International Journal of Technology Engineering Arts Mathematics Science
Vol. 1, Iss. 1, January- June 2021, pp. 8~14

IoT Based Approach for Tamper Detection of Energy Meters

Mrs. A.D. Shiralkar, Dr. S.M. Bakre

[1]Head, Electrical Engineering Department, AISSMS IOIT, Pune, Maharashtra, India
[2]Associate Professor, Electrical Engineering Department, AISSMS IOIT, Pune, Maharashtra, India

Corresponding Author: Dr. S.M. Bakre (shashikant.bakre@aissmsioit.org)

Article Information

Article history:

Received April 17, 2021
Revised April 25, 2021
Accepted April 25, 2021

AISSMS IOIT RESEARCH
International Journal of TEAMS

ABSTRACT

One of the major issues being faced by distribution utility today is the theft of electricity. For instance, the distribution loss of 13.63% and Aggregate Technical and Commercial (AT&C) loss of 16.94% in Maharashtra State for the year 2018-19 is mainly attributed to the theft of electricity. Theft of electricity is suspected as a main cause behind higher commercial losses. Various modus of operandi of theft of electricity committed by miscreants are tampering electric meter, applying hooks on incoming lines, tampering Current Transformer Potential Transformer (CTPT) units etc. Number of tamper events have been reported such as CT reverse, CT short, CT unbalance, PT low, PT missing, meter bypass, magnetic theft, series/parallel resistance etc. This paper highlights the act of tampering of meter by inserting resistance in parallel as well as series across the meter and reducing amount of billing current. Also the novice and cost effective method to detect this event is suggested in this paper. In the advent of upcoming Internet of Things (IoT) technology, the tamper can be detected using intelligent sensors provided at instrument transformers and meter. The inputs received from IoT based sensors are fed to the microcontroller through an internet media. It has proposed here that the microcontroller based comparator can be used here for detecting current unbalance caused by parallel resistance. The proposed method can be applicable to all types of meters.

KEYWORDS: Meter tamper, IoT Sensors, numeric meter, current transformer, potential transformer, CT Sensor, microcontroller, comparator

1. INTRODUCTION

The issue of theft of electrical energy is generally identified by conducting energy audit and estimating losses. Broadly the losses are classified as follows-

- Transmission and Distribution losses (T&D losses) and
- Aggregate Technical and Commercial losses (AT&C losses).

As the distribution utility does not have transmission network (66 kV and above), the distribution loss is taken into consideration. The distribution voltage levels are 33 kV, 22 kV, 11 kV (high voltage) and 440 Volts and 230 Volts (Low voltage).Therefore, while conducting energy audit and accounting, the distribution utility takes into consideration two types of losses viz. distribution losses and AT&C loss[1]. The losses are attributed as technical losses and commercial losses. Technical losses include copper losses and iron losses. Copper losses are I^2R losses which are observed in conductors and transformer windings. Iron losses mainly comprise of hysteresis losses and eddy current losses. These technical losses can be minimized by proper maintenance, using standard material, keeping useful service life and maintaining dimensions. The technical losses usually do not exceed 5%.

The commercial losses comprise of theft, pilferage, incorrect recording and defective meters [2]. In Maharashtra state, the main distribution utility is owned by the Government of Maharashtra namely, Maharashtra State Electricity Distribution Company Ltd (MSEDCL) [1]. The financial report of MSEDCL for the year 2019-20 has mentioned losses for five years as furnished in Table 1(Reference- Maharashtra State Electricity Distribution Co. Ltd- 14th Annual Report, 2018-19). It is mentioned in the report that total number of consumers in Maharashtra are 2,7331725out of which the number of residential consumers are 2, 0455281. It is therefore a challenging task to monitor theft control of such a huge amount of consumers [2]. The losses for five years are expressed in percentage in Table I.

The target objectives for the year 2018-19 were given to bring down distribution losses below 8.00% and AT&C losses below 10.00%. However, as seen from Table1, slight reduction less than 6% in losses has been noticed over a period of five years. On an average, the distribution loss and AT&C losses are found to be higher over the period of last five years. No significant reduction in losses is found. This results in a higher revenue loss. Electrical theft is the main culprit in higher losses and resulting loss of revenue [3]. Therefore theft detection and control is an ultimate objective for loss minimization and revenue optimization [4].

The theft of electricity is committed by miscreants in number of ways [5]. This is called as modus of operandi. Various modus of operandi of theft of electricity committed by miscreants are tampering electric meter, applying hooks on incoming lines, tampering CTPT units etc. Number of tamper events have been reported such as CT reverse, CT short, CT unbalance, PT low, PT missing, meter bypass, magnetic theft, series/parallel resistance etc. This paper discusses an act of tampering of meter by inserting resistance in parallel across the meter [6]. It is reported by the distribution utility that the practice of tampering the meter is found to be followed by the miscreants at number of metering installations and there is an increasing trend [7].

The objectives of this paper are stated below-

- Analysis of effects of tampering meter by inserting series, parallel or series-parallel resistors.
- A novel and cost effective approach for detection of such type of theft.

1.1 Review of Microcontrollers

The microprocessor unit comprises of number of components connected to it. The complete microprocessor kit is formed from the combination of several components such as processor, RAM, ROM, timer, system bus comprising of address bus, data bus and control bus, peripheral chips such as 8255, 8279 and 8257. These components are mounted in form of different chips on printed circuit board [8]. All such components are embedded in a single chip called microcontroller.

Table 1. DISCOM Losses for last five years

Year	Distribution losses in %	AT&C losses in %
2014-15	14.17	17.86
2015-16	14.51	18.79
2016-17	14.68	18.88
2017-18	13.90	17.41
2018-19	13.63	16.94

The main advantage of microcontroller over microprocessor is reduction in space. The desktop computer has microprocessor because there is enough space on its motherboard. There are certain applications however having space constraints. For such applications, microcontroller is a right choice. Microcontrollers are widely used in appliances such as Television, Washing machines, remote control units, microwave oven etc. Desktop computer has microprocessor, but is peripherals such as keyboard, mouse, DVD drive have in-built microcontrollers. 8051 is a small and low cost microcontroller. It is designed to perform specific tasks required by the embedded systems such as receiving information, sending and receiving signals etc. The microcontroller comprises of the following main components-

- Processor
- Memory- RAM/ROM/EPROM
- Serial IO Ports
- Peripherals such as Timers, Counters, & Buses
- Areas Such As Energy Management, Monitoring and metering, and motion detection.

Arduino is an open source electronic platform used to build electronic projects [9]. It comprises of microcontroller board and Integrated Development Environment (IDE) Software. The user writes his source code and uploads it on Arduino board. Arduino boards are available commercially in preassembled form or as do-it-yourself (DIY) kits. Arduino can be used over a wide range of products from 8-bit boards to modern IoT based embedded systems.

Raspberry Pi was developed by Raspberry Pi foundation in the year 2012 to teach school going children on how to write a program from scratch. Initially, it was set up at University of Cambridge, UK. Today, Raspberry Pi is a low cost credit card size computer having USB port, blue tooth, Wi-Fi features. It can be housed in a glass case which is available in the market. Number of versions of raspberry Pi were released subsequently such as A, A+, B, and B+. Raspberry Pi is the combination of Raspberry operating system and Pi as Python language.

The Raspberry Pi is a credit-card-sized computer that plugs into your television and a keyboard [10]. It is possible to connect keyboard, mouse and monitor to the raspberry pi board and use it as a computer. The pen drive can be inserted at USB port. The raspberry pi can be connected to internet through an Ethernet cable. It can also connect be connected to Wi-Fi. The charger can be connected to the ports available. Using Raspberry Pi, it is possible to work on spreadsheets, word processing, browsing the internet, and playing games. If Raspberry Pi is used as computer, it would consume only 10% of the power consumed by your regular PC.

In this paper, the microcontroller is used for comparison of signals received from IoT Sensors. Based on these input signals, the tamper is detected if any.

1.2 Review of Internet of Things (IoT) Technology

At present, the access to internet is mainly available through computers and smart phones. Through IoT, it is possible to extend this power beyond computers and mobile phones. The IoT enables devices have access to internet. Thus IoT is the system comprising of interrelated devices having ability to transfer data over a network without requiring human to human or human to computer interaction. The IoT enabled devices are provided with unique identifiers. The IoT enabled sensors collect the specified information automatically from the environment which is used to take intelligent decision. For example, the IoT sensors provided at CT, PT and meter collect values of current voltages from the electrical installation and send them to the microcontroller. The internet mechanism in the proposed scenario works in the following manner [11].

1. There are three ways by which the data can be sent from instrument transformer to the Central Monitoring Station (CMS). The server is provided at CMS that receives data from various terminals such as CTs, PTs, modems and routers and processes it further.
   - Peer to Peer communication- it is a point to point communication between instrument transformer and CMS server. The additional terminals cannot be added to this network.
   - Master Slave communication- in this case one terminal works as Master (e.g. CMS Server) and other terminals as Slave. Their roles cannot be interchanged.
   - Client Server communication- there may be any number of clients and server terminals and their roles are interchangeable. In this scenario, the CMS works as server and other terminals like CT Sensor, OT Sensors and routers work as clients. The communication takes place as follows-
   - Server sends data request to the client.
   - Server sends acknowledgement and sends data to the server.
   - The process of communication continues.
2. The optical fibre cable (OFC) can be connected between CMS Server and other terminals. The advantage of using OFC is lesser noise and distortion. It is feasible to provide OFC as the distance between CMS and terminals is lesser. The other option is use of wireless media.
3. The addressing is analogues to postal system. The letter (data) is send to the receiver through his postal address (IP Address).
4. IP address is a dot quad address specified in 123.45.67.89 format. Each component of the network is having unique IP address. For example, CMS Server, router, CT Sensor, PT Sensor has different IP addresses. The IP address is allocated by the agency called Internet Provider Service (IPS). Thus ip address is a shipping address at which the information reaches its destination. The server stores number of websites. Therefore it is possible to have access to the website through IP address of a server.
5. It is difficult to remember IP address of every entity. Therefore providing domain name is the available option. The IP address corresponds to domain name. For example, the domain name and IP address can be configured are shown in Table 2.
6. DNS Server – DNS Server is a huge phone book. The DNS server is similar to telephone directory comprising of domain name and corresponding IP address.
7. The data comprises of huge information in form of zeros and ones. This data is divided into number of packets. The size of each packet is 6bits. Each packet is assigned an IP address. Analogous to postal envelop having address and sequence number. Each packet takes it path in a network to reach user. Once received, all the packets are reassembled as per sequence number. In case some packet is not received, the request is send by receiving end to resend.
8. The transmission of packets is based on rules of communication called protocols. Some main protocols are given below.

1.3 Review of Python Programming

Python is an interpreter, high level, general purpose, object oriented, platform independent; web enabled dynamically typed programming language developed by Guido Van Rossum at National Research Institute for Mathematics and Computer Science in Netherlands. As of today, it is one of popular programming languages all over the world [12]. The working on Python was started in late 1980s as a successor of ABC language. The first version of Python was released in the year 1991. Initially Python was successfully used in Ameba Operation System. Python was named after a famous TV show in Netherlands called 'Month Python Flying Circus'. Python 2.0 was released in the pear 2000 wherein number of additional features such as garbage collection and list comprehensions were introduced. Python 3.0 was released in 2008. There has been a lot of difference in Python 2.0 and Python 3.0. The code written in 2.0 versions cannot be executed on 3.0 unmodified. Python language is simple and easy to understand, yet it is a powerful language. It comprises of extensive set of libraries. It is widely used in new technologies such as data science, big data, machine learning, Internet of Things, cloud computing and modern artificial intelligence.

Table 2: Domain name and IP address

Name of protocol	purpose
TCP/IP	Data transport
http/https	Web access
FTP	File Transfer Protocol

Google, You Tube, Instagram, Dropbox, Quora, Big Torrent, Delug, Cinema 4D and Mozilla Firefox are some of famous and globally used applications based on Python. The significant features of Python are stated below:

- Simple but powerful - Python is simple and easy to understand. At the same time, it has powerful features.
- Platform independent- Python program written on one platform can be executed on other with or without major changes. Thus Python is 'write once and run anywhere' language.
- Open Source language – Python downloading is available free of cost.
- Versatile – Python is suitable in web applications, desktop applications, database management systems, graphics, animation and automation.
- Extensive Library- Python provides large number of libraries. The programme has an access to these libraries for developing his or her application.
- Healthy active community - The Python community provides interactive documentation to their users. This community is available to the users in case they need any help.
- Big data and cloud- Python is used effectively for data analysis and cloud computing.
- Python is an interpreted language- The code can be executed line by line. It runs directly without any previous compilation.
- Python, by design, is an *interpreted* language (as opposed to a *compiled* language). Programs written with interpreted languages do tend to execute a little more slowly than do compiled programs, but for most tasks the difference is insignificant. The big advantage of an interpreted language is experimentation: A programmer can try out algorithms and play around with different commands interactively (that is, without having to write a complete program to do either). For people just starting to learn programming in general, or Python in particular, interactive experimentation is very useful.
- Structured language- like C language, Python can also be used as a structured programming language.
- Scripting language - Python is used widely as scripting language for web applications.
- High level language- like C, C++ and Java, Python is used as High level general purpose programming language.
- Object oriented language- Python supports OOPS features such as encapsulation, inheritance, Polymorphism and abstraction. Thus it can be used as OOPS programming language.
- Modular language – the program can be divided in number of subprograms called modules. The modularity ensures greater simplicity.
- Integrated Language- Python can be integrated with other programming languages such as C/C++ and Java.
- Indentation- The unique feature namely indentation make program readable.
- Embedded Systems Language- Python can be used as in embedded systems. The Python source code is about 10 times shorter than that of C+ and Java.

2.STATE OF ART – ENERGY METERS

There are three generations of meters namely electromechanical, static and numeric [3]. Electromechanical meters are the first generation meters. These meters were developed by the scientist Lord Ferrari in the year 1918. The electromechanical Ferrari meters comprises of pressure coil, current coil and aluminum disc. The voltage applied across pressure coil and load current flowing through current coil develops a torque that rotates aluminum disc. The meter starts recording based on the principle, 'rotations per kwh'.

The static meters are second generations meters which are more accurate and low cost as compared to electromechanical meters belonging to the first generation. In case of static meters, the rotating disc of first generation meters is replaced by a static component called thyristor. Numeric meters are the third generation meters. The numeric meters are numeric sampling meters. As such these meters are microprocessor based meters that work on the principle of sampling as shown in Fig. 1.

The numeric meters work on polling approach. The components of meter can be accessed by two ways- interrupt approach and polling approach. In case of interrupt approach, an interrupt signal is generated that interrupts the processer indicating that some abnormality has been observed in some component. The other approach is the polled approach wherein the processor checks each and every component sequentially. The numeric meters installed at various electrical installations for the measurement of electric energy are the examples of embedded systems. The numeric meters perform a dedicated function of measurement of electrical energy [8].

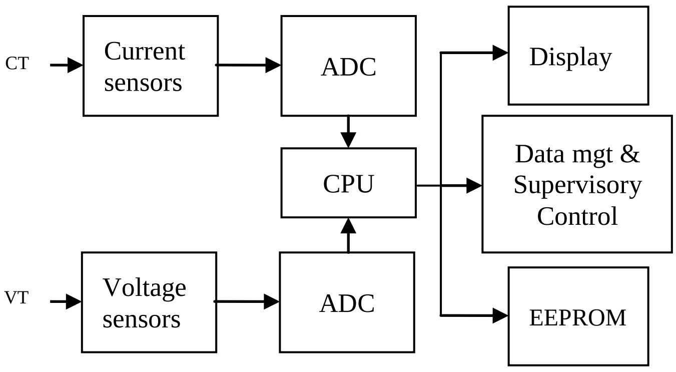

Fig. 1. Functional block diagram of numeric meter [13]

Fig. 1 shows the functional details of a numeric meter. The meter comprises of main components such as sensors, sample and hold circuit, ADC, microcontroller (MC) etc. These components can be embedded on a single chip that forms an embedded system. The input signals are received from Current Transformer (CT) and Potential Transformer (PT). These signals are sampled into number of pieces (about 3000). The sampled signals are analog signals and converted to digital signals by ADC. The output of ADC is given to the processor. The processor calculates the parameters such as $V_{rms,}$ $I_{rms,}$ W and power factor (cos Φ). In order to measure energy, kWh parameter is converted to pulses using ‘energy to frequency converter’. The counter counts number of pulses and registers number of units consumed and sent to SCADA System [14]. Comparison of meters is given below in Table 3.

With reference to the above comparison, the significant features of numeric meters are furnished below-

- High accuracy-the accuracy of numeric meters is very high of the order of 0.2 and 0.5.
- Storage capacity- the storage capacity of numeric meters is 60 days First In First Out (FIFO). As such, the numeric meters are capable of storing large amount of data for the period of two months.
- Tamper detection- through polled approach, the numeric meters all components such as current transformers, potential transformers, power supply and earthing and check anomaly if any.
- AMR/AMI applications- the numeric meters are able to communicate and transfer data. Therefore numeric meters are the basic building blocks of Automated Meter Reading (AMR) and Advanced Metering Infrastructure (AMI) based applications.
- Long Term economy- Although the initial cost of numeric meter is high, these are economical on long term basis.

3. METER TAMPERING THROUGH PARALLEL RESISTANCE

As shown in Fig. 2, the meter is tempered by connecting resistor is parallel with the meter so that the incoming current is bifurcated into billing current and resistive current. In this way the billing current is reduced by dividing it in two parts. For example as shown in Fig. 2, the billing current is 5 Amp. By connecting resistor in parallel with meter the 5 Amp current is reduced to 2 Amp and balance 3 Amp current flows through resistor. Thus instead of 5 Amp the billing would be done on 2 Amp. Unfortunately the microcontroller provided in numeric meter would be unable to detect this tamper event as it is based on 3 Amp input current. How to detect this tamper event is therefore a matter of concern.

The processor of the meter cannot detect that the current is diverted to resistive path. Therefore, no tamper event is generated. Using IoTtechnology it is possible to detect tamper through parallel, series and series parallel combination. Therefore it is required to provide IoT based smart sensors for the detection for such cases.

The detection of tamper event by connecting resistor in parallel with meter can be worked out as follows. Select two identical CT Sensors suitable to the secondary current of CTs. Such sensors are usually available with the manufacturers of instrument transformers. Connect one Sensor at the secondary of current transformer and the other inside the numeric meter as shown in Fig 2.

Usually the CT Sensor is provided inside meter. In that case, only one Sensor would be required. Let the outputs of these two sensors are A and B as shown in Fig. 3. Now connect these two outputs to the microcontroller based comparator.

Table 2. Comparison of various types of meters

Particulars	Electromechanical	Static meter	Numeric meter
Generation	first	second	third
Principle of working	Electromagnetic induction	Thyristor control	Sampling
Component	Current coil, pressure coil, disc	SCR,UJT, BJT, MOSFET	Microcontrollers, RAM,, ROM
Class of accuracy	2.75	2.0 to 3.0	0.2 and 0.5
Current type	Whole current	Whole current	CT operated
Current range	5-30 Amp 5-40 Amp	5-30 Amp 5-40 Amp	50/5, 100/5, 150/5 Amp
Cost	Lesser	lesser	higher

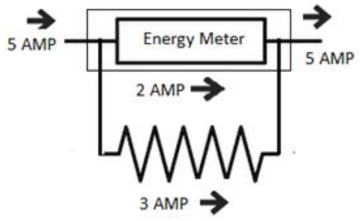

Fig. 2.Schematic of Meter tampers through parallel resistor

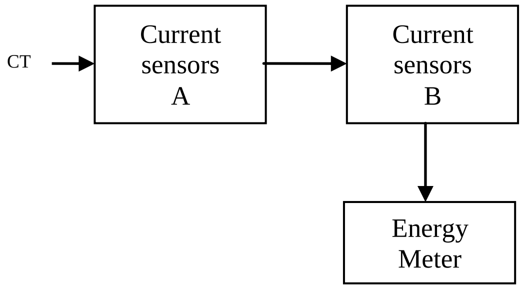

Fig. 3. Connection of Tensor

The signals at A and B can be made available to the microcontroller based comparator through an internet media. The comparison of signals A and B would yield two possibilities – A and B are equal or A and B are not equal. The output A=B indicates that the meter is not tampered. No attempt to divert current has been made. On other hand the output A≠B indicates that the meter has been tampered. The overall procedure would be furnished as given below.

- Through simultaneous checking, the currents at CT secondary (A) and meter CT sensor (B) are read continuously.
- The IoT sensor sends A and B to the inputs of microcontroller through an internet media.
- The microcontroller can be Arduino, Raspberry Pi or Intel type. The source code can be written in any language such as C/C++/Python/Assembly Language. In this paper, the code is written using assembly language programming.
- The microcontroller compares signals A and B for equality or inequality. As stated above if no tamper is committed by providing resistive path, currents A and B would be equal. Otherwise the currents would be unequal. Only magnitude of currents should be taken inconsideration. It would not be required to measure phase angle.
- In case currents are unequal, the tamper event would be registered through message or LED glowing indication. This event would also be shown in the tamper report generated by the meter.

Figure 5 illustrates the flowchart illustrating the overall working. With this flowchart as a base, the source code can be written in C/C++/Python or Assembly Language Program (ALP).

With reference to the flowchart, the Assembly Language Code is prepared. The 8 bit microcontroller has number of 8 bit registers including Accumulator (A) and Memory (M). An accumulator is the 8 bit register that performs arithmetic and logic operations. The accumulator can also work as general purpose register. Register M is the memory unit that works as an 8 bit general purpose register.

The IN command reads the 8 bit data from the input device specified by the 8 bit port address. The port address of input/output devices is 8 bit whereas the address of memory is 16bit. Thus the command IN PA reads the contents of sensor A having port address PA. These contents are copied in an accumulator. Through MOV M,Acommand, the contents of accumulator are copied in an 8 bit memory register M. Now as the accumulator is free, the contents of B are read using IN PB command indicating that the contents of sensor B spectfied by port address PB are copied in the accumulator. In this way both currents at sensors A and B are available in memory register M and accumulator respectively. In order to compare these currents let us perform their subtraction. The subtraction is performed by thecommand SUB M indicating that the contents ofaccumulator are subtracted from accumulator and the subtraction is stored in an accumulator. Mathematicall it can be stated as A=A-M. It is also possible to use the command CMP (Compare A and B) followed by the command JC (Jump if carry). Here we have used JZ (Jump if zero) command indicating that if A-B≠0, the tamper eventis generated. In anormal practice A-B=0 i.e. A=B which indicates that the current wire is not tapped by other wire. The process of checking will continue via CONT label. Whenever the tamper is detected, the message would be generatedby the system and LED of the microcontroller wouldglow. This event will be added in a tamper report generated by themeter or energy management system.

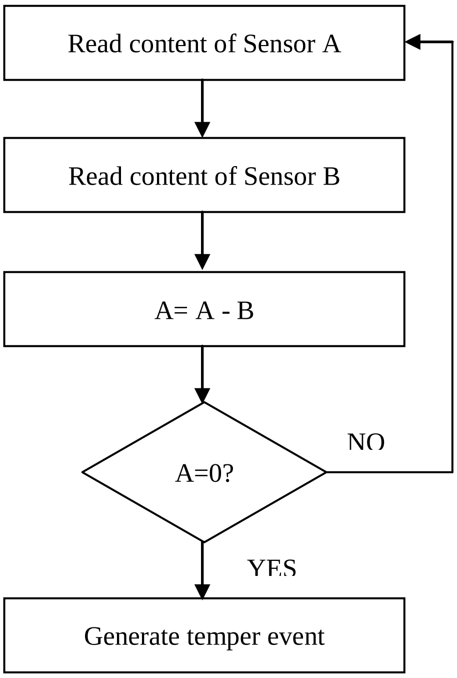

Fig. 5. Flow chart for tamper detection

4. METER TAMPERING THROUGH SERIES RESISTANCE

The meter can also be tampered by connecting it in series with the pressure coil. Under this situation, the current would be the same. However, the voltage would be divided using voltage divider circuit in such a way that lesser voltage will be there across the meter. Therefore the meter would record lesser power consumption than the actual. Forinstance if the voltage applied to the pressure coil of the meter is v, it would be divited into two parts V_1 and V_2. The voltage V1 would be there across the resistor connectedinseries of the meter and voltage V_2 would be across the pressure coil.This arrangement would be made in such a way that V_2 is lesser. For example if the system voltage is

63.5 Volts, it would be divided into 53.5 Volts across resistor and 10 Volts across meter.

The logicto create tamper detection mechanism would be the same as that usedfor parallel resistor. The IoT voltage sensors A and B wouldbe provided at the secondary of PT and pressure coil of the meter respectively. The inequality between signals A and B indicates the tamper event.

The input values of A and B are entered manually. However, while implenting actual program, theinputs would be receivedfrom system. The program would receive data on-line through IoT Sensors. This would be based on peer-to-peer communication model. The code for data communication can be written using Python or Java programming languages.The followingfour sets of inputs has been taken as a sample for running a program.

- Currents and voltages are same. The currents are 5 Amp, 5 Amp and the voltages are 63.5 volts, 63.5 volts. The output of the program indicates that the system is normal and no occurrence of tamper event is noticed.
- Currents are unequal but the voltages are same.The current st CT secondary is 5 Amp,whereas that at Meter is 2 Amp. Voltages at PT secondary and meter are 60 volts and 60 volts respectively. The tamperevent of parallel resistance isgenerated.
- Currents are equal that is 4.5 Amp each and the voltages are unequal i.e. 63.5volts at PT secondary and 10 volts at the meter pressure coil. The tamper eventof series resistance isrecorded.
- Both currents and voltages are unequal i.e. 4.2 amp , 2.1amp , 63.3volts and12.2 volts respectively at CT, meter, PT and pressure coil respectively. This indicates that themeter is tampered by providing series andparallel resistance both.

5. CONCLUSION

The main hurdles in revenue generation of the utility are T&D and AT&C losses. The technical losses are lesser and can be mitigated. Higher commercial losses indicate probability of theft of electricity. The billing meters installed at consumer installations are smart enough to detect tamper events such asCT reverse, CT Short, CT unbalance, PT low, PT missing and meter bypass. However, the existing arrangement is unable to detect tampering of meter done through series/parallel resistors. This paper has discussed an act of tampering of meter by inserting resistance in parallel and series with the meter. The novice and cost effective method to detect this event using IoT Sensors and microcontroller is suggested in this paper.

REFERENCES

[1] Finantial report published by *Maharashtra State Electricity Distribution Co. Ltd (MSEDCL),* Corporate Office, Prakashgad, Mumbai for the year 2019-20 (www.mahadiscom.in).

[2] Maharashtra State Electricity Distribution Co. Ltd- 14th Annual Report, 2018-19).

[3] R. Sudhir Kumar, T. Raghunatha, R.a. daeshpande, ‘Segregation of Techanical and Commercial losses in 11 Kv Feeder’. *2013 IEEE GCC Conference.*

[4] Surekha Bhalshankar, C.S.Thorat, Mahadiscom, Electrical Theft Controlling mechanism : smart grid advanced metering infrastructure and drone operated technology controling theft by direct hooking, *IEEE 2017 International Conference.*

[5] Mohd Uvais, ‘ Controller based power theft location detection technique’, *IEEE 2020 International conference.*

[6] Guo Lingging, Chen Xiaobin, Liu Zhaoming, Kang Jinping, Liu Bingchen, Liu Sha,’ Detection method ofpower theft based on SOM Neural Networks and K-means,’ clustering algorithm’, *2019- 22nd IEEE International Conference.*

[7] Salil Manocha, Vivek Bansal, Ishan Kaushal, Dr. Aruna Bhat, ‘Efficient Power theft detection using smart meterdatain in advanced metering infrastructure’, *proceedingson international conference on intelligent computing and control systems IEEE ICICCS2020*

[8] Ramesh Gaonkar, ‘ Fundamental of microcontrollers in embedded systems’, PHI Publishing.

[9] RL Reka, C. Ravikumar,’Microprocessor and Microcontrollers’, *Lakshmi Publishing, Chennai*

[10] Tim Cox, ‘Rasberry Pi Cookbook for Python Programmers’, *Prentice Hall of India Publishing. Second edition*

[11] RMD Sundaram,K.Vasudevan, Abhishek Nagarajan, ‘Internet of things’, *Wiley Publishing House*

[12] Dr. Shashikant Bakre, ‘Python Programmingin easy steps’, *Amezon KDP Publishing*

[13] Dr. Shashikant Bakre,’Electricity meteringin easy steps, an outline book on smart energy meters for every one’, *Amezon KDP Publishing*

[14] Dr. Shashikant Bakre,’Smart Grid’ , *Nirali Prakashan , Budhwar Peth, Pune*