BUSITEMA UNIVERSITY
FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTER ENGINEERING

PREPAID ENERGY METER TAMPER NOTIFICATION SYSTEM

By
Opio Isaac
BU/UG/2012/2032
0700420726 / 0784807453
isaacop04@gmail.com

SUPERVISOR:
Mr. ODONGTOO GODFREY

A Project Report submitted to the Department of Computer Engineering in partial fulfillment of the requirements for the Degree of Computer Engineering of Busitema University.

May, 2016

DECLARATION

This Project report is my original work and has not been presented for a degree in any other University or any other award.

Sign: ……

Date: ……

APPROVAL

The undersigned certify that they have read and hereby recommend for acceptance of Busitema University a Project report entitled “Prepaid Energy Meter Tamper Notification System”.

Mr. Odongtoo Godfrey

Department of Computer Engineering

Sign:…….

Date:…….

DEDICATION

This work is with sincere affection and gratitude dedicated to my dearest mother, Imat Helene Mutu and all the family members whose efforts have seen me this far. I thank you all for facilitating me financially, socially, morally throughout my education. I am immensely overwhelmed by the love you have always shown me.

ACKNOWLEDGEMENT

To the Almighty God, I appreciate the unending love and strength you have always given me to withstand all my endeavors.

I'm so grateful for the supervision by Mr. Odongtoo Godfrey and entire staff of Department of Computer Engineering, Busitema University for the knowledge, guidance and support during the preparation of this report and throughout my academic period at Busitema University.

Finally, I would like to acknowledge and appreciate all my friends and colleagues whom we worked together to acquire the best from the University.

ABSTRACT

The prepaid Meter tamper notification system is a system prototype designed to detect the tampers with the smart electric energy meter. The prototype combines tamper detection module that consist of the capacitive touch sensor, light dependent resistor as the light sensor and tilt sensor with an Atmel chip the 8-bit ATMega-328PU microcontroller in 28 pin DIP package, with double flash space and relay switch that automatically switches off the residence in case of tamper detection. The SIM900 GSM Modem is used to send notifications to the nearest utility supervisor/manager about what happens in real-time where the meter is installed and LCD- JHD162A model to display the meter status. The overall objective of this project is to reduce on the power distribution losses incurred by the Utility companies due to energy meter tampering in a remote locations where they are installed. This project was therefore aimed at developing a GSM based system that would solve the above problem through the following ways; monitoring and detecting the physical tampers on the meter installed at a residence and then automatically cutoff power in case of tamper, notifications to the responsible person(s) about the state of meter at home. The work is arranged mainly in six chapters, Chapter one includes the introduction of a prepaid meter tamper notification system. Chapter two discusses the literature related to the system, Chapter three illustrates the methodologies used in coming up with the working prototype of the system, Chapter four includes system design and analysis, Chapter five is contains the implementation and testing of the system and chapter six contains the summary of the work, discussions and recommendations.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AC/DC	Alternating Current/Direct Current
AMR	Automatic Meter Reading
CT	Current Transformer
ETSI	European Telecommunications Standard Institute
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
ICT	Information and Communication Technology
ID	Identification
IDE	Integrated Development Environment
LED	Light Emitting Diode
LDR	Light Dependent Resistor
PUB	Public Utility Board
RISC	Reduced Instruction Set Computer
RTC	Real Time Clock
SMS	Short Messaging Service
V_{DD}	Supply Voltage
VSM	Virtual System Modelling
WAP	Wireless Application Protocol
WAMR	Wireless Automatic Meter Reading
PEMNS	Prepaid Energy Meter Notification System

CHAPTER ONE
INTRODUCTION

This chapter gives an introduction that led to the proposal of Prepaid Energy Meter Tamper Notification System. It is composed of the following subsections: the background of the project, problem statement, objectives of the proposed project, significance/justification and the scope to cover a while designing the project.

1.1 Background

Due to the increasing cost of electricity, energy theft is becoming a major concern for Utility providers across the globe [12, 26]. In utility metering applications, the hacker might want to extract information and/or modify the internal settings in order to manipulate the system settings. Many of these methods include tweaking the time so as to fool the system. Electricity distribution companies may have different billing rates depending on time of the day, maximum demand, load, etc., thus requiring the real time clock (RTC) to provide accurate time reference. One may tamper the clock or manipulate the time to fool the system so as to charge differently, e.g. changing PM to AM such that metering firmware charges less due to nonpeak load tariff during the changed time. The RTC usually relies on a 32.768 kHz external crystal oscillator [15, 16], and a hacker may change the RTC crystal to slow it down so as to count less, thus introducing inaccuracies in measurement and billing. A large portion of these revenue losses can be recovered by installing electronic energy meters because they can detect tamper conditions and assure proper billing, unlike electromechanical meters [8]. However, a delay in tamper awareness can also increase the magnitude of the loss in such meter settings. Additionally, as these meters become networked with the introduction of advanced metering technologies like AMR or smart grid in developed world, utility companies will benefit by automatically knowing any tampering events that might happen remotely [6].

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

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

As a company, UMEME expects to address some challenges like poor payment of electricity bills, current high cost of billing as well as create an opportunity for easier monitoring of consumers' meters and energy consumption. It was also anticipated that this new system will reduce the fraud that has been largely peddled by illegal electricity technicians who prey on unsuspecting customers by extorting money out of them under the guise of disconnecting and reconnecting them. By the first half of 2013, the company had 32,000 customers converted to the pre-paid Yaka system a number that is likely to have doubled by the close of 2014 [11].

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

Governments globally are rooting for Smarter metering systems in order to encourage better and sustainable usage of the limited electricity energy available. This has led to a sudden boom in the production of smart meters as utility companies are buoyed to take on this direction in response to Government support [7].

However, these smart meters are vulnerable and subject to tampering by intruders with the wrong intentions. The lack of proper security controls can make them susceptible to attacks [4,29]. Now hackers have the ability to carry out billing related fraud and shutdown electricity supplies at will. By accessing their memory chips, one can carry out some re-programming as well as exploit any flawed code there-in to tamper with meter readings, transfer readings to other customers as well as insert network worms that can potentially leave entire neighborhoods in a blackout [5]. This is easily achievable if one takes control of the meter box since they can switch its unique ID to mimic another customer's or use it to launch attacks on the network [3].

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

false data. Other flaws these meters are likely to have are shared IDs like factory default passwords and poor protection from tampering.

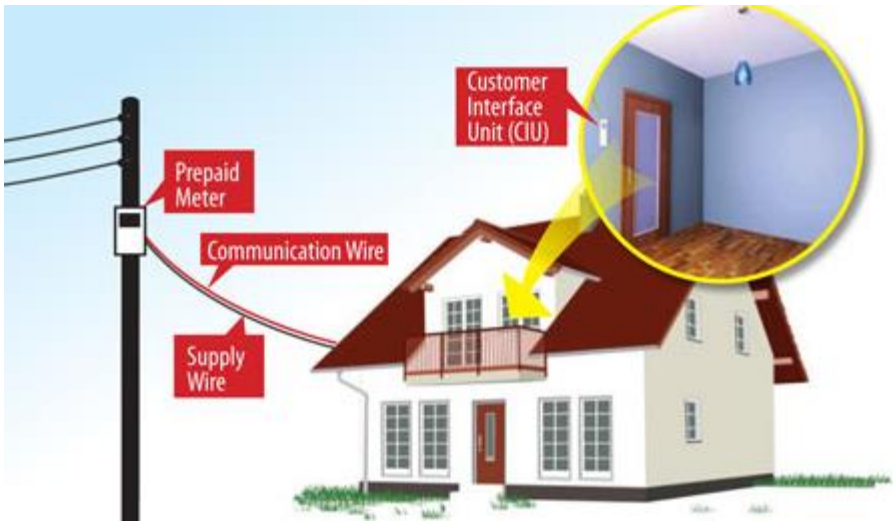

Figure 1: Showing prepaid metering layout[7]

1.2 Problem Statement

Energy theft and meter tampering for prepaid meter systems is a nation-wide problem that contributes heavily to revenue losses. Consumers have manipulated/tampered with their electric meters in order to stop or under-register the power usage within their premises. Since these devices are not strong enough to tolerate tampers and secure enough to handle sensitive information about the consumer, there is a need for a monitoring strategy of such facilities from the utilities' company side.

1.3 Objectives:

To develop a Prepaid energy meter tamper notification for Yaka systems.

1.4 Specific objectives:

i. To investigate literature on the prepaid meter tampering techniques used in both domestic and industrial/commercial power usage settings.
ii. To identify the requirements necessary to design the wireless energy meter tamper notification system
iii. To design the system
iv. To implement the tamper notification system.
v. To test and validate the designed system.

1.5 Justification:

Pre-paid energy meters have not fully addressed the issues of energy theft since a master meter is used to automate the billing process and with the utility controlling relay switch remotely to disconnect/connect electricity supply from a computer terminal.

Lack of proper security controls features to detect tampers in Yaka energy meters necessitates the development of a system that detects tampers in real time and notifies the area manager about what happens.

1.6 Significance:

UMEME-the utility company will benefit by automatically knowing any tampering events that might happen remotely.

Also the presence of an anti-tamper alarm will be a preventive approach to scare hackers from continuing with the bad act. Consequently, the company will lower the losses due to electricity theft.

1.7 Scope:

The project consist of the system prototype for a Prepaid Energy meter tamper notification system. The device shall be based on an 8-bit RISC Atmel ATMEGA328P-PU microcontroller interfaced with a SIM900 GSM module to provide remote notification by SMS. The device is able to detect tamper by sensing meter touch and light exposure of internal parts and automatically switches OFF the residence using a Relay switch.

1.8 Assumptions

i. Tampers can never be done in total darkness.
ii. The good network coverage in the areas where the meter is installed.
iii. The employees are loyal and can never connive with the customers in tampering.
iv. The system is abstract to the end users.
v. Tampers can never be done using a non-conducting materials (applies to touch sensor only).
vi. Every household has its individual energy meter.

1.9 Limitations of the system

i. The system is limited to monitor and detect the physical tampers on the energy meter and notify the nearest person available.

ii. The poor network coverage in some areas in the country may limit the remote notifications in real-time by the GSM.

REFERENCES:

[1] J. Wire, "*Is UMEME's Yaka Smart Metering a time bomb?",* The New Vision, 2014. [Online]. Available: http://newvision.co.ug [Accessed: 11- Sep- 2015].

[2] FBI, "*Smart Electric Energy meters altered to steal electricity*", 2010. [Online]. Available: http://fbi.gov/cybercrime. [Accessed: 27- Aug- 2015].

[3] Patriot & Paulies (Editors), "*5 Hacks that render Smart Meters dumb*", 2012. [Online]. Available: http://patriotandpaulies.wordpress.com. [Accessed: 16- Aug- 2015].

[4] T. Leautier, "*Is Mandating "Smart Meters" Smart?", EJ*, vol. 35, no. 4, 2014. [Accessed 04-Sep-2015]

[5] D. Baker, "*Malware based Smart meters' attack*", *Ioactive.com*. Available: http://www.ioactive.com [Accessed: 08- Oct- 2013].

[6] H. M. Zahid Igbal, M. Waseem and Dr. Tahir Mahmood," *Automatic Energy Meter Reading using Smart Energy Meter*", International Conference on Engineering & Emerging Technologies (ICEET), Superior University Lahore, 20th March 2014 to 21st March 2014 [Accessed 17-Aug-2015]

[7] S. Arun and Dr. Sidappa Naidu, "*Hybrid Automatic Meter Reading System*", ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, pp. 361-365, 2012.

[8] Depuru, S .S, Wang,L., Devabhaktuni, V., " *Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft*", Energy Policy. 39, 1007–1015 (2011)

[9] Kasita, I., "*UMEME starts pre-paid power billing*", The New Vision, Kampala (2011). http://www.newvision.co.ug [Accessed: 28-Jul-2015]

[10] Muneza, S., "*Umeme Seeks Help To Cut Electricity Theft*", The Red pepper, Kampala, Uganda, (2014). http://www.redpepper.co.ug [Accessed: 28-Jul-2015]

[11] LADU, I. M., "*Umeme to install 16,000 pre-paid meters*", Daily Monitor, Kampala (2014). http://www.monitor.co.ug [Accessed: 28-Jul-2015]

[12] Ssekika,, "*Uganda loses Shs 76bn annually to power theft*", The Observer, Kampala, Uganda, (2013). http://observer.ug [Accessed: 28-Jul-2015]

[13] N. Wesonga, "*Umeme in bid to reduce power distribution losses*," Daily Monitor,

Kampala, Uganda,(2012). [Accessed: 27-Jun-2014]

[14] Ashna. K, Sudhish N George, "*GSM Based Automatic Energy Meter Reading System with Instant Billing*", 978-1-4673-5090-7/13©2013 IEEE, pp. 65-71.

[15] Marvin E. Ferking, "*Crystal Oscillator Design and Temperature Compensation"*, Van Norstrand Reinhold Company, New York, 1978.

[16] Benjamin Parzen, "*Design of Crystal and other Harmonic Oscillators"*, John Wiley and Sons, Inc., New York, 1983.

[17] Jawarkar, N. P., Ahmed, V., Ladhake, S. A. & Thakare, R. D. (2008). "*Micro-controller based Remote Monitoring Using Mobile through Spoken Commands*", Journal of Networks, 3(2), 58-63, Accessed 4th August 2015.

[18] Jubi.K, MareenaJohn, "*Prepaid Energy Meter with GSM Technology*", AIJRSTEM, pp. 195- 98, June-August, 2015.

[19] Dr. K. Sheelasobanarani1, S. Dinesh Raja2, B. Dhanaraj3, K. Manickam4, K. KarthickRaja5. "*A Prepaid Energy meter for efficient Power Management*", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, July 2015

[20] Bharat Indorey, M.Lokhande, "*ZigBee Based Advanced Energy Prepaid Meter*", International Journal of Innovations in Engineering and Technology (IJIET), Volume 3 Issue3 July 2015

[21] Private Mobile Networks, "*The SMS Technology*", The Global Telecom Insight, Aug, 2012 http://www.mobilecomms-technology.com, Retrieved August, 2015

[22] D. Tom Tamarkin, "*Automatic Meter Reading*", Public Power Magazine, vol. 50, pp. 5. Sept-Oct 2015

[23] Dr.Boyina.S. Rao, B. Gnanasekaranathan, M. Raguram, S. Pravinkumar, P. Kamalesh, "*Domestic Prepaid Energy Distribution System for saving of Power Consumption*",IJAET/Vol.III/ Issue II/April- June, 2015/26-29.

[24] Anton A.Huurdemann, "*The world wide history of telecommunication*", John Wiley & Sons, pp. 529, 31 Jul 2015

[25] GSM, "*GSM Global System for Mobile Communications*", 4G Americas, retrieved 2015-09-22

[26] World Bank, "*Power Sector Issues And Options*", Honduras,2007 [Accessed: 06-11-2015]

[27] K. Ardis,"*Attacks on Smart Meter that don't involve hacking over network*", Smart Grid News, Jul 2014, http://SmartGridNews.com [Accessed: 08-11-2015]

[28] Umeme, O. Stephen, "*Manufacturers vandalize the prepaid meters*", Daily Monitor, Kampala, Uganda, 2016. [Accessed: 03-03-2016]