Pakistan Journal of Engineering and Technology, PakJET
ISSN (p): 2664-2042, ISSN (e): 2664-2050
Volume: 5, Number: 2, Pages: 171- 176, Year: 2022

Development of an Electricity Theft Detection System

Izhar Ud Din, Muhammad Aaqib, and Musawir Ghani

Department of Mechatronics Engineering, University of Engineering and Technology Peshawar, Pakistan
Corresponding Author: Muhammad Aaqib (enggraaqib@gmail.com).

Received: 15/04/2022, Revised: 20/08/2022, Accepted: 30/08/2022

Abstract- **Electricity theft stays a gigantic misfortune brought about by electricity appropriation organizations. This robbery emerges significantly increased when this is done by consumers. For example, meter bypassing, tempering meter, and so on. The main reason for the losses is the direct connection with distribution lines which means Kunda or hooking from electricity lines. So, an intensive method is required to stop this kind of electricity theft. This examination study offers a methodology for taking care of electricity meter bypassing and altering. The overall system or prototype is a real-time system and has been designed for 1 A load and two electricity meters, while it can be designed for the whole village or town, for low and high tension line we can't use this kind of sensor we have to use LT and HT CTs for example, 800/1, 500/1, 400/1, etc. and sending its data through GSM to the grad station. The system contains GSM modules, Arduino Mega, Arduino Nano, LCD, and three current sensors, in which one current sensor measures the incoming current from the main grid, and the other two sensors measure the current from the consumption side (electricity meter) and sent it through GSM to the grid station, in the grid station the consumption values coming from the electricity meters including possible losses in the transmission line and the values measured at the main line in the grad are comparing and shows on LCD if the grade station's current value is high from the sum of all the individual's values which is coming from every electricity meter in the region then there will be electricity theft and the system will detect theft and will cut off electricity automatically at that region. If compared values are the same then there is no theft of electricity.**

Index Terms-- **Kunda, Hooking, Tempering meter, GSM module, Arduino Mega, Arduino Nano, CT, and Current sensor.**

I. INTRODUCTION

The electricity losses in Pakistan are increasing day by day. Electricity robbery is a procedure wherein the consumer is utilizing electricity unlawfully, which makes enormous misfortunes for electric organizations. Electricity theft can be defined as, utilizing electricity from the utility without an agreement or changing its measurement [1]. The number of inhabitants in Pakistan is increasing with time and in this way, the utilization of electricity is likewise increasing. In Pakistan, electricity robbery is increasing among household consumers which causes financial losses to electric organizations and results in load shedding in the urban areas just as in the provincial territory. In 1998 the government of Pakistan took strong action and recovered Rs. 2.4 billion of unpaid electricity bills. [2]. Electricity theft happens in each locale in every area of Pakistan which is major trouble and has an awful impact on electricity. The significant reason for electricity robbery is meter misrepresentation and bypassing the meter and direct connection from the distribution lines [3]. A World Bank report shows that Pakistan privatized Karachi Electric Supply Company because of a poor operational and monetary system and a loss exceeding 30% of its total [4]. During electricity distribution in India, the losses are determined to be 30 to 45% [5]. The electricity losses are of two types one is technical losses, and the other is Non-Technical Losses (NTL). The major losses are non-technical losses. The 2014 report says the total generation of electricity in Pakistan is 17000 Mega Watts (MW) and the demand is 22957 Mega Watts. Thus, the electricity gap is approximately 6000 Mega Watts [6]. Multiple schemes and procedures are employed for electricity burglary identification worldwide. However, our attention is on those electric robberies which make a direct connection from electric distribution lines.

The project aims to design a GSM-based automatic electricity theft detection system. The discussion in this paper is to control electricity theft in Pakistan. Identification of illicit buyers is an incredibly testing issue in the present electricity design and utility's ordinary activities. Facing electricity loss is a challenging problem.

In this project, we worked mainly on two things to avoid electricity theft one is Global System for Mobile (GSM) and the Current sensors. The current sensor will take the consumption

units from the user and sends them to the grid station through the Global System for Mobile (GSM). This system will monitor the consumer units and send messages to the main grid stations and all the consumption values will be compared for theft detection.

The remaining of this article is organized as follows. Section 2 related work followed by the proposed method in section 3. Experimentation is presented in section 4. Section 5 provides the results of this paper and finally, section 6 conclusion and future works of this paper.

II. RELATED WORK

Many methods are used for electricity theft detection worldwide. However, the old previous method of electricity theft is manual. It is very difficult to move from house to house and find the exact location of electricity theft. In many developing countries' electricity theft is a big issue, and they face a lot of financial problems. Normally electricity consumers can be generalized as legal consumers and illegal consumers. There are different methods of stealing electricity. Some technique is used to harm meter terminals. Interface one of the heap terminals to the ground and open the ground wire from the vitality meter. When consumer demands are more in this case, they use illegal electricity. Sometimes the wrong calibrations of the meter reading also affect. In many countries, the usage of illegal electricity is punishable under their law. The easiest way to steal electricity is to make a direct connection from the distribution lines of electricity. The second easiest way to steal electricity is to tamper with the energy meter as shown in figure 1. There are many methods used to tamper meters, some of them are:

- Making a strong magnetic field near the meter.
- Putting high viscosity fluid in the disk to minimize the rotation of the disk.
- Making a shunt connection between incoming and outgoing terminals.
- Disturbing the coil of the meter.
- Mechanical shock to the meter.

In Pakistan, Islamic scholars gave Fatwa on the use of illegal electricity and termed it a sin. Different techniques are used to find illegal utilities against NTL. During the establishment of the system part of the issue is going to look if there should arise an occurrence of the wired system [7]. There are many issues with tempered meters, so it is important to make a proper setup of a meter [8]. Rubber-coated aluminum wire is also used which is banned [9]. One of the main problems with the electricity meter in the present day is to detect and eliminate theft [10]. The main reason for electricity theft is hooking from the distribution lines. At all the distribution and feeder lines, total phase current over a period is gathered, and both these current values are compared to evaluate the overall loss by electricity companies in the form of theft [11]. Some methods are selected to find power theft. These methods can gather, send, and make operations on the data between different meters. This method can help to control electricity theft. To develop this method, a remote method can also be implemented to control theft. Different kinds of sensors can also find electricity theft [12]. In many cases, sending a meter values ZigBee method is used [13]. An automatic system is established for electricity theft [14]. For theft detection current sensor is used, which measures the current flow in the lines. Electricity theft can be detected but not measured precisely [15]. It is an automatic system for finding electricity theft. The total electricity in the distribution lines from the main station is compared with the total consumption read by the meter. These current values are compared to find illegal consumption [16]. Moreover, the authors of [17][18] investigated electricity theft control system based on IoT, to monitor the current through the network (see Fig. 1).

FIGURE 1: Direct connection from electricity distributions lines

III. PROPOSED METHOD

The idea has been implemented and analyzed using data on the legal and illegal consumer sides. The easiest way to identify illegal consumers is to keep records of their energy consumption later several times in an hour and compare that data with the main line current in the grad station of that specific region. There are many ways of communication to send values from one place to another like the Wi-Fi module, Bluetooth module, and other different kinds of internet protocols. In this paper, GSM is used for wireless communication. The general block diagram that shows the electricity theft detection operation work is illustrated in Fig. 2. In the proposed method, the main components are Arduino Mega, Current Sensor, and GSM has been used.

A. ARDUINO MEGA

Arduino Mega is the main part of this system. Arduino Mega is interfaced with GSM Mini. The Arduino Mega received all the information from every home consumer through GSM and extract data to make a decision. It is also used to compare the difference between legal and illegal home consumers, to find whether electricity theft occurs or not when an electricity theft occurs the Arduino mega cut electricity through a relay. The Arduino model is shown in Fig. 3.

Specification:

Operating Voltage: 5V

Input Voltage: 12V

Digital I/O Pins: 54 (15 are PWM output)

Analog Input Pins: 16, UARTs: 4

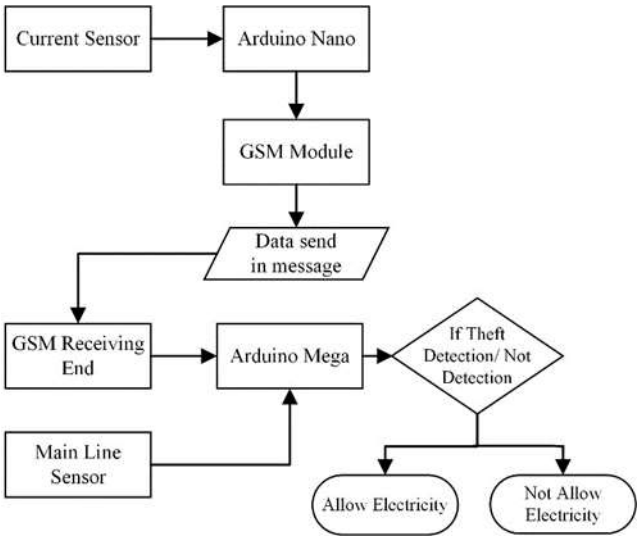

FIGURE 2: Block diagram of electricity theft operation

FIGURE 3: Arduino Mega

B. ARDUINO NANO

Every Arduino Nano is connected to home consumers. It extracts information from the current sensor and gives this information to GSM. This information is sent to the main station for comparison, to find electricity theft. Figure 4 shows the Arduino Nano model.

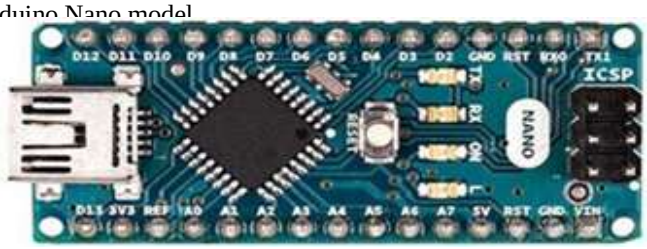

FIGURE 4: Arduino Nano

Specification:

- Operating Voltage: 5V
- Input Voltage: 12V
- Digital I/O Pins: 14 (6 are PWM output)
- Analog Input Pins: 8

C. CURRENT SENSOR

Current measurement is significant in many power and instrumentation frameworks. Current sensors are fundamentally used for circuit protection and control. Current sensor measure or detect current. The current sensor works on Hall-effect to measure all kinds of current like AC and DC. In this paper, the current sensor measures the current values of the home consumer and sends it to Arduino. The Arduino extracts the information from the current sensor and sends it to the main unit for electricity theft decision, Figure 5 shows the current sensor model.

FIGURE 5: Current Sensor

Specification:

- Operating voltage: 5V DC
- Current Range: 30 A
- Sensitivity: 66mV/A

GSM Mini: The GSM library contains numerous techniques for communication with the shield. This GSM modem can work with any GSM network administrator SIM card simply like a cell phone with its number. The preferred position of utilizing this modem will be that its RS 232 port can be utilized to convey and create embedded applications like SMS control, information transfer, controller, and logging can be grown effectively utilizing this SMS-based controller and alarms, security application, sensor observing, GPRS mode distant information logging. Here GSM module assumes an essential part of this task. The GSM Mini is interfaced with Arduino to send the extracted values from the current sensor to the main station for comparing the data and finding the theft. Figure 6 describes the specification and model of the GSM Mini model which has been used in the designed prototype.

Specification:

- Supply voltage range: 4.7V
- Operating current: 50mA
- Operating Temperature: -40°C to 85°C.

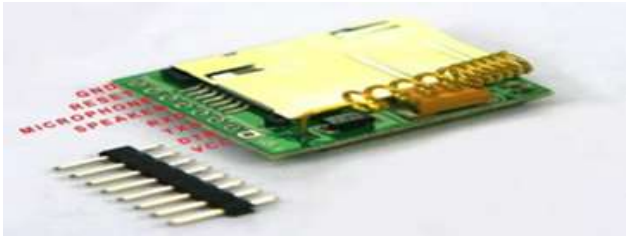

FIGURE 6: GSM 900A Module

D. RELAY

A relay is an electromagnetic switch. It is used to turn on or turn off a circuit by a low-power signal. In this paper relay control electricity to home consumers. The response of the relay is accurate and instant. When all calculation is done in the main station, then the main station decides an electricity theft occurs

and the Arduino mega give a signal to the relay to stop the theft of electricity. Figure 7 shows four- the channel relay model.
Specification:

- Input voltage: 12V
- Single Pole Double Through (SPDT)
- Input current: 5A
- Relay status LED

FIGURE 7: Four-channel relay

IV. EXPERIMENTAL WORK

On the consumer side, Arduino takes information from the current sensor. Then Arduino sends this data after a specific time through GSM to the main station. At the main station, the data is received from all connections which are made from the transformer.

All the data from every electricity meter in which we have installed this system, are send through GSM and received at the main station. When the last collected data is received at the main station then all the collected data are summed up and the Arduino takes figures (data) from the current sensor which has been installed at the main station for the whole area on the main line and compares that data with receiving data from all electricity meters and removing the possible power lost value which can occur due to heat and transmission line. Based on this comparison it decides if all the data are equal then it means no electricity theft occurs and it allows the electricity from the transformer to the home consumers if the data are not equal then it cut the electricity from the transformer through the relay cut off system. The first serial monitors show data on the screen and display all the commands which will be given to the GSM. With the IF condition, it checks whether the SMS is received or not from the home consumer.

IF the condition is true then the next step is to extract data from the SMS but if the condition is False then it checks the sensor data and display it on the LCD screen and again moves to the IF condition. After data is extracted from the message, then it converts information from the character type to the float type for making data suitable for calculation. As the calculation is completed the data is saved in the Arduino. After all the calculation is done, the next step is to compare this data with the sensor's statistics which was saved and displayed on the LCD before-after comparison, the next comes which to decide if the output data is equal to the input data, including possible line losses then a connection is allowed but if not then the connection of electricity to the homes are cut off. When the SMS is received, it is then converted to a character array, the SMS is changed to a character array because the ID of the individual meters is saved as a character. Now the message is checked one by one and by every identity

Which is saved in the Arduino data. If the message does not match the identity of the saved messages, then no further operations are done on the message and the array is reset to zero. The message-id is once checked, and it is matched with the identity of the saved meter. In FOR loop the message array extracts the digit one by one which contains the current sensor information. Every value is displayed on LCD and its follow meter-id which shows how much of every home consuming current. Outside the loop, all sensor value from the home consumers through GSM is stored in the Arduino to sum it. After summing all the values make it one output to decide in the IF condition whether to allow the power or not. The following Fig. 8 shows the flow chart of the developed method.

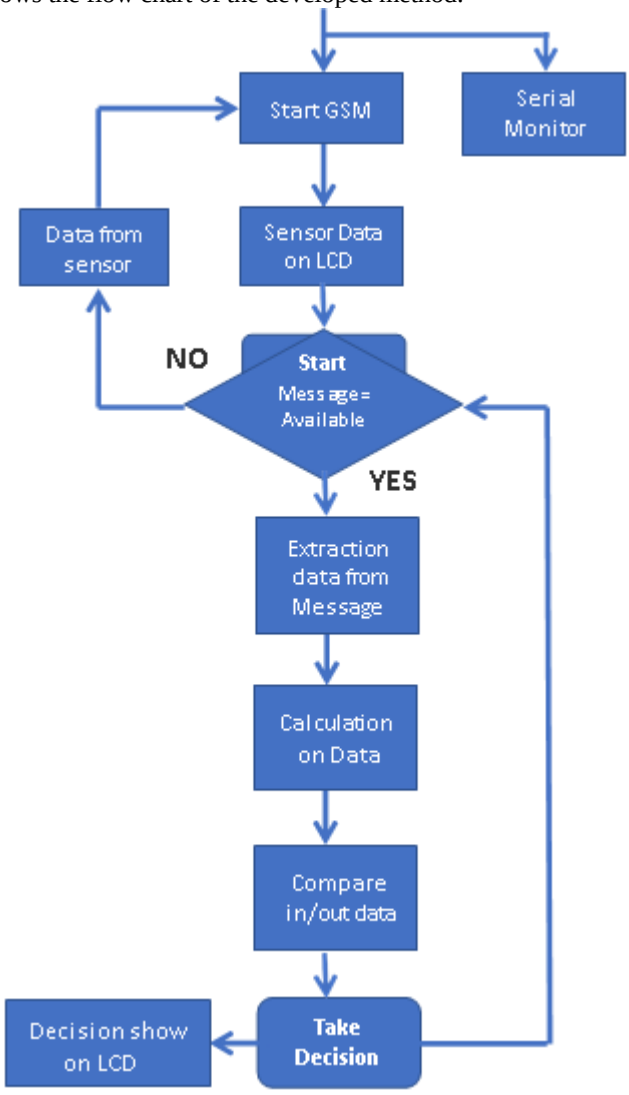

FIGURE 9: Flow Chart of Proposed System

V. RESULTS

A series of different experiments were performed on GSM and Current Sensors to get electricity theft. For this purpose, there are three kinds of load or home consumption were designed, two of them are legal home consumption and one is illegal home consumption. The legal home consumers are those consumers whose current consumption values send to the main comparing station through GSM. While illegal home consumers are those consumers whose current consumption values are not sent to the main station. The incoming current from the main station for the whole region is also measured by current sensors. When legal home consumers use electricity, their current values are sent to the main station. The current measured in the main line at the station and the sum of all the individual's current received from every home's electricity meter are compared. When both currents are equal including the possible losses in line so there is no theft of electricity, and the main station will allow current to home consumers. If the main station current and home consumer current are not equal it means electricity theft occurs and the main station will stop electricity to home consumers.

When only the legal home consumers use the electricity then no electricity theft will occur which is shown in table I.

TABLE I: Legal Home Consumer with No Electricity Theft

S. No	Legal home consumer 1	Legal home consumer 2	Illegal home consumer	Ele.Theft
1	0 A	1A	0 A	No
2	1 A	0 A	0 A	No
3	1 A	1 A	0 A	No

When the legal home consumers and the illegal home consumers use electricity, so the legal home consumer values will send to the main station and illegal home consumer values will not send to the main station. The main station will measure greater values than the legal home consumers and hence electricity theft will detect, and the main station will stop the electricity to the users as shown in table II.

TABLE II: Illegal home consumer with electricity theft

S. No	Legal home consumer 1	Legal home consumer 2	Illegal home consumer	Electricity theft
1	0 A	1A	1 A	Yes
2	1 A	0 A	1 A	Yes
3	0 A	0 A	1 A	Yes

Figure 10 shows the practical hardware design prototype for the overall system and also the experimental data has been taken by using the given hardware prototype. The prototype reflects the mechanism, procedure, data acquisition, and installation methodology for the overall system. It is a sample prototype design for 1 A current and for receiving values from two sides if we use it for actual grade station and for whole village and town then we have to change the sensors and use high capacity HT CTs and get their values compared from consumer's side and the main grade station's line values and detect the theft.

FIGURE 10: Hardware

VI. CONCLUSION

In this proposed framework a prepaid vitality meter takes the benefits of the GSM module and can access every home and every region. GSM is not only used for the communication of electricity but also for utilizing our energy meter to facilitate the use of electricity theft. The electricity theft information is directly sent to the main authorities and acts against the control of the supply of electricity. Whenever consumers use illegal electricity, the system will automatically detect electricity theft and will cut off the electricity.

GSM is used for sending information from consumption to the station but during testing GSM operating voltage is 4.7 volts and the voltages available are in standard volts like 5 volts and 12 volts. This is the main problem for GSM. To avoid this problem, Buck Converter is used to supply fixed operating voltage to GSM. Many times, the GSM signal is weak. Therefore, use the best Network SIM card. For sending data another module should be used.

For advancement internet of things can also be used in the project, it will facilitate the consumer easily their consumed unit will be sent to it and show the electricity theft. Do not use the WI-FI module because it will send your data but not receive it.

FUNDING STATEMENT

The author(s) received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] A. Chakraborty, B. Mahapatra, A. Das, and C. Sen, "Wireless Electric Theft Detector using Zigbee," vol. 6, no. 03, pp. 1401–1403, 2018.

[2] T. B. Smith, "Electricity theft: A comparative analysis," Energy Policy, vol. 32, no. 18, pp. 2067–2076, 2004.

[3] N. S. T, "Wireless Power Theft Monitoring System Using Zigbee," vol. 1, no. 5, pp. 144–147, 2017.

[4] P. Antmann, "Reducing technical and non- technical losses in the power sector.," Backgr. Pap. World Bank Gr. Energy Sect. Strateg., no. July 2009, pp. 1–35, 2009.

[5] A. R. Devidas and M. V. Ramesh, “Wireless smart grid design for monitoring and optimizing electric transmission in India,” Proc. - 4th Int. Conf. Sens. Technol. Appl. SENSORCOMM 2010, pp. 637–640, 2010.
[6] J. B. Faheem, “Energy Crisis in Pakistan,” IRA- International J. Technol. Eng. (ISSN 2455-4480), vol. 3, no. 1, 2016.
[7] A. Kamble, M. Torane, and P. D. M. A, “Electricity Theft Detection Using Zigbee,” pp. 2494–2497, 2018.
[8] L. Lq, H. Frqvxphu, and X. Dqg, “$Xwrpdwlf 3Rzhu 0Hwhu 5Hdglqj 6\Vwhp 8Vlqj *60 1Hwzrun,” Eng. Conf., pp. 465–469, 2007.
[9] M. Tarannu, “A Survey of Monitoring and Controlling Power Theft Problem in Local Area,” vol. 3, pp. 401–405.
[10] S. Arivazhagan, “GSM and Arduino based power theft detection and protection,” vol. 5, no. 4, pp. 581–588, 2019.
[11] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, “Measures and setbacks for controlling electricity theft,” North Am. Power Symp. 2010, NAPS 2010, 2010.
[12] I. Engineering, “Wireless Electricity Theft Detection System Using Zigbee Technology,” Int.J. Adv. Eng. Res. Dev., vol. 2, no. 06, pp. 1639– 1643, 2015.
[13] K.-I. Hwang, “Fault-tolerant ZigBee-based Automatic Meter Reading Infrastructure,” J. Inf. Process. Syst., vol. 5, no. 4, pp. 221–228, 2009.
[14] S. Thangalakshmi, G.Sangeetha bharath, and S.Muthu, “Power Theft Prevention in Distribution System Using Smart Devices,” Int. J. Appl. Eng. Res., vol. 10, no. 42, pp. 30841–30845, 2015.
[15] R. Kumar, S. Arora, S. Singh, and A. Tomar, “Design of Intelligent Electricity-Theft Monitoring System Using Matlab,” Int. J. Sci. Eng. Res., no. August, pp. 139–142, 2017.
[16] T. Kirankumar and S. M. G. N, “Power Theft Detection Using Probabilistic Neural Network Classifier,” pp. 834–838, 2018.
[17] B. Jaya Deepthi, J. Ramesh and P. Chandra Babu Naidu, "Detection of Electricity Theft in the Distribution System using Arduino and GSM," 2019 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), 2019, pp. 174-179.
[18] S. Mohanty, M. Mohamed Iqbal and P. Thampi M.S., "Controlling and Monitoring of Power Theft using Internet of Things," 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), 2021, pp. 111-115.