checks to see if current measured on live and neutral lines have no significant difference. If they do, a meter tamper flag is set high and stored on the SD Card and EEPROM.

7. All the other connected sensors; Hall Effect, Accelerometer and Tilt sensors, interrupt the MCU when there is a significant change in state. The MCU then sets the tamper flag high on the SD Card and EEPROM.

8. All stored data are transmitted to the utility every 15 minutes via the GSM/GPRS module. However, registered tamper flags and poor power quality measurements are transmitted instantaneously.

9. The GSM/GPRS module alerts the MCU each time a message is received from the utility. The MCU processes the message and carries out the required action. For example, upon request of (dis)connection the relay is triggered to do as such.

10. The LCD displays computed consumption data, tariffs and notifications in turns as depicted in Figure 5.4.

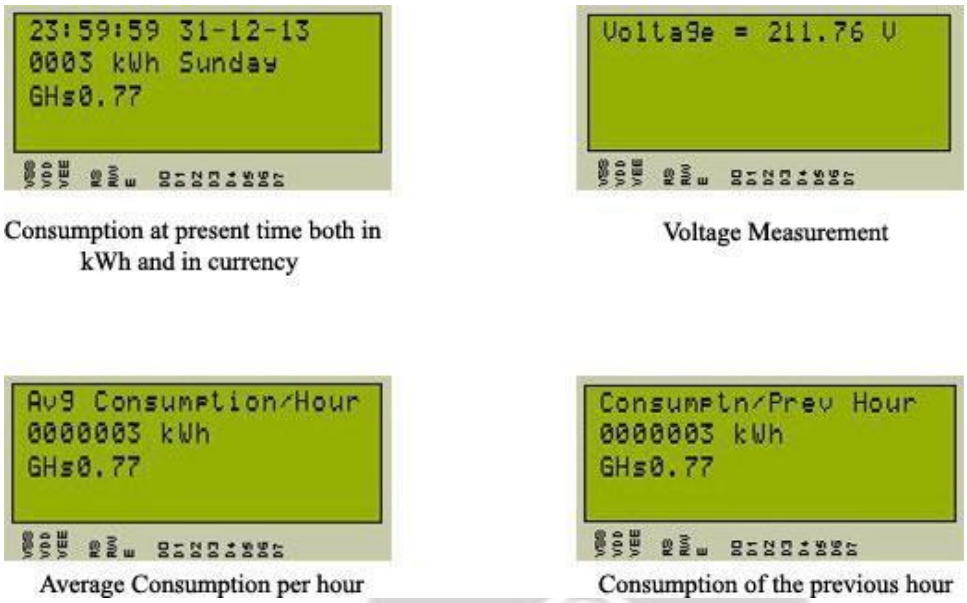


Figure 5.4 LCD displaying consumption data and power measurements

5.3 CONSTRUCTION OF SMART RETROFIT

After consistent desirable results were gathered from the system's simulations; some of which are depicted in Figure 5.4, a final schematic diagram was developed using Fritzing Software version 0.92b; an advanced and comprehensive tool for open source hardware circuit design. This circuit diagram depicts the underlying circuitry and interconnections of the earlier mentioned building blocks and other enabling components. The schematic diagram is presented in Figure 5.5.

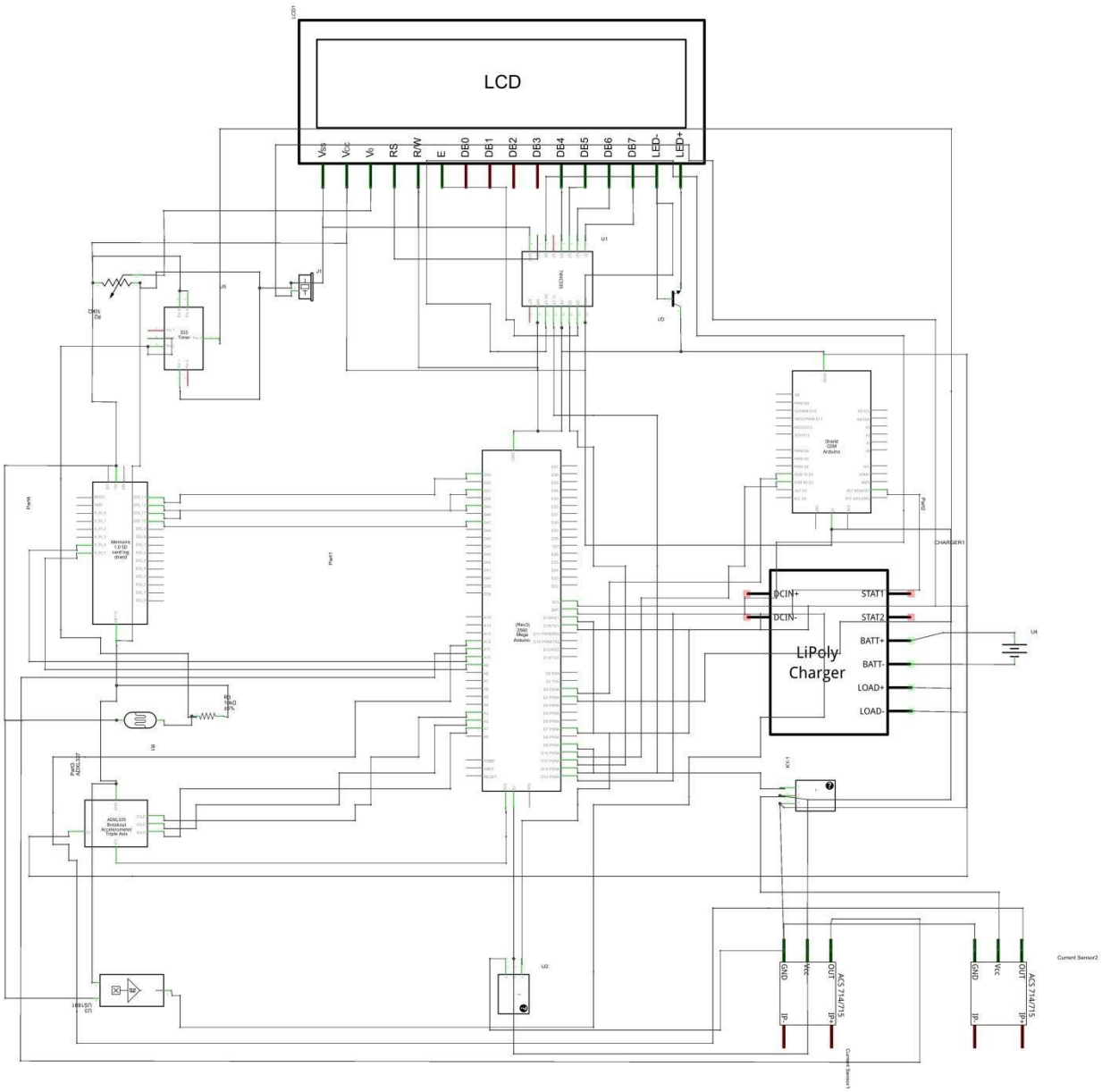


Figure 5.5 Schematic Diagram of Retrofit Design

A high level breadboard presentation of this schematic design is presented in Figure 5.6.

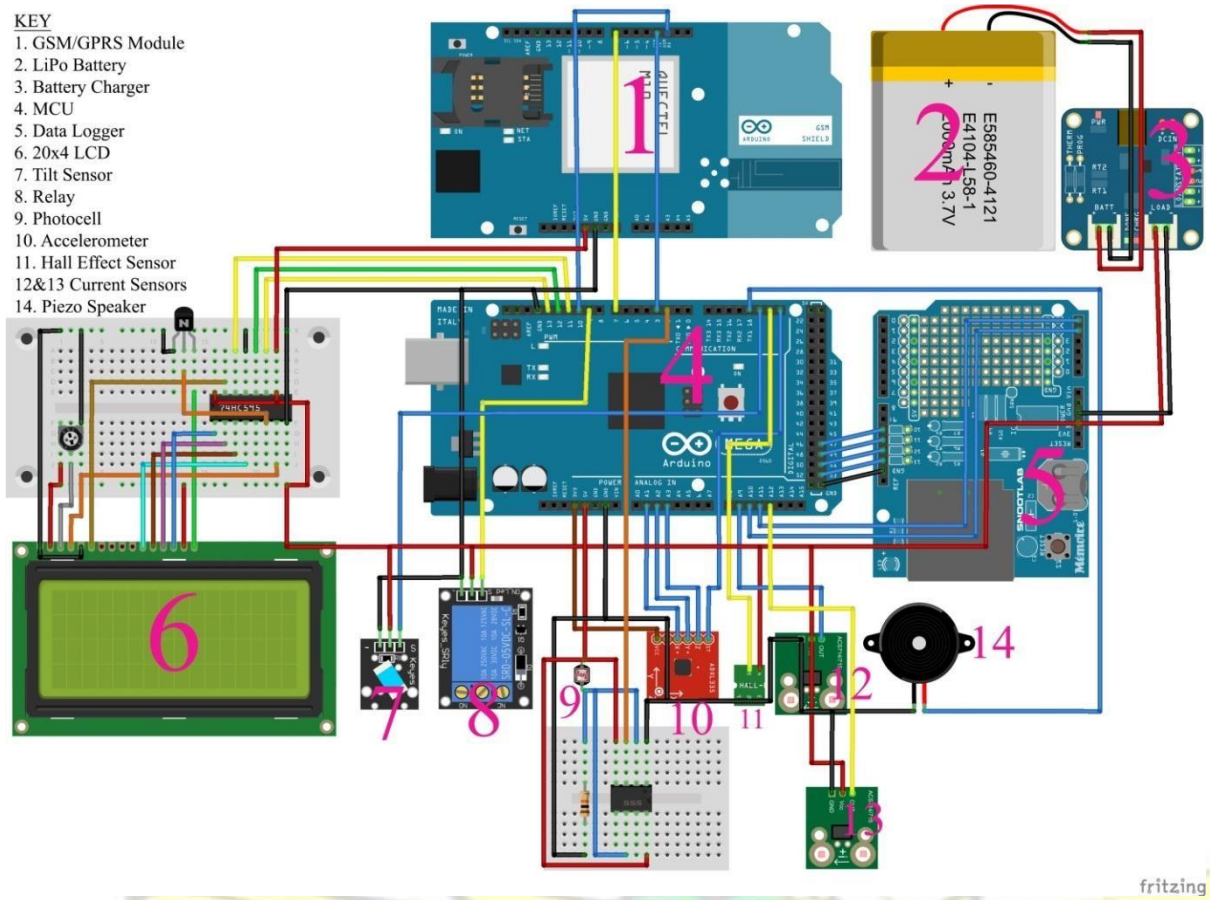


Figure 5.6 Breadboard Schematic Diagram of Smart Retrofit Design

Based on these schematics, the smart retrofit was constructed using the identified system components. These components were purchased online from Mouser and SparkFun. The MCU of this prototype was programmed in C++ using an Arduino Integrated Development Environment version 1.64. This program is presented in Appendix B. The constructed prototype is shown in Figure 5.7.

Figure 5.7 Prototype of Retrofit

To demonstrate more clearly how the retrofit and existing meter are connected, various three dimensional (3D) models were designed with SketchUp 3D modeling software. These models are depicted in Figures 5.8 - 5.11.

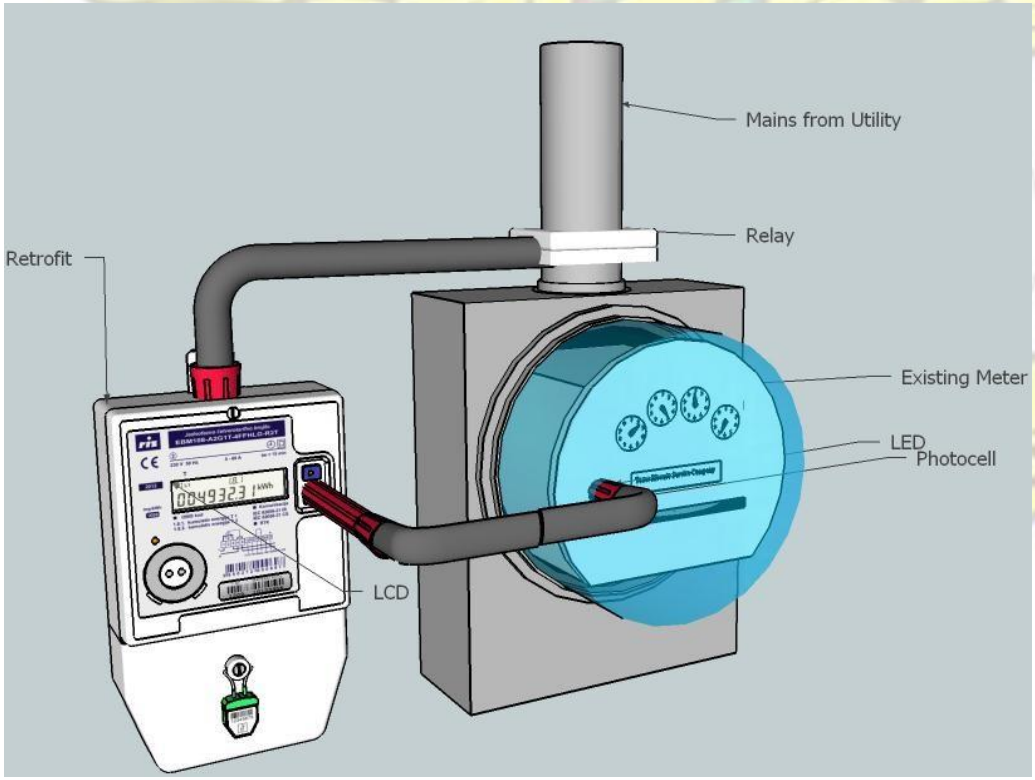


Figure 5.8 Left side view of Retrofit and Meter's 3D Model

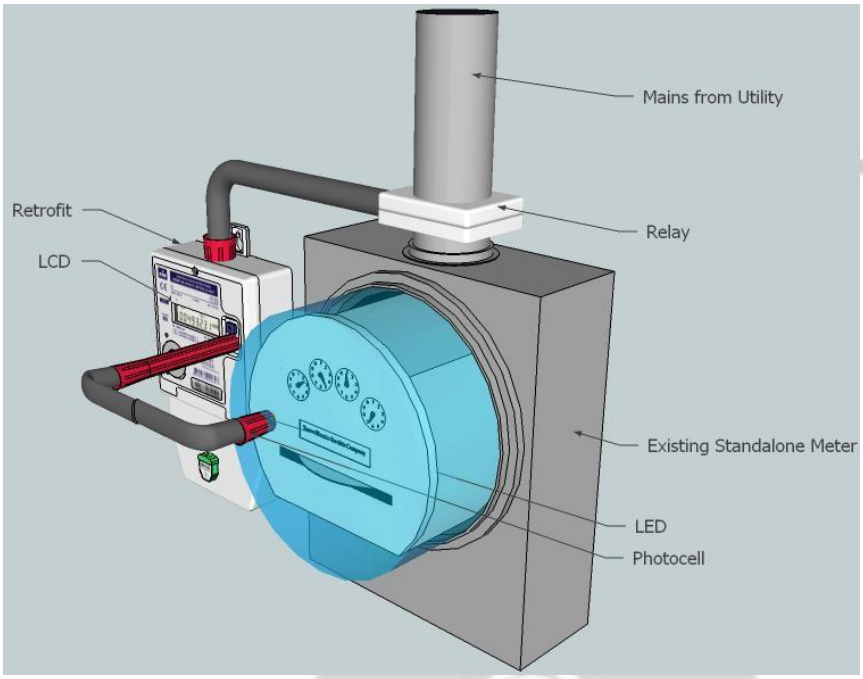


Figure 5.9 Right side view of Retrofit and Meter's 3D Model

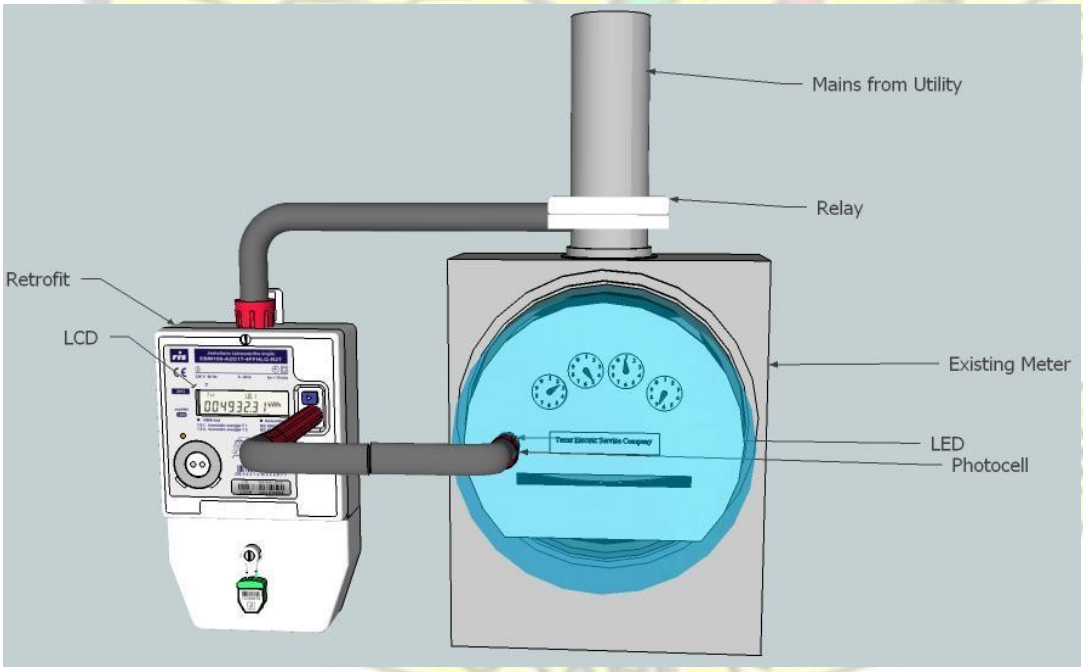


Figure 5.10 Front view of Retrofit and Meter's 3D Model

To safe guard the system from environmental factors and tamper it is recommended that the system is placed in a casing, as depicted in Figure 5.11. This casing should be transparent enough for the consumer to read the meter's display outside the casing. Also the retrofit's enclosure should be made to have direct contact with this casing. This would enable the retrofit's physical tamper sensors to detect any tamper with the transparent casing.

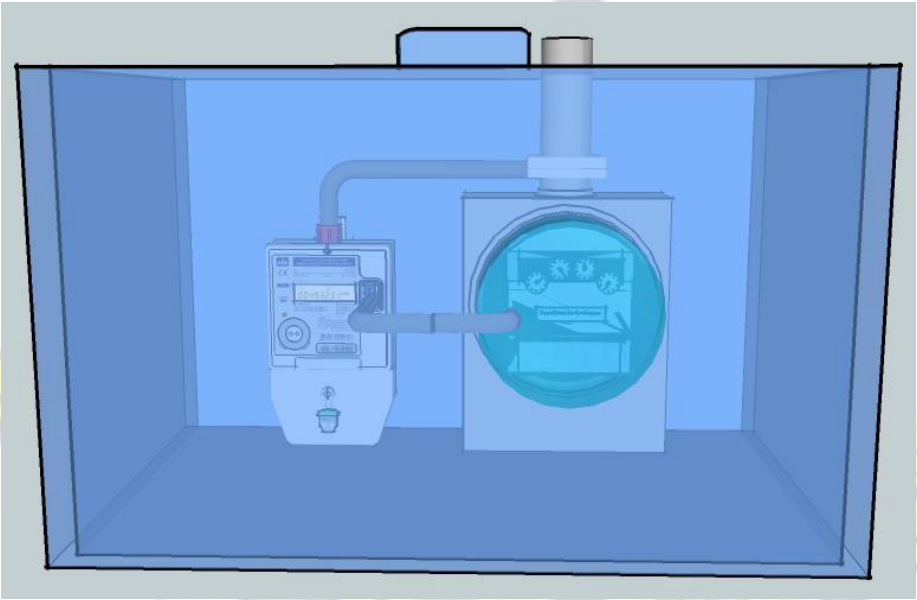


Figure 5.11 Front view of Retrofit and Meter's 3D Model in Transparent Casing

The research went further to develop a web service which served as a Meter Data Management System (MDMS). This server provided long term cloud storage for the meter's transmitted data as well as validated, managed and critically analyzed all meter data. This system was programmed with Django 1.8.2 which is a high level Python web development framework. The entire web service was hosted securely on a virtual private server and was accessible via the uniform resource locater http://159.203.118.203/. As depicted in Figure

5.12, access to the MDMS's database required login credentials; thus preventing access to unauthorized persons.

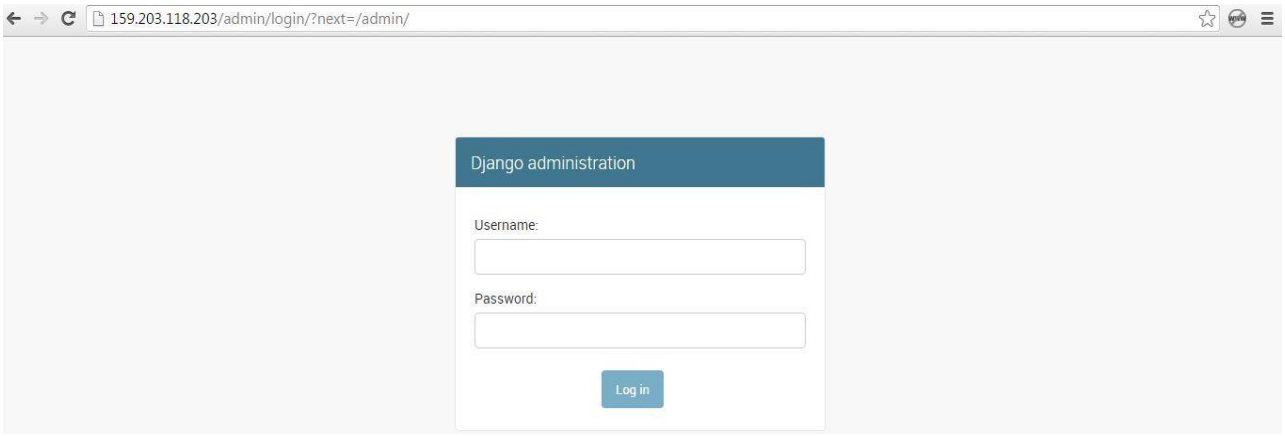


Figure 5.12 MDMS Login Panel

A snapshot of results of a query on the MDMS cloud database is presented in Figure 5.13.

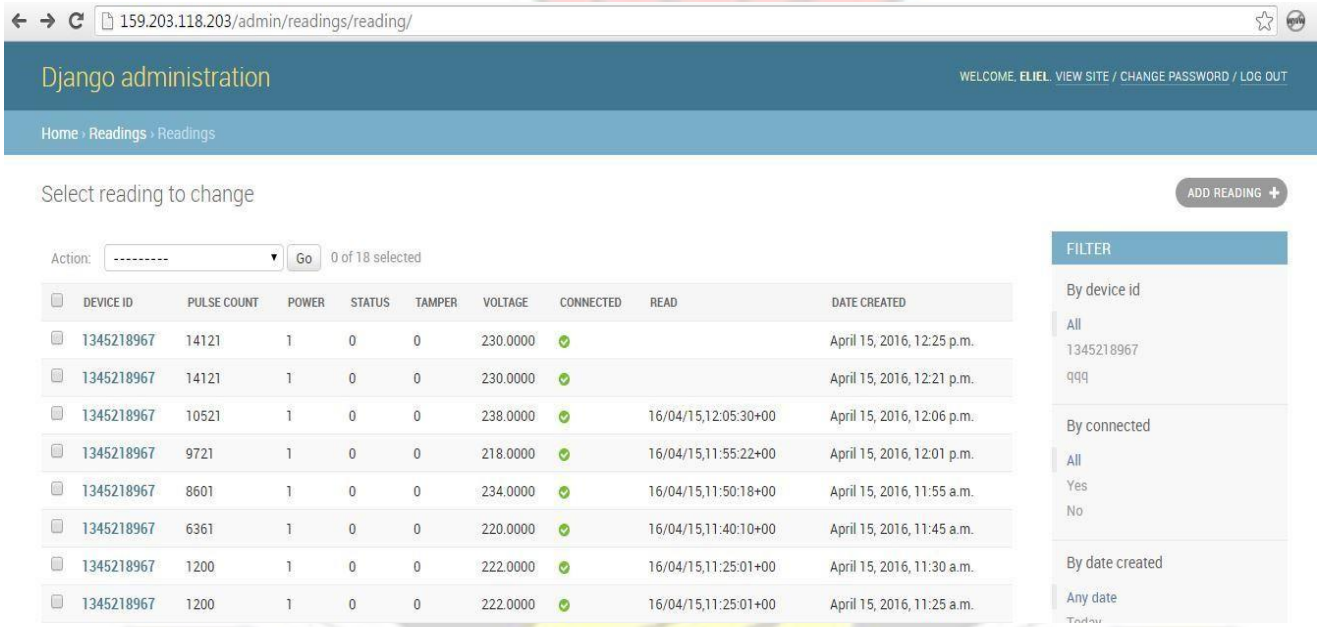


Figure 5.13 Sample Meter Data Readings on MDMS

From Figure 5.13, it is evident that the presented table collates information sent from the smart retrofit. The meaning of the various fields is provided in Table 5.3.

Table 5.3 Meaning of Fields in Meter Data Table

No.	Name of Field	Meaning
1	Device ID	Represents the smart retrofit's unique identification number
2	Pulse Count	Total number of pulses detected by the photocell as at the time of transmission
3	Power	A Boolean value which tells if the meter has power or not.
4	Status	A Boolean value which tells if consumption has exceeded a user set threshold.
5	Tamper	A Boolean value which tells if the meter has been tampered with.
6	Voltage	A floating point value that provides the voltage reading as at the time of transmission
7	Connected	A Boolean value which tells if the meter has been connected or disconnected by the utility
8	Read	The date and time of as at the time of transmitting the meter data.
9	Date Created	The data and time the meter reading was received and stored in the database.

Since this web service is accessible online, ample cyber security protocols are adhered to in communicating data to and from the MDMS and smart retrofit. Details of the entire cyber security framework designed for this smart metering system are provided in the next chapter.

5.4 SUMMARY

This chapter elaborated the various processes followed in implementing the smart retrofit. Guided by the adopted research methodology, the smart retrofit is constructed and a suitable cloud based MDMS is developed to store and manage its transmitted meter data.

CHAPTER SIX: NETWORK ENVIRONMENT

6.0 INTRODUCTION

This Chapter throws more light on the selected communication network for the deployment of the proposed smart metering system. It also suggests security measures required to guard the system from known attacks. In Section 6.1 the entire layout of the communication network is presented and explained. In Section 6.2 cyber and physical security measures are proposed for the smart metering system.

6.1 COMMINCATION NETWORK

In the Chapter Two, emphasis was laid on the importance of having a reliable communication network in the smart metering system. It was explained that the benefits smart meters have over standalone meters are as a result of the existing two-way communication ability. As such, after examining various communication technologies, the features of GSM made it a more likely candidate for deploying smart metering systems in African developing countries. A recap of some of its desirable features include

1. GSM is currently the most pervasive communication technology in Africa; covering over 70% of Africa's population. Its wide coverage implies that the necessary infrastructure has already been installed thus making it a suitable early adoption technology for establishing low cost smart metering communication – requiring little or no setup cost [6.1].
2. GSM has also been tested and tried over decades to reliably deliver data over long distances. As compared to the earlier mentioned wireless communication technologies, it has a high propensity of penetrating through concrete walls [6.2].

3. As a consequence of keen competition among Mobile Network Operators (MNO) in African developing countries, the rates for voice, short message service (SMS) and data via GSM keep subsiding [6.3].

Based on these favourable characteristics, this research proposes the adoption of GSM as the main communication technology for the proposed smart metering system. A suitable GSM/GPRS communication module has already been included in the retrofit's design to facilitate two-way communication between the smart retrofit and the utility.

To buttress the selection of this communication technology as a viable technology for the transmission of meter data, analysis of a performance evaluation of a deployed GSM network is conducted in the next section.

6.1.1 Performance Evaluation of A GSM Network

In [6.4], communication requirements were prescribed for common smart metering operations. These requirements bordered mainly on the following key performance indicators (KPIs):

1. Latency: The time which a data packet takes to travel from transmitter to the receiver.
2. Throughput: The rate at which data travels through the network.

Some of these requirements for smart metering operations are specified in Table 6.1.

Table 6.1 Typical Communication Requirements for Smart Metering Operations

Function	Description	Latency(ms)	Throughput(kbps)
Automatic Meter Reading	Periodic transmission of meter readings to a designated MDMS	12 – 2000	56
Real Time Pricing	Transmission of tariffs and notifications necessary for the rollout of DR Programs	30 – 400	10 – 100
Meter Control	Transmission of meter control information from MDMS	200 – 2000	56

In Table 6.1, it can be observed that most of the latencies have a wide range. This can be attributed to the differences in various application areas. For example where DR programs are implemented, utilities may transmit dynamic tariffs and DR notifications over very short periods of time – every minute, while others may transmit them after long periods of time – every 15 minutes. Where periods are longer, larger latencies can be tolerated since the time-to-transmit indicates that tariffs and notifications would not change quickly. However, latencies should always be smaller than the time-to-transmit.

Based on these requirements, a comparison is made with results of a performance evaluation of a GSM network at the Kwame Nkrumah University of Science and Technology [6.5]. The same KPIs listed above were taken into consideration during the survey. The survey area spans over 5 kilometers squared and is populated by approximately 25,000 people.

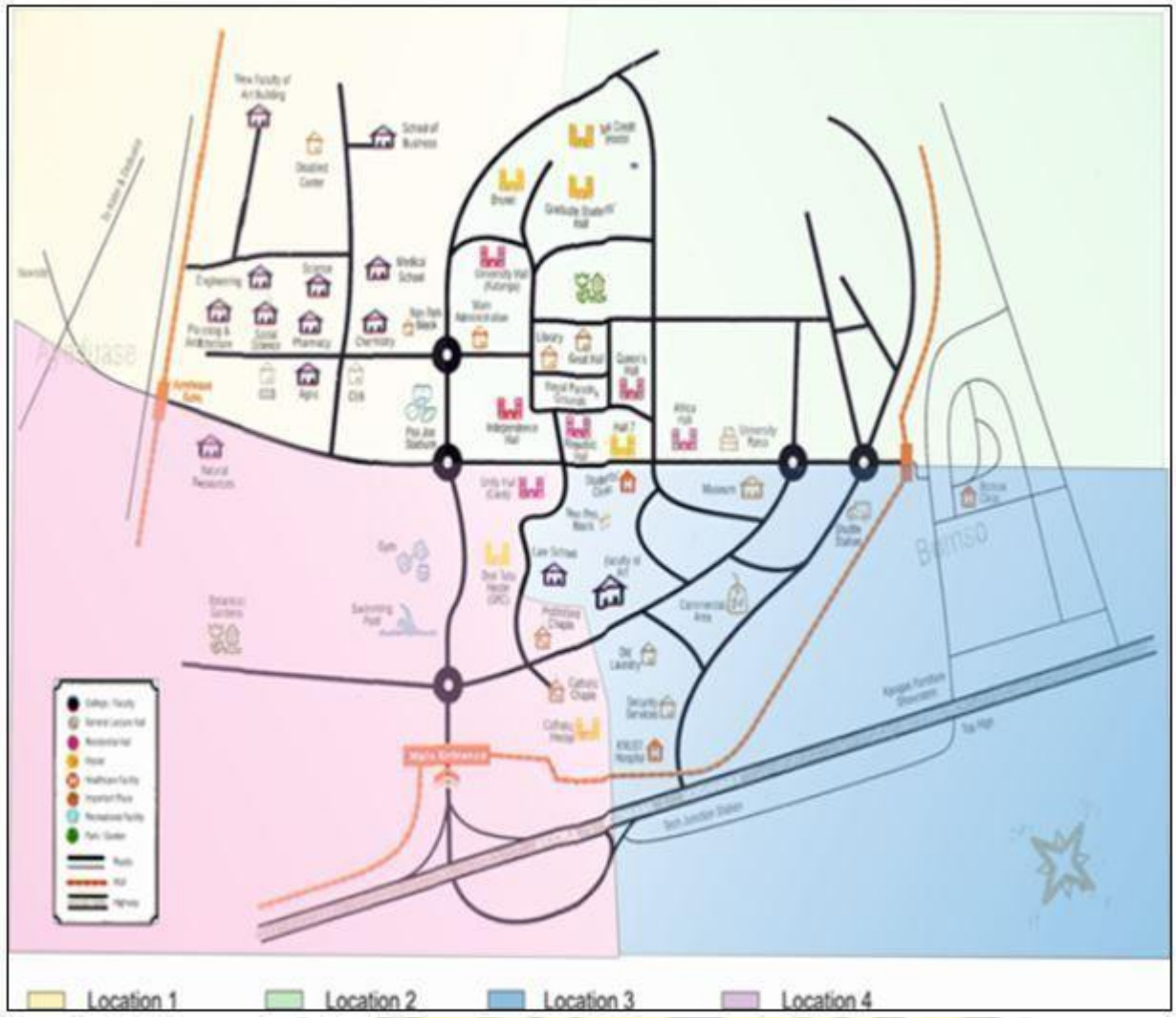


Figure 6.1 Survey Area for Performance Evaluation

As depicted in Figure 6.1, the survey was segmented into four locations. They include:

1. Location 1: Classroom blocks, administrative offices and labs
2. Location 2: Halls, hostels and residential facilities for staff
3. Location 3: Business Center
4. Location 4: University's main entrance

Adhering to an Analytic Hierarchy methodology, the earlier mentioned KPIs were measured for each location over a period of two weeks and the results were tabulated and graphed. Figure 6.2 and 6.3 presents a bar graph of the measured KPIs over the two week period.

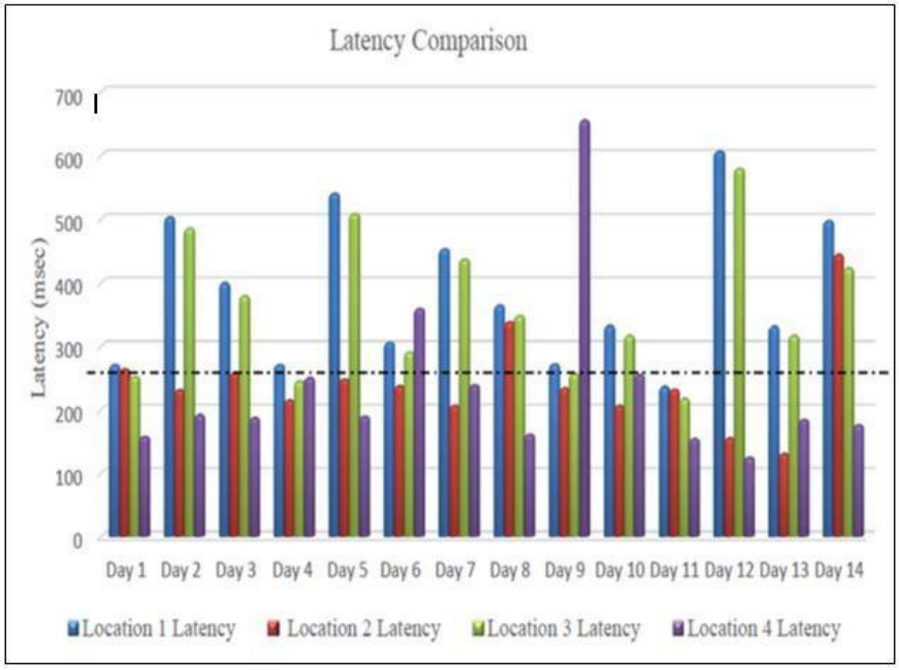


Figure 6.2 Measured Latencies from four locations

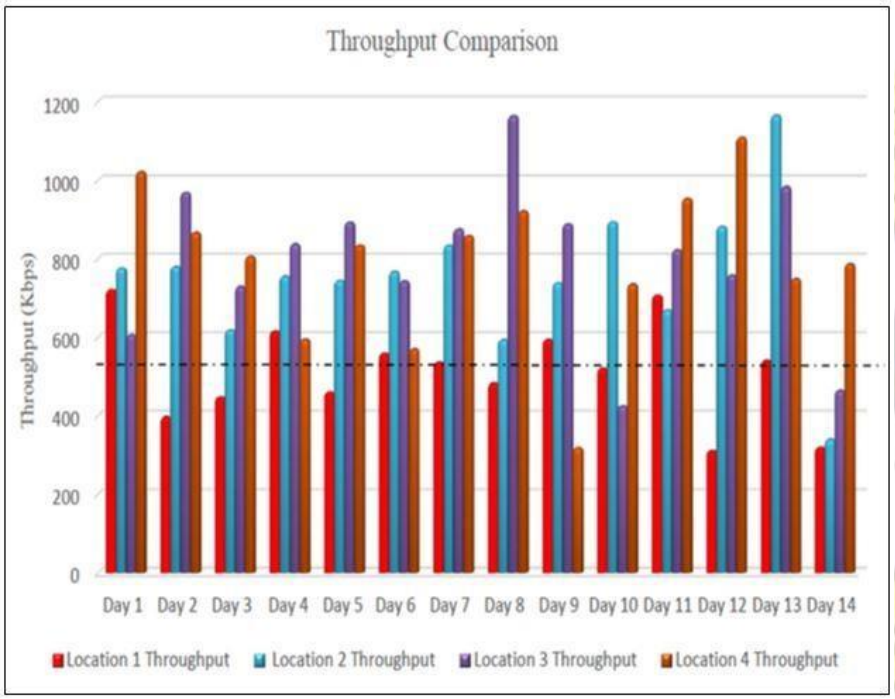


Figure 6.3 Measured Throughput from four different locations

The striking dotted black lines in the graphs represent International Telecommunication Union's (ITU) average measured value for GSM latency and throughput; which are 250

milliseconds (ms) and 512 kbps respectively. Table 6.2 presents the average latencies of the various locations.

Table 6.2 Average Latencies and Throughputs of Each Location

Location	Latency (ms)	Throughput (kbps)
Location 1	384.49	515.38
Location 2	243.09	754.20
Location 3	361.14	796.93
Location 4	234.79	794.61

From Table 6.2, it can be concluded that the latencies of the four selected locations range between 234 and 384 ms. Also the throughput of the four locations range between 515 and 797 kbps. The average of these measured KPIs for the entire survey area is presented in Table 6.3.

Table 6.3 Average Latency and Throughput of Survey Area

Location	Latency (ms)	Throughput (kbps)
KNUST survey area	305.88	715.28

From Table 6.3, it is obvious that the measured KPIs are higher than the values measured by the ITU. However, the difference is not too wide. These obtained average KPIs for the survey area, are further compared with the communication requirements presented in Table 6.1. Based on these requirements, one can verify whether GSM is a viable communication network for smart metering operations. It is important to note that, its viability is certain if the measured average latency does not exceed the maximum latency

requirement and the measured average throughput is not less than the prescribed throughput.

Based on the measured KPI's it is evident that the values obtained lie within the range for the typical communication requirements for smart energy metering operations. It can therefore be concluded that GSM is a suitable communication network for smart metering operations. However, it is important that the time-to-transmit is always kept exceedingly larger than the measured latency.

After having provided sufficient justifiable reasons for the use of the GSM network, the following subsections focus on laying out the entire communication infrastructure of the proposed smart metering system.

6.1.2 Communication Architecture of Proposed Smart System

Referring to the use cases presented in Chapter Four, the main communicating parties within the proposed system's network are:

1. The smart retrofitted meter
2. Utilities and
3. Consumers

The key communication links that exist between them are presented in Figure 6.4.

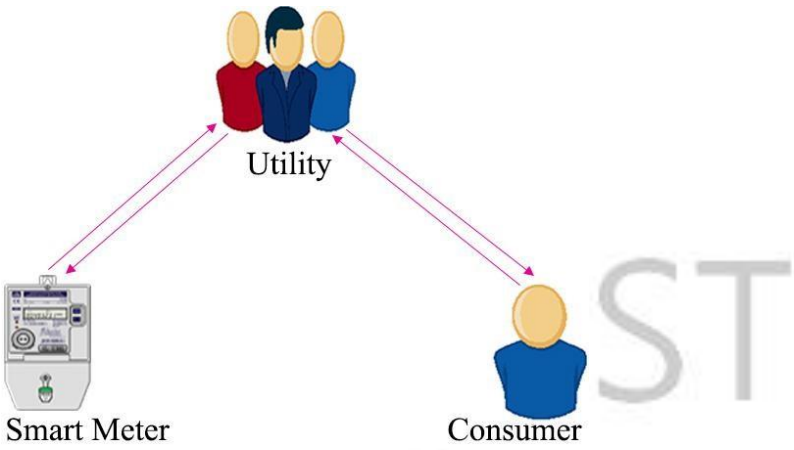


Figure 6.4 Communication links in smart metering system

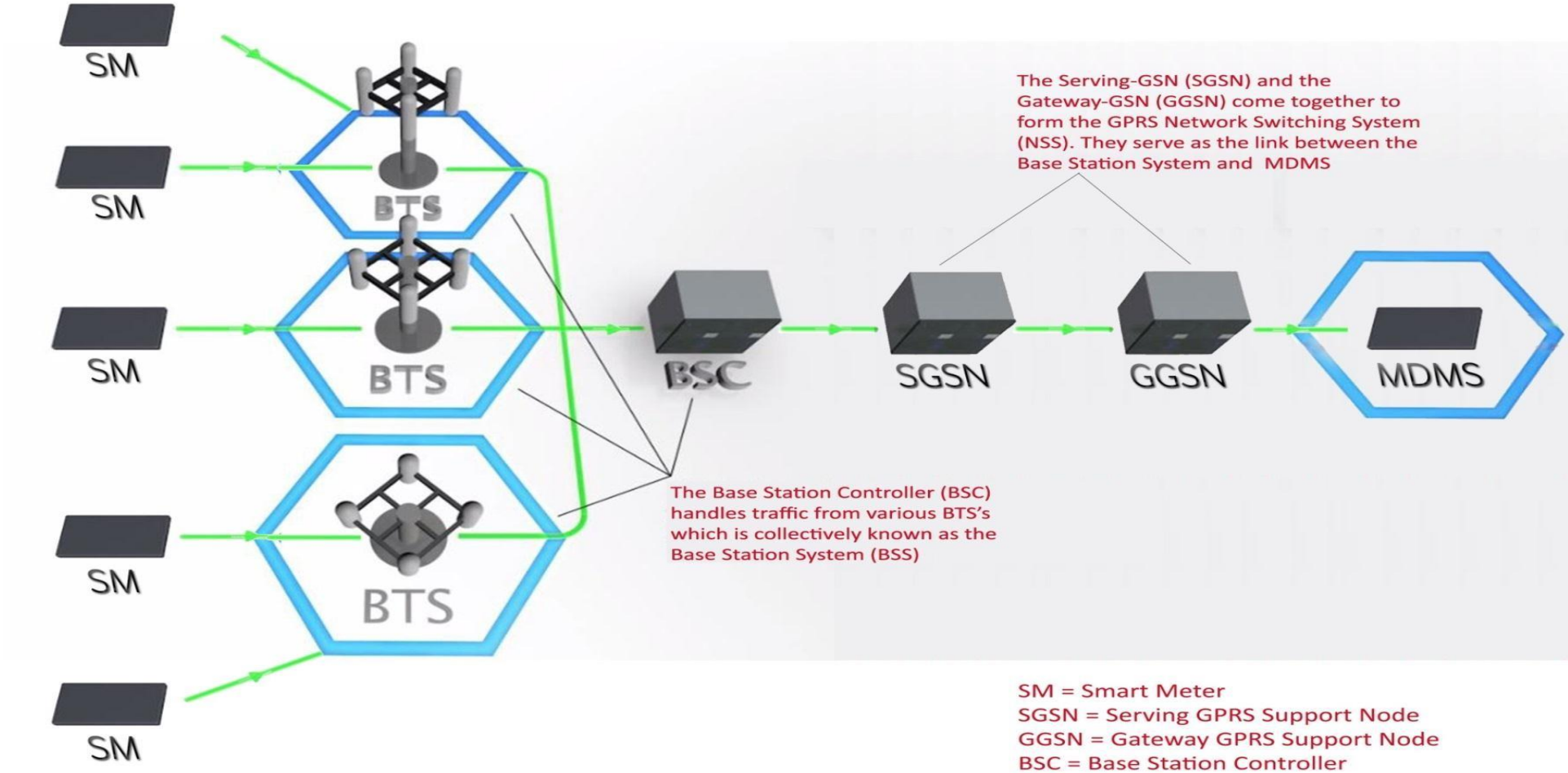
As depicted in the Figure 6.4, two-way communication links exist between the smart retrofitted meter and the utility as well as between the consumer and the utility. From this Figure, it is clear that no direct communication link exists between the consumer and the smart retrofitted meter; even if the meter is installed on his premise. The utility is responsible for handling consumer requests to their meter as well as delivering reports from their meters. This is so because the utility must first validate the request before authorizing it. Also they are responsible for delivering meter information in a format which would be easily understandable by the consumer. As stated in the Chapter Two, in smart metering systems, consumers can communicate to the utilities via mobile devices as well as online portals [6.6].

It is however important to note that, all communication goes through the centralized MDMS before reaching the final destination. For example, the transmission of consumption data from the smart meter to utilities (discos and generating stations) would go through the MDMS. When the message arrives at the MDMS, it would first save it, process it by reformatting it into styles that best suit the various designated utilities, before submitting it. Also at the end of specific periods it performs critical analysis of all the stored data and submits formatted reports to all concerned stakeholders. The MDMS can

therefore be seen as the main data storage and processing unit of the entire smart metering infrastructure [6.6]. Its existence has reduced the computation requirements of smart meters as well as the analyses carried out by utilities. All these reductions also reflect in the cost and time of carrying out these activities. The necessary systems required to keep the MDMS running without any failures are provided. Some of these systems include reliable power supplies and decentralized backup servers – local and cloud based.

In dealing with consumer requests, the MDMS works hand-in-hand with a Customer Information System (CIS) [6.6]. This system is responsible for managing and recording all consumer data, billing plans and consumer transactions. Since discos are the closest link to consumers; in terms of delivery of customer services, they are responsible for the setup and management of the CIS.

To demonstrate clearly how communication is done in the GSM/GPRS network among these parties, Figure 6.5 presents the communication architecture that exists between smart retrofitted meters and the centralized MDMS.



SM = Smart Meter
SGSN = Serving GPRS Support Node
GGSN = Gateway GPRS Support Node
BSC = Base Station Controller
BTS = Base Transceiver Station
MDMS = Meter Data Management System

Figure 6.5 GSM/GPRS communication architecture between smart retrofitted meter and MDMS

In Figure 6.5, a number of smart retrofitted meters, in transmitting consumption data, get access to the closest BTS via the air interface. The BTS forwards these data messages through the available idle radio channels to their designated Base Station Controller (BSC).

The BSC, which is responsible for providing control functions as well as connectivity to the GPRS Network Switching System (NSS), relays these messages to the Serving GPRS Support Node (SGSN). The SGSN is responsible for storing information about all the meters it serves as well as controlling their access to the Gateway GPRS Support Node (GGSN).

After the SGSN has successfully transmitted the meters' data to the GGSN, which serves as the main interface to remote data networks, the data messages are finally submitted to the MDMS [6.7]. This routine is similar to all other communication that takes place in the smart metering system.

It is however important that data messages are delivered promptly and in real-time, in order for the necessary analyses and decisions to be taken by consumers and utilities. This prompt delivery can be ensured by reducing transmission latencies. However such latencies are bound to occur when there is a high demand for very limited network resources. In such cases the communication network is described as being congested. In the next subsection the research attempts to suggest congestion avoidance models that the utility can adopt in order to minimize latencies.

6.1.3 Congestion Avoidance Models

From the earlier discussions the research proposes that the utility deploys the proposed smart metering system using an existing GSM network. This suggestion is mainly driven by the objective of providing a low cost early adoption strategy for implementing secured smart metering systems in African developing countries. As mentioned earlier, the use of an existing GSM network ensures the reduction in deployment cost as well as deployment time.

It also guarantees a high level of reliability since the existing GSM infrastructure has successfully facilitated communication over a long period of time.

Despite these advantages, an area of concern is the magnitude of simultaneous active connections (network traffic) that would be added when smart meters are massively rolled out. Knowing this magnitude would help in determining whether there would be congestion in the existing GSM/GPRS/EDGE network. In GSM architecture, Base Transceiver Stations (BTS) are mounted at various cell sites to provide transmission/reception services to Mobile Subscribers (MS) in the locality [6.8]. There is a limit to how many simultaneous active connections a BTS can handle. Any time subscribers' demand for network resources exceed the available, there is bound to be network congestion [6.9].

In an attempt to provide a congestion avoidance scheme, 3 models have been suggested. Utilities can adopt any of these models in order to have smart meters efficiently share network resources with existing MS. These models are based on an average MS-to-BTS Ratio and a Dynamic Traffic Class Prioritization (DTCP) Scheme. The average MS-to-BTS Ratio is a value which expresses the typical number of active connections a particular BTS handles at any given point in time. This value gives a clear indication of the likelihood of network congestion. DTCP is a scheme which dynamically changes the prioritization class, also known as Quality of Service (QoS) Class, of a transmitted message – the higher the class the more preferential treatment received from the BTS [6.10]. The default QoS Class for most subscriber messages is Best Effort Service Class. This class is lower than the following:

1. Unsolicited Grant Service Class
2. Extended Real-time Polling Service Class
3. Real-time Polling Service Class

4. Non-real-time Polling Service Class [6.11]

However, it is worth noting that not all Mobile Network Operators (MNOs) allow DTCP. A basic description of the mode of operation of the proposed models is provided in the following subsections.

6.1.3.1 Model 1

This model is adopted when the average MS-to-BTS Ratio is low and far from reaching its limit. This limit is highly dependent on the quantity of public network resources available to MS for communication. In this model utilities deploy smart meters without making any modifications in the network architecture. In other words, smart meters' communications to/from utilities via the BTS are treated in the same manner as the existing MS. There is no need for preferential treatment even if DTCP is allowed by the MNO. The low average MSto-BTS Ratio indicates that there are sufficient network resources to meet MS demand; thus congestion is not likely to occur. Low averages of MS-to-BTS Ratio are dominant in areas with low MS population such as rural settlements. Figure 6.6 presents the algorithm used by the BTS in allocating network resources.

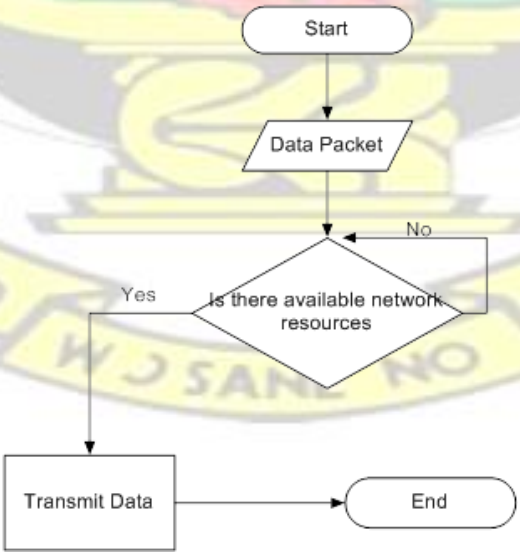


Figure 6.6 Network Resource Allocation Algorithm for Model 1

6.1.3.2 Model 2

This model is preferred in localities where the MS-to-BTS Ratio is high or fast approaching its limit and DTCP is allowed. A massive deployment of smart meters in this area would drastically affect the network's performance. This would have a negative impact on the timely delivery of the meter consumption data, utility control information and notifications. In this model the utility company comes into agreement with the MNO to give data messages to/from smart meters a higher QoS class. This is to ensure that these messages receive preferential treatment from the BTS and are delivered in a timely manner. This model is likely to be adopted for medium MS populated areas such as growing towns. Figure 6.7 presents the algorithm used by the BTS in allocating network resources.

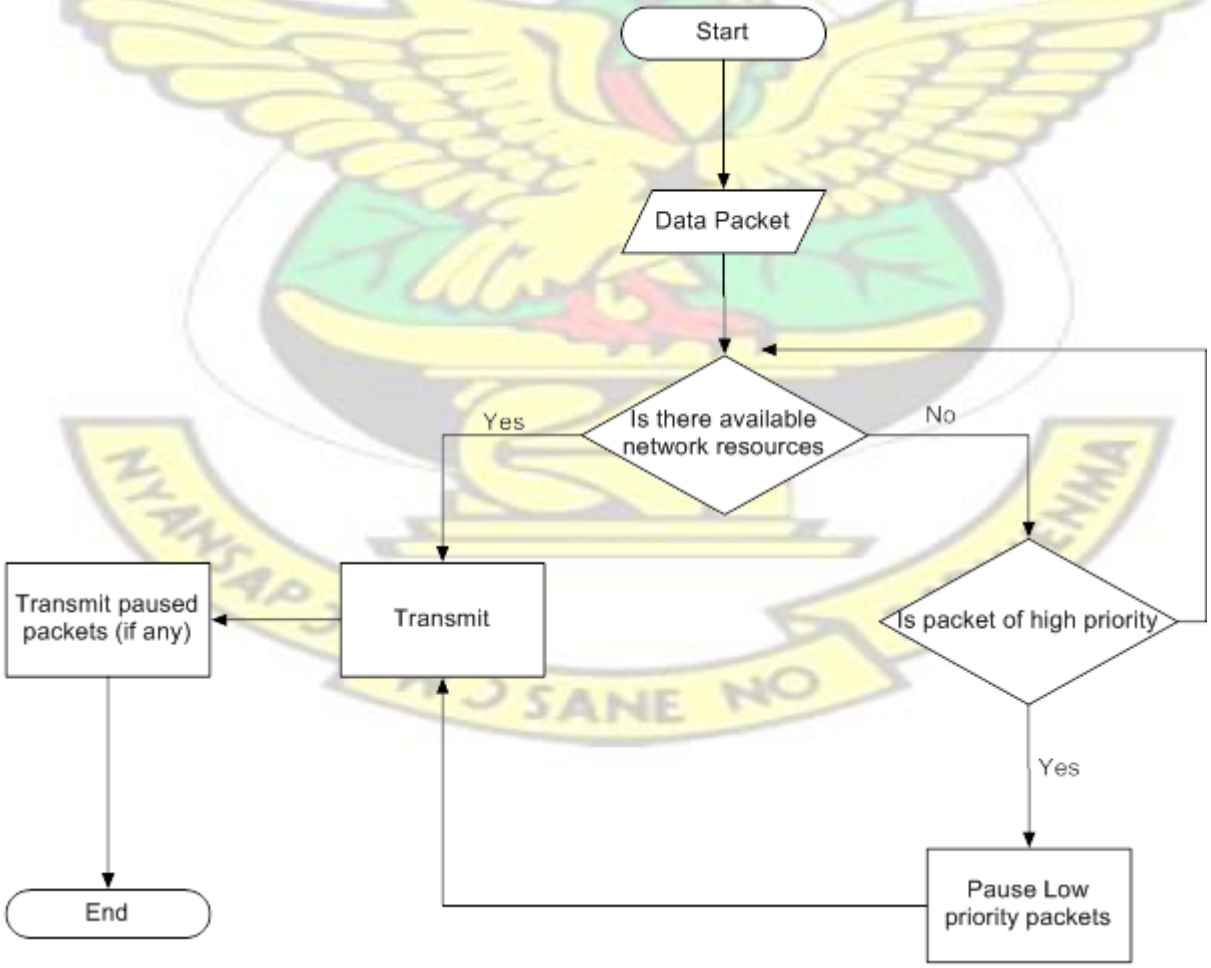


Figure 6.7 Network Resource Allocation Algorithm for Model 2

6.1.3.3 Model 3

This model is targeted for densely populated urban areas where the MS growth rate is high and as such the MS-to-BTS Ratio has either at one point reached its limit or about reaching it. In such areas, MNOs are often found upgrading the existing systems or mounting new BTS in order to ease congestion in the network. As a consequence of these conditions, MNOs cannot afford to give preferential treatment for the use of the public network resources – hence DTCP is not allowed. Smart meters deployed in such areas are likely to experience latencies in their communication with utilities.

To circumvent this problem, a proposition is made that utilities use Mobile Virtual Network Operator (MVNO) business approach. An MVNO is a mobile communication service provider that does not own the enabling communication infrastructure. It leases the infrastructure from an existing MNO or group of MNOs [6.12]. So in this model, the utility assumes the position of an MVNO and signs an agreement with an existing MNO(s) to provide the utility with a dedicated channel or a Mobile Virtual Private Network (MVPN) for its communication with smart meters [6.13]. The utility pays for the leased services at whole rates and makes no investment in the network infrastructure. This approach has been proven to be cost effective and highly scalable [6.14].

The utility could even further reengineer the leased dedicated channel to support higher simultaneous active M2M connections than is currently supported by 2G networks. This can be done by following Germán Corrales et al approach which requires that minor software updates are made to the GSM/GPRS/EDGE protocol stack [6.15] [6.16]. This approach has been tested to support up to 5×10^4 M2M devices transmitting 100 bytes of data every 15 minutes and promises network reliability of 99.99% [6.15]. This gives the utility the advantage

of communicating with more smart meters even with limited bandwidth. Figure 6.8 presents the algorithm used by the BTS in allocating network resources.

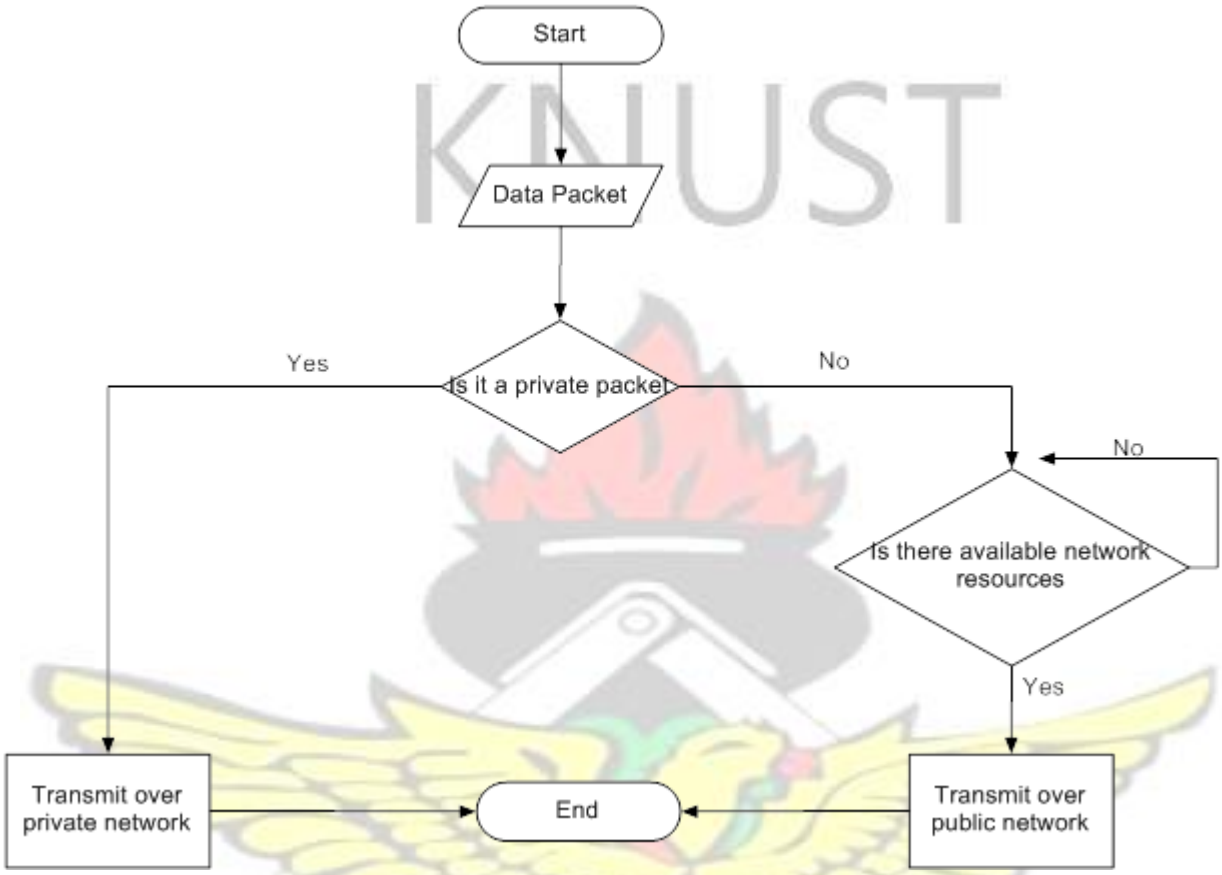


Figure 6.8 Network Resource Allocation Algorithm for Model 3

Table 6.4 summarizes the conditions that should guide utilities in their selection of which of the proposed models to adopt in deploying smart meters.

Table 6.4 Conditions to Guide Choice of Congestion Avoidance Model

Average MS-to-BTS Ratio	DTCP	Model to Adopt
Low	Allowed	Model 1
Low	Not Allowed	Model 1
High	Allowed	Model 2
High	Not Allowed	Model 3

In the next section MDMS models are discussed in an attempt to select an appropriate model for the proposed GSM-based smart metering network architecture.

6.1.4 MDMS Models

Alluding to a Council of European Energy Regulators' (CERR) report on Meter Data Management case studies, there are two main MDMS models; Centralized and Decentralized MDMS models [6.17]. To have a clearer understanding of how these models work, it is important to make plain how the various stakeholders interact. The major stakeholders in the electrical grid are Generating Stations (Suppliers), Distributing Companies (Discos) and Consumers.

In order to select an appropriate MDMS model it is important to understand the common features of the electrical grid found in most African developing countries. The following are key features of such grids

1. Suppliers generate electricity in bulk and transmit it to discos to be distributed to consumers.
2. A single supplier can generate power for several distributing companies and a single distributing company can receive power from several suppliers; thus representing a many-to-many relationship.
3. Discos can distribute power to several consumers, also representing a many-to-many relationship.
4. A single consumer, at any point in time, can receive power from a single disco. This represents a one-to-many relationship.

These relationships are illustrated in Figure 6.9.

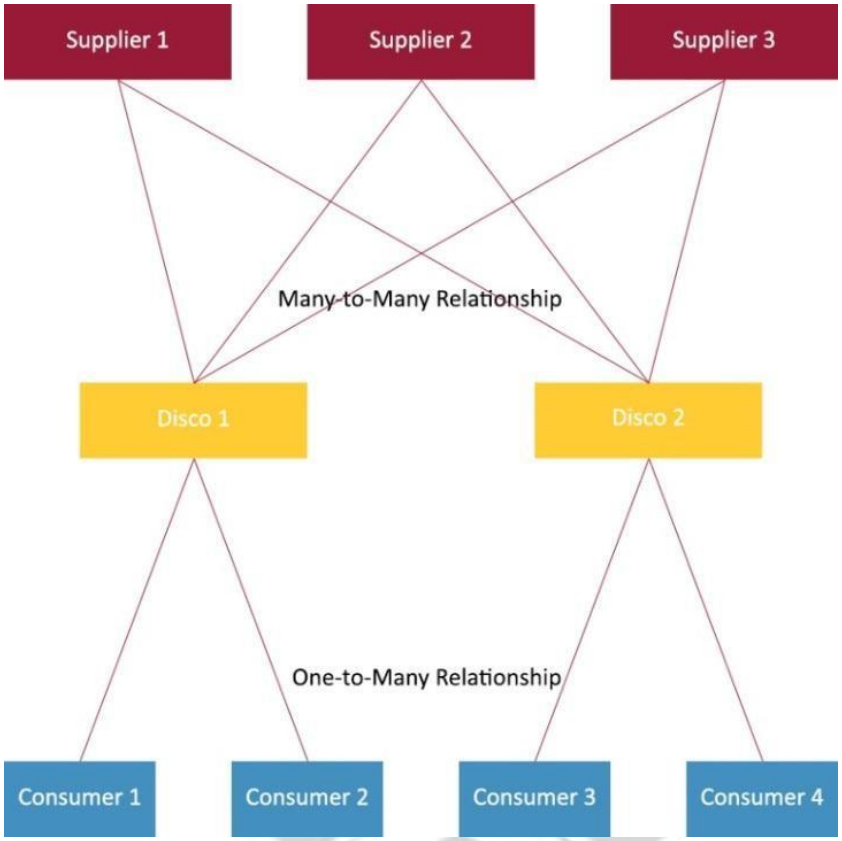


Figure 6.9 Functional Relationship between major stakeholders

It is however worth mentioning that in developed countries, consumers are free to switch among discos; this is not the case in Africa [6.17]. In the following subsections, descriptions are provided for the above mentioned MDMS models.

6.1.4.1 Decentralized MDMS Model

In this model, each disco has its own MDMS serving its entire client base. Consumption data from their respective consumer smart meters are sent to the disco's MDMS. Generating stations that supply power to that particular disco are given access to information generated on the MDMS. Each disco also provides a web portal for their consumers to access their load profiles online [6.17]. The format of presenting information to suppliers and customers may differ from disco to disco. Figure 6.10 illustrates this model.

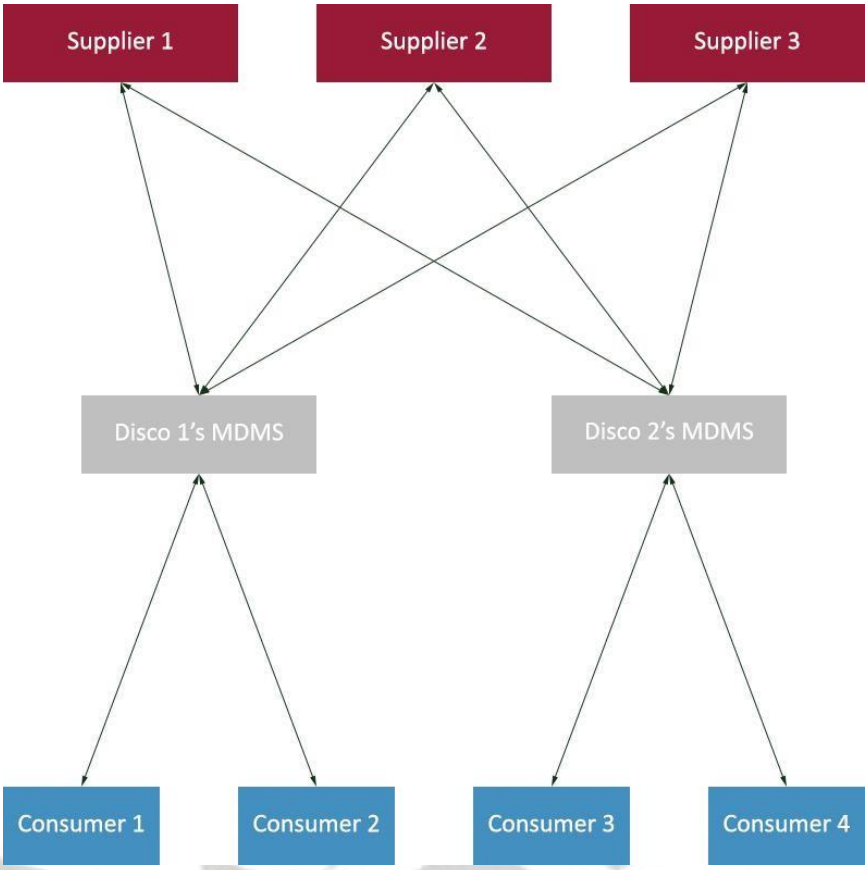


Figure 6.10 Decentralized MDMS Model

The layout of the decentralized model is very similar to the functional relationship that exists between the major stakeholders. Here, each disco has to invest in the setup, maintenance and smooth running of an MDMS. Suppliers serving two or more discos may have to find ways of integrating information they access from each disco. This may be time consuming, especially if they are not presented in the same format. New stakeholders; suppliers or discos, may spend longer time getting into the market since they would have to setup all the necessary systems as well as communication channels between them and the other stakeholders before operating.

This model however assures consumers of some level of privacy; in that their consumption data do not go to stakeholders they are not connected with. This model is currently being used for smart grids in Austria, Belgium and Netherlands [6.17].

6.1.4.2 Centralized MDMS Model

In this model there is a centralized hub for interactions between all stakeholders. All information to and from stakeholders go through one MDMS. This Centralized MDMS, also known as an Integrated Information System (IIS), is usually run by a third party. All interactions between stakeholders and the IIS follow a standardized format [6.17]. For example, consumer smart meters from different discos send their data in a prescribed format to the IIS. They then process this information by critically analyzing it and generating reports for the respective stakeholders also in a standardized format. This implies that generating stations that supply electricity to different discos spend less time integrating information they receive from the MDMS.

Also there is one generalized web portal where consumers under different discos access their consumption information. Discos and suppliers do not make any investments in the hardware or the necessary human resources needed to operate this MDMS. They only pay for the services rendered to them by the third party; thus making this model relatively cheaper to operate. As a result, it is easier for new stakeholders to join the market – highly scalable. The third party is responsible for insulating unrelated stakeholders in order to ensure privacy of data. It is important to note that because of the centrality of the MDMS, the third party provides copious backup and replication cloud based servers which record all transactions that are handled by the MDMS. These logical and physical redundancy measures are implemented purposely to mitigate the possibility of a single point of failure which could interrupt mission-critical services. Figure 6.11 presents an illustration of the centralized
MDMS model.

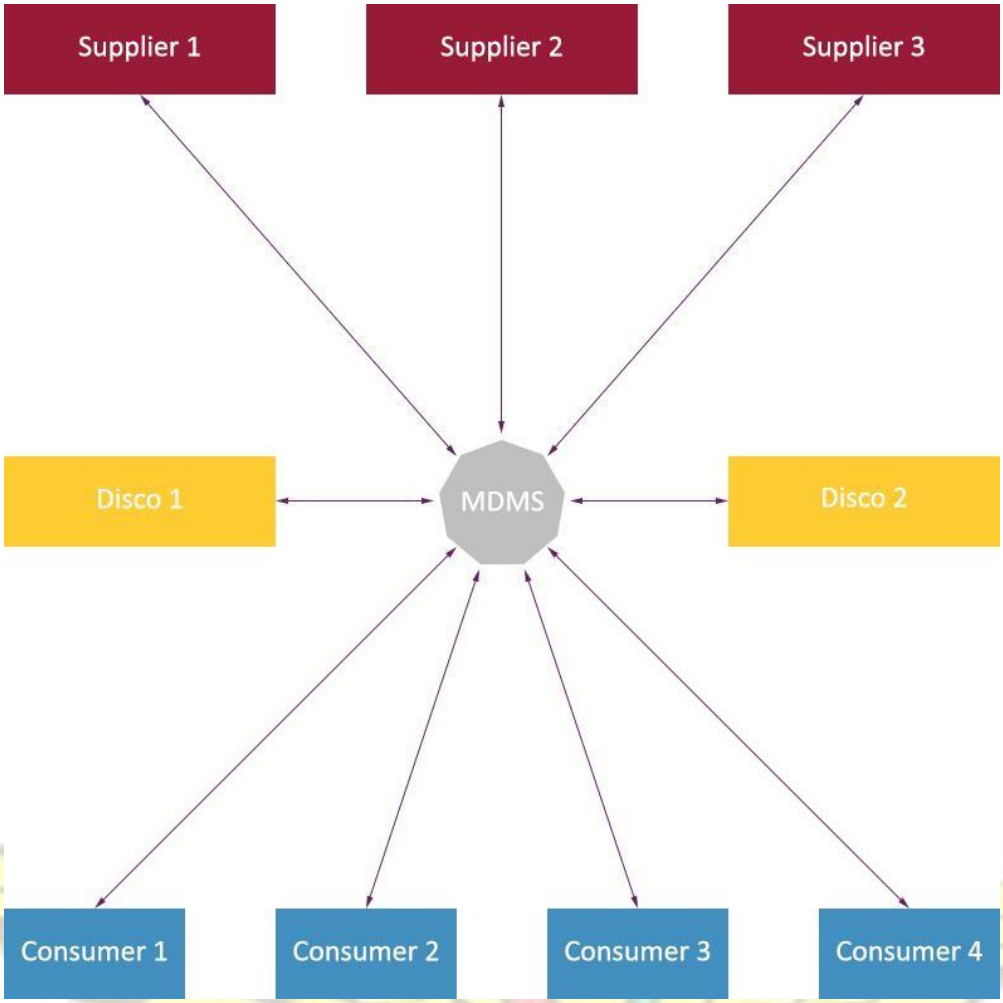


Figure 6.11 Centralized MDMS Model

Based on the simplicity and cost benefits associated with this model as against the Decentralized MDMS model, this model would be adopted for the proposed system for African developing countries. It is currently being used for smart grids in Denmark, Italy and Norway [6.17].

After having defined the architecture of the proposed smart metering communication network, the research proceeds further to provide the systems that would ensure the security of the data being transmitted in this network. These security measures are suggested in the next section.

6.2 SYSTEM SECURITY

6.2.1 Cyber Security

The proposed smart metering system offers a wide range of possibilities to utilities and consumers in their interaction with meters. Utilities can automatically read consumption data, detect meter tamper, disconnect and reconnect meters, update tariffs as well as detect power outages and system faults; all in real-time and from a remote location. Consumers on the other hand can receive outage notifications, energy saving tips, closely monitor their energy consumption over short periods of time as well as set energy thresholds via in-home displays, mobile devices and online portals. All these are possible because of the application of modern computing and two-way communication technologies in the proposed system.

It is however important to note that, all these benefits would be curtailed if proper end-to-end cyber and physical security measures are not implemented. Cyber security measures are necessary in safeguarding information and networking systems while Physical security measures are needed to protect equipment and their domains as well as set policies that would govern human interaction with the system.

A critical assessment of the proposed smart metering system would reveal various sources of threats and vulnerabilities which increase the risk of an attack on the system. The exploitation of these vulnerabilities can lead to catastrophes with irremediable effects. For example, if an attacker is able to hack into a utility's system and authorizes a massive disconnection of all its clients' smart meters over a long period of time, there is the possibility that clients on life supporting equipment may die, businesses may make losses in sales and productivity – thus affecting the nation's GDP and frustrated consumers who would like to reconnect their meters without assistance from the utility may be electrocuted [6.18].

To effectively mitigate risks in the smart metering system it is important to elicit and prioritize the system's assets that need to be protected as well as identify vulnerabilities and threats that may affect these assets. This would bring to light ways of detecting, avoiding and dealing with attacks on the system.

6.2.1.1 The Assets

In the area of cyber security the main assets to be considered are those that border on key data and information that affect system processes and decision making. They are often computed and transmitted via the available communication technology [6.19]. Table 6.5 enumerates assets which have been identified in the proposed smart metering system.

Table 6.5 Assets in the Smart Metering System

No.	Name	Description	Purpose
1.	Consumption Data	A record of how much energy has been consumed.	• For billing • Demand Estimation
2.	Power Quality Measurements	A record of voltage, current, active and reactive power.	• Monitor Power quality • Detect power outages and system faults • Detect meter bypass
3.	Tamper Information	A record of whether or not a meter has been tampered with	Detect energy theft in real-time
4.	Control Information	Instructions sent from utilities to be carried out on the meter	• (Dis)connects meter • Updates Tariff
5.	Notifications	Messages for the user's attention	• Energy conservation tips • Upcoming power outage • Tariffs for DR Programs
6.	Consumer Credentials	Consumer's user name and password for accessing value added services	• Logging in to online dashboard • Initiating consumer requests
7.	Meter ID	A unique 32-bit serial for identifying the smart meter	Required in transmitting meter data
8.	Meter Data Log	Data stored by meter's data logger on SD Card	• Serves as a backup of all meter data • Retransmits undelivered meter data

9.	Customer Requests	Requests sent by customers	• On demand meter data • Set consumption threshold • Request meter (dis)connection
10.	Public/Private Keys	A unique set of related keys required for secured communication	• Authentication • Encryption/Decryption of messages
11.	Firmware Updates	An upgrade of existing system software	• Enhance system capabilities • Fix bugs

6.2.1.2 Prioritization of Assets

In providing protection for the assets in Table 6.5, it is important to know the value of these assets. It would not be prudent to spend a lot more of the available limited resources in protecting an asset which is of very little value to the system. The real value of an asset can be carefully evaluated through Impact Assessment. This evaluation process should be guided by three main objectives set for delivering secure and reliable services in the smart metering system. These objectives are Confidentiality, Integrity and Availability (CIA) [6.20].

Confidentiality ensures that only authorized users can have access to the identified assets. It focuses on providing secrecy of information as well as controlling access to information. Integrity focuses on protecting the information from being altered or destroyed by malicious entities. It is centered on authenticating information as well as binding modifications to their respective owners – nonrepudiation. Availability ensures the timely delivery of informational assets to authorized parties for utilization and decision making.

In the following subsections the above identified assets are evaluated in the light of these explained objectives.

6.2.1.2.1 Consumption Data

In the proposed system, this data is transmitted to utilities at least four times in an hour.

Utilities need this information to be able to effectively plan to meet future demand as well as make efficient distribution of limited power resources. It is an important asset which is highly required for decision making. Without it there is a high tendency of utilities making waste of energy resources. In smart credit meters, utilities use this data to bill consumers. Consumers also need this information in order to properly manage their energy consumption.

From this description, it can be thus judged that prompt and reliable delivery of this data is very essential to the smooth running of the utility. However, where there are a few communication latencies in the order of a few minutes, utilities can sometimes rely on historic data trends to make decisions. Nevertheless, it is important that decisions made by consumers and utilities are based on data that represent the true value of consumption; which is not concocted in any form. Bearing in mind that the granular nature of consumption data makes it possible for almost anyone to know a lot more about consumers, it is important to hide this data from unauthorized parties. As described in Chapter two, criminals, telemarketers and the police would do anything to have such information.

6.2.1.2.2 Power Quality Measurements

This data also informs utilities and consumers about the stability of power. They are capable of inferring for power outages and system failures using these measurements. In critical power systems utilities need to continuously monitor these measurements to make sure power is uninterruptedly supplied. Also in cases of power outages or low voltages, the rapidity of a utility's response in restoring power is dependent on the availability of this data. Also in poor power conditions, consumers safeguard their gadgets by unplugging them from power sources.

The importance of this data necessitates that it is reliable, delivered promptly and without any modifications. However, since a majority of these measurements are often common to all meters in

a particular geographic area and can be easily measured from wall sockets, it is not necessary to hide this data.

6.2.1.2.3 Tamper Information

This information notifies utilities of a possible energy theft tamper on the smart retrofitted meter. To avoid revenue loss, the MDMS/utility would remotely disconnect the meter. After which a utility official is sent to the consumer's premise to carry out further investigations.

Any delay in acting on this information is detrimental to the utility's revenue. Also it is important that this information is correct if not utilities may mistakenly disconnect meters that have not been tampered with. It is also important that this information is kept confidential. With access to this information, unauthorized agents can either warn perpetrators of the utility's detection or pose as utility officials and demand large sums of money for the crime.

6.2.1.2.4 Control Information

These are utility instructions sent to authorize the smart retrofitted meter to carry out a particular action such as disconnecting it from the mains. These instructions should be authorized by only the right parties and carry out the specified action without delay.

6.2.1.2.5 Notifications

These are messages sent by the utility to consumers to sensitize them of upcoming system maintenance, provide them with energy conservation tips and notify them of tariff changes especially in demand response programs. This information is often common knowledge hence not confidential. Nevertheless, it is important that these messages are issued only by authorized utility officials. Also delays in the delivery of messages are tolerable as long as they arrive before the scheduled activity.

6.2.1.2.6 Consumer Credentials

These are a unique set of username and password the consumer uses to access information and make requests from his mobile device and online dashboard. It is important this information is kept securely; whoever has this information has access to the consumer's meter data and is capable of initiating meter requests such as change of billing plan and disconnections. It is however important to note that, consumers can still receive these services via monthly distributed bills and visiting the utility's office.

6.2.1.2.7 Meter Identification (ID) Number

Every meter is provided with a unique 32-bit identification number. This number is often quoted during transactions that involve the meter. These numbers are not confidential hence are often boldly displayed on the meter's casing and monthly energy bills. Having the meter's ID alone is not sufficient to request information from the utility hence is not very critical.

6.2.1.2.8 Meter Data Log

This is a local copy of all recorded meter data. It is stored on an SD card which sits inside the retrofit; making it not easily accessible. During network failures, undelivered messages are stored here and retransmitted when the network has been restored. This contingency storage medium is only accessed when there is the need to critically audit meter data. Notwithstanding, information stored on these media should be only readily available and accessible to authorized officials of the utility.

6.2.1.2.9 Customer Requests

These requests or consumer transactions with the MDMS/utility bear the same attributes of utility control information. They should be authorized by only the rightful users of the meter and specifically carried out without delay.

6.2.1.2.10 Public/Private Keys

These are values that are uniquely linked by a complex mathematical equation. They are required for authenticating, encrypting and decrypting information. Of the pair, public keys may be known to all but private keys should be kept confidential, always available for use by the meter and should be provided by a trusted party.

6.2.1.2.11 Firmware Updates

They are upgrades in software transmitted over the air to reprogram smart meters. They are often done to improve functionality and eliminate any identified bugs. It is important that these upgrades are only made possible by utilities and third parties are incapable of getting access or making sense of the transmitted information. It should be sent in a format only understood by the meter and there should not be any delays in the upgrading process since metering is often halted temporally while upgrades are installed.

Table 6.6 summarizes all the above evaluations of the identified assets.

Table 6.6 Summary of Impact Assessment on Assets

	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
CONSUMPTION DATA	HIGH	HIGH	MEDIUM
POWER QUALITY MEASUREMENTS	LOW	HIGH	HIGH
TAMPER INFORMATION	HIGH	HIGH	HIGH
CONTROL INFORMATION	HIGH	HIGH	HIGH
NOTIFICATIONS	LOW	HIGH	LOW
CONSUMER CREDENTIALS	HIGH	HIGH	LOW
METER ID	LOW	MEDIUM	LOW
METER DATA LOG	HIGH	HIGH	HIGH
CUSTOMER REQUEST	HIGH	HIGH	HIGH
PUBLIC/PRIVATE KEYS	HIGH	HIGH	HIGH
FIRMWARE UPDATES	HIGH	HIGH	HIGH

6.2.1.3 Threats and Vulnerabilities

In the light of cyber security, the main threats to smart metering systems and smart grids are targeted towards the communication network. This is because all the above mentioned assets are transmitted via GSM/GPRS/EDGE; which in the proposed system is a shared communication network – not owned by the utility. Considering the centrality of this role

played by the network it is important to identify all possible threats that may affect its performance.

A review of the security provisions of this 2G network revealed that it offers the following [6.21]:

1. **Temporal Anonymous Identity of Communicating Subscribers**: It hides the identity of a communicating mobile subscriber (MS) by providing it with a Temporal Mobile Subscriber Identity (TMSI).
2. **Authentication**: Using an A3 Authentication Algorithm, the BTS authenticates all MSs before responding to their service request. This is done primarily to make sure services are only granted to recognized mobile subscribers.
3. **Confidentiality:** Using an A5 Encryption Algorithm, all messages communicated to/from the MS are encrypted.

Despite the provision of these security measures, 2G communication networks have been associated with the following key vulnerabilities [6.22]:

1. Encryption is only limited to communication between the BTS and MS. All other communication lines between the BTS and the other nodes, such as the Visitor Location Register (VLR) and the Home Location Register (HLR), are not encrypted.
2. The A3 and A5 encryption and authentication algorithms used have been broken using methods such as brute force attack.

The existence of these vulnerabilities suggests that there is a high possibility of attackers compromising all the identified assets [6.22]. There is the need to provide measures for detecting, avoiding and handling these attacks in the communication network. To effectively do so a critical assessment was carried out to identify threats and attacks that could affect the three cyber security objectives.

Attacks that are targeted at the confidentiality of assets seek to lay hold of unauthorized information and fraudulently make use of them. Informational assets such as user credentials when accessed by criminals may have serious implications. Armed with this criminals can get into their online account and send unauthorized requests to their smart meter. In cases where consumers make payments of bills online using their credit/debit cards, criminals may be able to access their billing information. In short, these attacks intrude the privacy of the consumer.

Attacks on the integrity of informational assets aim at accessing and meddling with transmitted information. Control information that are sent from the utility to update a tariff, maybe concocted in such a way that the consumer pays less or nothing at all. Also false consumption data which are transmitted to utilities may lead them to make wrong decisions.

Attacks directed at the availability of informational assets have the objective of preventing or delaying them from reaching their destinations. They are often targeted at key nodes required to offer services in the communication network. These nodes are either completely shut down or kept extremely busy for long periods of time, preventing them from offering services to other nodes. In cases where assets such as power quality measurements are delayed or not transmitted utilities are incapable of knowing and responding quickly to system faults and power outages.

The above mentioned attacks and threats have been summarized in Table 6.7.

Table 6.7 Threats to the Communication Network

Affected Objective	Name of Threat/Attack	Description

Confidentiality	Eavesdroppers	They listen to real-time private communication in the smart metering system with the aim of stealing information.
	Traffic Analyzers	They intercept and analyze communication patterns to deduce information.
Integrity	Man-In-The-Middle (Active Eavesdropper)	Sits in the middle of two communicating entities, relays and possibly alters transmitted messages. This is successfully carried out by impersonating/spoofing the identities of the communicating nodes.
Availability	Denial of Service (DoS)	Deprives communicating nodes of access to the network's services and resources. They may either jam the signal or congest the network by flooding it with messages; thus delaying/preventing data messages from reaching their intended destination.

6.2.1.4 Countermeasures for Handling Threats

Judging from the extremely harmful effects of the above mentioned threats, it is necessary to provide counter measures that would prevent, detect and properly mitigate them. All these attacks are centered on the communication medium and as such it is a prerequisite to provide end-to-end security for every communicating node; ranging from physical protective covering, access control protocols and data security. However, it is important to note that a majority of the communication architecture is not owned by the utility; as such, it would be difficult and expensive, if not impossible, to provide all these security measures. For example, the utility cannot employ copious human resources for manning every BTS or even scrutinize the actions of all employees of the MNO. The utility only has a chance at guarding what it owns and controls; informational assets, its employees, smart meters, the MDMS, CIS and other logistics.

Nevertheless, these measures should be so effective that there is literally nothing or very little an attacker can do when targeting unguarded equipment/nodes which are not owned by the utility.

After carefully analyzing the attacks on confidentiality and integrity; which focus on unauthorized access and meddling with informational assets, it is quite obvious that these attacks would be ineffective if data messages are strongly encrypted, uniquely identified by providing them with non-repeating numbers (nonce), employing effective key management schemes and authenticating communicating parties. All these measures fall under the umbrella of Cryptography [6.23]. These cryptographic measures would be studied in detail in the next section in an attempt to suggest an effective way of dealing with these attacks in the proposed system.

It is however worth mentioning that these crypto measures are not capable of handling attacks which affect network performance – DoS attacks. These attacks on availability cannot be curtailed or their effects lessened by the application of these measures. They require passive detection schemes which monitor network traffic and alert utilities of potential DoS attacks. Since utilities know the network traffic metrics over specific periods, anytime these values dwindle there is the possibility that a DoS attack is in progress hence data messages should be safely rerouted. They can then trace the source of this attack and deal with it.

6.2.1.5 Crypto Schemes for Handling Attacks

These are mathematical based schemes used for securing the transmission of data over public channels. They encode the transmitted data into ciphers which can only be understood by parties which have the right keys to decipher them. They are placed into two broad categories; unconditionally and conditionally secure schemes [6.24]. The former can withstand all forms of attack since they can never be broken even if attackers have unlimited computational power.

They are however not practical in most applications since key sizes must be equivalent to message sizes. A typical example of such a scheme is one-time pad scheme.

Conditionally secure schemes on the other hand are based on the assumption of computational hardness. They are computationally infeasible to be broken. However in theory, these schemes can be broken with unlimited computational resources. These schemes are subcategorized into Symmetric and Asymmetric (Public) Key Cryptography [6.25].

In Symmetric Key Cryptographic (SKC) systems such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), one key is shared by all communicating parties. These schemes are fast in encrypting and decrypting messages. However, they suffer the difficulty of managing and distributing shared keys. There are challenges in the manner in which shared keys should be securely agreed upon as well as how to securely distribute the shared key [6.26]. Also in case the shared key is compromised all parties would be affected. In this system it is often hard to trace the source of compromise – repudiation. Nevertheless, they can be carefully combined with Asymmetric schemes to deal with these challenges.

In Asymmetric schemes such as RSA, Diffie-Hellman (DH), Digital Signature Algorithm (DSA), Cramer-Shoup Cryptosystem and ElGamal Encryption, two different but mathematically related keys are used – a public and private key. The public key may be freely distributed while the private key is kept secret. Though the keys are related mathematically, it is computationally infeasible to generate the private key from the public key. Unlike SKC systems, they do not suffer the difficulty of distributing and managing keys.

They are also good for implementing non-repudiation in security systems. However, they often require large key sizes in order to attain a high degree of computational hardness. This requires that systems using these schemes have large storage capacities, high computational power and high bandwidths to transmit encrypted data [6.26].

Considering the large number of communicating nodes in the proposed smart metering system, it is not practical to have a SKC system as the main means of exchanging secret keys or authenticating anonymous nodes. Also all the above mentioned Asymmetric schemes require high computational, storage and transmission requirements; such as are not found in smart metering systems. Bearing in mind that the proposed smart retrofitted meter has only 16MHz of processing power and 12 kilobytes of storage, it is important to select a public key cryptographic (PKC) system which offers smaller key sizes thus requiring lesser requirements as compared to the aforementioned systems.

After relative comparisons were conducted among all the available options, Elliptic Curve Cryptography (ECC) was selected. It is based on the difficulty of solving discrete logarithm equations. Among all PKC systems, it offers the same level of security while using smaller key sizes. This makes it an ideal choice in this application area of limited computational and transmission resources.

Table 6.8 presents a comparison between ECC and RSA key sizes.

Table 6.8 Comparison between ECC and RSA Key Sizes [6.26]

ECC Key Size (bits)	RSA Key Size (bits)	Key Size Ratio
163	1,024	1:6
256	3,072	1:12
384	7,680	1:20
512	15,360	1:30

From Table 6.8, it is obvious that ECC offers smaller key sizes than RSA to a very high degree, while offering the same level of security. The remaining section briefly introduces ECC and brings to light its computational hardness.

Elliptic curves are based on a generalized Weierstrass's equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad 6.1$$

$$(y + \frac{a_1x}{2} + \frac{a_3}{2})^2 = x^3 + (a_2 + \frac{{a_1}^2}{4})x^2 + a_4x + (\frac{{a_3}^2}{4} + a_6)$$

Assuming the characteristic of the field is not 2

$$Y^2 = x^3 + A'_2x^2 + A'_4x + A'_6 \quad 6.2$$

Assuming the characteristic of the field is not 3

$$Y^2 = x^3 + Ax + B \quad 6.3$$

∴ Elliptic Curve over a field L can be expressed as

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L | y^2 + \cdots = x^3 + \cdots\}$$

From equation 6.3 the elliptic curves in Figure 6.12 can be plotted within the region $[-3, 3]^2$

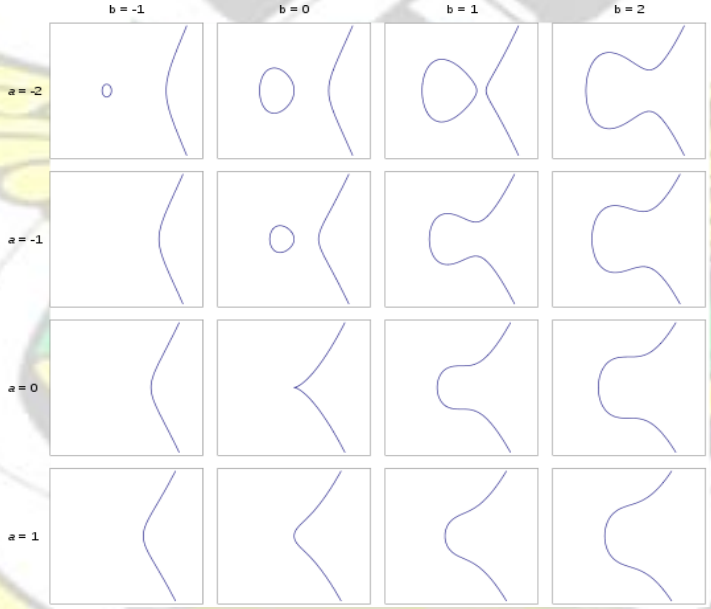


Figure 6.12 Sample Elliptic curves of the equation $y^2 = x^3 + ax + b$

The real number field is an infinite field; so drawing elliptic curves over them can span over a wide area. So for cryptographic implementations finite fields such as Prime fields (Fp) and Binary fields (F_2m) are used. In these fields, if $x^3 + ax + b$ contains no repeated factors, or

equivalently if $4a^3 + 27b^2$ is not **0**, then the elliptic curve of equation 5.3 can be used to form an Abelian group.

All Elliptic Curve groups are additive groups because the basic operation on the points of the curve is addition. Assuming **P, Q** and **R** are points on an elliptic curve and **O** is the point at infinity (identity element) in the field of real numbers, the addition laws of Elliptic Curves ***E*** work as follows:

- Identity : **P + O = O + P = P** $\forall P \in E$
- Inverse : **P + (-P) = O** $\forall P \in E$
- Associative : **P + (R + Q) = (P + R) + Q** $\forall P,Q,R \in E$
- Commutative : **P + Q = Q + P** $\forall P,Q \in E$

The addition law then makes all points of the curve ***E*** an Abelian group. Point addition and point doubling (adding the same point twice) are the main operations carried out on this Abelian group. Unlike RSA which requires complex operations such as factorization of large integers, these ECC operations are simple operations that can be carried out easily by smart metering systems.

In performing addition of two non-equivalent points **P** and **Q**; with **P** having affine coordinates (x_P, y_P) and **Q** having coordinates (x_Q, y_Q), the sum point **R** (x_R, y_R) is obtained by computing the following:

$$x_R = \lambda^2 - x_P - x_Q$$
$$y_R = \lambda(x_P - x_R) - y_P, \qquad 6.4$$

$$where\ \lambda = \frac{dy}{dx} = \frac{y_Q - y_P}{x_Q - x_P}$$

Point doubling is used when the same point is added. So for a point P with coordinates

(x_P, y_P) is doubled as **R = P + P = 2P** using the following formulae:

$$x_R = \lambda^2 - 2x_P$$

$$y_R = \lambda(x_P - x_R) - y_P, \qquad 6.5$$

$$where\ \lambda = \frac{3x_p^2 + a}{2y_p}$$

Geometric approaches of carrying out these basic operations are illustrated in Figure 6.13.

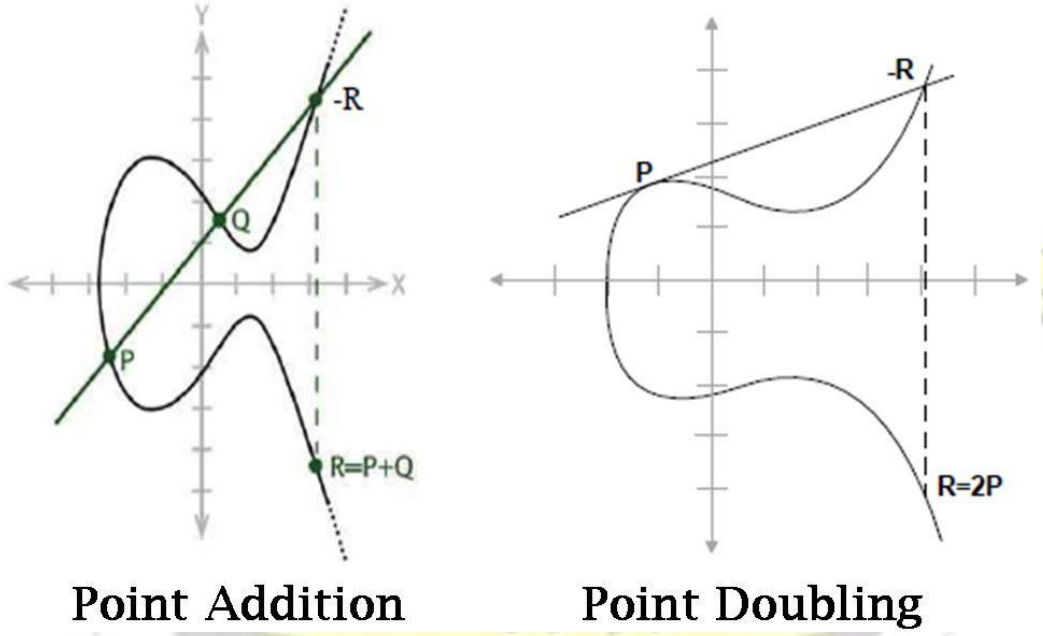


Figure 6.13 Geometric approaches to Point Addition and Doubling on Elliptic Curves

The ease of carrying out these operations, the use of small key sizes and its high computational hardness are part of the reasons why in 2005 United States of America's National Security Agency (NSA) included ECC in their Suite B Cryptography – a collection of cryptographic algorithms which are deemed fit for securing highly classified information [6.27]. This to a large extent guarantees that its application in the proposed system would effectively secure informational assets.

Based on its strengths, elliptic curves have been adopted in several communication protocols.

Some of which are Elliptic Curve Augmented Encryption Scheme (ECAES), Elliptic Curve Diffie-Hellman (ECDH) Key Agreement Protocol and Elliptic Curve Digital Signature Algorithm (ECDSA) [6.28]. In this research a proposition is made for the adoption of ECDH for anonymous key exchange and ECDSA for signing and verifying digital signatures. These protocols are explained in the following subsections.

6.2.1.5.1 ECDSA

This communication protocol is based on the earlier mentioned PKC scheme, Digital Signature Algorithm (DSA). It is mainly used for authentication purposes. When two parties want to initialize communication, they first want to verify if they are talking with the right party; to eliminate the possibility of a Man-In-The-Middle (MITM) attack.

For the purposes of demonstration, two parties – Ama and Badu, are used. In case Ama wants to initiate communication with Badu, she sends a message bearing her digital signature. This is to tell Badu, she is who she says she is. Badu receives and verifies this signature based on some already known parameters. In cases where mutual authentication is to be established before communication begins, Badu would also have to send his signature for Ama to verify. These processes are explained below.

Signing Process

1. An elliptic curve based on a Weierstrass' basic equation $y^2 = x^3 + ax + b$, having a base point G of a large prime multiplicative order n is first agreed upon by the two parties by some other secured means.

2. A key pair is generated, comprising a randomly selected private key d_A – found within the region of the selected curve, and a public key Q_A derived from the computation $Q_A = d_A \times G$ (scalar multiplication of base point and private key).
3. Based on an agreed upon Secured Hash Algorithm (SHA) like SHA-1 or SHA-2, the message m to be signed is hashed as $H(m)$.
4. The leftmost bit of $H(m)$ is stored as z
5. A randomly generated integer k which falls in the region of the curve is selected; less than n.
6. A curve point (x_1,y_1) is calculated by a scalar multiplication of k and G (i.e. $k \times G$)
7. Calculate and transmit the signature point (r,s) by computing $r = x_1 \bmod n$ and $s = k^{-1}(z + d_A) \bmod n$, where $r \neq 0$ and $s \neq 0$. [6.29]

After Badu receives the signed message, he verifies Ama's identity by going through the following process.

Verification Process

1. Based on the knowledge of the sender's public key Q_A and other curve parameters, the signature point (r,s) is first checked if it lies within the region of the curve.
2. Using the same hash function, the message m is hashed as $H(m)$
3. The leftmost bit of $H(m)$ is stored as z
4. Calculate $v = s^{-1} \bmod n$
5. Calculate $u_1 = zv \bmod n$ and $u_2 = rv \bmod n$

6. A curve point (x_1,y_1) is calculated as $(x_1,y_1) = u_1 \times G + u_2 \times Q_A$

7. The signature is correct if $r \equiv x_1 \bmod n$.

Obtaining a correct signature authenticates the identity of the communicating node [6.29].

6.2.1.5.2 ECDH

After Ama and Badu have been authenticated using ECDSA, communication can be initiated. Since the communication network is still an insecure public channel it is important that messages are encrypted before they are transmitted. This is to ensure that it remains confidential and meaningless to eavesdroppers. Encryption can be carried out using the PKC system. So a message from Ama to Badu is encrypted using Badu's known public key. When Badu receives the cipher, he decrypts it using his private key. No one else can decrypt this cipher without knowing Badu's private key.

Despite the effective key management advantage PKC systems have over SKC systems, they tend to require more processing time; hence are slower than the latter. To leverage the advantages of both systems; the speed of SKC and the effective key management of PKC systems, ECDH is recommended for the proposed smart metering system. In ECDH, a PKC system based on ECC is used in the initial communication between the two authenticated parties. In this they agree on a shared key which would be used thereafter for SKC encryption and decryption of messages [6.30].

The following steps explain how this is done when Ama and Badu employ ECDH in their communication over the insecure channel:

1. After the two parties have been authenticated. They agree; by some other secure means, on a particular elliptic curve equation having a base point G of a large prime multiplicative order n.
2. Each party generates a key pair, comprising a randomly selected private key d – found within the region of the selected curve, and a public key Q derived from the computation $Q = d \times G$ (scalar multiplication of base point and private key). So Ama's pair would be (d_A, Q_A) and Badu's pair would be (d_B, Q_B).
3. With each party knowing the other's public key, Ama computes $(x_k, y_k) = d_A \times Q_B$ and Badu computes $(x_k, y_k) = d_B \times Q_A$, which is the scalar multiplication of their private key and the public key of the other party. Both computations would result in the same curve point (x_k, y_k) because $d_A \times Q_B = d_A \times d_B \times G \equiv d_B \times Q_A = d_B \times d_A \times G$. So both result in the same point (x_k, y_k) .
4. x_k is then used as the shared key for SKC encryption and decryption [6.30].

6.2.2 Secured Communication Scheme For Proposed System

After having unearthed the vulnerabilities and sources of threats in the GSM/GPRS/EDGE communication network a secured communication scheme is proposed for the developed smart metering system. This scheme leverages on the strengths of ECDH, ECDSA, SHA-2 and AES. These cryptographic algorithms are all found in NSA's Suite B Cryptography and are highly recommended for securing highly classified information [6.27]. It is worth mentioning that AES is more secure and faster to compute than all other SKC systems. Also
SHA-2 offers a higher level of security than SHA-1.

The scheme heavily employs the use of a Certificate Authority (CA) which is a trusted third party. This party is responsible for certifying public keys of all communicating devices in the smart metering system. To ensure that the receiving party owns and is recognized by the public key it holds, the sender checks first with the CA. The CA has a secured database containing the public keys of all registered smart meters, MDMS, CIS and utilities.

To demonstrate how the proposed scheme works the following use cases are considered:

1. Initializing and registering a newly installed smart retrofit
2. Transmitting data messages from the smart retrofit to the MDMS
3. Transmitting data messages from the MDMS to the smart retrofit

6.2.2.1 Initializing & Registering a Newly Installed Smart Retrofit

During the manufacture of the smart retrofit, the manufacturer includes an Atmel ATECC508A chip to the Arduino Microcontroller. This is a low powered chip which is dedicated for all crypto processes – authentication, encryption and decryption. Its unit price is less than 1 USD hence adds no significant cost to the cost of the retrofit [6.31]. It has support for all the above mentioned cryptographic algorithms. Figure 6.14 shows an Atmel ATECC508A chip plugged into an Arduino Microcontroller.

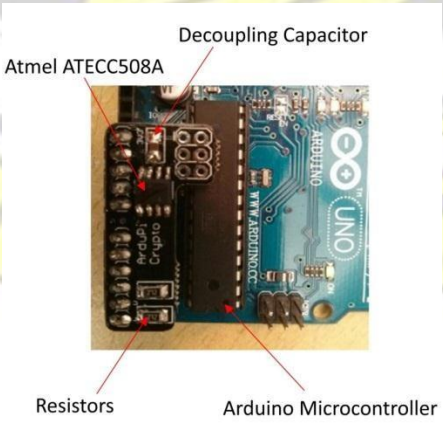


Figure 6.14 Atmel ATECC508A Chip on an Arduino Microcontroller [6.32]

A trusted manufacturer or utility official configures these chips before plugging them into the meters. These chips automatically generate a random ECC private key which would never be known; even by the one who configures it. They can only retrieve its associated public key. This public key is made known to a trusted CA. The chips are also configured to know the public key of this CA. This is all that is needed to configure these chips.

It is important to mention that these chips are all based on a particular Weierstrass' elliptic curve equation having a base point $\boldsymbol{G}$ of a large prime multiplicative order $\boldsymbol{n}$. They also use the same SHA256 digest generation function. So there is no need for preliminary agreements via other secured channels before initiating communication.

After the meter is installed and turned on, its first communication is with the CA. After mutual authentication between the CA and the meter using ECDSA, by using ECDH the CA sends it the public key of the MDMS as well as a shared key for decrypting multicast messages. Multicast messages would often be sent from the MDMS to all meters. Typical multicast messages include outage notifications, energy saving tips and tariffs for DR programs. Details of how these are done are provided in the Figures 6.15 and 6.16.

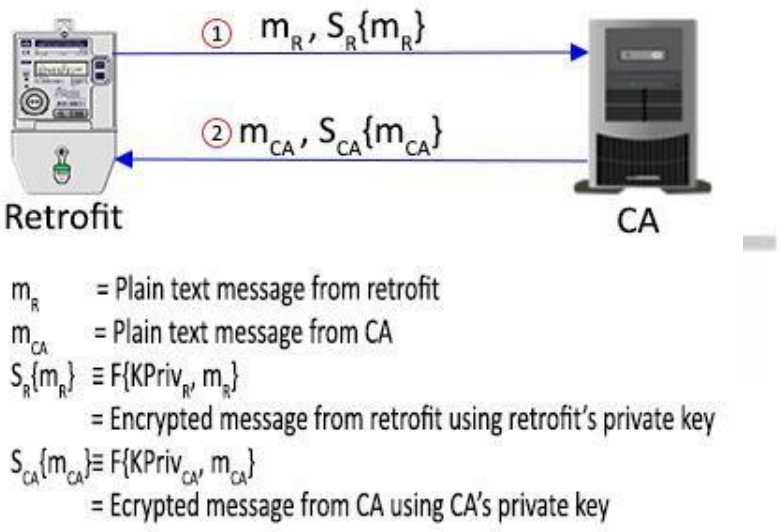


Figure 6.15 Authentication Process between Smart Retrofit and CA

The authentication process in Figure 5.4 goes through the following steps:

1. The smart retrofit sends a plaintext message together with an encryption of the plaintext to the CA. This encryption is done using the retrofit's auto-generated private key which is not known to any other communicating party. The plaintext message in this process would be the meter's 32-bit ID number.
2. After receiving the message, the CA looks through its database for the corresponding public key of the meter with that ID. It then uses its public key to decrypt the message such as shown below.

$$\text{Verification} = V_R\{S_R\{m_R\}\}$$

$$= F'\{KPub_R, F\{KPriv_R, m_R\}\}$$

$$= m_R$$

If after decrypting the cipher it gets the same message as in the plaintext then the identity of the retrofit is authenticated. It records the meter's serial as an active meter in its database and notifies the corresponding MDMS and utility of the activation of the new meter. For the purposes of mutual authentication the CA also sends the retrofit its digital signature which comprises a plaintext message and an encryption of the

plaintext. The encryption is done using the CA's private key. The plaintext would be the 32-bit serial of the CA.

The retrofit goes through the same steps in authenticating the identity of the CA. After authentication, the smart retrofit requests the public key of the MDMS. This process is demonstrated in Figure 5.5.

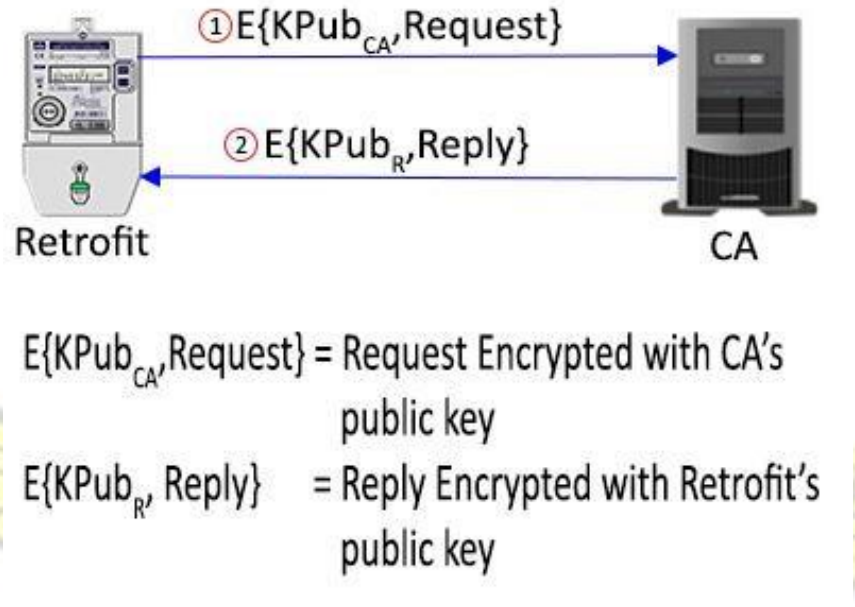


Figure 6.16 Retrofit making a request for MDMS' public key

The following steps explain how the smart retrofit obtains the public key of the MDMS from the CA.

1. The smart retrofit encrypts its request using the public key of the CA. The encrypted message is then transmitted to the CA.
2. Upon receipt of the encrypted message, the CA decrypts it using its private key. After decrypting the message, it fetches the corresponding public key of the meter with the sent ID. It uses this public key to encrypt the requested MDMS' public key and transmits it to the smart retrofit.

3. The smart retrofit decrypts the reply with its private key and stores the MDMS' public key for future communication.

After going through all the above described processes, the newly installed smart retrofit has been successfully initialized. It is now capable of offering smart metering functionality to the existing standalone meter.

6.2.2.2 Transmitting Data from the Smart Retrofit to the MDMS

As stated earlier, the CA has notified the MDMS of the addition and activation of the new smart retrofit. The MDMS and retrofit have each other's ID and public key. Whenever the retrofit has to transmit recorded data to the MDMS, it first checks if the last session it had with MDMS has not expired. If it has, it initiates the process of mutual authentication. After they have both been authenticated, the retrofit transmits an encrypted message which comprises a shared key and the recorded data. The shared key is encrypted using the MDMS' public key while the data is encrypted using the shared key. After the MDMS has successfully received and decrypted the transmitted data it sends an acknowledgement. These steps are depicted in Figure 6.17.

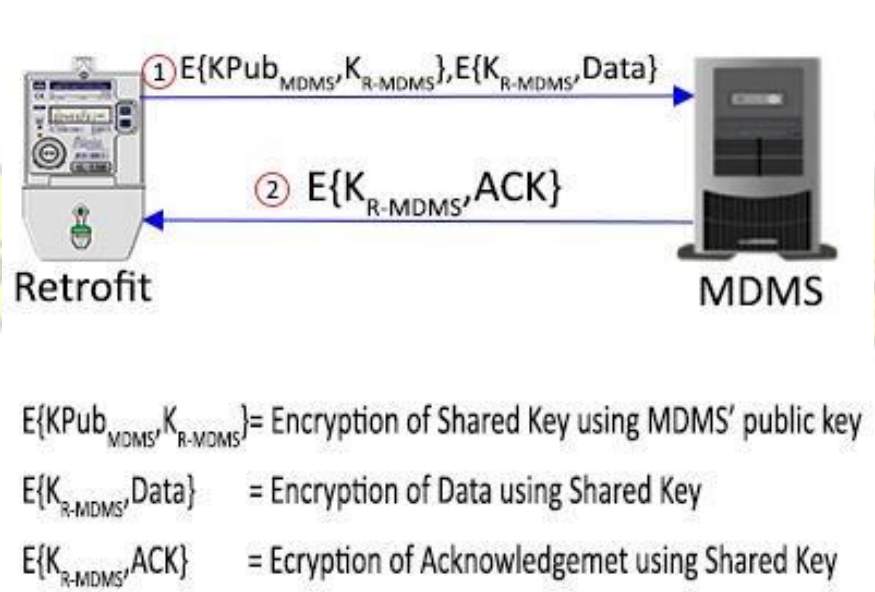


Figure 6.17 Transmission of data from smart retrofit to MDMS

As explained earlier in EDCH, the shared key is used because it is faster to compute – encrypt and decrypt. The specific cryptographic algorithm used with this shared key is AES128.

6.2.2.3 Transmitting Data from the MDMS to the Smart Retrofit

When transmitting data messages, such as control information, from the MDMS to the smart retrofit, the MDMS goes through the following processes.

1. Initiates mutual authentication with the retrofit; that is if the last communication session has expired.
2. Transmits an encrypted message which comprises a shared key and the message (control information). The shared key is encrypted using the public key of the retrofit while the message is encrypted using the shared key.

After the retrofit receives the message and successfully decrypts it, it sends an acknowledgement. These steps are depicted in Figure 6.18.

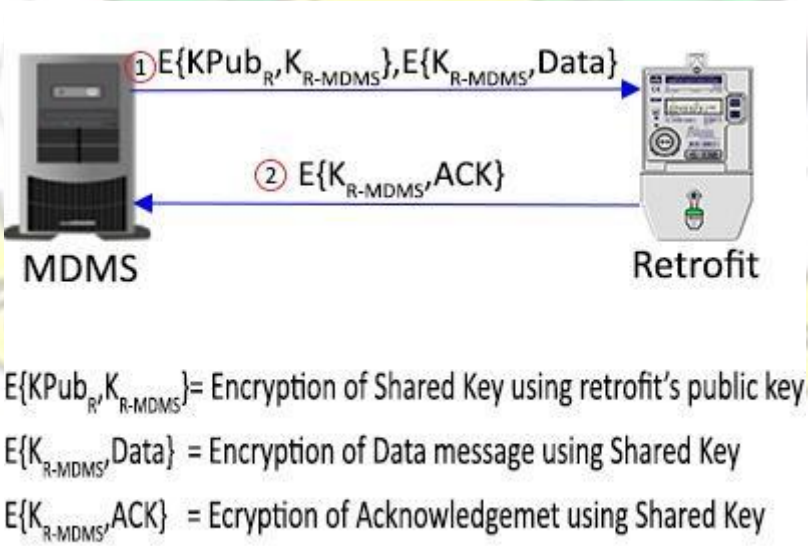


Figure 6.18 Transmission of unicast data messages from MDMS to Retrofit

Unlike control information that is unicast in nature, consumer notifications have to be multicast to a large group of smart retrofits. So in multicast messages the earlier mentioned multicast shared key, which is provided by the CA during initialization, is used for encryption and decryption. This is depicted in Figure 6.19.

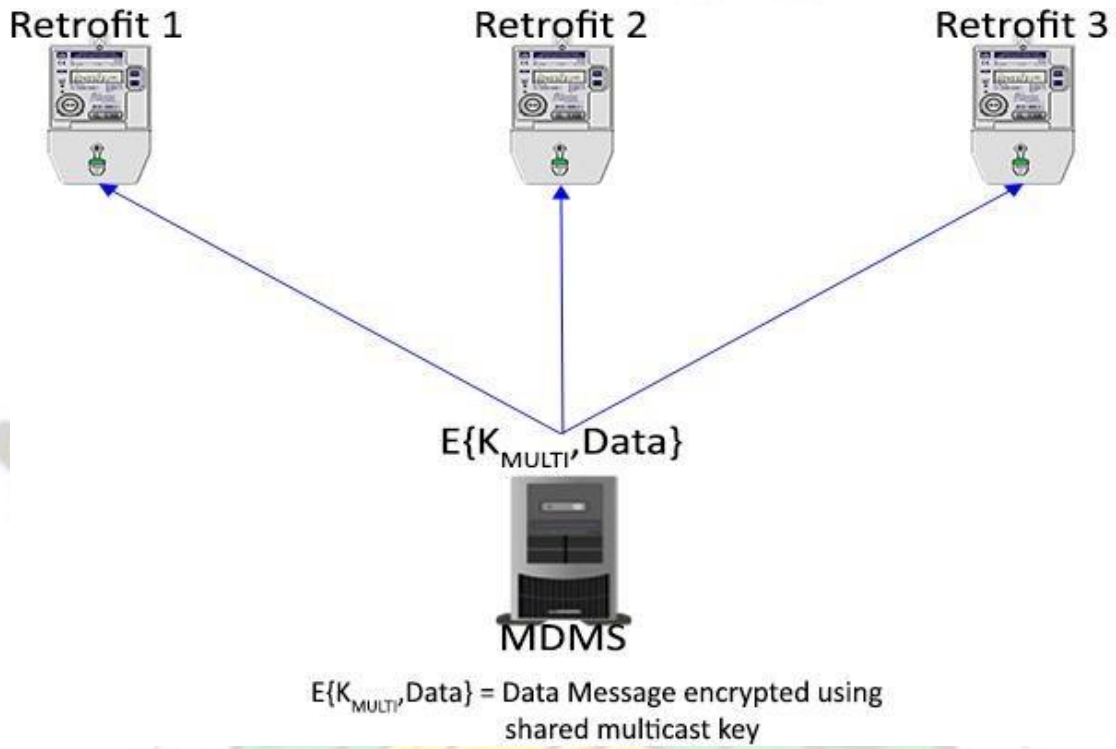


Figure 6.19 Transmission of an encrypted multicast message

It is however important to note that, in the proposed scheme, the shared multicast key is only limited to disseminating consumer notifications. For security reasons, it cannot be used for other functions such as transmitting control information/instructions. The consequences of doing otherwise may result in introducing the risk of controlling all meters with one command. If ever the shared key is compromised, there is a tendency of attackers using this key to disconnect all meters or reconnect meters of defaulting customers.

6.2.2.4 Proposed Datagram Format

A datagram format with a fixed length of 1,024 bytes (1 kB) is proposed for the transmission of data messages in the proposed smart metering system. It comprises an 8 byte base header and a 1,016 byte data area (payload). The fixed length allows for faster computation. It also makes it hard for eavesdroppers and traffic analyzers to make sense of any transmitted data, because they are all very similar. Figure 6.20 shows the proposed format and Table 6.9 shows the bit size and purpose for each field.

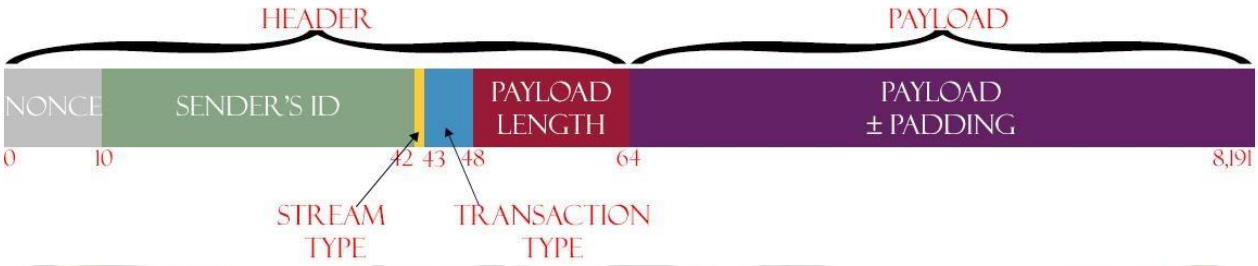


Figure 6.20 Proposed Datagram Format

Table 6.9 Bit size and function of fields in the proposed Datagram format

Field	Size (Bits)	Purpose
Nonce	10	Non-repeating numbers used to numerate transmitted messages. Helps detect replay attacks and lost messages.
Sender's ID	32	A unique ID of the communicating node.
Stream Type	1	Denotes whether message stream is unicast or multicast.
Transaction Type	5	Indicates the type of transaction or message sent.
Payload length	16	Shows the size of the transmitted message.
Payload	8,128	Transmitted data message. Padded with zeros/ones if not full.

With the exception of the nonce, sender's ID and stream type fields, all other fields in the datagram are encrypted using the above discussed encryption protocols. Mutual authentication transactions happen when two parties are communicating for the first time or each time a session expires. For these transactions a special 10-bit nonce zero – ―0000000000‖, is used. This nonce together with the sender's ID and stream type are submitted as plaintext to the receiving party. The receiving party uses the sender's known public key to decrypt the rest of the datagram. If the decrypted payload is equivalent to the plaintext, the sender is authenticated.

The 10-bit nonce, which can numerate as much as 1,024 transactions, can never be exhausted in any session for any two communicating parties. Conservatively, there are 96 transactions between the meter and the MDMS every day; 4 times every hour. Sessions in the proposed system, by default, expire at midnight. This number of transactions is 10 times less than the total number of transactions that can be covered by the nonce.

The sender's ID number is a 32-bit unique serial provided for every communicating party. Just like Internet Protocol Version 4 (IPv4), it is capable of addressing more than 4 billion (2^{32}) connected devices. This is very copious, considering the fact that IPv4 works on a global scale while this is targeted for a particular geographic area – say a country.

The stream type field uses 1 bit to tell if the stream is multicast or unicast. It uses a ―0‖ for multicast messages and a ―1‖ for unicast messages. Whenever the stream is indicated as multicast, the receiving party uses the shared multicast key, provided by the CA, to decrypt the encrypted message.

The transaction type field can specify up to 32 (2^5) different transactions. Table 6.10 lists 14 of the transaction codes used in the proposed system with room for 18 more transaction codes.

Table 6.10 Transaction codes used in proposed system

Transaction Code	Purpose
00000	Mutual Authentication
00001	Acknowledgement
00010	MDMS Public Key Request
00011	Retrofit Public Key Request
00100	Consumption Data Request
00101	Consumption Data Reply
00110	Power Quality Measurement Request
00111	Power Quality Measurement Reply
01000	Tamper Info Request
01001	Tamper Info Reply
01010	Control Information/Instruction
01011	Consumer Notification
01100	Customer Request
01101	Firmware Update

The payload length is a 16-bit value that shows the size in bytes of the transmitted payload. This helps the microcontroller to differentiate the actual message from the additional padding of zeros or ones. It also helps in detecting if the message has been concocted or not. Bearing in mind that the payload has a maximum size of 8,128 bits (1,016 bytes), the payload length field would have a value of ―0000001111111000‖ when the payload is exactly 1,016 bytes. In case the transmitted message (payload) size has a decimal point it is rounded up (ceiled) to the nearest whole number. For example, if the size of the transmitted payload is 1,001.5 bytes, it is rounded up to 1,002 bytes; thus the payload length field would be ―0000001111101010‖.

To know whether to pad with zeros or ones, the last bit of the data message is inverted. So if the message when converted to bits ends with a ―1‖, the remaining space would be padded with zeros; otherwise with ones.

The typical payload size of smart metering devices ranges between 100 and 1,000 bytes; which is less than the 1,016 bytes of space made available for the payload in the proposed datagram format [6.15]. However, just in case the payload size ever goes beyond the allotted space, the payload can be chunked into different packets (in different datagrams), each having a maximum size of 1,016 bytes. These chunks would be accounted for by the nonce and the payload length field. Currently the payload length field can account for 8,192 bytes (2^{16}) of transmitted data. This is more than 8 times the size of the maximum payload size, thus making it possible to account for 8 packets of transmitted data. So whenever the payload length field is greater than the maximum payload size, the microcontroller/MDMS detects that the rest of the payload would be found in the upcoming packets. These packets would be ordered, stored and decrypted according to their nonce values.

6.2.3 Physical Security

In the earlier submissions, it was stated that there is the need to provide both cyber and physical security measures. Most of the above discussions suggested measures for ensuring cyber security. In this section, effective analysis of consumption patterns are used in providing physical security for the utility's most basic asset – the meter.

In Chapters three and four various physical tamper techniques were discussed and their respective detection mechanisms were included in the retrofit design. It was however mentioned that consumption patterns can be used to detect all the discussed tamper techniques,

thus making it an essential versatile tamper detection mechanism. Via this mechanism most utilities that have adopted smart energy metering systems have been able to deal effectively with the issue of energy fraud. Mitigating these non-technical losses is one of the main drivers for deploying smart metering systems, since doing so has a significant positive impact on a utility's financial performance.

This thesis suggests the use of Support Vector Machines (SVM), a classification-based approach, in the detection of energy theft in the proposed smart metering system. In this approach, after raw consumption data from all the utility's consumers has been transmitted to the MDMS over a period of time; say a week or a month, they are processed and classified. Customers having similar load profiles are classified into one group [6.33]. For example, residential customers may be first classified into small, medium and large consumption customers as depicted in Table 6.11.

Table 6.11 Classification of residential customers

	Small	**Medium**	**Large**
Hourly Consumption (kWh)	0 – 0.5	0.5 - 1	1 – 1.5
Daily Consumption (kWh)	1.5 – 10	10 - 20	20 – 35
Monthly Consumption (kWh)	< 300	300 – 600	> 600

For each group, each customer's instantaneous consumption over the said period is studied using binary SVM algorithm [6.34]. This algorithm is a statistical based theory used to build an optimal decision function ***f(x)*** that precisely forecasts unseen data into two classes and minimizes the classification error using

$$f(x) = sgn\,(g(x)) \qquad 6.6$$

Where ***g(x)*** is the decision boundary between the two classes and is obtained using the principle of Structural Risk Minimization (SRM) given by

$$R < \frac{t}{n} + \sqrt{\frac{h(\ln(\frac{2n}{h})+1)-\ln(\frac{\vartheta}{4})}{n}} \qquad 6.7$$

Where *R = classification error* *t*

= number of training errors *n =*

number of training samples

ϑ = confidence measure

The SVM identifies the trend or pattern in the consumer's consumption and hence can be made to detect anomalies or deviations in the pattern of future consumption data. Deviations of wide margins are likely to be energy theft. In detecting energy theft SVM has been proven to have a detection rate ranging between 60 and 98.4 %. This is highly desirable and better than using other classification based schemes such as Fuzzy Classification and Neural Network Pattern Recognition [6.34].

It is however important to note that the use of SVM requires high computational resources and time, as such utilities can first use the initial customer classification in order to minimize the consumption data to be examined. In using the first classification the utility determines from periodic consumption data, customers who have consumed energy below their identified class margin. For example, as depicted in Table 6.11 if a medium scale residential consumer's hourly, daily or monthly consumption has suddenly dropped below the specified consumption range, it is marked as possible energy fraud. Only such marked consumptions are further examined using the SVM approach. This saves the utility computational time and resources. If

after further study, there are significant deviations from the consumer's expected consumption pattern, utility officials with the help of the appropriate law enforcement agency would visit the premises of the suspected consumer to carry further investigations and possibly make an arrest. An example of a comparison between the transmitted energy readings and the consumer's regular consumption pattern is presented in Figure 6.21.

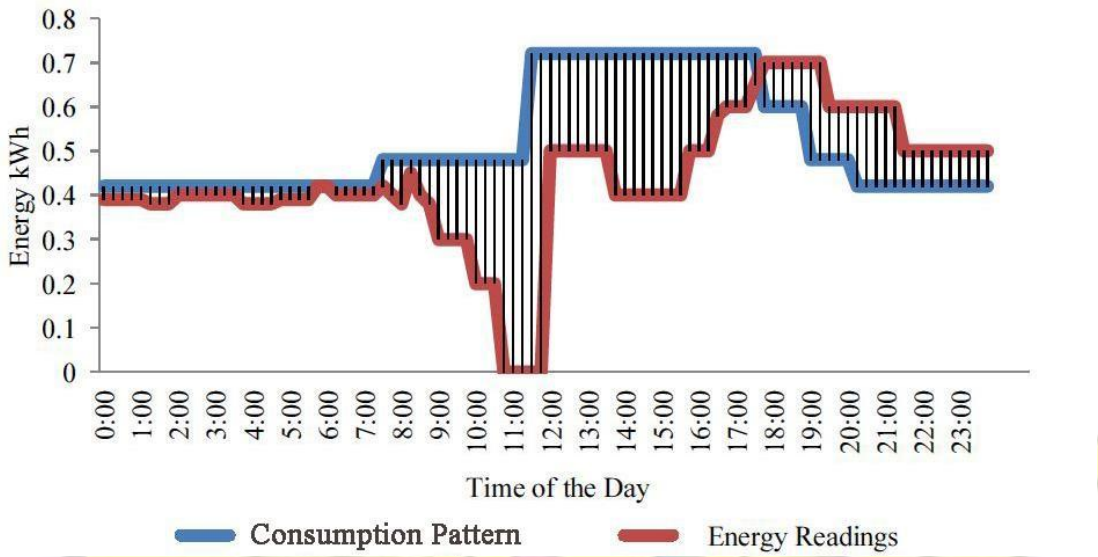


Figure 6.21 Comparison between transmitted data and consumption pattern [6.33]

It is also worth mentioning that in generating the consumer's regular consumption pattern using SVM, it is important to consider other external factors such as weather patterns, billing and payment information. These factors are necessary in determining the probability of energy theft occurring. For example, during winters or cold seasons there is the likelihood that most customers would not use their air conditioning systems and as such their consumption may dwindle as compared to seasons of summer. The opposite is also true – during summers their consumption is expected to rise especially if they own ventilating and cooling systems. Also by making reference to historic billing information, consumption patterns would be generated to match consumption of similar periods in previous years. Utilities can also use payment information to ascertain the likelihood of energy theft occurring. Payment defaulting

consumers are often known to be the main perpetrators of energy theft; as such utilities would easily follow up on such consumers when they have little deviations from the generated pattern.

This classification based approach is not only limited to providing physical security for deployed smart meters but also it helps utilities detect billing errors, faulty meters and latencies in transmission of consumption data [6.35].

6.3 SUMMARY

This Chapter presented the entire GSM based network architecture for the proposed smart metering system. Also cyber and physical security measures are discussed in an attempt to provide an end-to-end security for the proposed system. Key among these discussions is the proposition of a secured communication protocol and a datagram format for transmitting data in the smart metering system.

REFERENCES

[6.1] ―GSM Coverage Population‖, Mobile for Development Impact, https://mobiledevelopmentintelligence.com/statistics/67-gsm-coverage-population, January 2015.

[6.2] Future Electronics, ―Comparison of Wireless Technologies, (NFC - WIFI - Zigbee - Bluetooth - GSM)‖, Future Electronics Limited, Egypt, http://www.futelectronics.com/wpcontent/plugins/fe_downloads/Uploads/Comparison%20of%20Wi reless%20Technologies.pdf, June 2015.

[6.3] Enrico Calandro, Chenai Chair and Alison Gillwald, ―Shift from just voice services: African markets gearing for internet‖, Research ICT Africa, 2014.

[6.4] V. Cagri Gungor, Dilan SahinTaskin Kocak, Salih Ergut,Concettina Buccella, Carlo Cecati and Gerhard P. Hancke, ―A Survey on Smart Grid Potential Applications and Communication Requirements‖, IEEE Transactions On Industrial Informatics, Vol. 9, No. 1, February 2013.

[6.5] K.A.P Agyekum and Eric Tchao, ―Quality of Service of a Deployed 3G Data Network‖, International Journal of Advanced Computer Science and Applications(IJACSA). Volume 4 No. 6, pp 292-297, June 2013.

[6.6] Sharelynn Moore, ―Key Features of Meter Data Management Systems‖, Itron White Paper, Meter Data Management, 2008.

[6.7] Brahim Ghribi and Luigi Logrippo, ―Understanding GPRS: The GSM Packet Radio Service‖, School of Information Technology and Engineering, University of Ottawa, 2000.

[6.8] David A. Burgess, Harvind S. Samra, ―The Open BTS Project‖, Kestrel Signal Processing Incorporated, August 2008.

[6.9] Ye Ouyang and M. Hosein Fallah, ―The Impact of Cell Site Re-Homing On The performance of UMTS Core Networks‖, International Journal of Next Generation Network (IJNGN), Vol.2, No.1, March 2010.

[6.10] ―IEEE 802.16‖, Wikipedia, http://en.wikipedia.org/wiki/IEEE_802.16, December 2014.

[6.11] Cisco, ―Congestion Management Overview‖, Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2, pp. 83-106, May 2005.

[6.12] Comarch Telecoms, ―MVNO Business – Creating a Win-Win Model‖, A short guide for MVNOs and mobile network operators, Comarch, White Paper, June 2010.

[6.13] Alex Shneyderman and Alessio Casati, ―Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems‖, Wiley Publishing Incorporated, pp. 265-267, 2003.

[6.14] Dario Talmesio and Daniele Tricarico, ―The Future of MVNOs Strategies to succeed with MVNOs in Latin America‖, Informa Telecoms and Media, 2012.

[6.15] Germán Corrales Maduêno, Čedomir Stefanović, Petar Popovski, ―How Many Smart Meters can be Deployed in a GSM cell‖, Department of Electronic Systems, Aalborg University, Denmark, Danish Council for Independent Research (Det Frie Forskningsråd), Sapere Aude Research Leader program, Grant No. 11-105159 Dependable Wireless bits for Machineto-Machine (M2M) Communications, October 2014.

[6.16] Germán Corrales Maduêno, Čedomir Stefanović, Petar Popovski, ―Reengineering GSM/GPRS Towards a Dedicated Network for Massive Smart Metering‖, Department of Electronic Systems, Aalborg University, Denmark, Danish Council for Independent Research (Det Frie Forskningsråd), Sapere Aude Research Leader

program, Grant No. 11-105159 Dependable Wireless bits for Machine-to-Machine (M2M) Communications, October 2014.

[6.17] Council of European Energy Regulators ASBL, ―CEER Benchmarking Report on Meter Data Management Case Studies‖, Ref: C12-RMF-46-05, November 2012.

[6.18] Ross Anderson and Shailendra Fuloria, ―Who controls the off Switch?‖, IEEE International Conference on Smart Grid Communications (SmartGridComm), October 2010.

[6.19] Brandon J. Murrill, Edward C. Liu and Richard M. Thompson II, ―Smart Meter Data: Privacy and Cybersecurity‖, Congressional Research Service, February 2012.

[6.20] W. Wang and Z. Lu, ―Survey Paper Cyber security in the Smart Grid: Survey and challenges‖, Elsevier Computer Networks 57, pp. 1344–1371, 2013.

[6.21] Paul Yousef, ―GSM-Security: a Survey and Evaluation of the Current Situation‖, ISY, Linköping Institute of Technology, March 2004.

[6.22] Madhav M. Ajwalia and Nilesh K. Modi, ―Vulnerabilities in Existing GSM Technology that causes Exploitation‖, International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345, Vol. 4 No. 05, May 2013.

[6.23] Swapna Iyer, ―Cyber Security for Smart Grid, Cryptography, and Privacy‖, International Journal of Digital Multimedia Broadcasting, Volume 2011, July 2011.

[6.24] Fuwen Liu, ―A Tutorial on Elliptic Curve Cryptography‖, Brandenburg Technical University of Cottbus, Computer Networking Group, 2010.

[6.25] ―Cryptography‖, Wikipedia, https://en.wikipedia.org/wiki/Cryptography, September 2015.

[6.26] Ritu Tripathi and Sanjay Agrawal, ―Comparative Study of Symmetric and Asymmetric Cryptography Techniques‖, International Journal of Advance Foundation and Research in Computer (IJAFRC),Volume 1, Issue 6, ISSN 2348 – 4853, June 2014.

[6.27] ―NSA Suite B Cryptography‖, Wikipedia, https://en.wikipedia.org/wiki/NSA_Suite_B_Cryptography, August 2015.

[6.28] ―Elliptic Curve Cryptography‖, Wikipedia, https://en.wikipedia.org/wiki/Elliptic_curve_cryptography, August 2015.

[6.29] Don Johnson, Alfred Menezes and Scott Vanstone, ―The Elliptic Curve Digital Signature Algorithm (ECDSA)‖, Certicom Cooperation, 2001.

[6.30] Neha Jha and Brajesh Patel, ―Forward Secrecy For Google HTTPS using Elliptic Curve Diffie-Hellman Key Exchange Algorithm‖, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 9, November 2012.

[6.31] ―Atmel ATECC508A-MAHDA-T‖, Digikey, http://www.digikey.com/productdetail/en/ATECC508A-MAHDA-T/ATECC508A-MAHDA-TCT-ND/5213071, June 2015.

[6.32] Andrew Andrew, ―Developing an IoT Security solution‖, Thing Innovations, http://thinginnovations.uk/developing-an-iot-security-solution, June 2015.

[6.33] Soma Shekara Sreenadh Reddy Depuru, ―Modeling, Detection, and Prevention of Electricity Theft for Enhanced Performance and Security of Power Grid‖, University of Toledo, August 2012.

[6.34] Rong Jiang, Rongxing Lu, Ye Wang, Jun Luo, Changxiang Shen, and Xuemin (Sherman) Shen, ―Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid‖, Tsinghua Science and Technology, ISSNLL10070214ll01/12llpp105-120, Volume 19, Number 2, April 2014.

[6.35] SAS Institute Inc.,‖ Detect Nontechnical Loss Accurately and Efficiently to Reduce Energy Theft‖, Solution Brief, 106064_S143526.0915, 2012.

CHAPTER SEVEN: SYSTEM VALIDATION

7.0 INTRODUCTION

This chapter validates the system based on the set functional requirements and research objectives. Section 7.1 validates the retrofit system and Section 7.2 validates the low cost of the entire system design and communication.

7.1 RETROFIT VALIDATION

After the smart retrofit was implemented, a performance evaluation exercise was conducted to verify its functional requirements. These functional requirements were earlier elicited in Chapter Four using appropriate engineering tools and system analysis of two Siemens smart energy meters – IM100 and IM300. These two smart meters comply with DLMS/IEC 62056 standards. A recap of the summarized functional requirements of the smart retrofit is presented below:

1. Display of accurate consumption data in kWh and currency via in-home display.
2. Reception and display of utility transmitted notifications and control information.
3. Real-time transmission of accurate consumption data and power quality measurements to utilities.
4. Real-time detection and remote reporting of meter tamper.
5. Remote disconnection and reconnection of power supply.

The smart retrofit was then connected to an existing digital pulsed electronic standalone ECG energy meter. The meter had the following characteristics:

1. 1 Phase 2 Wire

2. Rated Voltage of 240V (±25%)
3. Maximum Current Rating of 30A
4. Frequency rated at 50Hz (±5%)
5. Impulse rate of 200imp/kWh

The meter had a pulsating LED of approximately 400 lumens which pulsed at the specified impulse rate. The smart retrofit's GL5528 Mini Photocell was carefully placed over this LED and provided with ample isolation in order to minimize external noise. The entire setup was left over a period of two days to measure consumption data from the existing standalone energy meter. The smart retrofit was programmed to transmit data to the cloud-based MDMS every 15 minutes; when no external interrupts occur. Figure 7.1 shows sample results of meter readings collected on the MDMS.

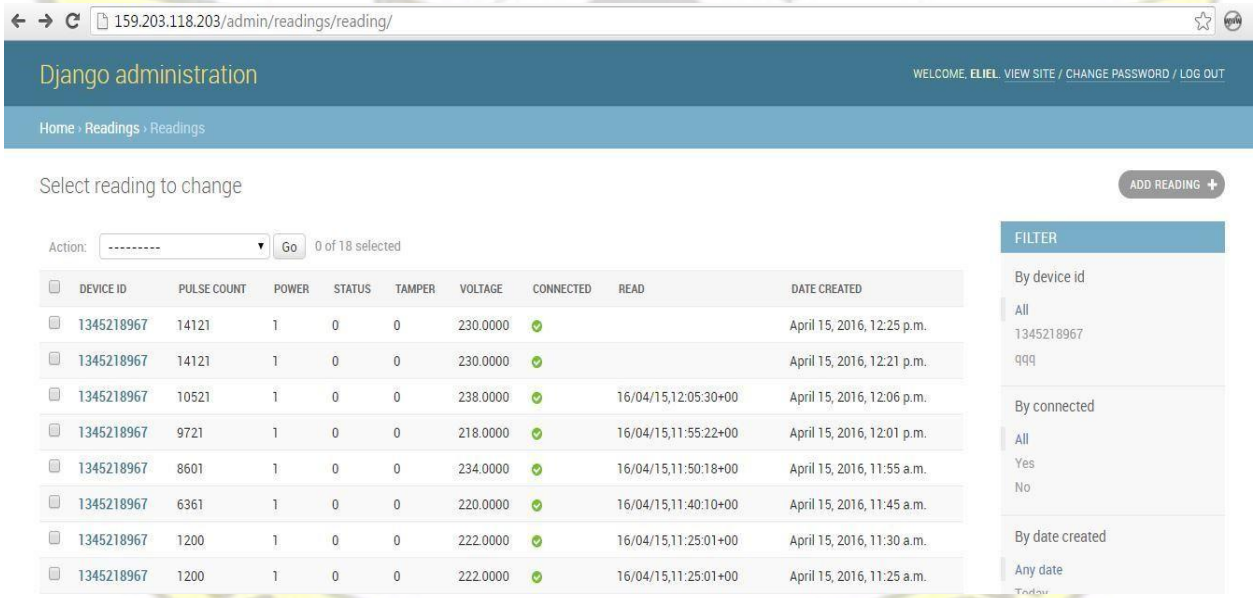


Figure 7.1 Sample Transmitted Meter Readings on MDMS

From the results, it is evident that the pulse count of the energy meter increased with time. It is also evident that meter data is transmitted periodically. When the transmitted consumption data was compared with the existing standalone meter, they were found to be accurate. This same

data was displayed on the smart retrofit's in-home display. Also from Figure 7.1, it can be observed that the voltage reading for power quality measurements were also transmitted and it ranged between 218 and 238V. These voltage ratings are found within the specified operational voltage range of the existing retrofit. The voltage readings were taken using the ACS715 Hall Effect Current Sensor connected to the live wire of the existing meter.

Performance tests were also conducted to verify the functionality of the tamper detection system. Various energy theft methods were attempted in order to provide the necessary triggering conditions of the four energy theft detection sensors. Results from these tests are provided in Table 7.1. The temperature reading as at the time of testing was 28ºC.

Table 7.1 Results of Energy Theft Detection Performance Test

Sensor	Function	Trigger Description	Varying Condition	Triggered
AT407 Ball Rolling Switch (Tilt Sensor)	Detects physical tamper of meter.	Tilting/moving the meter at an angle of	15º	✘
			30º	✘
			45º	✓
			60º	✓
ADXL337 Triple Axis Accelerometer	Detects motion and shock.	Applying a shock of	±1g	
			±2g	
			±3g	
			±4g	✓
US1881 Hall Effect Sensor	Detects external magnetic fields.	Applying a Neodymium Earth magnet having a magnetic density of 1.17 Tesla at a distance of	40cm	
			30cm	
			20cm	
			10cm	✓
ACS715 Hall Effect Based Linear Current Sensor	Detects meter bypass.	Applying a bypass load of	250mA	
			500mA	
			750mA	
			1000mA	✓

The results presented in Table 7.1 shows that the sensors are capable of detecting energy theft for specific conditions. These conditions are summarized in Table 7.2.

Table 7.2 Basic Conditions for Energy Theft Detection by Sensors

Sensor	Trigger Description	Triggers When Reading Is
AT407 Ball Rolling Switch (Tilt Sensor)	Tilting/moving the meter at an angle of	≥ 45 º
ADXL337 Triple Axis Accelerometer	Applying a shock of	≥ 4g
US1881 Hall Effect Sensor	Applying a Neodymium Earth magnet having a magnetic density of 1.17 Tesla at a distance of	≤ 10cm
ACS715 Hall Effect Based Linear Current Sensor	Applying a bypass load of	≥ 1000mA

Tests were also conducted to ascertain how long the 6,600 milliamp hour (mAh) Lithium Polymer Ion Battery can last without charging. To do so, the battery was first fully charged using its connected charger. Then the charger was unplugged from the mains and the retrofit was allowed to operate solely on the backup battery power. The smart retrofit which has a maximum current rating of 500mA lasted 12 hours and 40 minutes on this power source. This value was then compared to the duration the battery was expected to last. This duration was obtained using the formula below.

$$\text{Capacity (Amp hours)} = \text{Current Rating (Amps)} \times \text{Duration (hours)} \quad 7.1$$

Since the battery capacity is 6.6 Ah and the maximum operational current of the smart retrofit is 0.5A, the expected duration of the battery should be 13 hours and 12 minutes. The calculated value is approximately equal to what was obtained when the smart retrofit was left unplugged. This value represents the total duration the backup battery can supply power to the retrofit during power outages.

Another area that requires validation is the cost savings achieved by adopting the proposed model. This is necessary to validate if the set objective of providing a low-cost smart retrofit was achieved. These cost-benefit analyses are provided in the next section.

7.2 COST-BENEFIT ANALYSES

7.2.1 Cost Savings: Retrofit Design

From a research conducted by Siemens, the average cost of most deployed smart meters is 221 USD [7.1]. Also inferring from a recent massive deployment of 15,257,931 smart meters in the United States of America under a Smart Grid Investment Grant (SGIG) program, the total cost of the meters was 2,545,320,027 USD. This brings the average cost of each smart meter to 166.82 USD [7.2].

In this research, the cost-benefit analysis is done by gathering prices of all the above mentioned components of the smart retrofit from trusted online stores such as SparkFun, Adafruit and Mouser. These stores were selected because they are among the few that allow retail and bulk purchases. Table 7.3 shows the prices displayed on their sites for the following components of the retrofit.

Table 7.3 Prices of Components

Name of Component	Quantity	Price (USD)
GL5528 Mini Photocell	1-24	1.50
	25-99	1.43
	100+	1.35
Sim900 GSM Communication Module	1-9	69.95
	10-24	66.45
	25-99	62.96
	100+	59.46
Xiamen Ocular GDM2004D 20x4 LCD	1-24	17.95
	25-99	17.05

	100+	16.16
Keyes 5V Electromagnetic Relay	1-2	2.52
	3-5	2.23
	6-9	2.22
	10+	2.21
Arduino Mega 2560 Revision 3	1-10	45.95
	10-99	44.95
	100+	44.45
AT407 Ball Rolling Switch	1-24	1.95
	25-99	1.85
	100+	1.76
ADXL337 Triple Axis Accelerometer	1-9	9.95
	10-24	9.45
	25-99	8.96
	100+	8.46
US1881 Hall Effect Sensor	1-24	0.95
	25-99	0.90
	100+	0.86
ACS715 Linear Current Sensor	1-9	7.95
	10-24	7.55
	25-99	7.16
	100+	6.76
Adafruit Data Logging Shield	1-9	19.95
	10-99	17.96
	100+	15.96
Piezo Speaker	1-24	1.95
	25-99	1.85
	100+	1.76
Lithium Ion Battery Pack - 3.7V 6600mAh	1-9	29.50
	10-99	26.55
	100+	23.60
USB LiIon/LiPoly charger - v1.2	1-9	12.50
	10-99	11.25
	100+	10.00

From Table 7.3 it is evident that the prices of these components decrease as their quantities increase. Bearing in mind that utilities usually have client bases that span from hundreds of thousands to millions, it is important to obtain the cost of these components when producing

for such volumes. As such logarithmic extrapolations were done using the prices displayed in Table 7.3. Table 7.4 shows the logarithmic equations obtained for each of the components.

Table 7.4 Logarithmic Extrapolation of Cost of Component

Component	Equation
Photocell	-0.074*ln(x)+1.4986
GSM/GPRS Communication Module	-3.386*ln(x) + 69.299
Liquid Crystal Display (LCD)	-0.893*ln(x) + 17.907
Relay	-0.183*ln(x) + 2.4557
Microcontroller (MCU)	-0.359*ln(x) + 45.567
Tilt Sensor	-0.096*ln(x) + 1.9435
Triple Axis Accelerometer	-0.479*ln(x) + 9.8559
Hall Effect Sensors	0.046*ln(x)+0.9458
Current Sensor	-0.382*ln(x) + 7.8745
Data Logger	-0.861*ln(x) + 19.329
Piezo Speaker	-0.096*ln(x) + 1.9435
LiPo Battery	-1.274*ln(x) + 28.577
LiPo Charger	-0.54*ln(x) + 12.109

In the table ―ln‖ represents the natural log function, ―*‖ represents multiplication and ―x‖ represents the purchased quantity of the component. After computing these equations for quantities spanning from hundred thousand to one million, Figure 7.2 and Table 7.5 were obtained.

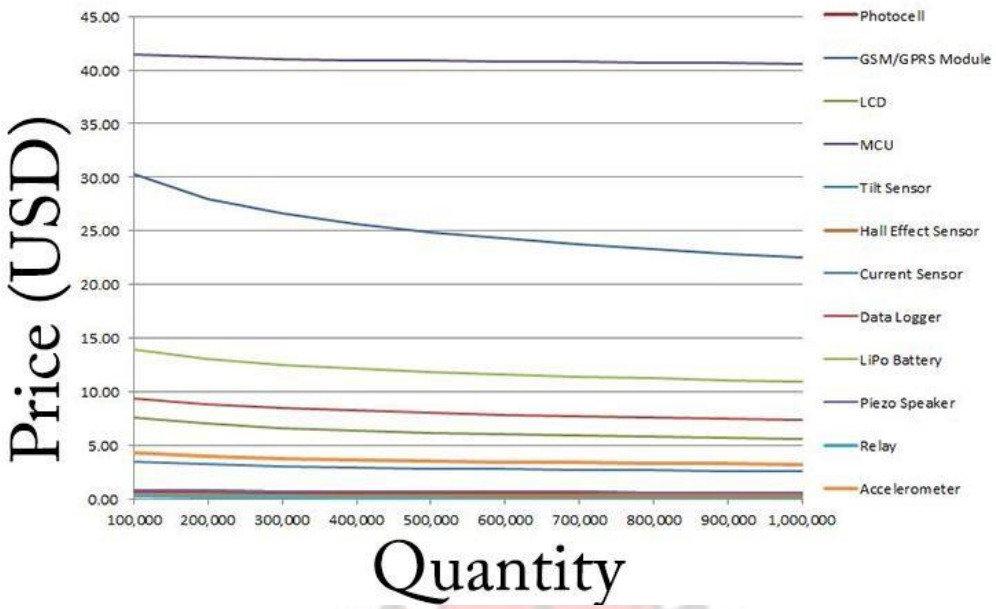


Figure 7.2 Logarithmic extrapolation of cost of component

Table 7.5 Logarithmic extrapolation of Component Cost (USD)

Quantity	Photocell	GSM/GPRS Module	LCD	Relay	MCU	Tilt Sensor	Hall Effect Sensor	Current Sensor	Data Logger
100,000	0.65	30.32	7.63	0.35	41.43	0.84	0.42	3.48	9.42
200,000	0.60	27.97	7.01	0.22	41.19	0.77	0.38	3.21	8.82
300,000	0.57	26.60	6.64	0.15	41.04	0.73	0.37	3.06	8.47
400,000	0.54	25.62	6.39	0.10	40.94	0.71	0.35	2.95	8.22
500,000	0.53	24.87	6.19	0.05	40.86	0.68	0.34	2.86	8.03
600,000	0.51	24.25	6.03	0.02	40.79	0.67	0.33	2.79	7.87
700,000	0.50	23.73	5.89	0.02	40.74	0.65	0.33	2.73	7.74
800,000	0.49	23.28	5.77	0.02	40.69	0.64	0.32	2.68	7.63
900,000	0.48	22.88	5.66	0.02	40.65	0.63	0.32	2.64	7.52
1,000,000	0.48	22.52	5.57	0.02	40.61	0.62	0.31	2.60	7.43

Quantity	LiPo Battery	LiPo Charger	Piezo Speaker	Accelerometer	TOTAL 1	TOTAL 2	TOTAL 3	TOTAL 4
100,000	13.91	5.89	0.84	4.34	119.50	143.40	179.25	239.00
200,000	13.03	5.52	0.77	4.01	113.49	136.19	170.24	226.98
300,000	12.51	5.30	0.73	3.81	109.98	131.97	164.96	219.95
400,000	12.14	5.14	0.71	3.68	107.48	128.98	161.22	214.96
500,000	11.86	5.02	0.68	3.57	105.55	126.66	158.32	211.10
600,000	11.63	4.92	0.67	3.48	103.97	124.76	155.95	207.93
700,000	11.43	4.84	0.65	3.41	102.66	123.19	153.99	205.32
800,000	11.26	4.77	0.64	3.35	101.52	121.83	152.29	203.05
900,000	11.11	4.71	0.63	3.29	100.53	120.63	150.79	201.05
1,000,000	10.98	4.65	0.62	3.24	99.63	119.56	149.45	199.26

In Table 7.5 there are four totals presented, namely Total 1, Total 2, Total 3 and Total 4. Their differences are explained as follows:

1. Total 1 represents the unit cost of retrofit when manufacturing at the specified volume without any miscellaneous cost.
2. Total 2 represents the unit cost of retrofit when manufacturing at the specified volume in addition to a 20% miscellaneous cost.
3. Total 3 represents the unit cost of retrofit when manufacturing at the specified volume in addition to a 50% miscellaneous cost.
4. Total 4 represents the unit cost of retrofit when manufacturing at the specified volume in addition to a 100% miscellaneous cost.

The miscellaneous cost was added to take care of any additional cost that may be incurred during the manufacture of the retrofit. Since this cost often comes as a percentage of the unit cost of the retrofit, the above mentioned percentages were provided just to give an idea of what the final cost of the retrofit would be. To verify how cost efficient this retrofit design is, Table 7.6 compares the unit cost of the retrofit with that of the average unit cost of the smart meter deployed in the SGIG program [7.2]. The unit cost of the retrofit is the logarithmic extrapolated value when manufacturing for a volume of 15,257,931; which is the same as the quantity of meters deployed in the SGIG program.

Table 7.6 Cost-Benefit Analysis: Comparison between retrofit and SGIG Deployed Meter

SGIG Meter	Retrofit			
	TOTAL 1	TOTAL 2	TOTAL 3	TOTAL 4
166.82 USD	76.51 USD	91.81 USD	114.76 USD	153.01 USD
	Percentage of Cost Savings			
	54.14%	44.96%	31.21%	8.28%

The same comparison is done with the average unit cost of 221 USD, as quoted as the average unit cost of smart meters by Siemens [7.1]. This is presented in Table 7.7.

Table 7.7 Cost-Benefit Analysis: Comparison between retrofit and Siemens Meter

Siemens Meter	Retrofit			
	TOTAL 1	TOTAL 2	TOTAL 3	TOTAL 4
221.00 USD	76.51 USD	91.81 USD	114.76 USD	153.01 USD
	Percentage of Cost Savings			
	65.38%	58.46%	48.07%	30.76%

From Tables 4.6 and 4.7, it is evident that the retrofit is of a low cost than the other deployed smart meters. Its cost savings ranges between 8.28% and 65.38%. African developing countries with low budgets are therefore likely to spend less in adopting this low cost retrofit; thus reducing the wait time between saving for deployment and deployment. Also the process of deployment is further expedited and its cost reduced via the use of the already existing GSM/GPRS communication infrastructure. In addition, the retrofit is simply installed without tampering with the existing standalone meter; there is no need to open it up or reengineer it. This reduction in wait time and cost of deployment as well as the ease of deployment makes this scheme a low cost early adoption strategy for implementing smart metering systems in African developing countries.

Further cost benefit analyses are conducted in the next subsection to ascertain the savings made by adopting the proposed datagram format.

7.2.2 Cost of Using Proposed Datagram Format

It is important to determine the cost utilities or customers would incur when this fixed sized datagram format is used. Considering the fact that there are at least 96 transactions every day; 4 times every hour for 24 hours, between the meter and the MDMS. In addition to acknowledgement sent for each message received, the total number of transactions comes to 192. In each transaction there is a fixed data size of 1,024 bytes; thus a total of 196,608 bytes (192 kB) of data every day. Table 7.8 shows the average cost of mobile broadband services of three different MNOs in Ghana. These MNOs were chosen because they are widely spread in Africa.

Table 7.8 Average cost of mobile internet data of 3 MNOs in Africa [7.3]

Name of MNO	**Airtel**	**MTN**	**Vodafone**
Average cost per kB (USD)	0.000003	0.000004	0.000004
Average cost for daily transactions: 192kB (USD)	0.000576	0.000768	0.000768
Average cost for monthly transactions: 5.6MB (USD)	0.017280	0.023040	0.023040
Average cost for annual transactions: 67.5MB (USD)	0.207360	0.276480	0.276480

From Table 7.8, the average cost for annual transactions, using tariffs from the three MNOs, is 0.25344 USD. This means that utilities/consumers pay less than one-third of 1 USD each year for transactions between the smart retrofit and the MDMS when using the proposed datagram format. This is very inexpensive thus making it an ideal option for African developing countries.

7.3 SUMMARY

In this chapter various steps are taken to validate the retrofit design and ascertain cost-savings derived from using the proposed system. Results presented suggest that the system performs according to the set functional requirements and is a cost-effective option for implementing smart metering systems in African developing countries.

REFERENCES

[7.1] Su-Lin Tan and Michael West, ―Smart meters, but at whose expense? - Do consumers pay too much?‖, The Sunday Morning Herald, Business Day, http://www.smh.com.au/business/smart-meters-but-at-whose-expense-201212232btjd.html, December 2012.

[7.2] ―Advanced Metering Infrastructure and Customer Systems‖, US Department of Energy, Office of Electricity Delivery and Energy Reliability, https://www.smartgrid.gov/recovery_act/deployment_status/ami_and_customer_systems, February 2015.

[7.3] Webhostghana, ―Ghana Mobile Broadband‖, Cedi Compare, http://cedicompare.com/ghanabroadbandinternet/broadbandoptions/ghanamobilebroadband.html#, October 2014.

CHAPTER EIGHT: APPLICATION – A SMART QUOTA POLICY

8.0 INTRODUCTION

This chapter proposes a smart quota policy for rationing electric power in African developing countries as an effective alternative to blackouts. It is an application of the earlier proposed secured low cost smart metering system. Section 8.1 presents the current method of rationing power in Africa. Section 8.2 explains the concept of quota systems in rationing electric power. Section 8.3 provides details of the proposed Smart Quota Policy and its advantages over other systems.

8.1 POWER RATIONING IN AFRICA

As explained in chapters one and two, the continent of Africa is severely plagued with power crises [8.1]. It was revealed that the nemesis of these power crises lie in the inability to curtail power shortages through the provision of copious energy supplies and generation capacities in tandem with accurate demand analyses [8.2]. It is estimated that 30 out of 48 countries in Africa are currently using rotational load shedding (blackouts) as the main method of managing these crises [8.3].

This method of rationing power is often preferred because it is simpler to implement; not requiring the utility to gain consent of the affected consumers. Utilities simply switch off feeders distributing power to particular geographic areas anytime they realize they cannot meet the expected demand. Consumers may or may not be informed of these blackouts. A critical assessment of this power rationing scheme reveals that it is not deployed in a socially equitable manner; both consumers who are energy efficient and those who are not are denied access to power. This discourages the former from adhering to energy saving ethics.

This scheme still proves to be inefficient even in well-organized rotational load shedding schemes, where consumers are made fully aware of the blackout schedule. There is no guarantee that by turning off power in the scheduled periods the utility makes energy savings or reduces the cost of electricity generation. This is because, being fully aware of the schedule, consumers only need to shift all their consumption to times when there would be power. So for example if a consumer had planned to do the laundry using a washing machine he checks the schedule and does it at a time where there would be power. In this case the same amount of power is still being consumed and the utility has not saved by switching off power either in the day or night. In other words, this scheme fails to efficiently ration scarce energy resources. This is partly the reason why African developing countries that ration power using this method have

hardly made any considerable improvement in effectively meeting demand. As a consequence of this, countries like Ghana have had to increase the scheduled blackout periods from 12 to 24 hours [8.4].

Considering the inefficacies of this scheme in addition to the fact that this scheme causes African businesses 6 – 20% losses in sales and productivity, it is important to replace this scheme with a more efficient one [8.5]. This replacement should be socially equitable, inculcate energy saving ethics in consumers and guarantee utilities of reduction in the cost of electricity generation. After conducting research into best practices of rationing power the Quota System was identified as an effective replacement [8.6].

8.2 QUOTA POLICY

In this power rationing scheme, each consumer is given a quota of energy for a particular consumption period – typically one month. Consumers are compelled to reduce their monthly consumption to a specified amount. This scheme is rolled out in tandem with price signals; where overachievers are rewarded and defaulters are penalized [8.7]. Punitive measures for defaulters often range between meter disconnections for extended periods and fines.

In this scheme, as long as consumers remain within their quota they are assured of reliable energy supply; only those who exceed their quota are denied access to power. Utilities no longer have to rollout blackouts over large geographic areas rather each consumer determines when he is disconnected from regular power supply. As such, this scheme ensures that power is distributed in a socially equitable way.

A consumer, knowing he is responsible for how long he enjoys power, would ensure that he makes efficient use of his allotted energy quota. So it can be said that this scheme inculcates in consumers energy saving habits. Businesses are also capable of planning their operations in

order to avoid losses in productivity. Utilities, also knowing the total quotas that have been allotted to consumers, can effectively plan to meet them and avoid unprecedented demands. Effectively meeting these demands would curtail energy crises in these countries.

In cases where consumers require more than is allotted them, they can apply for extra quotas which are often priced at higher rates than the norm. Distribution companies use these payments to purchase extra power from generating companies [8.7]. This scheme is therefore established on the premise of the consumer's disposition to either conserve energy or pay extra for power without necessarily authorizing blackouts.

A successful implementation of this scheme was carried out in Brazil. The next section describes how this was done.

8.2.1 Quota Policy Implementation in Brazil

Just like most African developing countries are currently, Brazil was heavily hydrodependent in the year 2001 [8.7] [8.8]. Having suffered vagaries of rainfall in the previous years coupled with the wait-and-see canker, they were plunged into a grave period of power crisis which lasted from March 2001 till February 2002. This called for the implementation of a stringent power rationing scheme. After careful deliberations on various power rationing schemes, in May 2001 they chose and implemented the Quota System incorporating price signals (bonuses and penalties) [8.7].

In rolling out this system, the various classes of consumers were identified and each consumer was given a quota of energy. This quota was often 20% less of their average consumption during the same period in the previous year. So for example, a consumer who consumed 100 kilowatt hours in June 2000 was now given a quota of 80 kilowatt hours for June 2001. This

percentage was however different for other classes of consumers. Table 8.1 shows the initial quotas allotted to the different classes of consumers.

Table 8.1 Initial Quota Allocation by Consumer Group [8.7]

CONSUMER CLASS	QUOTA
Residential < 100 kWh/month	100%
Residential > 100 kWh/month	80%
Low-voltage industrial, commercial and services	80%
High voltage industrial, commercial and services	70 – 85% (in relation to type of activity)
Rural	90%
Other consumers (mostly government)	65%

Consumers who transgressed their given quota were penalized. The magnitude of the penalties was dependent on how far he had crossed the quota and how many times he had done so. Penalties ranged from several days of power interruption to payment of higher tariffs than the norm. Monies paid by offenders were often used to incentivize overachievers. Consumers who were not satisfied with their given quotas could apply for higher quotas at higher rates [8.7].

This power rationing scheme was very successful and yielded 20-25 percent reduction in consumption as depicted in Table 8.2. It was however noticed that more than 60 percent of this reduction was contributed by low-income consumers. This could be attributed to the fact that they were highly motivated by the bonuses awarded them for consuming below the baseline. It also meant that in this scheme the poor is protected from high tariffs. This success also proved that this rationing scheme is feasible and scalable.

Table 8.2 Average Energy Savings in Brazil [8.7]

REGION	PERCENTAGE OF ENERGY SAVED IN YEAR

	2000	2001
North	18.3%	24.6%
Northeast	19.5%	20.7%
Southeast/ Center-West	19.8%	21.2%

Based on the above results, the Brazilian implementation of the quota system has been recognized as an international best practice [8.7]. The country was not only able to live on its scarce energy resources but was capable of making savings which increased their national energy reservoirs, thus making a future of little or no energy crises possible. The prospects of this power rationing scheme make it a viable replacement for Africa's rotational load shedding programs. However, before adopting the very same method of implementation it is important to critically analyze whether it would deliver the same results for all the various types of power shortages in Africa.

8.2.2 Analyses of Brazilian Implementation

It is worth noting that during the implementation of this scheme in Brazil, the main electric meters used were standalone credit meters [8.7]. The mode of operation of these meters required that utilities sent manual meter readers at the end of every consumption period to read the meters. Since these meters have no direct communication ability, utilities could not interact with these meters remotely. This method of implementation introduced the following drawbacks:

1. **Manual Distribution of Quotas:** The most important element of this scheme is the quota and consumers are to be provided with their individual quotas before the consumption period begins. Since these meters are standalone meters, utilities had to

manually distribute quotas via human meter readers. This method of distribution is subject to human errors and delays, which could negatively affect the expected results of this scheme.

2. **Targeted for Only Energy-Constrained Environments:** A careful study of Brazil's implementation of this scheme reveals that it was targeted towards an energyconstrained environment where the primary energy resource is scarce [8.6][8.7]. Utilities can estimate how much energy resources they have for a particular consumption period and create and distribute quotas to match their estimates. They are certain that if consumers stay within their quotas they would not run out of energy resources. However, this method of implementation would not do for capacityconstrained environments. In such environments the main cause of power shortages stems from the limited capacity of the power generation plant(s). No matter the copiousness of the energy resources, the system is still incapable of meeting peak demand. This implementation is not designed for minimizing demand during peak hours of the day and hence is incapable of rationing power in capacity-constrained countries such as Ethiopia, Ghana and Rwanda.

To mitigate the identified drawbacks of this system, a proposition is made for the adoption of a Smart Quota System. This system is based on the earlier proposed secured low cost smart metering system targeted for African developing countries. Details of how this system mitigates these drawbacks are discussed in the next section.

8.3 PROPOSED SMART QUOTA POLICY

This policy is specially developed to leverage the communication ability of the proposed smart metering architecture in automating and dynamically rationing power in both energyconstrained and capacity-constrained environments. They are also implemented in tandem with price signals – rewards and penalties; where overachievers are rewarded and defaulters are penalized.

Each consumer's standalone meter is provided with the earlier proposed smart retrofit which furnishes the existing meter with smart metering capabilities. Unlike in the Brazilian implementation, utilities are capable of directly communicating with the meter. Therefore the distribution of quotas are no longer done manually, but are automatically transmitted via wireless communication media to consumers. The ease of this function allows utilities to notify consumers of their quotas in good time before the consumption period begins. To ensure that consumers are duly notified, utilities can use redundancy measures to send quotas multiple times to all the various notification access points – in-home meter displays, online dashboards, mobile devices and emails. This proposed method eliminates the possibility of human errors and delays in the distribution of quotas.

After consumers have been duly notified, utilities remotely instruct the smart retrofits at the beginning of the consumption period to automatically disconnect the meter after the consumer has exceeded his allotted quota. Utilities do not have to visit the consumer's premises to read meter data at the end of the consumption period before determining whether the consumer has exceeded his quota or not. Therefore the proposed method eliminates the possibility of consumers transgressing far beyond the allotted quota before they are detected. This guarantees utilities that the energy resources allocated for the consumption period would be sufficient.

In rationing power in capacity-constrained environments, the proposed Smart Quota System reduces the consumption period into periods which reflect off-peak and peak demand periods and allocates quotas for each period. So instead of having a quota for the typical consumption period of one month, the proposed system provides quotas for hours where demand is likely to be low and different quotas for hours where demand is likely to be high. This is similar to the concept of Time of Use tariffs, where tariffs are dynamic and reflect the cost of energy generation at the time of consumption. Utilities, knowing the estimated demand and the available energy resources, calculate and notify consumers of their quotas for each period. The ease of communication via these wireless channels makes this proposed system feasible and easily scalable.

For energy-constrained environments where the capacity of generation stations is not a problem, quotas can be made to cover longer periods than periods used in capacityconstrained environments. As long as the utility is able to estimate and make provision for the energy resources needed for that consumption period, quotas can be calculated and disseminated. In countries which suffer energy-and-capacity-constraints, a careful blend of the two mechanisms can be used to effectively ration power.

From these discussions, it is clear that the proposed Smart Quota System provides features which mitigate the drawbacks of the Quota System implemented in Brazil. It is also carried out in a social equitable manner and helps consumers to cultivate energy saving lifestyles. African utilities who have already adopted the proposed secured low cost smart metering system do not need to provide any additional equipment in implementing this smart system of rationing power – no additional cost. Its implementation reduces the need for rolling out blackouts over wide geographic areas and assures consumers of reliable power supply.

Consumers are completely in control of how long they have access to power.

8.4 SUMMARY

In this chapter the proposed secured low cost smart metering system is applied in providing an effective system for rationing power in African developing countries. This system is an improved version of the Quota System implemented in Brazil. It mitigates identified drawbacks in the previous system and serves as an effective replacement for rotational load shedding programs in Africa.

REFERENCES

[8.1] APR Energy, ―A View on Global Energy - Africa Energy for Progress‖, APR Energy, LLC, 3600 Port Jacksonville Parkway, Jacksonville, FL 32226 USA, January 2013.

[8.2] Energy Sector Management Assistance Program (ESMAP), ―Implementing Energy Efficiency and Demand Side Management - South Africa's Standard Offer Model‖, Briefing Note, South Africa, July 2011.

[8.3] Saliem Fakir, Manisha Gulati, Louise Scholtz and Ellen Davies, ―South Africa, Africa's Energy Future and Regional Economic Integration: Energy as a Way to Power Change‖, Atlantic Energy Forum, April 2014.

[8.4] ―Energy crisis takes a toll on Ghana's workforce‖, Ghana Web, http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=353749, April 2015.

[8.5] Chloë Oliver, Rahul Kitchlu,Elvira Morella, Jamal Saghir, Lucio Monari and Meike van Ginneken , ―Turning the Lights on Across Africa – An Action Agenda for Transformation‖, Sustainable Development Series, The World Bank, pp. 11-17, April 2013.

[8.6] Energy Sector Management Assistance Program (ESMAP), ―Best Practices for Market-Based Power Rationing – Implications for South Africa‖, Briefing Note, South Africa, August 2011.

[8.7] Energy Sector Management Assistance Program (ESMAP), ―Implementing Power Rationing in a Sensible Way - Lessons Learned and International Best Practices‖, Report 305/05, August 2005.

[8.8] Energy Sector Management Assistance Program (ESMAP), ―South Africa's Market Based Power Rationing Program‖, Low Carbon Growth Country Studies Program, Briefing Note, August 2010.

CHAPTER NINE: CONCLUSION AND CONTRIBUTION

9.0 CONTRIBUTION OF THESIS

In providing a low cost early adoption strategy for implementing secured smart metering systems in African developing countries, the following major contributions are made:

1. A low cost smart non-intrusive retrofit design which furnishes a wide range of existing digital pulse standalone energy meters with smart meter functions. This design does not require the replacement of existing energy meters. It has features which allow two-way communication via GSM between the utility and the meter, remote detection of energy theft, remote (dis)connection, remote accurate meter reading and bill distribution, power quality measurements and display of consumer notifications.
2. Guidelines for the selection of a suitable communication technology to be used in the proposed smart energy metering system and an effective Meter Data Management System (MDMS) Model for stakeholder interactions in the electrical grid are suggested.
3. A secured communication protocol which leverages the computational hardness of Elliptic Curve Discrete Logarithm Problem in encrypting, decrypting and carrying out mutual authentication between communicating nodes. A key aspect of this protocol is

a fixed length datagram format of 1,024 bytes which is designed for all types of wireless communication in the proposed smart metering system. The protocol has features which mitigates the cyber security vulnerabilities of GSM/GPRS/EDGE public networks.

These contributions provide African developing countries with options as to how they can easily migrate to secured smart metering systems. These concepts can be extensively applied to other developing countries in other parts of the world.

9.1 CONCLUSION

Developing countries in Africa are often plunged into extensive periods of energy crises because of their inability to critically analyze demand from day-to-day consumption. This inability results in unprecedented demand which is the nemesis of these crises. To mitigate these crises it is important that African utilities migrate from standalone energy metering systems to smart metering systems. Based on the premise that this migration has often been highly cost intensive to developed countries, this thesis provides a plausible low-cost earlyadoption strategy for implementing secured smart energy metering systems in African developing countries. In providing this strategy it first determines, through critical analysis, factors that are necessary in steering the system design. Based on these factors, a simple lowcost smart retrofit which furnishes existing digital pulse standalone energy meters with smart metering functions is designed. After identifying and prioritizing key assets in a proposed metering infrastructure, cyber and physical security protocols which are requisite in mitigating identified threats are provided. Finally a Smart Quota Policy which leverages key features of the proposed infrastructure is provided as an effective alternative to rationing limited power resources with blackouts.

9.2 RECOMMENDATIONS FOR FUTURE RESEARCH

The Smart metering system is the foundational block of Smart Grids – a sophisticated network comprising smart meters, smart gadgets, renewable energy resources and utility energy delivery systems which use information technology to efficiently, securely and reliably deliver electricity. Most developed worlds are currently identifying and developing standards for the massive rollout of Smart Grids, with few others in the early stages of implementing them. There is therefore the need to study how the proposed smart retrofit, secured communication protocol and Smart Quota System can be further developed in preparation for a full-fledged secured low cost Smart Grid for African developing countries.

LIST OF PUBLICATIONS RELATED TO THESIS

1. Eliel Keelson, K.O. Boateng, Isaac Ghansah, ―A Smart Retrofitted Meter for Developing Countries‖, International Journal for Computer Applications (0975 – 8887), Volume 90 – No. 5, March 2014.
2. Eliel Keelson, Isaac Ghansah, K.O. Boateng, ―A Smart Quota System for Rationing Power in African Developing Countries‖, International Journal of Computer Applications (0975 – 8887) , Volume 103 - No.15, October 2014.
3. Eliel Keelson, K.O. Boateng and Isaac Ghansah, ―Low Cost Early Adoption Procedures for Implementing Smart Prepaid Metering Systems in African Developing Countries : An Effective Way of Dealing With Energy Crises‖, Journal of Multidisciplinary Engineering Science and Technology (JMEST), ISSN: 3159-0040, Vol. 2 Issue 2, February 2015.

APPENDIX A: C CODE FOR RETROFIT SIMULATION IN ISIS

```
#include <18F458.h>
//!#FUSES NOWDT,PUT,NOPROTECT,NOBROWNOUT,NOLVP,NOCPD,INTRC_IO
#fuses HS,NOWDT,NOPROTECT,NOLVP
#DEVICE ADC=10
#use delay(clock=200000000)
#include <LCD-on-D.c>
#include "ds1307_12_1.c"

unsigned int8 sec; unsigned int8
min; unsigned int8 hrs; unsigned
int8 hrs_24; unsigned int8
day,mth,year,dow;
unsigned int8 temp_hrs,temp_dow,temp_mth,temp_year; int
energy_hrs[24]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0}; int
energy_dow[7]={0,0,0,0,0,0,0}; int
energy_mth[12]={0,0,0,0,0,0,0,0,0,0,0,0}; int
energy_year[10]={0,0,0,0,0,0,0,0,0,0}; unsigned int8
array_of_years[10]={0,0,0,0,0,0,0,0,0,0}; unsigned int8
year_counter_index = 0;
float total_energy_hrs = 0,avg_energy_hrs = 0,total_energy_dow = 0,avg_energy_dow = 0,total_energy_mth =
0,avg_energy_mth = 0,total_energy_year = 0,avg_energy_year = 0;
unsigned int8 hrs_counter= 0,dow_counter= 0,mth_counter= 0,year_counter= 0, i = 0;
char week_day[12]; char time; unsigned int1 am_pm; unsigned int8 sec_cache=0; int
```

```
count = 0, count_kwh = 0; float count_ghs = 0.00; int impulse_rate = 2; float
tariff_kwh = 0.258;
unsigned int8 prev_consum_hrs = 0, prev_consum_dow = 0,prev_consum_mth = 0,prev_consum_year = 0;


int ZC = 0; //Zero Crossing
unsigned int8 phase_time[10]; // for checking when the phase or zero crossing occurs
unsigned int8 sum_phase_time = 0; float avg_phase_time = 0.00; unsigned int8
counter_zc = 0, j;
unsigned long int value = 0,value1=0, value2=0,value4=0,value3=0; float
final_value =0.00;


#INT_EXT
void interrupt_1(){
  if(!input(PIN_B0))        // keep button action sychronized wth button flag
    {
      count++;


      if ((count % impulse_rate) == 0)
      {
        count_kwh++;            count_ghs =
count_kwh * tariff_kwh;
      }
    }
 clear_interrupt(INT_EXT);
}


#INT_EXT2
void interrupt_2(){
  if(!input(PIN_B2))        // keep button action sychronized wth button flag
    {
      ZC=1;


    }


 clear_interrupt(INT_EXT2);
} void
calc_phase()
{
  enable_interrupts(INT_EXT2);// turn on interrupts


  i = 0;    counter_zc =
0;    sum_phase_time =
0;    while(i < 5)
  {
    ds1307_get_time(hrs,am_pm,min,sec);
     if (ZC)
    {
      output_high(PIN_C2);
delay_ms(1);
output_low(PIN_C2);
ZC = 0;         counter_zc++;
      phase_time[counter_zc-1] = sec;
    }
i++;
  }


 for(j=0; j<(counter_zc-1); j++)
 {
    sum_phase_time = sum_phase_time + (phase_time[j+1] - phase_time[j]);
 }
```

```
 if(counter_zc > 0)
 {
  avg_phase_time = sum_phase_time/counter_zc;
 }

//!  printf(lcd_putc,"\fPhase Angle=%.2fs",avg_phase_time);

//!  delay_ms(16);
  disable_interrupts(INT_EXT2);// turn off interrupts INT2
}

void calc_current()
{    delay_ms( 8
);

   value = read_adc();

   delay_ms( 8 );

   value1 = read_adc();

   delay_ms( 8 );

   value2 = read_adc();

   value3 = (value + value1 +value2)/3;

   value4 = (value3 != 511)?((value3)-512): 0 ;

   final_value = 0.02450980392 *value4;

//!   printf(lcd_putc,"\fVoltage = %f V\r", final_value * 50 * 2.7);

//!   delay_ms(16);

   read_adc(ADC_START_ONLY);

//!   sleep();

   value=read_adc(ADC_READ_ONLY);

} void
main(){
   setup_adc_ports(      RA0_ANALOG      );
SET_TRIS_A(    0x9    );              setup_adc(
ADC_CLOCK_INTERNAL                    );
set_adc_channel(0);

   output_low(PIN_B0);
output_low(PIN_B1);    output_low(PIN_B2);
output_low(PIN_B3);    output_low(PIN_B4);
output_low(PIN_B5);    output_low(PIN_B6);
output_low(PIN_B7);

   SET_TRIS_B( 0x07 );
```

```
  output_low(PIN_C0);
output_low(PIN_C1);    output_low(PIN_C2);
output_low(PIN_C3);    output_low(PIN_C4);
output_low(PIN_C5);    output_low(PIN_C6);
output_low(PIN_C7);

  SET_TRIS_C( 0x00 );// set all ports on C as output


  ext_int_edge(H_TO_L);      // init interrupt triggering for button press
enable_interrupts(INT_EXT);// turn on interrupts

  ext_int_edge(2, H_TO_L);      // init interrupt triggering for button press ON INT2
disable_interrupts(INT_EXT2);// turn off interrupts INT2

  enable_interrupts(GLOBAL);

  ds1307_init();
  /// ds1307_set_date_time(day,mth,year,dow,hour,am_pm,min,sec)  Set the date/time
ds1307_set_date_time(31,12,13,7,11,1,59,45);    lcd_init();

  ds1307_get_time(hrs,am_pm,min,sec);
ds1307_get_date(day,mth,year,dow);



//initializing temporary values of the 24hour, dow,month,year
if(am_pm)
  {       time
='P';      if( hrs
< 12 )
    {          temp_hrs  = (hrs
+ 12) ;
    }
else
    {
       temp_hrs = hrs;
    }   }    else
{       time='A';
if( hrs == 12 )
{          temp_hrs
= 0 ;
    }
else
    {         temp_hrs
= hrs;
    }
  }

//!   temp_hrs = hrs;
temp_dow = dow;
temp_mth = mth;    temp_year
= year;

  while(true){

      ds1307_get_time(hrs,am_pm,min,sec);
      ds1307_get_date(day,mth,year,dow);
```

```
        if(am_pm)
        {            time
='P';           if( hrs
< 12 )
          {              hrs_24  =
(hrs + 12) ;
          }              else
{               hrs_24 =
hrs;
          }         }
else         {
time='A';            if( hrs
== 12 )           {
hrs_24  = 0 ;             }
else           {
hrs_24 = hrs;
          }
        }

    dow_switch:

        switch(dow)
        {



          case 1: week_day = "Monday";
                break;
          case 2: week_day = "Tuesday";
break;
          case 3: week_day = "Wednesday";
                break;
          case 4: week_day = "Thursday";
                break;
          case 5: week_day = "Friday";
                break;
          case 6: week_day = "Saturday";
                break;
          case 7: week_day = "Sunday";
                break;
default: dow = 1;
goto dow_switch;         }

        if(sec_cache!=sec){
          sec_cache=sec;


          printf(lcd_putc,"\f\%02d:\%02d:\%02d\ %02d-%02d-%02d \n%04d kWh %s\nGHs%.2g",
hrs_24,min,sec,day,mth,year,count_kwh,week_day, count_ghs);           delay_ms(16);


          if(hrs_24 != temp_hrs)
          {
            energy_hrs[hrs_24]= count_kwh; //Energy consumed by this hour
if(hrs_24 > 0)
            {
              prev_consum_hrs = energy_hrs[hrs_24] - energy_hrs[hrs_24-1];
            }
else
{
              prev_consum_hrs = energy_hrs[0] - energy_hrs[23];;
            }
```

```
            total_energy_hrs = 0;
            hrs_counter = 0;

            if((energy_hrs[0])>0)
            {
              if(energy_hrs[0] - energy_hrs[23])
              {
                total_energy_hrs += (energy_hrs[0] - energy_hrs[23]);
hrs_counter++;
              }

            }

            for(i = 1; i < 24 ; i++)
            {
              if((energy_hrs[i])>0)
              {
                if(energy_hrs[i] - energy_hrs[i-1])
                {
                  total_energy_hrs += (energy_hrs[i] - energy_hrs[i-1]);
hrs_counter++;
                }
              }
            }

            if(hrs_counter > 0)
            {
              avg_energy_hrs = total_energy_hrs/hrs_counter;
            }

            calc_phase();
calc_current();
temp_hrs = hrs_24;
          }

          if(dow != temp_dow)
          {
            energy_dow[dow - 1]= count_kwh; //Energy consumed by this day of the week
if(dow > 1)
            {
              prev_consum_dow = energy_dow[dow - 1]  - energy_dow[dow - 2];
            }
            else
            {

              prev_consum_dow = energy_dow[0] - energy_dow[6];
            }

            total_energy_dow = 0;
dow_counter = 0;

            if((energy_dow[0])>0)
            {
              if(energy_dow[0] - energy_dow[6])
              {
                total_energy_dow += (energy_dow[0] - energy_dow[6]);
                dow_counter++;
              }
```

```
        }

        for(i = 1; i < 7 ; i++)
        {
          if((energy_dow[i]) >0)
          {
            if(energy_dow[i] - energy_dow[i-1])
            {
              total_energy_dow += (energy_dow[i] - energy_dow[i-1]);
dow_counter++;
            }
          }
        }


        if(dow_counter > 0)
        {
          avg_energy_dow = total_energy_dow/dow_counter;
        }



        temp_dow = dow;

      }
      if(mth != temp_mth)
      {
        energy_mth[mth-1]= count_kwh; //Energy consumed by this month

if(mth > 1)
        {
          prev_consum_mth = energy_mth[mth-1] - energy_mth[mth-2];
        }
else
{
          prev_consum_mth = energy_mth[0] - energy_mth[11];
        }



        total_energy_mth = 0;
        mth_counter = 0;


        if((energy_mth[0])>0)
        {
            if(energy_mth[0] - energy_mth[11])
            {
              total_energy_mth += (energy_mth[0] - energy_mth[11]);
mth_counter++;
            } }

        for(i = 1; i < 12 ; i++)
        {
          if((energy_mth[i])>0)
          {
            if(energy_mth[i] - energy_mth[i-1])
            {
              total_energy_mth += (energy_mth[i] - energy_mth[i-1]);
mth_counter++;
            }
```

```
        }
      }


      if(mth_counter > 0)
      {
        avg_energy_mth = total_energy_mth/mth_counter;
      }

      temp_mth = mth;
    }

    if(year != temp_year)
    {
      energy_year[year_counter_index]= count_kwh; //Energy consumed by this year

      array_of_years[year_counter_index]= year;

      if(year_counter_index > 0)
      {
        prev_consum_year = energy_year[year_counter_index] - energy_year[year_counter_index-1];
      }
else
{
        prev_consum_year = energy_year[0] - energy_year[9];
      }

      total_energy_year = 0;
      year_counter = 0;

      if((energy_year[0])>0)
      {
        if(energy_year[0] - energy_year[9])
        {
          total_energy_year += (energy_year[0] - energy_year[9]);
year_counter++;
        }

      }

      for(i = 1; i < 10 ; i++)
      {
        if((energy_year[i])>0)
        {
          if(energy_year[i] - energy_year[i-1])
          {
            total_energy_year += (energy_year[i] - energy_year[i-1]);
year_counter++;
          }

        }
      }


      if(year_counter > 0)
      {
        avg_energy_year = total_energy_year/year_counter;
```

```
            }

            if(year_counter_index < 9)
            {
              year_counter_index++;   // if index is between 0-8 keep increasing by one
            }
else
            {
              year_counter_index = 0; //if index is 9 reset ie. the tenth year
            }

            temp_year = year;
          }

          if(avg_energy_hrs > 0)
          {
            printf(lcd_putc,"\fConsumptn/Prev Hour\n%07d kWh \nGHs%.2g",prev_consum_hrs,prev_consum_hrs *
tariff_kwh);
            delay_ms(16);

            printf(lcd_putc,"\fAvg Consumption/Hour\n%07.0g kWh
\nGHs%.2g",avg_energy_hrs,avg_energy_hrs*tariff_kwh);
delay_ms(16);
          }
//!
          if(avg_energy_dow > 0)
          {
            printf(lcd_putc,"\fConsumptn/Prev Day\n%07d kWh
\nGHs%.2g",prev_consum_dow,prev_consum_dow*tariff_kwh);
delay_ms(16);

            printf(lcd_putc,"\fAvg Consumption/Day\n%07.0g kWh
\nGHs%.2g",avg_energy_dow,avg_energy_dow*tariff_kwh);
delay_ms(16);
          }
//!
          if(avg_energy_mth > 0)
          {
            printf(lcd_putc,"\fConsumptn/Prev Mth\n%07d kWh
\nGHs%.2g",prev_consum_mth,prev_consum_mth*tariff_kwh);
delay_ms(16);

            printf(lcd_putc,"\fAvg Consumption/Mth\n%07.0g kWh
\nGHs%.2g",avg_energy_mth,avg_energy_mth*tariff_kwh);
delay_ms(16);
          }
//!
          if(avg_energy_year > 0)
          {
            printf(lcd_putc,"\fConsumptn/Prev Yr\n%07d kWh \nGHs%.2g",prev_consum_year,prev_consum_year *
tariff_kwh); //display this when the year is the ONLY changing factor              delay_ms(16);

            printf(lcd_putc,"\fAvg Consumption/Yr\n%07.0g kWh
\nGHs%.2g",avg_energy_year,avg_energy_year*tariff_kwh);
delay_ms(16);
          }
//!
          if(counter_zc > 0)
          {
            printf(lcd_putc,"\fPhase Angle=%.2fs",avg_phase_time);
delay_ms(16);
```

```
        }

        if(final_value > 0)
        {
          printf(lcd_putc,"\fVoltage = %f V\r", final_value * 50 * 2.7); // 50 is the rate of ac to dc i.e 250V ac = 5v dc, 2.7 is
the rating of the resistor
          delay_ms(16);
        }

        printf(lcd_putc,"\fCurrent Tariff \n1 kWh = GHs%.2g", tariff_kwh);
delay_ms(16);
      }
  } }
```

APPENDIX B: C++ CODE FOR RETROFIT IMPLEMENTATION

```
#include <LiquidCrystal.h>
#include <SoftwareSerial.h>

LiquidCrystal lcd (13,12,11,10,9,8); int
count = 0;

long previousMillis = 0;        // will store last time LED was updated

// the follow variables is a long because the time, measured in miliseconds, //
will quickly become a bigger number than can be stored in an int.

long interval = 300000;          // interval at which to blink (900000 milliseconds) which is equivalent to 15 minutes

String Time;                    // stores the time
char dLine[50];                  // temporal character array
SoftwareSerial mySerial(7, 8);    // for communicating with the gsm module

float voltage = 0;

void setup() {
  // put your setup code here, to run once:
mySerial.begin(19200); // the GPRS baud rate
Serial.begin(19200); // the GPRS baud rate
  attachInterrupt(0,countBlink, RISING);  //options are FALLING RISING LOW CHANGE
lcd.begin (40,2);
}

void loop() {
  // put your main code here, to run repeatedly:
unsigned long currentMillis = millis();
  if(currentMillis - previousMillis > interval)
  {
      // save the last time you blinked the LED
previousMillis = currentMillis;          setClock();
      mySerial.println("AT+CSQ");
      delay(100);
      ShowSerialData();// this code is to show the data from gprs shield,
      //in order to easily see the process of
      //how the gprs shield submit a http request, and the following is for this purpose too.
      mySerial.println("AT+CGATT?");
delay(100);       ShowSerialData();
      mySerial.println("AT+SAPBR=3,1,\"CONTYPE\",\"GPRS\"");//setting the SAPBR, the connection
      //type is using gprs
delay(1000);       ShowSerialData();
      mySerial.println("AT+SAPBR=3,1,\"APN\",\"internet\"");//setting the APN,
      //the second need you fill in your local apn server
delay(4000);       ShowSerialData();
      mySerial.println("AT+SAPBR=1,1");//setting the SAPBR, for detail you can refer to
      //the AT command mamual
      delay(2000);
ShowSerialData();



      mySerial.println("AT+HTTPINIT"); //init the HTTP request
delay(2000);         ShowSerialData();
```

```
      mySerial.print("AT+HTTPPARA=\"URL\",\"");// setting the httppara, the second parameter is the website you want to access
//
mySerial.print("http://anamens.myfirebook.com/api/read?deviceid=11223344&read=15%2F02%2F28%2C22%3A00%3A00%2B00&power=50&level=70&temperature=24&status=1");
//
mySerial.print("http://159.203.118.203/read?device_id=qqq&pulse_count=1&power=1&status=1&tamper=1&voltage=20.2&connected=1&read=15%2F12%2F30%2C09%3A21%3A48%2B0100");
//      mySerial.print("http://anamens.myfirebook.com/api/read?deviceid=");
mySerial.print("http://159.203.118.203/read?device_id=");
mySerial.print("1345218967");       mySerial.print("&pulse_count=");
mySerial.print(count);       mySerial.print("&power=");
mySerial.print("1");
     mySerial.print("&status=");
mySerial.print("0");
mySerial.print("&tamper=");
mySerial.print("0");
mySerial.print("&voltage=");          voltage
= random (215,240);
mySerial.print(voltage);
     mySerial.print("&connected=");
mySerial.print("1");
mySerial.print("&read=");
     mySerial.print(Time);


//       mySerial.print(tankID[i][j]);
//       mySerial.print("&device_id=");
//       mySerial.print(tankID[i][j] );
//       mySerial.print("&reading_timestamp=");
//       mySerial.print(Time);
//       mySerial.print("&power_level=");
//       mySerial.print(power_level);
//       mySerial.print("&level_reading=");
//       mySerial.print(tankLevel);
//       mySerial.print("&temperature_reading=");
//       mySerial.print(temperature_reading);
//       mySerial.print("&power_status=");
//       mySerial.print(power_status);


      mySerial.println("\"");
delay(1000);


      ShowSerialData();


      mySerial.println("AT+HTTPACTION=0");//submit the request as GET        delay(10000);//the delay is very important, the delay time is base on the return from the website, if the return datas are very large, the time required longer.
      //while(!mySerial.available());


      ShowSerialData();


      mySerial.println("AT+HTTPREAD");// read the data from the website you access
delay(300);


      mySerial.println("");
delay(100);
      Serial.println("Done");


//       Serial.print("http://anamens.myfirebook.com/api/read?deviceid=");
     Serial.print("http://159.203.118.203/read?device_id=");
     Serial.print("1345218967");
```

```
      Serial.print("&pulse_count=");
      Serial.print(count);
      Serial.print("&power=");
      Serial.print("1");
      Serial.print("&status=");
      Serial.print("0");
      Serial.print("&tamper=");
      Serial.print("0");
      Serial.print("&voltage=");
      Serial.print(voltage);
      Serial.print("&connected=");
      Serial.print("1");
      Serial.print("&read=");
      Serial.print(Time);

  }
}

void countBlink()
{
count++;
  Serial.println("detected");
Serial.println(count);
lcd.clear();   lcd.setCursor(0,0);
  lcd.print(count);

}

void setClock()
{
  getTime_firebook();
  String timeTrim = Time.substring(29,49);

  Serial.println("");
  Serial.println("Time is ");


  Serial.println("");
  Serial.println("Time String:");
  Serial.println(timeTrim);
  Serial.println("");

  delay (2000);

  mySerial.print("AT+CCLK=\"");
mySerial.print(timeTrim);
mySerial.println("\"");   delay(1000);
  ShowSerialData();

  delay (5000);
  mySerial.println("AT+CCLK?");
  delay(1000);
ShowSerialData();
delay(1000);   reformatTime();
}

void getTime_firebook()
{
mySerial.println("AT+CSQ");
```

```
  delay(100);
  ShowSerialData();// this code is to show the data from gprs shield,
  //in order to easily see the process of
  //how the gprs shield submit a http request, and the following is for this purpose too.
  mySerial.println("AT+CGATT?");
  delay(100);
ShowSerialData();
  mySerial.println("AT+SAPBR=3,1,\"CONTYPE\",\"GPRS\"");//setting the SAPBR, the connection
  //type is using gprs
delay(1000);   ShowSerialData();
mySerial.println("AT+SAPBR=3
,1,\"APN\",\"internet\"");//setting
the APN,
  //the second need you fill in your local apn server
delay(4000);   ShowSerialData();
  mySerial.println("AT+SAPBR=1,1");//setting the SAPBR, for detail you can refer to
  //the AT command mamual
  delay(2000);
ShowSerialData();



  mySerial.println("AT+HTTPINIT"); //init the HTTP request
delay(2000);    ShowSerialData();

   mySerial.print("AT+HTTPPARA=\"URL\",\"");// setting the httppara, the second parameter is the website you want to
access    mySerial.println("http://anamens.myfirebook.com/api/time\""); //
mySerial.println("http://68.169.63.63/meter/getTime.php\"");

   delay(10000);

   ShowSerialData();

   mySerial.println("AT+HTTPACTION=0");//submit the request as GET    delay(20000);//the delay is very important,
the delay time is base on the return from the website, if the return datas are very large, the time required longer.

   ShowSerialData();

   mySerial.println("AT+HTTPREAD");// read the data from the website you access

   delay(2000);

 //  ShowSerialData();
storeTime();
 //  setTime();
 //  checkForResponse();

   mySerial.println("");
Serial.println("");
   delay(100);

   Serial.println("Done");

}

void reformatTime()
{
 Time = "" ;
 Serial.println("reformatting the time");
```

```
  mySerial.println("AT+CCLK?");
  delay(300);
  checkForResponse_1();

  for(int i=20; i<40;i++)
  {
    Serial.print(dLine[i]);
    Time = Time +  dLine[i];
  }

  Serial.println("");
  Serial.println("Time String:");
  Serial.println(Time);
  Serial.println("");

//  Time = 20 + Time;

  Serial.println("");
  Serial.println("New 20 Time String:");
  Serial.println(Time);
  Serial.println("");

//  Time.replace("/", "-");
//  Time.replace(",", "+");
  Time.replace(":", "%3A");
  Time.replace("+", "%2B");

  Serial.println("");
  Serial.println("New Server Time String:");
  Serial.println(Time);
  Serial.println("");
}



void storeTime()
{   char var ;  Time = "";
while(mySerial.available()!=0)
// Serial.write(mySerial.read());
 {
   var = mySerial.read();
   Time = Time + var;
 }

  Serial.println("This is the output");
  Serial.println(Time);

}

void checkForResponse_1(){ //this part for text parsing and processing. get 10101010 from //
the website and parse it.

    memset(dLine, '\0', 50);
 Serial.println("Checking response");

// while(mySerial.available()!=0)
// {
//
```

```
//   for (int i = 0; i < 50; i++)
//   {
//     dLine[i] = mySerial.read();
//
//     Serial.print(dLine[i]);
//   }
//    // }
int k = 0;
 while(mySerial.available()!=0)
 {


    dLine[k] = mySerial.read();


    Serial.print(dLine[k]);
k = k + 1;


 }
}

void ShowSerialData()
{
while(mySerial.available()!=0)
Serial.write(mySerial.read()); }
```