iJRASET

International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6087

Prevention of Power and Theft Detection through Consumer Load Profiling

R. Guruprasath[1], M. Abiram[2], P. Elangovan[3], C. Deepankumar[4], D. Jeeva[5]
[1]*Assistant Professor,* [2, 3, 4, 5]*U.G Student, Department of Electronics and Communication Engineering, Gnanamani College of Technology, Namakkal, Tamilnadu, India*

Abstract: Nowadays a development of technology growing today there are many technical solutions for power theft detection. Usually an electric power system can never be 100% secure from theft. Most of the systems the amount of theft is small in terms of the electricity generated.
But, the financial loss is high due to the large amount of electricity is disturbed. This paper develops an energy detection system called Smart Energy Theft System (SETS) based on machine learning and statistical models.
Keywords: Power theft detection, Power theft prevention, Consumer load profile, tapping transformer

I. INTRODUCTION

In developing countries electricity theft is a common practice especially in remote areas, as they do not pay utility bills to a government company. To solve these problem governments must think of as a electrical engineer to provide help in this issue. Proposed system contains Hall Effect sensor for measure the current and GSM modem for sending information via SMS and also sends throughout.

The system is used for immediate knowledge about electrical theft to concerned energy theft detecting squad. Electricity is a very precious resource. It has become an integral part of our daily life and we cannot think of a single task that can be done without electricity [1]-[2]. It is used in our home appliances and it is running our industries. It is in a way playing an important part in the world's economy.

In Karachi only, the estimated losses due to Power theft are almost at the price of Rs 53 billion. A recent report disclosed that electricity thefts from the national grid stood at 3.9 percent. Based on an energy supply of 120,400.5 GWh and unit scale price of Rs 11.37 KWh, the power theft came out to be 53.4 billion. The penalties for the loss are paid in form of more billings and load-shedding. Illegal consumers who commit these thefts remain unpunished and the penalties are paid by the legal consumers.

There are different types of electricity thefts, (i) Meter tampering, (ii) Direct tapings i.e. hooking system, (iii) Physical destruction of the meter and, (iv) stopping the rotating disk of the meter through some mechanism. All these types of theft are done either at consumer end or at the distribution line. The main objective of our proposed system is to develop an algorithm which detects thefts at both at the consumer end (meter tampering) and at the distribution line end (Hooking) with the help of consumer load profiling. Secondly, prevention of theft by penalizing the illegal consumer by damaging illegal connected loads. There are five different ways to generate electricity.

1) *Solar:* Mainly harnesses the power of the Sun to generate electricity.
2) *Wind Turbines:* Uses wind to generate electricity.
3) *Ground/Air/Biomass:* This method includes burning of fossil fuels to generate electricity.
4) *Nuclear:* Nuclear power can also be used to generate electricity.
5) *Hydroelectricity:* Water is used to generate electricity.

Most of the electric power production is through hydro power plants in Pakistan. The total hydro power resources in Pakistan are estimated to be about 50,000 MW. Hydro capacity in operation includes major plants at Tarbela (3,478 MW), Ghazi Barotha (1,450 MW) and Mangla (1000 MW). Gross hydro-electricity output during 2018 was 27.7 TWh accounting for 30 percent of Pakistan's electricity generation. Theft of this generated electricity through various means gives a severe blow to our country's already declining economy. Thus, there is a need for a simple, yet effective electricity theft detection and prevention solution which catches and punishes the culprits.

II. RELATEDWORK

Several authors have written papers on these thefts, their effects on their country's economy and methods to reduce those losses. In [3], the authors proposed a method to protect against theft using Zigbee module. This project consists of two subsystems; one part detects and measures the distributed voltage and current through transformer windings. If these measured parameters are above or below the previously measured levels then system automatically operate the circuit breaker, whereas, the other subsystem will only detect any theft occurred along the distribution line. In this system all the consumers consumed units are measured and if the total units of any consumer bypasses its energy meter then this system will detect theft occurrence in that particular area and send this information via GSM to related electrical office.

In [4], the authors proposed a system for detecting the power theft with an automatic circuit breaker and disseminating the information to concerned authorities using wireless radio line. Also, a statistical estimation procedure is used to minimize the error and noise in the measuring process. In [5], the authors proposed a system which is used to detect theft automatically. The main portion of theft that is being detected is the Hooking. A current sensor is used to detect the current flow in the system. If the taping draws more current than usual, then a hooking theft is detected. The occurrence of theft is quickly detected and reported to operator using GSM module. Authors in [6] have used Compressed Sensing to detect electricity thefts. In [7], the authors have used a Raspberry Pi and a fixed threshold voltage and current is set at the Raspberry Pi. Whenever the voltage level increases then power theft is detected. A cost- effective theft detection and prevention based on Internet of Things (IoT) is proposed in this paper [8].

Our system is based on the "Consumers load profile". It consists of three nodes, consumer node, intermediate node and an operator node. Theft detection is performed through formation of a load profile of the power usage and observing the abnormality in readings. We are also preventing theft on distribution line by using tapping transformer and by providing high voltages we are preventing illegal loads. Our projects works in a way that each consumer node reads power consumption of every consumer, the data is sent to intermediate node which reads output power of transformer and maintains each consumers load profile. This output power is compared with sum of power consumption of all consumers.

III. BLOCK DIAGRAM OF PROPOSEDSYSTEM

The block diagram of our proposed solution is shown in Fig. 1. There are three major nodes of operation in our project. These are (i) consumer node, (ii) intermediate node and (iii) operator node. These three are the major nodes that will explain the complete functionality of our proposed system; they are explained along with their functionality and further elaborated with the help of figures.

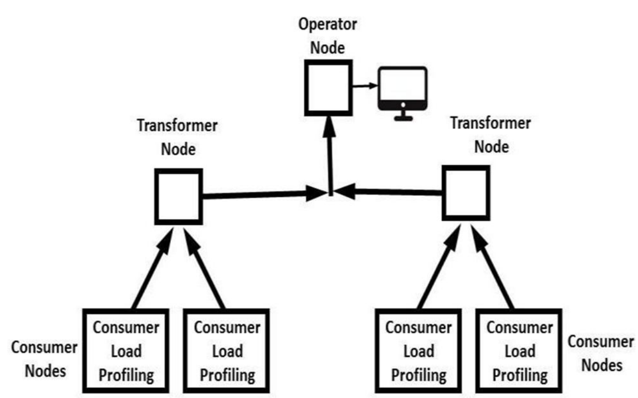


Fig. 1 Block Diagram of Proposed System

A. Consumer Node

Consumer node reads power consumption of each consumer and it transmits consumer power to the respective transformer node. The schematic diagram of the consumer node is shown in Fig. 2.

B. Transformer Node Or Intermediate Node

The intermediate node reads output power of transformer. It maintains load profile of all its consumer nodes and also compares the power supplied by the transformer with the sum of powers of all consumers connected to it. The schematic diagram of the intermediate node is shown in Fig. 3.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

C. Tapping Transformer

We have used 110/24 Volts transformer at the distributor line. It is a tapping transformer and has two output voltages i.e. 24 Volts and 30 Volts. In the two voltage values 24 Volts is normal voltage and 30 Volts is used to give high voltage when used for prevention. Following are the calculations for 110/24-30 Volts transformer that we have designed:

Core: 1.25" – 2.125"

A = 2:65625 in^2 = 2.65625 – 0.645 x 10^{-3m2}= 1.7137 x 10^{3m2}

Np = equiv248turns (21SWG; 1.5A)

B = 110/4.44 x 50 x 2488 x 1.7137 x 10^{-3}= 110/94.349

B = 1.165Wb/m^2

Ns = 56, 68turns (SWG - 17; 4.5A) Ip = 1.36 for 150VA, 110V

Is = 5A for 30V

E = 4:44fNø = 4.44fNBA N = E/4.44fBA

N = 110/4.44x50x1.165x1.713x10^{-3} = 48.28 turns

Where,

N=Number of turn

Np=Number of primary turns Ns=Number of secondary turns

Ip=Primary current

Is= Secondary current B=Magnetic flux density A=Area of core

SWG= Standard wire gauge

Fig. 4 depicts the designed tapping transformer that is used to provide 24 Volts and 30 Volts output.

D. Operator Node

The transformer node transmits the thefts detected and its location to the operator node. The operator node shows results on the PC. The overall working of our proposed theft detection and prevention system is as follows:

1) Consumer load profiling is used to detect any abnormality and identify the location of theft i.e. on consumer end or distribution line.
2) Consumer node of each consumer transmits consumer power to the respective transformer node.
3) The intermediate node maintains load profile of all its consumer nodes and also compares the power supplied by the transformer with the sum of powers of all consumers connected to it.
4) The intermediate node transmits any detected theft and its location to the operator node.

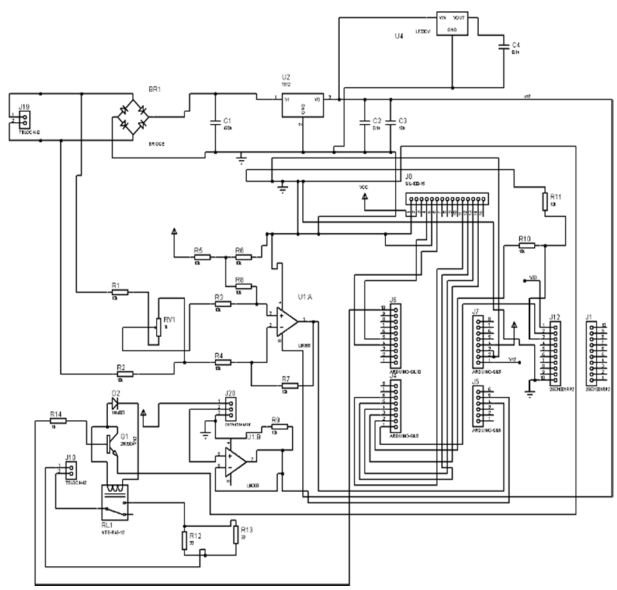


Fig. 2 Schematic Diagram of Consumer Node

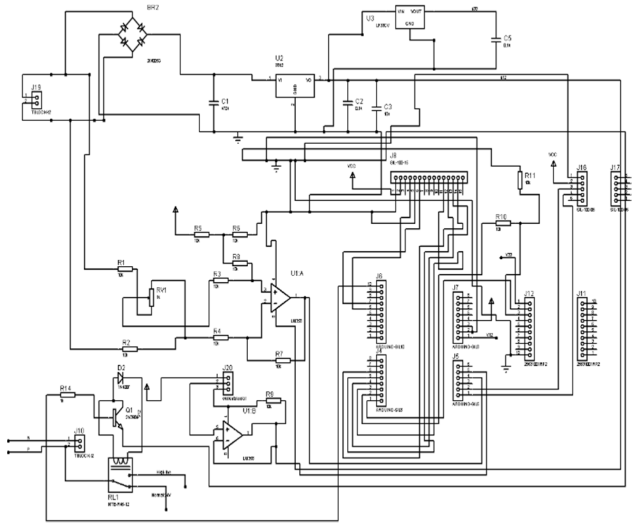


Fig. 3 Schematic Diagram of Intermediate Node

Fig. 4 Tapping Transformer

IV. POWER THEFT DETECTIONALGORITHM

This section details the theft detection algorithm as shown in Fig. 5. The step by step working is as follow,

1) Each consumer node reads power consumption.
2) Each intermediate node reads power output.
3) The output power of transformer is compared with the sum of power consumption of all consumers.
4) If there is abnormality, then it means there is theft and each consumer node maintains its load profile.
5) Each load profile of consumer node is compared with its previous value and it indicates the location of theft i.e. on consumer end or distributor line.
6) The intermediate node informs operator node about the theft.
7) If it is on consumer end (Meter Tampering), it sends consumer id of illegal consumer to the operator node.
8) If it is on distributor line, it tells operator node about illegal connection (Hooking) on the line.
9) Prevention is done on distribution line by giving high voltage to illegal consumer.

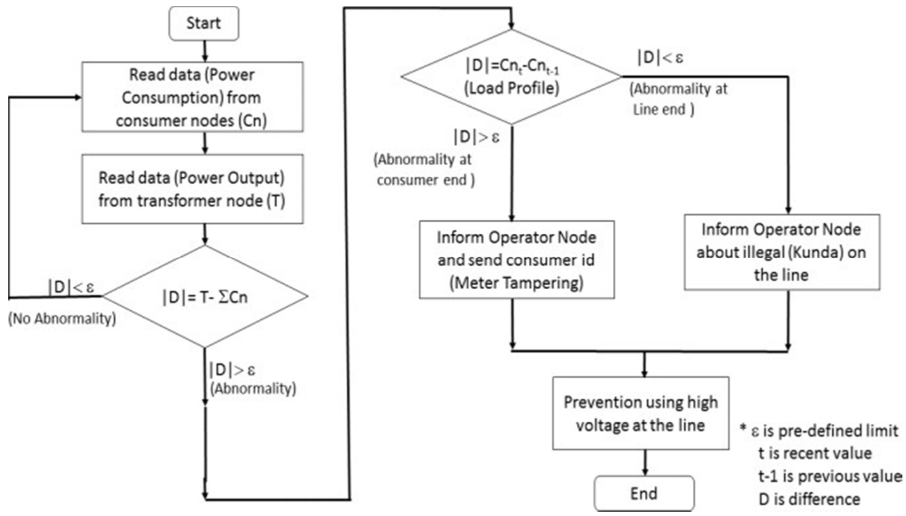


Fig. 5 Theft Detection Algorithm

A. *Theft Prevention Flow Chart*

After theft detection comes prevention. Fig. 6 shows the process diagram of how our proposed system prevents further power thefts. The step by step process for theft prevention is highlighted below.

1) For prevention, the intermediate node sends signals to turn off the legal consumers.
2) The legal consumers turn OFF when current reaches 0A.
3) The tapping transformer changes its voltage from normal 24 V to high 30 V using 12V DC relay.
4) The high voltage is given to illegal consumer to make their loads in-operational.
5) When the load of illegal consumer is in-operational, then voltage is changed from high to normal.
6) The legal consumers are turned ON.

V. LOAD PROFILE OFCONSUMERS

We performed consumer load profiling in visual studio using C Sharp. We have used three nodes, 2 consumer nodes and 1 intermediate node. The PC is connected with intermediate node using Arduino cable. When supply is turned on, the real times values of power consumption by the three nodes are displayed on the LCD are also displayed on PC. The power of intermediate node is compared with the sum of both consumer nodes. When the difference is greater than the predefined limit then it means there is theft on the distribution line which is called Hooking, or it is at consumer end which is meter tampering. And if the compared value is below the limit it indicates normal performance. This predefined limit is set to 200 Watts. The rationale behind choosing 200 W is that at our consumer node 1, the consumption of power is 2000 Watts, and at consumer node 2, the consumed power is 1000 watts because of load variation in the day and from load-profiling graph we see that the difference between both nodes is no more the 200 Watts, therefore, we set the limit to 200 Watts to save our legal consumers.

Now to explain the load-profiling graph, the Y-axis in the graph represents the power in Watts and X-axis represents the time in hours. Any node is turned off by pressing red button and is turned on by pressing green button. Following figures show the load profile of consumers both in case of normal performance and in case of theft.

A. *Normal Performance*

In case of normal performance, the compared power of both consumers and the intermediate node is below 200 W indicating the normal operation, as shown in Fig. 7.

The graph shown in Fig. 7. shows normal operation of consumers in a way that,

Predefined limit = 200Watts

Consumer 1 = 1891Watts and Consumer 2 = 763Watts Total = CN1 + CN2 = 1891 + 763 = 2654Watts

Intermediate Node = 2717Watts 2717 - 2654 = 63 < 200

So, there is no theft.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

B. Theft Detection

In case of theft, the compared values of the consumer nodes and the intermediate node are above the predefined limit indicating the presence of theft. This theft is indicated in Fig. 8. The graph shown in Fig. 8. shows theft detection when our predefined limit is exceeded,

Predefined limit = 200Watts

Consumer 1=1906Watts and Consumer 2=594Watts Total = CN1 + CN2 = 1906 + 594 = 2500Watts

Intermediate Node = 2783Watts 2783 - 2500 = 283 > 200.

So, theft is detected because our preset limit is exceeded.

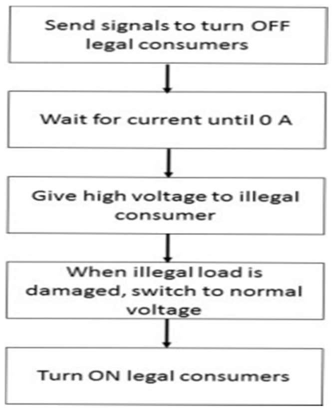


Fig. 6 Process Block Diagram of Theft Prevention

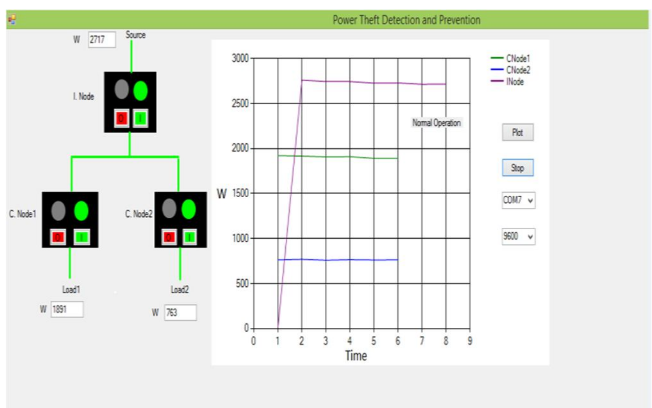


Fig. 7 Normal operation of Load-Profile

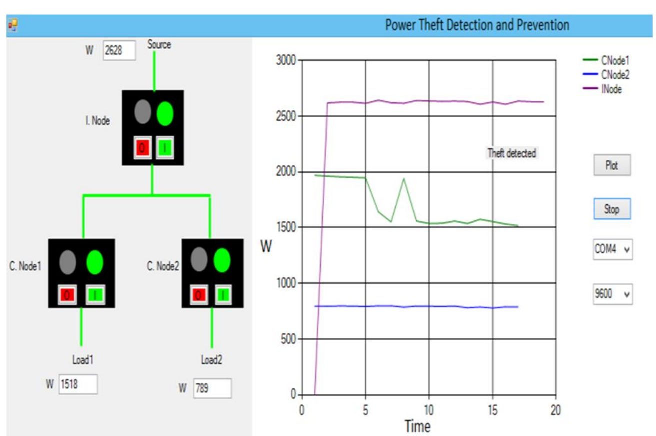


Fig. 8 Load-Profile Indicating Theft

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

VI. HARDWARE PARTS

Table.1shows the list of major components that we use ardiuno project along with their description and the purpose for which they were used in our project.

Table1. Description of Components Utilized

Components	Description	Purpose
Arduino UNO	Open-source micro-controller board based on the microchip Atmega 328P micro-controller, Operating voltage of 5 volts, Input voltage between 7 and 20 volts, 14 digital I/O pins and 6 analog input pins	Serial Communication
Zigbee	Wireless communication module which uses IEEE 802.15.4 standard, can be used as a transmitter and receiver both, Operating frequency 2.5GHz, Supply voltage 3.3 Volts	Data Transmission

Fig. 9 shows the complete operating hardware diagram of our project. The figure clearly shows different nodes. As shown in the figure, consumer nodes of each consumer transmit calculated power to the intermediate node, which after storing the consumer load profile compares the power transmitted by consumers with the power supplied by the transformer. After comparing the two values, the intermediate node sends the detected theft and its location to the operator node. For prevention, the legal consumers are first disconnected from the distribution line (through Visual Studio application) and then a high voltage of 30 V is applied to make the illegal connected loads in- operational and restrict further power theft.

Table 2. Final Description of Hardware parts

LF33CV	3.3v voltage regulator which provides 3.3v output voltage, 0.5 Amps current, three terminal device	To supply power to zigbee
ACS712	30 Amps Current Sensor, measurement range -30A to +30A, Supply voltage 5Volts	To detect electric current
12 Volts DC Relay	Relays control one electrical circuit by opening and closing contacts. When a relay contact is normally open (NO), there is an open contact when the relay is not energized	Circuit Switching
Transistor	2N3904 NPN bipolar junction transistor, used for low power amplification and circuit switching	Used for Switching
Bridge Rectifier	Converts AC voltage into DC voltage	Rectification
LM7812	12V voltage regulator, provides upto 1A, three terminal device	Power Supply

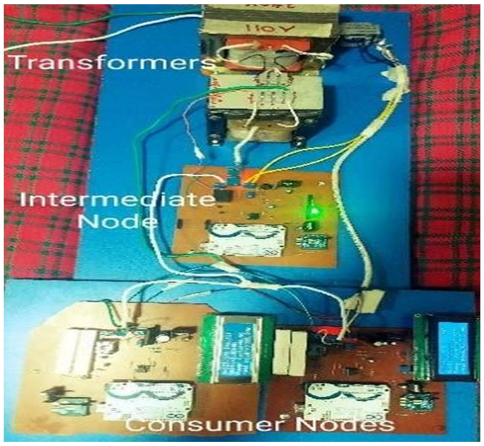


Fig. 9. Hardware Kit

VII. CONCLUSION

The project is determined and done in the case of seeing the real time examples in many of the places people do power theft for their own purpose that's why this has been done. This system is an automated system and requires no human interaction for its working once the system is installed. The proposed system provides an effective and easy way to detect electrical theft and gives effective solution for problems faced by Pakistan's electricity distribution system such as power theft on distribution line. The proposed system consists of two consumer nodes which measure the amount of power consumed and creates a load profile of the consumers. The intermediate node calculates the difference in the power values and through load profile checks for power thefts. A pre- defined limit of 200W is set as threshold for theft detection. Once a theft is detected, the prevention process disconnects all legal consumers from the line and then through the tapping transformer, high voltage is fed to the line to make illegal loads in-operational. The proposed solution is cheap and effective.

A. Advantage

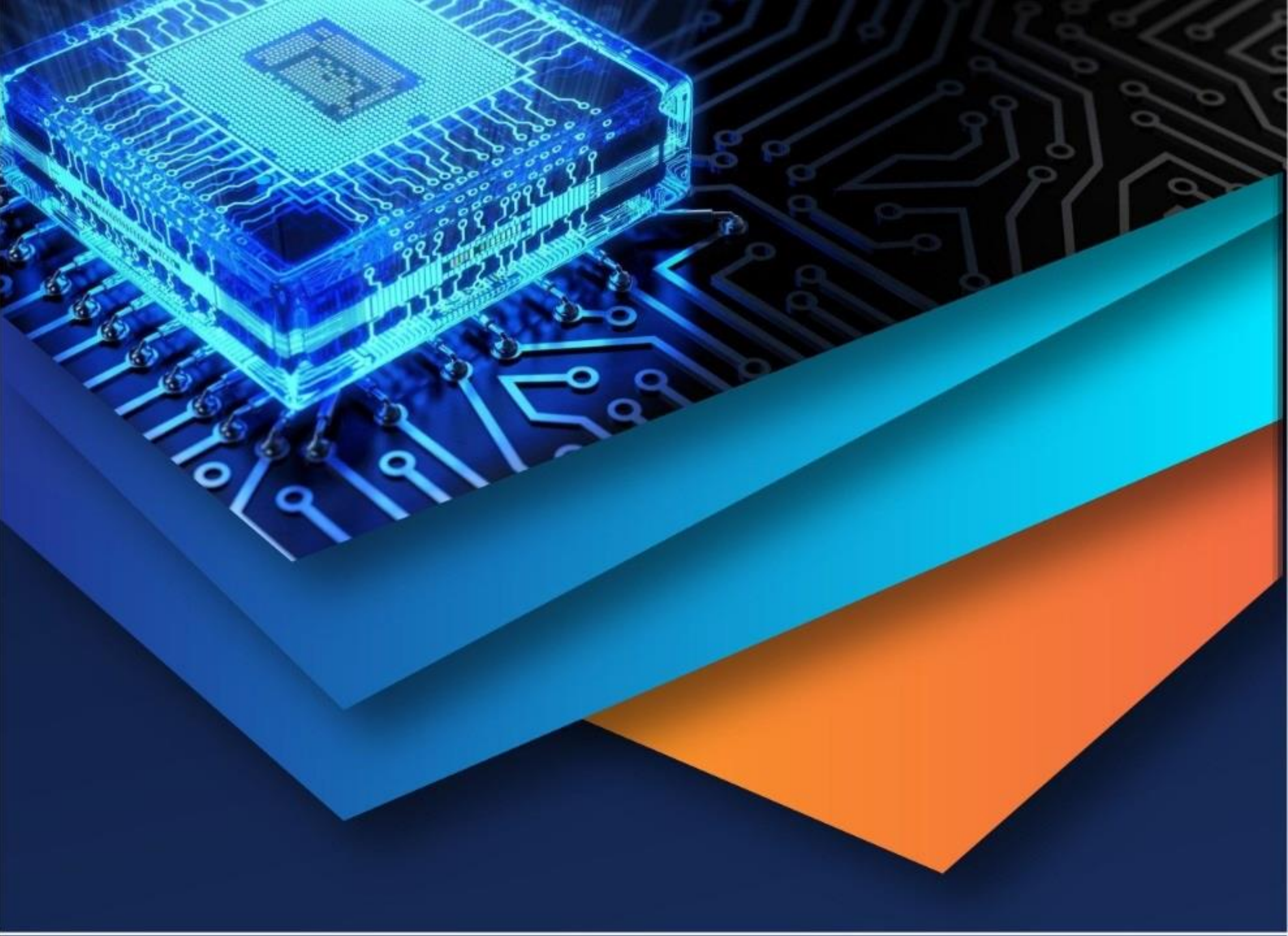
1) We can detect the location from where the power is being stolen which was not possible before.
2) Optimized use of energy.
3) We can get the information about electrical parameter values in power station itself

B. Disadvantage

1) One major disadvantage of this project is that it is not capable of detecting the exact location from where the power is being stolen giving only a approximation to that place.
2) Cannot determine who is stealing, but even no other existing system is capable of doing this.
3) If implemented on a large scale it may take a lot of time.

REFERENCES

[1] Rinkesh (2019) Conserve Energy Future, Available at: https://www.conserve-energy- future.com/different-energy- sources.php (Accessed: April 03,2019).
[2] World Energy Council (2019) World Energy Council, Available at: https://www.worldenergy.org/data/resources/country/ pakistan/hydr opower/ (Accessed: April 04,2019).
[3] Ashwini S. Pawar, Shagufta J. Jamadar, Pournima C. Mandle,VishwashreeV.Chawan,VishalS.Wadkar,
[4] `` Three phase distribution protection and theft detection using zigbee '', International Journal of Industrial Electronics and Electrical Engineering, vol. 4, no. 4, pp. 6-11.April-2016.
[5] Thangalakshmi Prakash `` Power theft prevention in distribution systems using smart devices '', International Jounral of Applied Engineering Research, vol. 10, no. 42, pp- 30841-30845. October 2015.
[6] L. Hinduja, M. Nivedha, B. Priyavadhana, `` GSM based electricity theft detection using arduino '', International Journal of Electronics, Electrical and Computational Systems, vol. 7, no. 3, pp-472-475. March2018.
[7] M. Lydia, G. E. P. Kumar and Y. Levron, "Detection of Electricity Theft based on Compressed Sensing," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp.995-1000.
[8] P. Leninpugalhanthi, J. R, N. s, M. RV, K. I and R. Senthil Kumar, "Power Theft Identification System Using Iot," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp.825-830.



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY