Bulletin of Electrical Engineering and Informatics
Vol. 10, No. 4, August 2021, pp. 1828~1837
ISSN: 2302-9285, DOI: 10.11591/eei.v10i4.3014

An efficient and improved model for power theft detection in Pakistan

Abid Afridi[1], Abdul Wahab[2], Shamsher Khan[3], Wasi Ullah[4], Sheharyar Khan[5], Syed Zia Ul Islam[6], Kashif Hussain[7]
[1,6]School of Automation Science and Engineering, South China University of Technology, Guanghzou, China
[2]School of Automation, Northwestern Polytechnical University, Xian, China
[3]Department of Mechanical Engineering, University of Engineering and Technology Peshawar, Pakistan
[4]Department of Electrical (Telecom) University of Science and Technology, Bannu, Pakistan
[5]School of Software, Northwestern Polytechnical University, Xian, China
[7]School of Information Science and Technology, Dalian Maritime University, Dalian, China

Article Info

Article history:

Received Oct 21, 2020
Revised Dec 20, 2020
Accepted Mar 27, 2021

Keywords:

Automated meter reading
Microcontroller unit receiver transmitter
Subscriber identification module
Universal asynchronous
Universal synchronous receiver transmitter

ABSTRACT

This paper describes an improved model for the monitoring of power used by a party such as household users and different industries in Pakistan. The power theft detection was done using the intelligent internet of things (IoT) service system for calculating the user's power simultaneously. The power meter catches a theft detection device that is instantly transmitted to the central system which compares both the data by means of microcontroller and if there is any difference found, it informs the power utility about the hooking, meter relief or theft activities happen. Information of the theft detection through the global mobile communications system is transmitted and notified theft is displayed on the terminal monitor or won. As a result, although consumers continue to use excess fuel, the customer's power supply is cut in the electricity boards segment. The general radio package module system sends central circuit and meter data via an internet protocol address to a web server. GSM's IoT based perception is used to monitor the power supply and billing information calculated with a microcontroller continuously with the determination of the electricity table area. With this unit, the duplicate user can be located at the rear of the electricity office with the power meter status.

Corresponding Author:

Abdul Wahab
School of Automation
Northwestern Polytechnical University, Xian, China
Dongda Road, Changan campus of NPU, Xian, Shanxi province, China
Email: abdul_wahab@mail.nwpu.edu.cn, wahab.engr55@yahoo.com

1. INTRODUCTION

Since the beginning of electricity, it has become an essential part of our life. From the first electric bulb by Edison to the Tesla coil we humans have come a long way. Currently every little appliance operates on electricity from the electric toothbrush to huge motors [1]. Every year power theft is a major issue in the global power grid network, and it is both illegal and strictly forbidden. Pakistan is under develop country which has energy crisis, as everyday there is loadshieding of around 10 to 12 hrs and one of the causes of this issue is also power theft. In recent years, power theft has emerged as the most severe and widespread problem, resulting in major losses for electric utilities. As a consequence of the value of considering this problem, prices have been raised to resolve and overcome these losses [2]. Acoording to the different statistics provided by the WAPDA, Pakistan, they suffer each year more than 53 billion rupees per year

(0.3million USD) of power theft. The power theft across the globe is highest in Russia, which has the 16.2 million$ USD loss per year. According to the statistics Brazil has the second highest loss of 10.5$, where as USA with the total loss of 6million$ has the third and India with total loss of 5.10 million $ secured the forth highest per year. Power theft is the illegal use of electricity without a contract with the supplier. Illegal connections by electricity consumers cost power providers a large amount of money. Electricity theft is described as "a dishonest or unlawful use of electricity or service with the intent not to have a billing charge [3]." It's difficult to differentiate between truthful and dishonest consumers. They will never be able to completely eradicate fraud, but they can take steps to detect, deter, and remove it [4].

The implications of technical losses in generation, transmission, and distribution networks, as well as the overall performance of power networks, are being studied by power utilities. Since consumers are unaware of their energy usage before their electricity bills arrive, energy monitoring is possible. Electricity supply must be reliable, quality and secured. To do so, utilities need to have better information about the operation and the state of the distribution networks. For this to materialize, in the future, there will an increasing penetration of distributed generation connected to customer's premises and a shift from the traditional dominant large central power plants electricity generation concept to more complex power delivery [5]. Generation, transmission, and distribution networks all suffer from operational losses. Though generation losses can theoretically be established, transmission and distribution losses cannot be accurately measured using the data sent at the end [6]. It illustrates the existence of non-technical parameters in transmission and distribution lines for electricity. Power dissipation losses on transmission lines, transformers, and other power system components typically occur randomly [7].

The cumulative energy bill and the overall load are used to measure transmission and distribution technical losses. Despite the advancement of technology, illegal activity is also on the rise. With a professional look. Power theft is a serious offence that has far-reaching consequences for a country's economy. Non-technical power pilferage losses contribute to a large portion of the annual losses in the energy sector, which total about 25 billion dollars in world currency [8]. Electricity theft is a social problem that must be stopped at all costs. To make the most productive use of the generated electricity, power consumption and losses must be closely monitored. This system prevents unauthorized power use. At this point in technological growth, the issue of illegal electricity use can be solved using GSM and internet of thing (IoT) without human intervention. The client and the supplier have an arrangement in which the customer pays for the energy he uses. However, nearly 32% of electrical power consumed in India is not paid for, meaning that the consumer is cheated, necessitating the creation of a scheme to address this problem. This system primarily consists of a microcontroller, sensors, and an IoT module for detecting electricity theft and sending a message to an approved electricity management agency. Remote access to device functionality is included in today's submission. Connecting a device (energy meter) to the internet with efficiency [9] is one method of accomplishing the task. This device would save a significant amount of energy and provide power to a greater number of customers. The electricity board section uses an IoT-based concept to continuously track power consumption in the area. Power theft causes major impact on electricity system and institutions are:

- Theft of electricity leads to loss of income for the utility/institution
- Because of the undesirable load of the transformer, it causes blackouts or brownouts
- Property damage to the utilities, such as distribution transformers, protective instruments
- Increased losses in transmission and distribution due to cable and wire tampering

2. TECHNIQUES OF ELECTRICITY THEFT

There are numerous reasons for power theft, including high kilowatt–hour and secondary electricity charges, a consumer's low subsistence level, tax purposes, law enforcement's lack of accountability, economic crisis, and resulting increased poverty [10], [11]. Several power theft techniques are discussed as:

- Direct connection from the pole: Because the metres and equipment in this category are for 220 V systems, where the customers are largely residences and small enterprises, a direct connection from the pole is much easier than for high-voltage systems. Now, at least more securely, a pair of rubber gloves might provide all the protection needed and a lever and all the required equipment, in contrast to climbing up the HV lines. This is by far the most popular electric theft method.
- Use of Remote: On the market, there are certain remote controls that slow down the metre speed.
- Phase-to-phase connection: This is comparable to utilising an additional neutral line, with the exception that at 240 or 380 volts, the system voltage becomes the phasetophase voltage.
- Using alternate neutral lines: The single-phase system usually just has one cable coming into a residence, the hot line. Neutral (electrically linked to the earth) is normally grounded and occasionally generic via

the base of the building. So if a person manages to employ a tiny transformer and use it as "neutral," the metre that utilises the same neutral source reads down the input voltage to a decreased unit count.

- Meter tampering/breaking seal: This is quite similar to what happens with the HV metres.
- Other methods of electricity theft include: Detect a paying consumer nearby, damage to metre boxes and slow the spinning discs in the metre box using magnets [12].

3. RELATED WORK

The use of the high voltage distribution system (HVDS) was highlighted as a source of power and energy theft. The voltage line is normally 230v, but it must be increased to 350v by a voltage regulator, which is why it is 350v, but when it arrives at delivery, the voltage is again lowered by 230v alternative current (alternating current). The supply can be in 3 or 1 phases, depending on the load. The supply and consumption of energy determines a country's economic growth [13].

Power line communications (PLC) provides a range of new data transfer services that do not require the use of external cables [14]. Electricity tampering and safety have become a major concern for government agencies around the world as power prices have risen. Electric metering and energy theft have grown in popularity, particularly in populous countries like India and China [15]. The supervisory mechanism for power theft is the AMR (automatic metering system). The following are the key pathways of AMR; power supply, sensors, and controlling process are all included in the system meter module. Data transmission, telemetry, and loading systems are all examples of communication systems. The host modem for the PLC should be the same. The energy disparity between the host PLC modem and the PLC modem error arises if unlawful load is allowed [16]. The smart energy meter has been proposed as a revolutionary arrangement to encourage moderation and lower utility costs in recent years [17].

Electronic meters are used to keep track of how much electricity is used. It's a two-way touch that detects any power theft or power system problem [18]. A box is set up two meters away from the transmission and reception points. Around the head are current outlets, inspectors, and consumers. When shoplifting occurs, the current flow changes, and the inspector issues an alert to track the power theft. In this paper, the detection of fraud is addressed [19]. Smart meters make it possible to interpret non-technical loss functions, which were previously difficult. The smart meter also has functions that measure energy consumption and help consumers better understand their behavior [20]. We can use intelligent meters to track power theft in this way. Assume that the number of people staying in an apartment is' n. ' An inspector box must be installed in the center, and the transmission and reception sides must be separated by two meters. The present passes into the hands of the head, the inspector, and the consumers. If theft occurs, the current flow shifts, and the inspector issues a warning, allowing us to keep track of power theft [21], but our proposed system will have improved efficiency and will be economical as shown in Table 1.

Table 1. Comparison of all the method used for theft detection

S/NO	Methods used for controlling	Reliability of system	Economy	Efficiency of system	Methods used for controlling
1	Detection identification based on HDVS system	Normal	High	Poor	Detection identification based on HDVS system
2	Using PLC	Good	Normal	High	Using PLC
3	Using smart meter	Perfect	High	High	Using smart meter
4	Proposed power theft detection system	Perfect	Less	High	Proposed power theft detection system

4. PROPOSED METHODOLOGY

Many people engaged in illegal power theft in Pakistan, such as taping lines at events without permission, bypassing the meter, and so on. All the transmission lines are very old in Pakistan and it is very easy for peoples to do it so, as it is necessary to prevent electricity theft because many peoples and industries are at the loss because of this issue. IoT is a relatively modern technology [22]. Our proposed system states to identify power theft in real time also provide information about the nearest location of electricity theft as shown in Figure 1. This system has an online database that records all information about the delivery system, as well as the time and date [23]. The transmitted electricity, the voltage absorbed at a pole, and the electric pole serial number are all included in these figures. The voltage is measured against the passage of time. The pole number tells us where power theft is most likely to occur.

After the generation of electricity in power plant by means of turbines it is stepped-up and transmitted to transmission substation, where it is further transmitted to distribution substations. Hence, Power theft cannot be done in generation and transmission system, but it is possible in distribution system [24]. Hence, we have installed our central circuit on distribution transformer to measure the actual current value as well installed at consumer end which sends data through GSM to central circuit where the actual value of current and collective value of current received from consumer end are compared by means of microcontroller. If there is any difference between the actual and end users' current values, it means that theft is detected, and a text message is sent to authorize person through GSM else the same process will be in operation continuously.

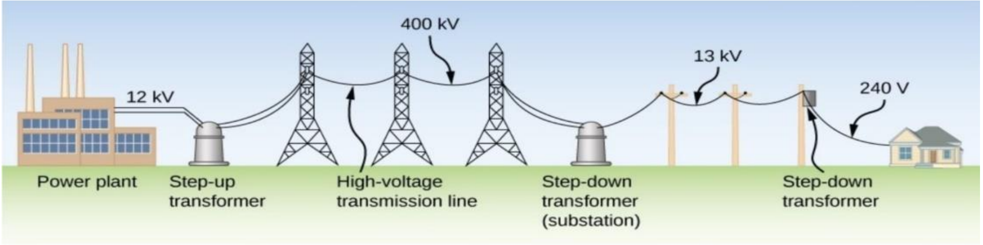


Figure 1. Implementation sciencario of proposed theft detection system

Power theft is an unlawful method of collecting energy for different purposes, resulting in substantial losses for successful businesses. Every year, almost $25 billion is lost around the world. By calculating the energy given and subtracting the actual amount of energy charged, losses can be measured. Electricity theft can be accomplished in a variety of ways, including bypassing a meter, modifying meters, billing irregularities, and unpaid accounts. Various scientific and non-technical approaches for detecting electric theft have been implemented in the past. Identification of clients with a suspect load profile is one example of a nontechnical technique. Periodic inspections can help to reduce robberies, but such measures necessitate a large workforce and a lot of hard work [25]. It fails in the majority of cases due to the staff's dishonesty.

4.1. Block diagram

The circuit is composed of a microcontroller ATMEGA328P, GSM, LCD and hall effect current sensor as shown in Figure 2. Meters should not be used for high currents because hall effect current sensors perform a current sensing. Two hall effect controllers are used, one of which is connected to the load side for the charging of the current and the other hall effect current sensor is connected to supply terminals for the evaluation of the current supplied by the source. The proposed method asserts that power theft and the nearest location of theft can be detected in real time. The system has an online database that records the data of the delivery system combined with the time and date. These statistics include transmission of electricity, voltage consumption at the bars and serial no electric pole. The voltage value is measured by time. The pole number shows us where the power theft is located. The important aspect of this circuit is the ATMEGA328P microprocessor. The current signal is acquired through a bridge rectifier from two hall effect current sensors. Then the conditional operator equals these two current magnitudes. Since the two hall effect current sensors disclose essentially identical numbers if there is no theft load. The system here is healthy. The microcontroller ATMEGA328P can not access the current signal. The hall effect current sensors therefore just need to be attached to a voltage source. In this scenario, the current signal must be translated into a voltage signal. The resistor can be linked to voltage in series. The ATMEGA328P microprocessor receives resistance and voltage information. Since the secondary current sensor Hall Effect is never able to open the circuit, a resistor is employed. Adjustments to the comparable current may be performed. Calibration can also be performed by connecting different loads, calculating different voltages and currents, and turning a current signal into a voltage signal with a correction system. The output over the resistor linked to the rectifier circuit, when the rectifier transforms the AC to a DC signal, can be used as a voltage signal. The input of the bridge corrector is attached to the side of the hall effect sensor. This voltage signal is received by the ATMEGA328P microcontroller and the calibration measures the related current. This translates the current signal from the current hall effect sensor into a voltage signal to access the microcontroller ATMEGA328P. If the hall effect current sensor is connected on the loading side, the same protocol is use. The aim of this program is to gain access to the voltage signals produced by the rectifier circuits. The software defines the condition for comparing voltage magnitudes. If the difference exceeds the specified number, the condition has been broken, and the control will switch to the SMS and email warning functions.

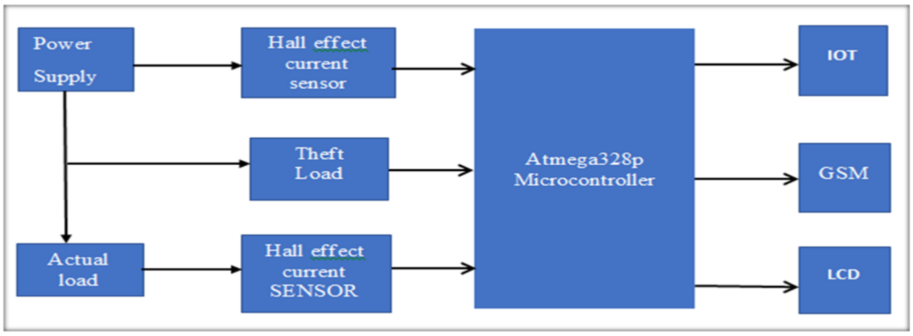

Power Supply
Hall effect current sensor
Theft Load
Actual load
Hall effect current SENSOR
Atmega328p Microcontroller
IOT
GSM
LCD

Figure 2. Proposed block diagram

5. RESEARCH METHOD

5.1. Software development & Implementation

Flow charts

a. Centre flow chart

The chart in Figure 3 illustrates the working process of central circuit. As it starts, first we declare and initialize variables like bit variable, it has values of 1 or 0, strings, integers (saves integers). Furthermore, we also initiate some modules like universal asynchronous receiver transmitter (UART) which is used for GSM connectivity because both are having transmitters and receivers & connect them in inverse fashion for better communication between them therefore, we also maintain same speed at both ends. In addition, ADC is also initiated because it converts analog signal to digital signal as microcontroller cannot read analog signal. Afterwards, we read ACS 712 sensor by means of analog channel as we have given the output of sensor to analog channel 0, thus we read this analog channel 0 and it gives us a number, so we find voltage from that given number and then find current.

Moreover, we have also developed a block for GSM which will receive values and after decoding we will get the overall current value sent by individuals. Now after getting both the actual value of central circuit and houses we can decide, if there is no difference between actual current and current value of houses it means that no theft is detected so if log time is not reached the same cycle will be in progress & if log time is reached then data will be sent to server. However, if there is a difference between both these current values it means that theft is detected, and message will be sent to authorize person & the process will be recycled.

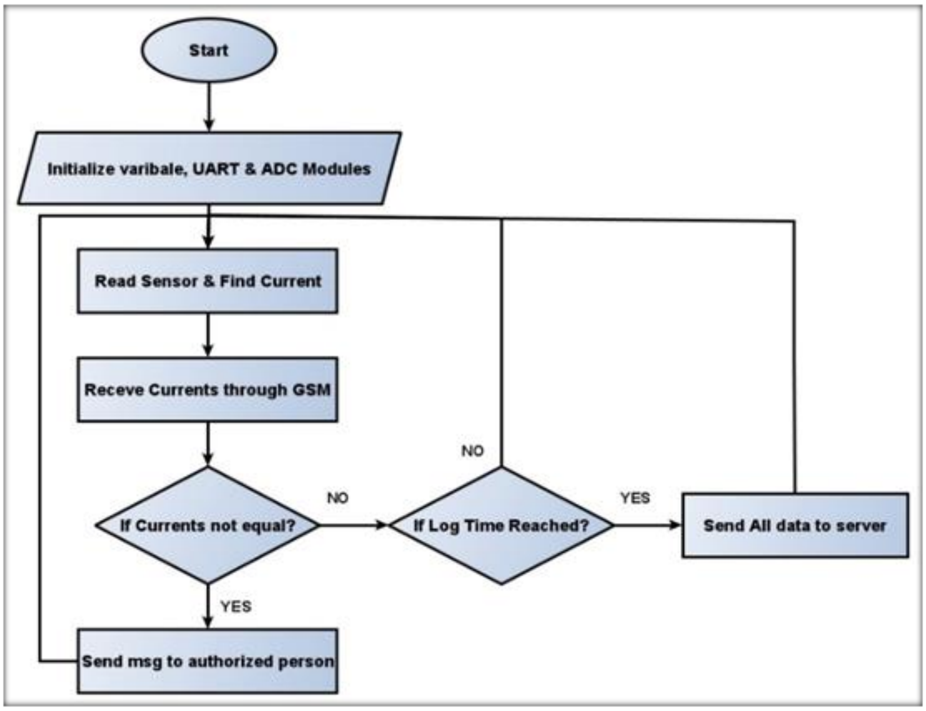

Start
Initialize varibale, UART & ADC Modules
Read Sensor & Find Current
Receve Currents through GSM
If Currents not equal?
NO
If Log Time Reached?
NO
YES
Send All data to server
YES
Send msg to authorized person

Figure 3. Center flow chart

b. House flow chart

Flow chart in Figure 4 describes the working process of house circuit. It is the simpler form of central circuit where it also initiates some variables needed like bit variables, strings or characters and modules like UART for GSM connectivity & ADC module for analog to digital conversion. Furthermore, we read current sensor and find current. At the phase of decision making, if log time is not reached the process will be continuously in progress & if the assigned time is reached the house circuit will send current value to central circuit.

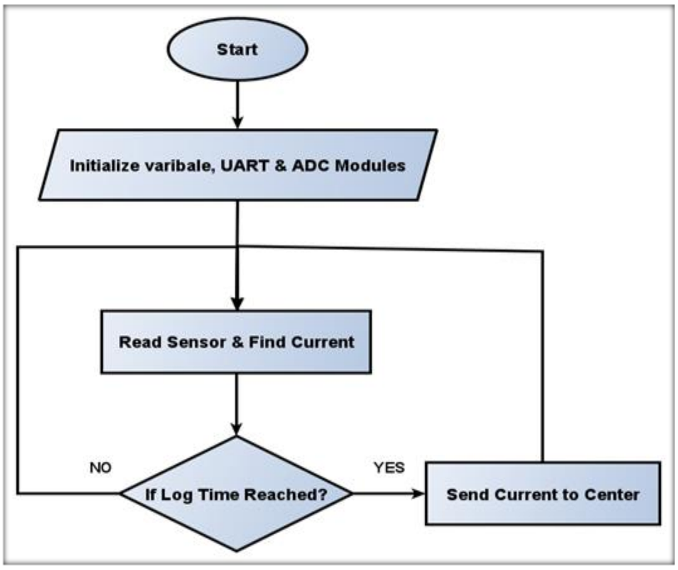

Start
Initialize varibale, UART & ADC Modules
Read Sensor & Find Current
NO
YES
If Log Time Reached?
Send Current to Center

Figure 4. House flowchart

6. SIMULATION RESULTS AND DISCUSSION

The work has been performed using the proposed methodology for the detection of power theft using IoT, as Figure 5 describes the normal load when there is no theft activity happened. when the is normal load it means that there is no theft occur and the house circuit is the replica of the central circuit and consist of hall effect sensor these sensors generate a hall voltage when a magnetic field is detected, which is used to measure the magnetic flux density. This sensor compares the supply voltage and actual voltage. The LCD displayed on the central circuit so same current reading as it is shown on the LCD on the house circuit it means that there is no theft occur. In this situation normal operation for circuits will be in progress and house & central circuits communicate regularly through GSM/GPRS module.

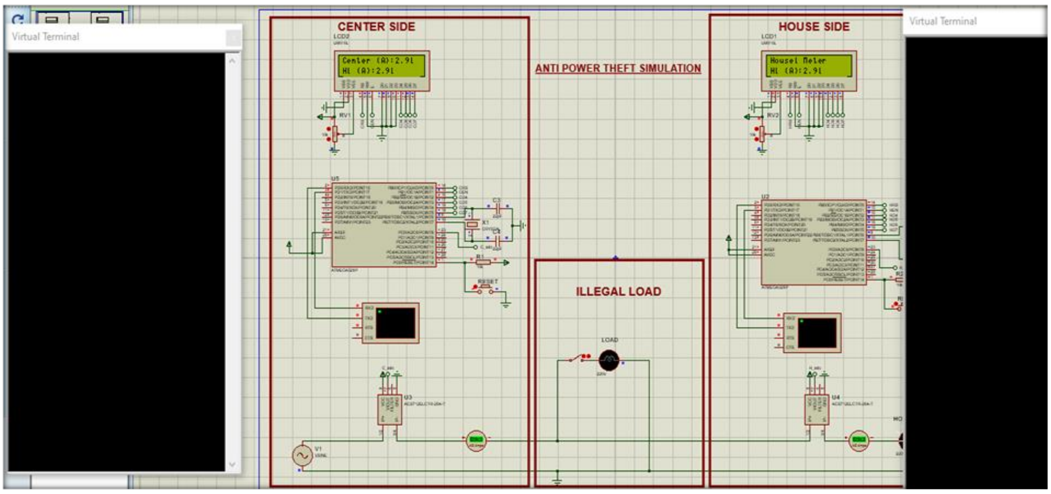
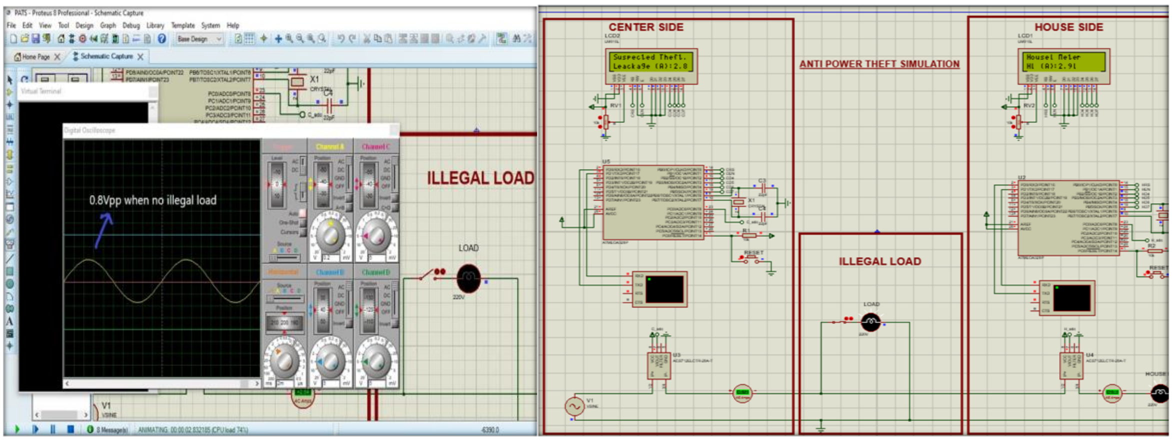


Figure 5. Normal load

6.1. Display of no illegal load

The given figure describes that when there is no theft occurred mean when there is no difference between supply voltage and actual voltage, the graph shown on oscilloscope will be normal and shows 0.8Vpp as it is shown in Figure 6 (a). This graph illustrates that there is no difference found between house and central circuit's value and the conditional operators on MCU detected no variance. This simulation shown in Figure 6 (b) shows when there was any theft, the house circuit sending data to central circuit for further process to compare it with the actual load. The entire connected house circuits send data to central circuit and collectively it is compared with actual value by means of microcontroller. There difference between both values occurred and "Suspected Theft" on both center and house circuits' LCDs as well a command was sent to GSM to send text message to authorized person.



(a) (b)

Figure 6. These figures are; (a) normal load when there is no illegal load, (b) theft load ON

6.2. Display of illegal load

When there is illegal load connected to the normal load the above graph shows such type of result as it as shown in Figure 7. This graph value is noted 1.6Vpp which is doubled as normal value when no theft was there. This result describes that there was a difference between the supply voltage of consumer side and actual voltage which means that there was an illegal connection. Reviewing the general concepts of Energy theft its types and detection methods. Moreover, we also discussed the previous work done in power theft using IoT. Thus, we developed a system named IoT based power theft detection system which is designed because of the flaws in the previous work like, HVD system efficiency was poor, PLC system was not much reliable while smart metering was costly & some deficiencies in IoT based detection systems. To avoid these flaws, we developed a smart system which requires no human contact, reliable, highly efficient and less costly to stop power theft.

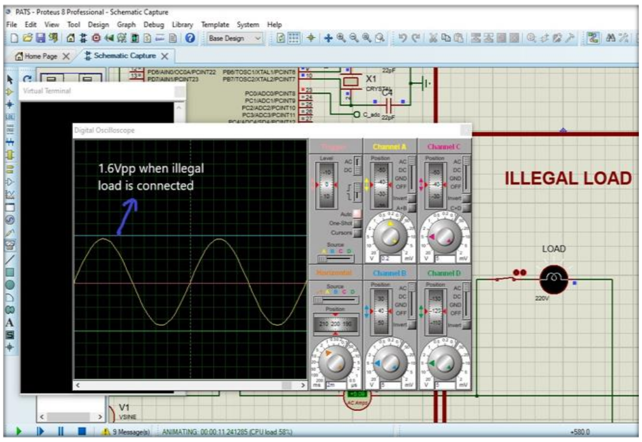


Figure 7. Demonstration of illegal load

7. CONCLUSION

We have concluded in this paper that the proposed theft detection system is used to solve major issues with existing electric supply systems, such as energy waste, power theft, and so on. The distributor will be aware of how much power in that area is to be used or how much energy will be stolen by people in that area if this system is used. When the difference between current values exceeds a certain threshold, an automatic message is sent to the appropriate authority and displayed on circuit LCDs, as well as data being sent from the power utility side to an online web server. It uses the GSM module to send the SMS to the distributor, and the proposed system will digitally alert or send data to a remote station using the GSM module. Some governments, such as Pakistan's, have proposed the development of intelligent cities based on the use of IoT related sensors, which are already being used in operational energy management, transportation, waste disposal, and resource conservation strategies around the world.

REFERENCES

[1] R Giridhar Balakrishna, P Yogananda Reddy, "IOT based Power Theft Detection," *International Journal of Innovations in Engineering and Technology IJIET*,vol. 8, no. 3, pp. 111-115, 2017, doi: http://dx.doi.org/10.21172/ijiet.83.016.

[2] Mazdi Muhammad Ali, Majdi Janice Gillespie, McKinley Rollin D, "The 8051 Microcontroller and Embedded System," *Prentice hall I ndia*, 3rd edition, 2002.

[3] Srujana Uddanti, Christeena Joseph, P. C. Kishoreraja, "IoT Based Energy Metering And Theft Detection," *International Journal of Pure and Applied Mathematics*, vol. 117, no. 9, pp. 47-51, 2017, doi: 10.12732/ijpam.v117i9.9.

[4] George M. M, Nikos D. H, "Review of non-technical loss detection methods," *Electric Power Systems Research*, vol. 158, pp. 250-266, 2018, doi: https://doi.org/10.1016/j.epsr.2018.01.005.

[5] A. A. Isqeel, S. M. Eyiomika, T. B. Ismaeel, "Consumer Load Prediction Based on NARX for Electricity Theft Detection," *International Conference on Computer and Communication Engineering ICCCE*, 2016, pp. 294-299, doi: 10.1109/ICCCE.2016.70.

[6] C. J. Bandim *et al.*, "Identification of energy theft and tampered meters using a central observer meter: a mathematical approach," *2003 IEEE PES Transmission and Distribution Conference and Exposition IEEE Cat*, No.03CH37495), 2003, vol. 1, pp. 163-168, doi: 10.1109/TDC.2003.1335175.

[7] S. Patil, G. Pawaskar, K. Patil, "Electrical Power Theft Detection and Wireless Meter Reading," *International Journal of Innovative Research in Scien*ce, Engineering and Technology, vol. 2, no. 4, pp. 1114-1119, 2013.

[8] Joaquim L.Viegas, Paulo R. Esteves, R. Melício, V. M. F.Mendes, Susana M.Vieira, "Solutions for detection of non-technical losses in the electricity grid: A review," *Renewable and Sustainable Energy Review*, vol. 80, pp. 1256-1268, 2017, doi: https://doi.org/10.1016/j.rser.2017.05.193.

[9] S. S. S. R Depuru, L. Wang, V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter-based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007-1015, 2011, doi: https://doi.org/10.1016/j.enpol.2010.11.037.

[10] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, P. Nelapati, "A hybrid neural network model and encoding technique for enhanced classification of energy consumption data," *IEEE Power and Energy Society General Meeting*, 2011, pp. 1-8, doi: 10.1109/PES.2011.6039050.

[11] A. H. Nizar, Z. Y. Dong, Y. Wang, "Power Utility Nontechnical Loss Analysis With Extreme Learning Machine Method," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 946-955, 2008, doi: 10.1109/TPWRS.2008.926431.

[12] Konstantinos, B. Georgios S, "Efficient Power Theft Detection for Residential Consumers Using Mean Shift Data Mining Knowledge Discovery Process," *International Journal of Artificial Intelligence and Applications IJAIA*, vol. 10, no. 1, pp. 69-85, 2019.

[13] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, M. Mohamad, "Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines," *IEEE Transactions on Power Delivery*, vol. 25, no. 2, pp. 1162-1171, 2010, doi: 10.1109/TPWRD.2009.2030890.

[14] Mayank Kumar Arjariya, Amita Mahor, "Modified Distribution Networks using HVDS Techniques," *International Journal of Engineering Research and Applications*, vol. 3, no. 5, pp. 1952-1955, 2013.

[15] I. H. Cavdar, "A solution to remote detection of illegal electricity usage via power line communications," *IEEE Transactions on Power Delivery*, vol. 19, no. 4, pp. 1663-1667, Oct. 2004, doi: 10.1109/TPWRD.2003.822540.

[16] A. Biranje, S. S. Lokhande, "Wireless ARM-Based Automatic Meter Reading & control system (WAMRCS)," *International Conference on Pervasive Computing ICPC*, 2015, pp. 1-6, doi: 10.1109/PERVASIVE.2015.7087019.

[17] Z. Xiao, Y. Xiao, D. H. Du, "Exploring Malicious Meter Inspection in Neighborhood Area Smart Grids," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 214-226, 2013, doi: 10.1109/TSG.2012.2229397.

[18] Prabhu. R, Geetha. A, Vadivelan. P, Ilayabharathy. L, "Smart Energy Meter with GSM Technology and Self Thermal Printing Technology," *International Journalof Emerging Technologyin Computer Science & Electronics IJETCSE*, vol. 12, no. 1, pp. 58-66, 2014.

[19] R. Jiang, R. Lu, Chengzhe Lai, J. Luo, X. Shen, "Robust group key management with revocation and collusion resistance for SCADA in smart grid," *IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 802-807, doi: 10.1109/GLOCOM.2013.6831171.

[20] C. Brasek, “Urban utilities warm up to the idea of wireless meter reading,” *Computer and Control Engineering*, vol. 15, no. 6, pp. 10-14, 2004, doi: 10.1049/cce:20040606.

[21] J. Nezhad, T. K. Wijaya, M. Vasirani, K. Aberer, “SmartD: Smart Meter Data Analytics Dashboard,” *Proceedings of the 5th international conference on Future energy systems*, pp. 213-214, 2014, Doi: 10.1145/2602044.2602046.

[22] T. A. Short, “Advanced Metering for Phase Identification, Transformer Identification, and Secondary Modeling,” *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 651-658, 2013, doi: 10.1109/TSG.2012.2219081.

[23] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, “Vision and challenges for realising the Internet of Things,” *Cluster of European Research Projects on the Internet of Things - CERP IoT*, 2010.

[24] R Giridhar Balakrishna, P Yogananda Reddy, M L N Vital, “IOT based Power Theft Detection,” *International Journal of Innovations in Engineering and Technology IJIET,* vol. 8, no. 3, pp. 111-115, 2017, doi: http://dx.doi.org/10.21172/ijiet.83.016.

[25] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, A. M. Mohammad, “Detection of abnormalities and electricity theft using genetic Support Vector Machines,” *TENCON 2008 - 2008 IEEE Region 10 Conferenc*e, 2008, pp. 1-6, doi: 10.1109/TENCON.2008.4766403.

BIOGRAPHIES OF AUTHORS

Abid Afridi was born in District Khyber KPK Pakistan. He received his bachelor degree from University of Science and Technology,Bannu KPK Pakistan with major in the Electrical Engineering (Telecom) in 2020. Currently he is enrolled with the school of Automation Science and Engineering, South China University of Technology, Guangzhou, China, for his Master degree in Electrical and Computer Engineering. His current research interest includes IoT and Time Sensitive Networking.

Abdul Wahab was born in Mardan KPK Pakistan. He received his bachelor degree in electrical (Telecom) engineering from University of Science and Technology, KPK Pakistan in 2018.He did his master degree from Chongqing University, Chongqing, China with major in electronics and communications engineering in session 2020. Currently he is enrolled at Northwestern Polytechnical University, Xian China for a PhD degree in control science and engineering. He is working as a postgraduate researcher in the state key laboratory of school of automation. His current research interest include adaptive signal and processing, filtering, radars and power electronics.

Shamsher Khan was born in District Orakzai KPK Pakistan. He received his bachelor degree from Balochistan University of Engineering & Technology Khuzdar Pakistan with major in the Mechanical Engineering in 2019. Currently he is completed coursework of master degree in Mechanical Engineering (Design) from N.W.F.P University of Engineering and Technology Peshawar, Pakistan His current research interest includes IoT and Time Sensitive Networking.

Wasi Ullah Khan was born in District Kohat KPK Pakistan. He received his bachelor degree from University of Science and Technology, Bannu KPK Pakistan with major in the Electrical Engineering (Telecom) in 2020.

Shahryar Khan was born in Haripur KPK Pakistan. He received his bachelor degree from University of Haripur University KPK Pakistan with major in the computer science in 2016. Later on in 2020 he received his master degree from southwest university of science and technology, Sichuan, China. Currently he is enrolled with the school of software, Northwestern Polytechnical University, Xian China, for his PhD degree in software engineering. His current research interest includes smart grid and android apps development.

Syed Zia Ul Islam Zia was born in District Swabi KPK Pakistan. He received his bachelor degree from University of Peshawar, Peshawar KPK Pakistan with major in Electronics in 2019. Currently he is enrolled with the school of Automation Science and Engineering, South China University of Technology, Guangzhou, China, for his Master degree in Electrical and Computer Engineering. His current research interest includes IoT, Time Sensitive Networking and Embedded Systems Technology.

Kashif Hussain is a PhD candidate majoring in Information and Communication Engineering at Dalian Maritime University, China. He received his Masters degree from Chongqing University in 2020. His research interest includes cognitive networks, smart grid, deep learning theory for efficient and reliable information transfer.