A Framework for Monitoring Electricity theft in Zimbabwe using Mobile Technologies

Samuel Musungwini

Midlands State University
Gweru, Zimbabwe

musungwinis5@gmail.com

DOI: 10.20470/jsi.v7i3.259

Abstract: *The capabilities of mobile technology paradigm have indicated that almost every infrastructure, system or device has the potential to capture data and report it to the back-end system in real-time. Utilities need to deliver operational analytics by knowing what is happening across their entire infrastructure. The purpose of the study was to develop a framework for mobile technologies in monitoring electricity theft in Zimbabwe. Using a qualitative research in conjunction with the design science paradigm, data was collected through semi-structured interviews, participant observation, document review and qualitative questionnaire. The findings of the study revealed that the power utility in Zimbabwe uses very basic methods and techniques in detecting and countering electricity theft. This has made it difficult to deal with all the possible electricity theft strategies that are employed by the consumers. This study recommends that the power utility in Zimbabwe should use a framework for mobile technologies to monitor electricity theft in order to reduce revenue leakages caused by electricity theft.*

Key words: Mobile technology, Framework, Electricity theft, USSD, Design Science, Prepaid metering, Post paid metering.

1. Introduction

Mobile technologies have introduced a profound change in the world of computing due to its dramatic expansion in the digital arena. This technology allow actions and operations to create a high degree of real-time data to enhance a competent organisation (Accenture, 2013). Various types of mobile technologies exist in the mobility arena (Gartner, 2012), with different communication capabilities and characteristics which include speed, range, location, etc. Due to the capabilities of mobile technology paradigm, previous studies have indicated that almost every infrastructure, system or device has the potential to capture data and report it to the back-end system in real-time (Morales & Palma, 2010).

Utilities need to deliver operational analytics by knowing what is happening across their entire infrastructure (Pandey, Gill, & Sharma, 2013). This includes insight on faults, anomaly events, and capacity usage, configuration states and security states. This will enable effective monitoring of serviceability, usage, changes in configurations and security tracking of infrastructure. Mobile technology is slowly being adopted to support monitoring systems and remote control by providing real-time information on usage, security and physical state of the devices, equipment or infrastructure. The growth in the use of mobile technologies in monitoring systems will increase the value of data being captured within each system connected (Morales & Palma, 2010). This technology will let many organisations transcend remote control and monitoring issues for faster decision making and eliminate too much human involvement or interventions.

2. Background

The world over it is a norm that there is one electricity Power Company and Zimbabwe is no exception. The power utility is the sole distributor and provider of electricity in Zimbabwe.

Its core business is the transmission and distribution of electricity for domestic, commercial and maximum demand consumers. Over the past years, consumers would pay for electricity after use, i.e. post-paid. In 2012, the Zimbabwe Power utility company carried out a business decision to change from post-paid to prepaid electricity metering system because of the advantages it offers (ZETDC Business Document, 2012). Being result oriented towards electricity efficiency and proper management of distributed electricity has been the key driver behind the prepaid electricity metering system in first world countries. To some extent, the problems encountered in trying to recover electricity debt have forced the installation of these systems, especially in the United Kingdom (UK) (Jain & Bagree, 2011; Malama et al., 2014).

However, in third world countries Zimbabwe included, the driver to migrate to prepaid electricity metering system was the need for revenue protection of power utilities and high administrative costs of billing postpaid consumers in both urban and rural areas. Prior to the introduction of the prepaid electricity meters, ESKOM, South Africa's power utility had observed that servicing rural areas under the postpaid billing system implied high administrative costs (Malama et al., 2014). This was further complicated by the absence of personal physical addresses to send the electricity bills to the consumers. Most consumers in rural areas rely on postal addresses for business centers and schools. ESKOM has inspired other power utilizes across the world to consider the adoption of the prepaid electricity metering system because of its benefits as compare to postpaid metering systems (Quayson-Dadzie , 2012).

In Zimbabwe, a prepaid electricity metering system was launched in 2012 for both domestic and commercial consumers to replace the conventional post-paid meters and estimation billing (Megawatt Bulletin, 2012). The concept of prepayment is built around paying before using a product or service. Prepayment systems provide a disbursement for goods and services before consumption or use (Casarin & Nicollier, 2010). In the context of electricity distribution, the aspect of prepayment calls for the consumers to hold electricity credit on their accounts (Miyogo, Ondieki & Nashappi., 2013). The consumer can only use electricity as a commodity or service when the account is paid up in advance. Prepaid electricity metering system enables consumers to purchase electricity prior to use from the electricity utility in the form of a token charged in KWh units (Pabla, 2008). The buying of electricity is done before consumption is made.

However, the installation of prepaid electricity metering system has seen the power utility being deprived of millions of dollars by the consumers who have found ways to steal from prepaid electricity meters. The power utility is losing about US$10 million a month in revenue from electricity theft (Share, 2014). Electricity theft has also seen the country experiencing more loads shedding than ever in recent months, because the power utility cannot raise enough revenue for continuous electricity generations. The system was introduced without proper feasibility study to check the polarity of the prepaid electricity meters, hence, the consumers tampering with the system.

The power utility has reacted to electricity theft by introducing a Revenue Protection Unit (RPU) to conduct field inspections/checks, investigate and report consumers engaging in electricity thefts. Farawo & Towindo (2013) reported that the power utility now offers monetary incentives as a way to persuade consumers to provide information about electricity theft. Since it is laborious to monitor all the current 900 000 and more prepaid electricity meters to be installed by means of field checks/inspection, there is need to protect the system and ensure the security of the installed infrastructure (prepaid electricity meter) so as to yield projected revenues for the investments made.

A real-time electricity power theft monitoring and detecting system needs to be created with a well-built end-to-end monitoring capabilities between the power utility and the consumers. The system should monitor the infrastructure and report any unexpected event detected/noticed during observation. The system should act as an observer and provide instant report to the back-end system of any infrastructure that has been disjoined from the power utility's electricity grid system. Hence, this study aims to propose a solution for the effective and efficient monitoring of electricity theft from the recently introduced prepayment electricity system.

3. Prepayment System business case

The concept of prepayment is built around paying before using a product or service. Prepayment systems provide a disbursement for goods and services before consumption or use (Casarin & Nicollier, 2010). In the context of electricity distribution, the aspect of prepayment calls for the consumers to hold electricity credit on their accounts (Miyogo, Ondieki & Nashappi., 2013). Being result oriented towards electricity efficiency and proper management of distributed electricity has been the key driver behind the prepaid electricity metering system in first world countries (Jain & Bagree, 2011; Malama et al., 2014). However, in third world countries particularly Zimbabwe, the driver to migrate to prepaid electricity metering system was the need for revenue protection of power utilities and high administrative costs of billing postpaid consumers in both urban and rural areas. Prior to the introduction of the prepaid electricity meters, ESKOM, South Africa's power utility had observed that servicing rural areas under the postpaid billing system implied high administrative costs (Malama et al., 2014). ESKOM has inspired other power utilities across the world to consider the adoption of the prepaid electricity metering system because of the benefits such as reduced operational costs, reduced consumer debt and responsible use of electricity (Quayson-Dadzie , 2012), (Tuckova, Novak, 2016).

4. Challenges in Prepaid Electricity Metering System

Electricity theft in prepaid metering system is one of the new challenges confronting the power utilities. It has become a world-wide concern in the transmission and distribution supply of electricity, more so in recent years where most utilities are adopting prepaid electricity metering systems (Pandey et al., 2013; Selvapriya, 2014). Most developing countries are estimated to be losing between 20% and 45% of revenue through electricity theft (SARPA, 2013), while those in the developed world loses between 3.5% and 30% (Balasubramanya, 2014). The estimated losses run from the period 2008 to 2014.

One of the challenges in preventing electricity theft is the difficulty in detecting the actual location of electricity theft in real-time (Tasdoven, Fiedler & Garayev, 2012). A real-time electricity power theft monitoring and detecting system needs to be developed with a well-built end-to-end monitoring capabilities between the power utility and the consumers. The system should monitor the prepaid meter and report any unexpected event detected during observation. The system should act as an observer and provide instant report to the back-end system of any meter that has been disjoined from the power utility's electricity grid system. Hence, this study aims to propose a solution for the effective and efficient monitoring of electricity theft from the recently introduced prepayment electricity system in Zimbabwe.

The empirical study have indicated that no studies in Zimbabwe have been carried out to establish how mobile technologies can be used to detect electricity theft. There is a need to detect electricity theft at the exact location, in real-time and transmit the information through mobile technologies to the back-end system for decision making. Mobile technologies offer a real-time platform in achieving the required information. They also provide the capability to monitor individually installed infrastructure. The use of mobile technologies is central in detecting electricity theft. However, most power utilities world over are still lacking behind in this regard (Pargal, 2014). Therefore the problem statement to be addressed in this study can be defined as;

Zimbabwe's power utility does not have a real-time monitoring system that is able to detect the exact location where electricity theft is taking place. For this reason, the power utility has found it challenging to address electricity theft in the country.

5. Research Design and Methodology

The study was guided by the design science methodology which was implemented within a qualitative study. Within the design science paradigm, a single case approach with a single unit analysis was carried out at ZETDC. This study used semi-structured interviews, qualitative questionnaires, participant observation, and document review to collect primary data. Secondary data was obtained through literature review from related studies, case studies, books, journals, newspapers articles and conference proceedings. A purposive sampling strategy was used in the study, whereby participants were chosen using a non-probability sampling technique. The sample population comprised the employees from the prepayment department at ZETDC's Harare region and consumers using prepaid electricity meter.

5.1 Design Science

The dominant methodology for this study was the design science paradigm which was used in conjunction with its research methods. The paradigm was chosen in this study because an artefact in the form of a framework to solve the problem of electricity theft was to be developed. The development of the framework was guided by the seven guidelines proposed by Hevner et al. (2004). These are presented below.

Guideline One: Design as an Artefact

The design science research must produce a viable artefact in various with the capacity to solve a problem in a specific domain. With this, the study was not aimed at solving the entire electricity theft problem on a broader level. But it rather aimed to provide an innovative artefact, which will add its part to the complete solution of electricity theft within the power utility industry. The artefact of this study is

"A framework for mobile technologies in monitoring electricity theft in Zimbabwe" that may be used by the power utility to detect and counter electricity theft.

Guideline Two: Problem Relevance

This guideline specifies that design science should be relevant to a specific problem domain and capable to meet the business needs of an organization. The problem was derived from the way electricity is stolen and the methods that are currently used to detect and counter electricity theft by the power utility. The problem that was identified from the study is the shortcoming of the organization to detect the exact location where electricity theft would be taking place. This has resulted in revenue losses or leakages within the power utility.

Guideline Three: Design Evaluation

The artefact should be evaluated to gain feedback on the features required to meet the business needs and its purpose. Since feedback of the evaluation process has great influence on the final product, it should be used to further refine the product. The process of evaluation and refining will cause the process to be iterative. The evaluation process may involve expert review or focus group discussion. In this study, four experts were presented with the initial framework to critique its usability as a monitoring tool for electricity theft. The feedback from the experts was used to refine the framework.

Guideline Four: Research contributions

An artefact is viewed as a contribution of design science research by its very nature. It should add value to the knowledge base and the application environment by extending theories and methods from previous studies. The research contribution of this study is the artefact in the form of a framework aimed at addressing electricity theft from the prepaid electricity meters. The current methods will move from general location identification to a specific location of electricity theft. The framework can also be used as a theory base (generic framework) by other researchers studying towards the monitoring systems in various domains.

Guideline Five: Research Rigor Design

Design science paradigm is rooted in the rigorous methods used for building and evaluating the artefact since it uses theories provided by scientific knowledge bases. To achieve research rigor, the researchers carried out an extensive literature review on previous theories, frameworks and methods used by reputable researchers. The information from the existing knowledge base was used to conceptualize the development of a monitoring system using mobile technologies.

Guideline Six: Design as a search process

Design science is a methodology characterizing a repeated process that aims to search for the most desirable and suitable design that best solve the identified problem. The process is done until the artefact is seen to be relevant to the business problem and needs. The process of this design was guided by research rigor, building/developing the artefact and evaluating the developed artefact.

Guideline Seven: Communication of Research

The output of the design science research should be effectively availed to different target audiences. The target audience of this study is information systems researchers, power utilities and other organizations interested in monitoring systems. The framework was presented to the power utility of Zimbabwe for further consideration.

6. Findings

6.1 Strategies used to steal electricity from prepaid electricity meter

Physical bypass

This strategy can be defined as either wholly or partial bypass, where in the former the prepaid electricity meter does not record any electricity usage while in the latter some of the electricity is recorded. This method is the most common and easiest. The disconnection can be done inside or outside the meter. The cables from the prepaid electricity meter are disconnected and re-routed directly to the load. It is said to be physical because it is concerned with physically disturbing the wiring integrity of the electricity meter

Mechanical interference

The mechanical built-up of the electricity meter especially the disk is the most important part that enables the power utilities to calculate the amount of electricity that have been consumed (passed through the electricity meter). The movement of the disk is designed in such a way that it rotates (rotary movement) in proportion to the electricity usage through a particular meter. Once the rotation is disturbed, electricity usage will no longer be proportional to rotary movement. The slower the movement of the disk, the fewer number of units recorded by the electricity meter. The aim of this strategy is to reduce the speed of the disk so that electricity is billed at a very slow rate. It can be achieved through manually resetting the speed of the disk, inserting metallic or non-metallic objects, subjecting the meter to strong heat or strong magnet and using gadgets which require more than 100Amps the maximum electricity the prepaid meter can supply.

Instrumentation control (Cyber-attack)

Some consumers have found smart and intelligent ways of stealing electricity, especially those that are knowledgeable in computer systems. They can reprogram the prepaid electricity meter using software than can be downloaded from the internet. Others may use a remote device equipped with an optical light (infra-red). The aim is to alter the billing and the energy registers of the prepaid meter. The infra-red of the meter makes it vulnerable to cyber-attack.

6.2 Electricity theft detection techniques

Detection of electricity theft by power utilities can be done using technological and non-technological approaches. These two approaches complement each other since the power utility has no real-time monitoring system. The technological approach acts as a guide on how the inspection on suspected consumers will be conducted. The technological approach is guided by two major aspects. Firstly, the Zero-Low purchase reports whereby consumers that have purchased very minimum amounts or have not purchased any electricity within 120 days are enlisted for inspection. Secondly, the load/purchase analysis is used to find a mismatch between purchase and consumption in a given sub-station. If consumption is greater than purchases, it’s an indication of electricity theft.

Using the non-technological approach, the inspection is guided by the information received from the public about electricity theft activities. The inspection can also be done based on the standard procedure, which is a requirement of international standards that power utilities should inspect electricity meters three months after installation. Apart from these guidelines, random inspections cannot be ignored so that it complements the weaknesses of other approaches.

6.3 Challenges faced by the power utility in detecting and countering electricity theft

In detecting and countering electricity theft from prepaid meters, power utilities are faced with both technical and operational challenges. The major technical problem which was highlighted during the study is the database integrity. In some occasions, there will be missing information about the electricity meter and the consumer from the database. For example, the address of the consumer may not be found from the database which makes it difficult to locate the consumers stealing the electricity.

The other concerns for monitoring electricity theft were the legitimate timings the power utility is supposed to operate and cooperation from the consumers. Using the current monitoring techniques, the power utility can only monitor electricity theft during the day hours. Therefore, consumers can steal electricity overnight and restore the connections or configurations during the day. Subsequently, some consumers do not cooperate with the inspection teams. This involves not attending to their gates in time if they suspect its ZETDC inspectors and refusing to safe handle their dogs or not showing up at all.

7. Discussion of Results

Electricity theft from prepaid meters may be conducted in a variety of forms (Campos & Pradham, 2007). The method chosen may depend upon the braveness, technical and the technological expertise the perpetrator possesses. Some of the methods are common while others are sophisticated. Hence, power utilities employ different strategies to detect and deter electricity theft.

Traditionally, electricity theft detection in Zimbabwe has been addressed by the means of physical inspections carried out by the Revenue Protection Unit (RPU) on consumers who are suspected to be stealing electricity. The inspection may confirm that there is electricity theft or it may refute the theft of electricity. If theft is confirmed to have taken place, this will be beneficiary to the power utility since lost revenue can be recovered using revenue recovery procedure. But if electricity theft is refuted, this will be a loss to the power utility in terms of resources such as time and allowances used to carry out the inspection. However, this method is labour intensive and time consuming considering that the power utility serves many consumers.

While most power utilities including Zimbabwe has tried to employ both technological and non-technological approaches to detect electricity theft, these methods are seen to be too basic to effectively and efficiently combat the electricity theft. This is because these methods gives the general location where electricity theft will be taking place. Moreover, the prepaid electricity meter itself has limited monitoring functionalities.

With the advances in technology, consumers are now moving from the old basic way of stealing electricity (meter bypassing), to more sophisticated ways (meter tampering). This has made it difficult to detect electricity theft, especially using basic means like zero-low purchase analysis, load-purchase analysis and field inspections. The need for the adoption of solutions with real-time monitoring and reporting has been the major focus of this study. This is a clear indication of the pervasiveness of ICTs in every facet of life addressing different but critical challenges. The envisaged ICT framework proposed here results in reducing if not totally eliminating electricity theft in Zimbabwe, improving revenue collection for the organisation and this in turn enables the organisation to generate more electricity which is critical for the resuscitation of the ailing Zimbabwe economy. The framework also results in the reduction of expenditure for the organisation which may result affordable electricity for general consumers and industry.

8. Proposed Framework

Considering the problem statement and information gathered during the study, “**A framework for mobile technologies in monitoring electricity theft**” has been conceptualised to consist of five (5) major layers which are connected one after the other to provide control of the preceding layers. Certain elements are included in each layer so that all the aspects of the monitoring procedures are found in the fiver layers as shown in Figure 1.

The layers are:

- Strategic layer
- Integration management layer
- Control and processing layer
- Management layer
- Evaluation layer

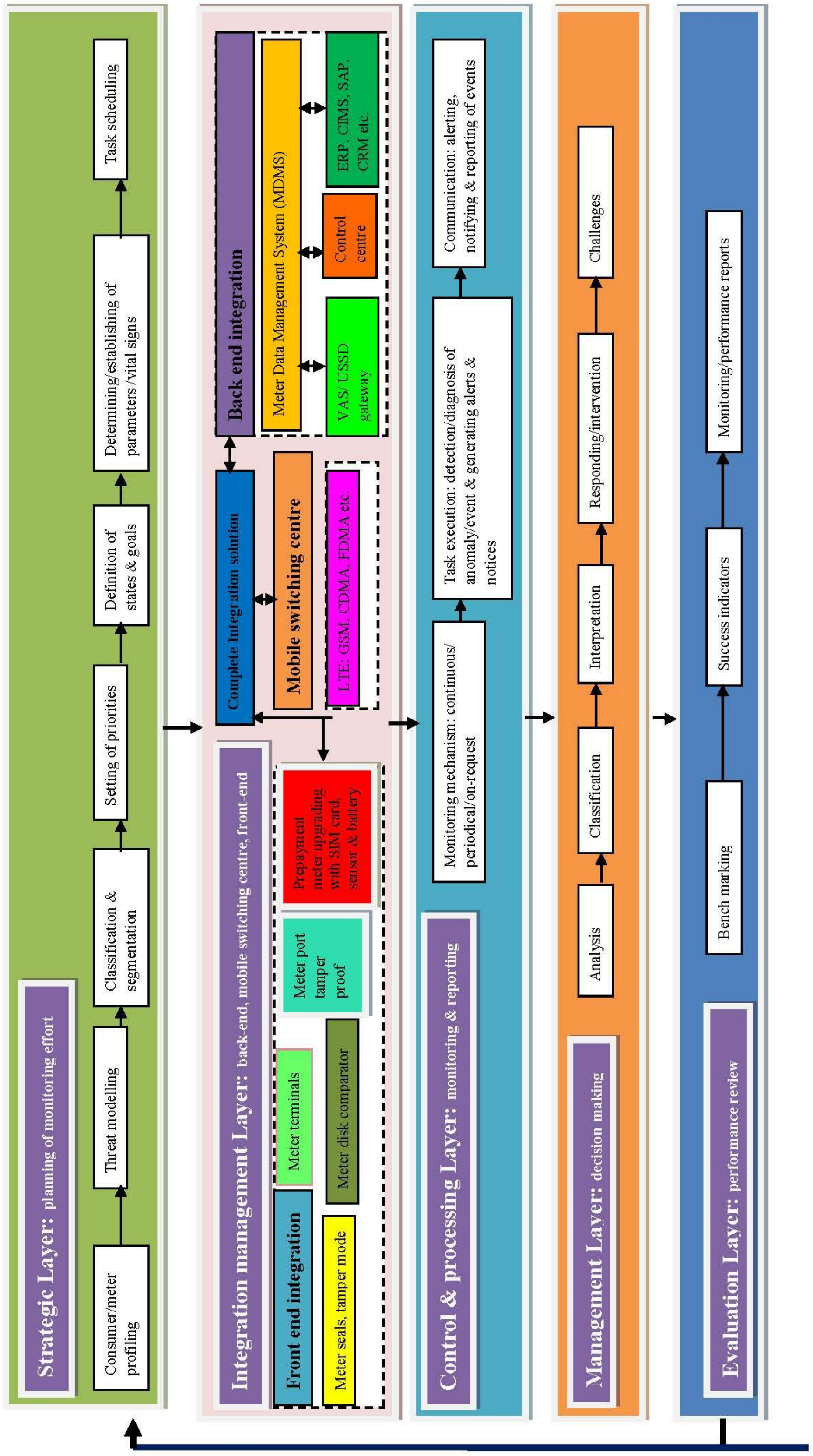
Strategic Layer: planning of monitoring effort
Consumer/meter profiling
Threat modelling
Classification & segmentation
Setting of priorities
Definition of states & goals
Determining/establishing of parameters /vital signs
Task scheduling
Integration management Layer: back-end, mobile switching centre, front-end
Front end integration
Meter seals, tamper mode
Meter terminals
Meter disk comparator
Meter port tamper proof
Prepayment meter upgrading with SIM card, sensor & battery
Complete Integration solution
Mobile switching centre
LTE, GSM, CDMA, FDMA etc
Back end integration
Meter Data Management System (MDMS)
VAS/ USSD gateway
Control centre
ERP, CIMS, SAP, CRM etc.
Control & processing Layer: monitoring & reporting
Monitoring mechanism: continuous/ periodical/on-request
Task execution: detection/diagnosis of anomaly/event & generating alerts & notices
Communication: alerting, notifying & reporting of events
Management Layer: decision making
Analysis
Classification
Interpretation
Responding/intervention
Challenges
Evaluation Layer: performance review
Bench marking
Success indicators
Monitoring/performance reports

Figure 1: Proposed Framework for mobile technologies in monitoring electricity theft

Strategic layer

This layer is concerned with the planning of the monitoring effort of the prepaid meter. The planning include:

Consumer/meter profiling- the database integrity requires that there are accurate details of both the consumer and the electricity meter. Profiling should be done in the early stages of the prepaid electricity meter installation. This will enable the power utility to match the details of the meter and the consumer. Therefore, database integrity will play a crucial role in achieving operational excellence.

Threat modelling- the installation of prepaid electricity meters to the consumer premises presents various threats to the infrastructure. The goal of threat modelling is to identify and build possible threats to the infrastructure in order to increase awareness and come up with adequate monitoring strategies. Threat should be modelled to identify vulnerabilities so that all the possible theft strategies could be addressed. The prepaid metering infrastructure is vulnerable to threat to wiring integrity, threat to the billing software configurations and threat to the mechanically built-up of the meter, particularly the meter disk, the magnet and other internal components.

Classification and segmentation- theft prone areas should be identified by means of periodic field checks or by a study of the distribution transformer or electricity balance sheets in variation of individual consumption. Field checks reports should reveal trends, problem areas, problem freight (rate of occurrence), and problem consumers. The areas that are prone to electricity theft can be classified according to threat level to facilitate segmentation. Threat level can be high, medium and low.

Setting of priorities- after classification and segmentation, priorities can be set according to areas to be monitored and the threat level. Priority setting should be viewed as a vital step in planning a monitoring program. In the absence of priorities, areas or infrastructures that are prone to risk will be ignored which may result in severe loss or damage. Thus, the need to divide areas being monitored will guide the control of allocation of monitoring resources.

Defining states and goals- the system should have clearly defined states and goals to be achieved in the monitoring process. These states and goals should be clearly defined so that the proposed framework can solve the threat that has been identified and also cater for all the possible electricity theft scenarios. The four major states that have been identified in prepaid electricity meter are; electricity meter state (tamper/normal), configuration state (normal/altered), flow of current (logical/reversed), speed of the electricity meter disk (slow/normal)

Determining/establishing of parameters or vital signs to be monitored- before making a decision on how to proceed with the monitoring program, it is important to determine/ establish parameters or vital signs to be monitored that are easy to identify. The parameters to be observed should be set in advance. This will provide the basis for the system to understand the normal and the abnormal state throughout the monitoring process. The parameters for monitoring electricity theft are billing cycle; the direction of flow of current; the direction and speed of the meter disk; tamper mode indicator. If these parameters are determined, the task to monitor these parameters can then be scheduled accordingly.

Task scheduling- task selection and scheduling should be part of the monitoring strategy in order to classify task into various categories. This is also essential to decide how events and notices will be detected and reported to the back-end system. Parameters and vital signs to be monitored should also be specified during task scheduling. Task scheduling will be enforced based on classification, segmentation and defined priorities. Monitoring as a task can be enforced periodical, continuous or on-request based upon the three variables; high, medium and low.

Integration management layer

The application of mobile technologies in monitoring electricity theft is based entirely on the complete integration of the back-end system, mobile switching centre and the front-end system (prepaid metering infrastructure). This layer is critical in achieving real-time monitoring and on-demand response. The integration process will enable the organisation to gain an insight on what is taking place in the infrastructure and take an informed decision. Although, various types of mobile technologies exist, the proposed framework will be implemented using the Life Time Evaluation (LTE) technology. LTE is the latest mobile network technology with many branches that provides easy connectivity for GSM/EDGE, CDMA and FDMA. These branches of technology can also be accessed by other different branches of technologies such as LAN or WLAN found in the back-end system. In this study, the major components for mobile technologies are Subscriber Identity Module (SIM) cards, Unstructured Supplementary Services Data (USSD) gateway and the mobile switching centre.

Back-end integration (internal integration)

The system should be linked to other internal systems such as ERP, CIMS, SAP, CRM, etc. The gateway is used to route messages from the front-end and the back-end system and will be implemented using USSD/Value Added Service (VAS) gateways. These two types of gateways are the most preferred routing protocols in GSM cellular networks because they provide mobile switching capabilities from one party to the other. This protocol will provide easy connectivity between the back-end system and the mobile switching centre to the front-end.

Mobile switching centre

Although, the power utility has its own communication facilities (Power Line Carrier) which uses the same line that transmit electricity to the consumer, this communication backbone cannot be relied on since it uses cable network. Once the meter has been disconnected from the electricity grid system, the signal cannot be sent to the back-end system; hence the mobile switching centre is ideal in this regard. Therefore, it is recommended that a single mobile network operator should be chosen to provide mobile switching facilities between the front-end and the back-end systems.

Front-end integration

The prepaid meter should be upgraded with the SIM card, sensor and battery in order to facilitate independent communication with the back-end system. The SIM card will allow the infrastructure to communicate with the back-end system even if it has been disconnected from the electricity grid system. The SIM card needs to have a tamper proof as it may be subjected to tampering.

Control and processing layer

This layer is concerned with the actual monitoring of electricity theft and reporting to the back-end system the parameters or signs that have been detected by the system. The process of event reporting involves detection, recognition and communication. The monitoring system should take into cognisance of any changes in parameters or configurations of the previously known state in order to facilitate the generation of alerts. The monitoring can be continuous, periodic or on-request, depending on the threat level identified in the Strategic layer. This will ensure that more effort is directed to high loss areas and at the same time saving the life span of the sensor and the battery. This layer is made up of three sublayers as presented below.

Monitoring mechanism- the three major monitoring mechanisms are continuous, periodical and on-request. In continuous monitoring, the observation of the infrastructure is an ongoing process. Periodical monitoring is whereby the monitoring mechanism is based on the duty cycle concept. The monitoring indicator goes to sleep and wake up if the time interval is detected. On-request, monitoring will require the system to store the events/notices at the front-end or back-end without automatically generating an alert. The events or notices can be accessed by the ping method or running database queries on the state of the infrastructure.

Task execution- the tasks will be executed by detecting any anomaly event, sign or parameters that have been specified to be monitored in task scheduling. This will also involve data acquisition about the event on the infrastructure, reporting immediately to the back-end system what has been detected to be an anomaly or storing the information for later reporting.

Communication- communication in monitoring systems involves alerting and notifying the operator about any event that has been detected to have changed the normal state of the system. In this framework, mobile technologies are the backbone system for sending reports and alerts to the control centre. Reporting procedure will be guided by the specified enforcement rules in task scheduling i.e. continuous, periodical or on-request.

Management layer

This layer pertains to decision making based on analysing reports and notices and classifying them according to set priorities. The layer is organised as;

Analysis- the data that has been received from the prepaid electricity meter through mobile technologies need to be analysed in order to aid decision making. The success of the other activities will be based on the analysis stage. During analysis the alarm is evaluated in order to generate appropriate reports. The reports are sent to the control centre (operator) as notices or alerts.

Classification- reports/events need to be classified so as to come up with the means of plotting time series. Events will be classified according to the strategy used to attack the infrastructure. The time series will involve rating of the performance of the monitoring system, the rise and fall of incidents concerning electricity meter bypassing or tampering.

Interpretation- the time series are used to aid interpretation in order to determine which areas need immediate response. The validity of the parameters being monitored also needs to be evaluated.

Intervention/responding- there must be a clearly defined intervention strategy so that urgent notices will be given first priority. There should be guidelines on how to respond to the events that have been detected and reported to the back-end system.

Challenges- challenges faced/encountered by the monitoring system should be identified in this layer so that they can be addressed in the next layer which deals with the evaluation of how the framework is performing. The challenges in this framework may include;

- Balancing priorities and the monitoring effort.
- Operational burden of maintaining the monitoring equipment.
- Changing enforcement rules and managing alerts.

Evaluation layer

The layer is concerned with reviewing the performance of the artefact through the evaluation loop to the Strategic layer. The loop that runs from Evaluation layer to the strategic layer indicates that performance review will cause other elements to change within the monitoring process. The changes may include the operational protocol and the task scheduling. After performance review have been carried out, the planning stage of the monitoring effort can be reviewed to check whether there are emerging threats to the infrastructure (strategies for stealing electricity) not covered by the framework. This will facilitate continuous improvement of the artefact so that it remains relevant to the business needs (i.e. to timeously detect and counter electricity theft).

Benchmarking- benchmarking allows the organisation to compare the performance of a system against success factors (goals) previously achieved. It is the foundation of building a comparative analysis between performance and success. The elements that will be used as benchmarks should be defined prior to evaluation. The evaluation of the performance of this framework has been benchmarked using the goals identified in the Strategic layer. Hence, the performance review needs to go back to the Strategic layer using an evaluation loop. If performance review indicates satisfactory results, there might be minor or no changes in the Strategic layer. But, if there is an indication of dissatisfaction, major changes will be needed.

Success indicators- success factors should be benchmarked against performance indicators so that monitoring reports can be reviewed to determine achievements of the monitoring program. Some of the success factors will include;

- Reduction in electricity meter tampering
- Few areas placed under continuous monitoring
- Reduction in electricity theft
- Electricity efficiency
- Early detection and “on-demand” response

Monitoring/performance reports- performance reports will be compared with the success factors that have been benchmarked for evaluation. Quantitative data for comparison will be collected from monitoring/performance reports. For example the number of prepaid electricity meters disconnected from the grid system, the number of electricity meters detected of mechanical induced theft strategy and the number of electricity metres tampered with instrumentation control strategy.

9. Conclusion

Most power utilities are faced with a daunting task in combating electricity theft. They have a crucial responsibility in ensuring that revenue leakages through electricity theft are brought to minimum levels. Electricity theft has threatened the life span of the prepaid electricity metering infrastructure and the business case of adopting a prepaid metering system by most power utilities. Detecting and countering electricity theft has been a major challenge in most power utilities. To understand how the proposed framework would address these challenges, it was important to establish how electricity from prepaid meters is being stolen. And what are the techniques that are currently used to detect electricity theft, as well as challenges faced.

The Framework developed here can be extended to other areas to address revenue theft problems. It is the starting point for other researchers interested in design science and Framework development. It illustrates the pervasive nature of ICTs as cross cutting across different area of social and economic life hence indicating that it is indispensable.

Acknowledgements

These researchers are indebted to people from the power utility in Zimbabwe and registered electricity consumers and the framework reviewers. It is the sterling work and valuable information they provided that places us in their debt. We would like to recognize the assistance rendered by these people as their valuable input enabled us to craft this piece of work. We are indeed grateful to these participants for availing themselves for the research and providing data that enabled this study to be carried out. For without them this research would not have been possible. Their priceless contribution is greatly appreciated.

References

Accenture, 2013: The New Energy Consumer Handbook, p.252. Available at: http://nstore.accenture.com/acn_com/PDF/Accenture-New-Energy-Consumer-Handbook-2013.pdf.

Balasubramanya, C., 2014: Electricity theft: is smart meter a solution? (March). pp. 1-12. Available at: http://www.slideshare.net/balasubramanyachandrashekariah/electricity-theft-is-

Campos, J. E. & Pradhan, S., (eds), 2007: The Many Faces of Corruption: Tracking Vulnerabilities at the Sector Level. Washington DC: World Bank. Available at: https://books.google.co.zw/books?id=Wy-oNmjqq-QC&pg=PA151&dq

Casarin, A. & Nicollier, L. A., 2010: Prepaid meters in electricity: a cost-benefit analysis. Available at: http://www.e-elgar.co.uk/bookentry_main.lasso?id=13551&breadcrumlink=&breadcrum=&sub_values=&site_Bus_Man=&site_dev=&site_eco=&site_env_eco=&site_inn_tech=&site_int_pol=&site_law=&site_pub_soc=

Gartner, G., 2012: Mobile Technologies for 2012 & 2013. Available at: http://www.alibabaoglan.com/blog/10-mobile-technologies-for-2012-2013/

Hevner, A.R., March, S., Park, J. & Ram, S., 2004: Design Science in Information Systems Research. *MIS Quarterly*. 28(1), pp.75–105. Available at: http://dblp.uni-trier.de/rec/bibtex/journals/misq/HevnerMPR04

Jain, A & Bagree, M., 2011: A prepaid meter using mobile communication. *International Journal of Engineering, Science and Technology*. 3(3), pp.160–166

Malama, A., Mudenda, P., Ng'ombe, A., Makashini, L. & Abandaet, H., 2014: The Effects of the Introduction of Prepayment Meters on the Energy Usage Behaviour of Different Housing Consumer Groups in Kitwe, Zambia. *AIMS Energy*. 2(3). pp.237–259. Available at: http://www.aimspress.com/aimse/ch/reader/view_abstract.aspx?doi=10.3934/energy.2014.3.237

Miyogo, C.N., Ondieki, N.S. & Nashappi., G. N., 2013: An Assessment of the Effect of Prepaid Service Transition in Electricity Bill Payment on KP Customers, a Survey of Kenya Power, *West Kenya Kisumu*. 3(9). pp.88–97

Morales, M. & Palma, M.J., 2010: Industry Developents and Models Intelligent Systems : The Next Big Opportunity. *IDC Analyse the Future*, 1(8). Available at: download.microsoft.com/.../IDC%20-%20Intelligent%20Systems%20-%...

Pandey, V., Gill, S.S. & Sharma, A., 2013: Wireless Electricity Theft Detection System Using Zigbee Technology. *International Journal on Recent and Innovation Trends in Computing and Communication*. 1(4). pp.364–367. Available at: http://www.ijritcc.org

Pargal, S., 2014: *Power to India - Open Knowledge Repository - World Bank.* Washington DC: International Bank for Reconstruction and Development. Available at: https://openknowledge.worldbank.org/.../889060PUB0978100Box3852...

Quayson-Dadzie, J.A., 2012: *Customer Perception and Acceptability on the Use of Prepaid Metering System in Accra West Region of Electricity Company of Ghana.*Thesis Submitted to the Institute Of Distance Learning , Kwame Nkrumah University of Science and Te.

SARPA., 2013: Dealing with electricity theft. (July). Available at: web.vdw.co.za/.../Association/SARPA%20Exco%20Minutes%2010%20J...

Selvapriya, C., 2014: Competent Approach For Inspecting Electricity Theft. *IJIRSET*, 3(3), pp.1763–1766

Tasdoven, H., Fiedler, B.A. & Garayev, V., 2012: Improving electricity efficiency in Turkey by addressing illegal electricity consumption: A governance approach. *Energy Policy*,k 11(43), pp.226–234. Available at: http://dx.doi.org/10.1016/j.enpol.2011.12.059.

Tuckova, Z., Novak, Z., 2016: Do the Czech Production Plants Measure the Performance of Energy Processes? *Journal of Systems Integration,* 7 (2): 42-53

JEL Classification: L94