

# Power Theft Detection and Automatic Elimination

Sourav Tarafder\*<sup>1</sup>, Kamalika Banerjee<sup>2</sup>

Department of Electrical Engineering Narula Institute of Technology  
Kolkata, India

**Abstract:-** A novel system has been devised to eliminate power theft by automatic release of high voltage in the transmission line in response to the command received by the remote termination unit (high voltage source) from Arduino in the event of theft being detected. Due to the high voltage in the transmission lines, the pilferer’s appliances drawing power illegally by way of tapping get impaired. This operation is transient (for five seconds) and during this time, the supply of voltage for normal consumers is kept suspended. However, in case of emergency i.e., when the normal supply cannot be disturbed, the bypass mode is activated so that consumers continue to get an uninterrupted power supply. During this period, the process of theft elimination is kept suspended. The actual working of this novel system has been demonstrated by simulating the process in Proteus 8.6 and a working hardware prototype is developed. The process thus developed is effective and reliable.

**Keywords:-** Power Theft Elimination, Automatic, Current Sensor, Arduino, Relay Module, LCD, High Voltage Source, Proteus 8.6

## I. INTRODUCTION

Electricity power theft is a major problem in the power system network all over the world. Although it is illegal, the prevalent laws are not stringent enough to stop the theft. Every year there is an increasing amount of electricity theft across domestic as well as industrial electricity supply. This illegal theft of electrical power has affected the economic status of the country. The theft of electricity is a criminal offense and power utilities are losing billions of rupees on this count. The planning for production and distribution of electricity may be difficult in case of unrecorded energy usage. The aim of the project is to design a system that detects as well as eliminates the power theft in transmission lines by switching over from regular supply to the high voltage supply. Table I shows the loss incurred in a country’s economy due to electrical power theft.

US	INDIA	BRAZIL	RUSSIA
\$89.3B	\$16.2B	\$10.5B	\$5.1B

Table 1:- (Recorded data of loss in economy of a country incurred due to electricity theft).

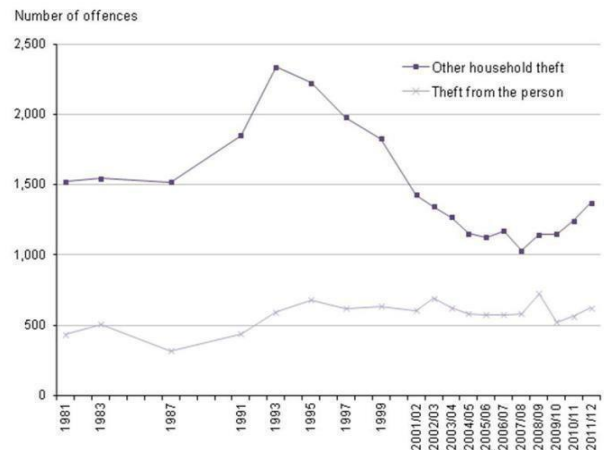


Fig 1:- Statistics of Power theft in India[ref.6].

## II. EXPERIMENTAL

### ➤ Materials and Methods

- Hardware used: Relay module, Current sensor, LED, High voltage transformer, and Arduino UNO.
- Software used: Proteus 8.6, Arduino IDE.
- Language:C.

## III. EXISTING SYSTEM

There are known reports on detection of power theft involving various techniques [1, 2]. These methods are mostly based on IoT using Arduino [3], IoT using microcontroller [4], GSM using Arduino [5] and IR sensor coupled with GSM using Arduino [6]. A system involving detection and disconnection of power theft from automated energy meter is also known [7]. Through an extant literature survey, it has been found that attempts have recently been made in eliminating power theft by way of switching system operated through the bit sequence generator involving microcontroller [6]. As far as this bit sequence is concerned, it allocates time for switching between these four lines (R, Y, B and Neutral). Therefore, neutral and phase lines are shifted after each allocation period i.e., at a particular time we can’t say which line conductor acts as neutral and which line conductor acts as phase conductor. If a smart energy meter were installed in the system, elimination of theft would be possible. However, the greatest limitation of this method is that by using an unregistered smart energy meter in between supply and drawl, the pilferers might uninterruptedly continue to draw or pilfer power as desired. The clever and intelligent way of misappropriating power by the pilferers may be explained with the analogy of the act of the resistant varieties of microbes/various pests, which otherwise evolve or adapt themselves suitably in order to overcome the effect

of the drug/insecticides administered to control them. So is the case with the power pilferers who reorient themselves to overcome/thwart the imposed mechanism of theft control by way of adopting suitable means (by using smart energy meter clandestinely). Besides, the feasibility of the system for practical applications is bit doubtful because so far the use of smart energy meter is limited in the country. Most of the villages, including semi-urban townships are still not using smart energy meters. In the recent past, a paper on the detection and elimination of theft using a combination of ZigBee and cycloconverter has been published [9]. In this work while transmission of data pertaining to power theft was carried out by using a device called ZigBee, the attendant elimination of theft was carried out by using cycloconverter, a device used for generating frequency distortion. In another similar work [10] cycloconverter has also been used for elimination of theft. In both the above cases, low frequency is used for damaging the appliances drawing illegal power. However, in the former case, the ZigBee used has a low transmission rate and cannot be used as an outdoor wireless device for communication system due to its short coverage limit. Therefore, apparently it cannot be a viable and pragmatic approach for power theft detection as well as elimination. Moreover, in both the system where they have used cycloconverter, the damage inflicted to the device drawing illegal power is not full proof because both the papers failed to demonstrate the real-time application of the working prototype.

The process of elimination of theft by way of inflicting damage to the illegally connected appliances is so slow (action of low frequency) that the actual damage caused is not instantaneous, and cannot be clearly ascertained/perceived. In another recent report [11], the authors have attempted to eliminate power theft by distorting the distribution voltage by placing a harmonic device near the distribution transformer. However, it is not clear whether the elimination is effective or not. It is quite likely that the smart pilferers might put a harmonic filter in between the points of supply and illegal drawl of power in order to overcome the purported theft elimination attempt made by the supplier.

#### IV. PROPOSED METHOD

A current sensor is used alongside to measure and compare the total incoming current into a zone with the sum total of the individual current consumed by the consumers. When there is an electricity theft in any part of the system either in the consumer premises or outside it i.e., between the distribution substation and the consumer (due to hooking or tapping the transmission line with a piece of wire), the sum total of current consumed by individual registered consumers is not equal to the total amount of current entering the zone (taking no-load losses in consideration). In such case, the Arduino senses that the theft is taking place in that particular zone, and accordingly switches on the theft LED which, in turn, effects automatic disconnection of the consumers

so as to safeguard them from the released high voltage of about 400V-500V (due to the command received by the remote termination unit from Arduino) which is obviously over and above the normal rated voltage (230V) in the transmission line. The magnitude of high voltage release towards the elimination of the theft can be varied over a wide range as per requirements.

As sensed by differential reading obtained from the system devised, a suitable voltage as per requirements is released into the system in order to eliminate the power theft. Thus, due to this high voltage, the normally rated appliances, which typically work at 230V, will be damaged at the theft side, thereby eliminating the theft. After 5 seconds the high voltage supply is turned off, and it checks whether theft is eliminated or not by comparing incoming current with the total current consumed by the individual registered consumers (taking into consideration the no-load losses). After elimination, the Arduino gives command to the relay to resume normal supply to the customers automatically. The whole process starting from theft detection, theft elimination and back to normal operation may take 5-10 seconds, which helps save the loss of huge amount of country's exchequer.

The system has also a bypass mode for individual zones, which skips the theft elimination process. This can be used at will when:

- There is an emergency during which power cannot be disconnected at any cost, for example, supply to hospitals etc., the system is put on bypass mode keeping the elimination of power theft in suspension.
- During instances when theft is not being eliminated by the release of high voltage.

Due to content/sustained use of this novel technique being put into operation for theft elimination, the process of electricity pilferage shall gradually reduce to almost nil because the pilferers shall ultimately stop pilferage as their very purpose of pilferage is defeated owing to their appliances getting constantly damaged due to high voltage being released into the transmission line in response to theft detection, thereby compelling the pilferers to refrain themselves from indulging into the practice of the very act of pilferage.

#### V. BLOCK DIAGRAM DESCRIPTION

##### A. LCD-16x2

It is named as 16x2 LCD (Liquid crystal display) because it has 16 columns and 2 rows. A 16x2 is a dot matrix LCD so in all it will have 32 characters, and each character is made of 5\*8 pixel dots.



Fig 2

**B. ArduinoUNO**

An open-source microcontroller board called Arduino UNO is based on microchip ATmega328P microcontroller. It is comprised of a set of digital as well as analog input/output (I/O) pins which can be interfaced as various expansion boards (shields) and other circuits. The board consists of 14 digital and 6 analog pins, and programmable with the Arduino IDE (Integrated Development Environment) through a B USB type of cable. It may be powered by an external 9V battery or a USB cable although it can accept voltages in range, 7 to 20 volts.

It works the similar fashion as Arduino Nano and Leonard do. The UNO board is the first of its kind in a series of USB Arduino boards as well as the reference model for the Arduino platform. The ATmega 328 on the Arduino UNO is available preprogrammed with a

bootloader, which allows uploading fresh code without the use of an External hardware programmer.

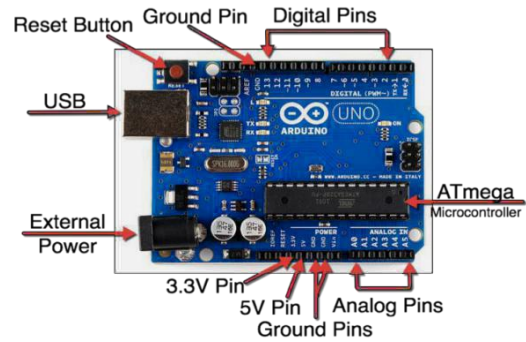


Fig 3

**C. Block Diagram**

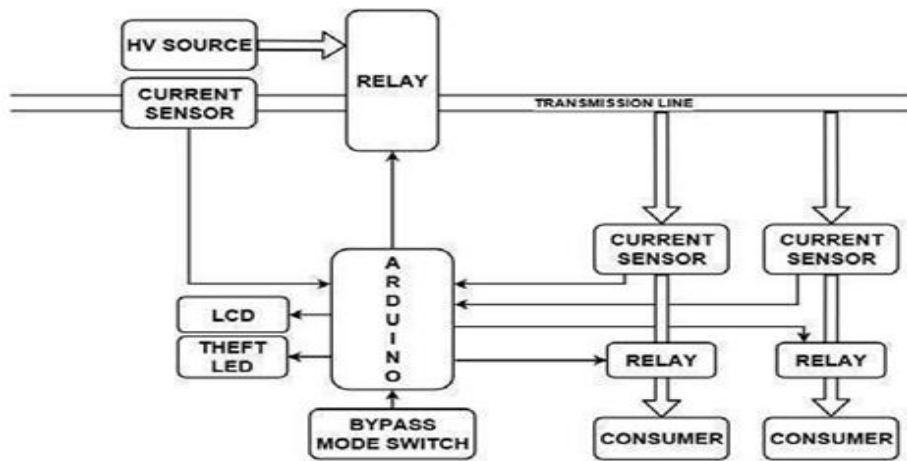


Fig 4

**D. RelayModule**

A relay is a switching circuit. In this work, we have used a 5V single channel relay to switch between normal and high voltage supply, also used for connecting and disconnecting the registered consumers with normal 230V supply. A 5V single channel relay has altogether 5 pins which are moving contact, N/O, N/C, and two coil terminals. When there is no theft in a zone (i.e. during normal supply), the moving armature makes a contact with N/C (normally closed) pin. And as soon as the theft is detected in a zone, the Arduino gives a command to energize the relay coil so that the moving armature makes a contact with the N/O (normally open) pin to release high voltage in the transmission line after disconnecting the regular consumers.

The current sensor ACS712 senses the current from ac supply and transfers the reading to the Arduino board. It is used to measure both AC and DC currents. The sensor is based on hall effect and the IC has an integrated Hall effect device. The applications of ACS712 current include motor control, detection of load, switch mode supplies, and overcurrent fault protection and management.

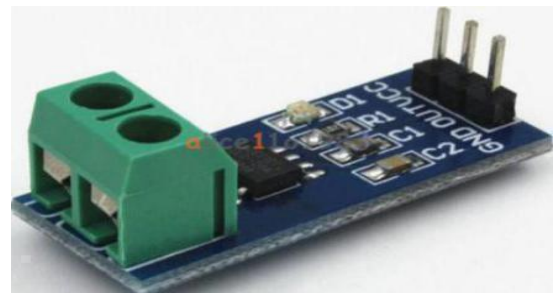


Fig 5



Fig 6

E. Flow Chart

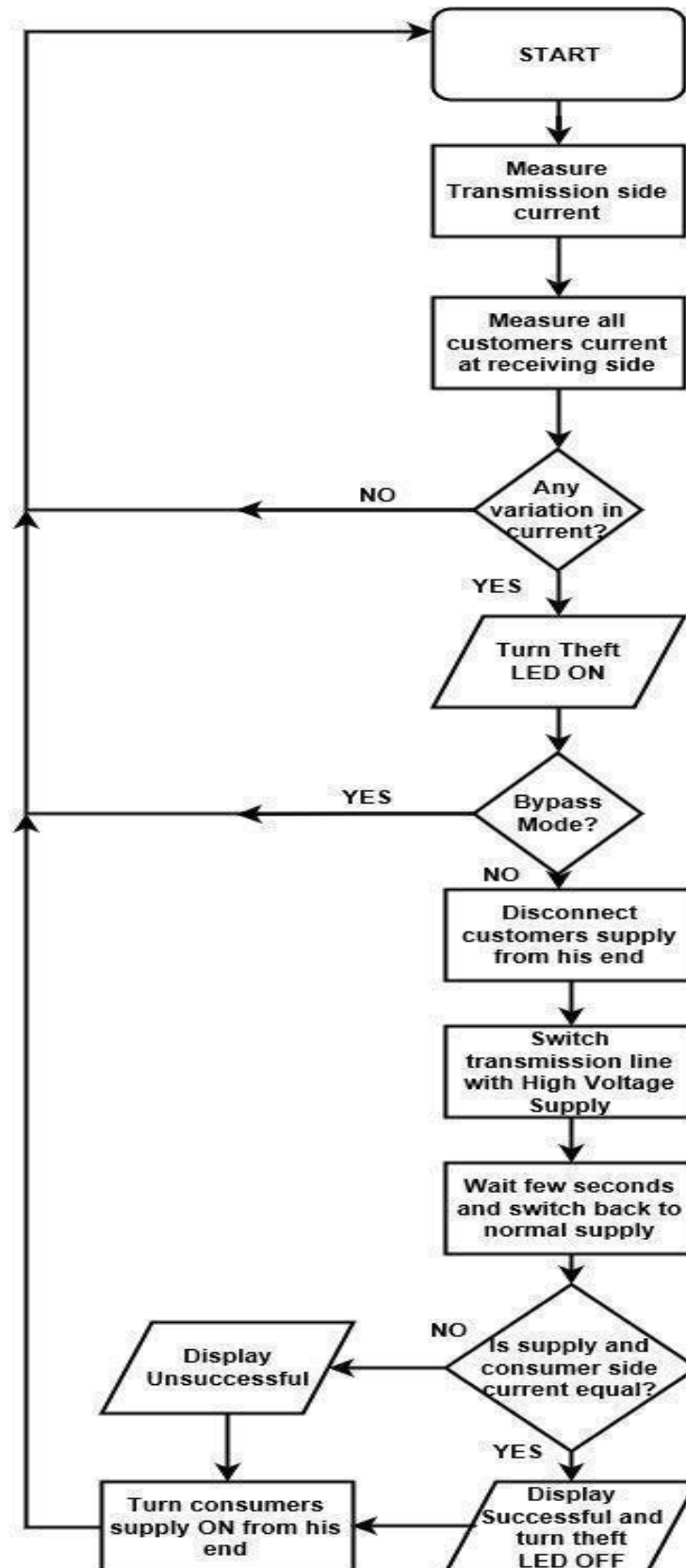


Fig 7:- Simulation Diagram



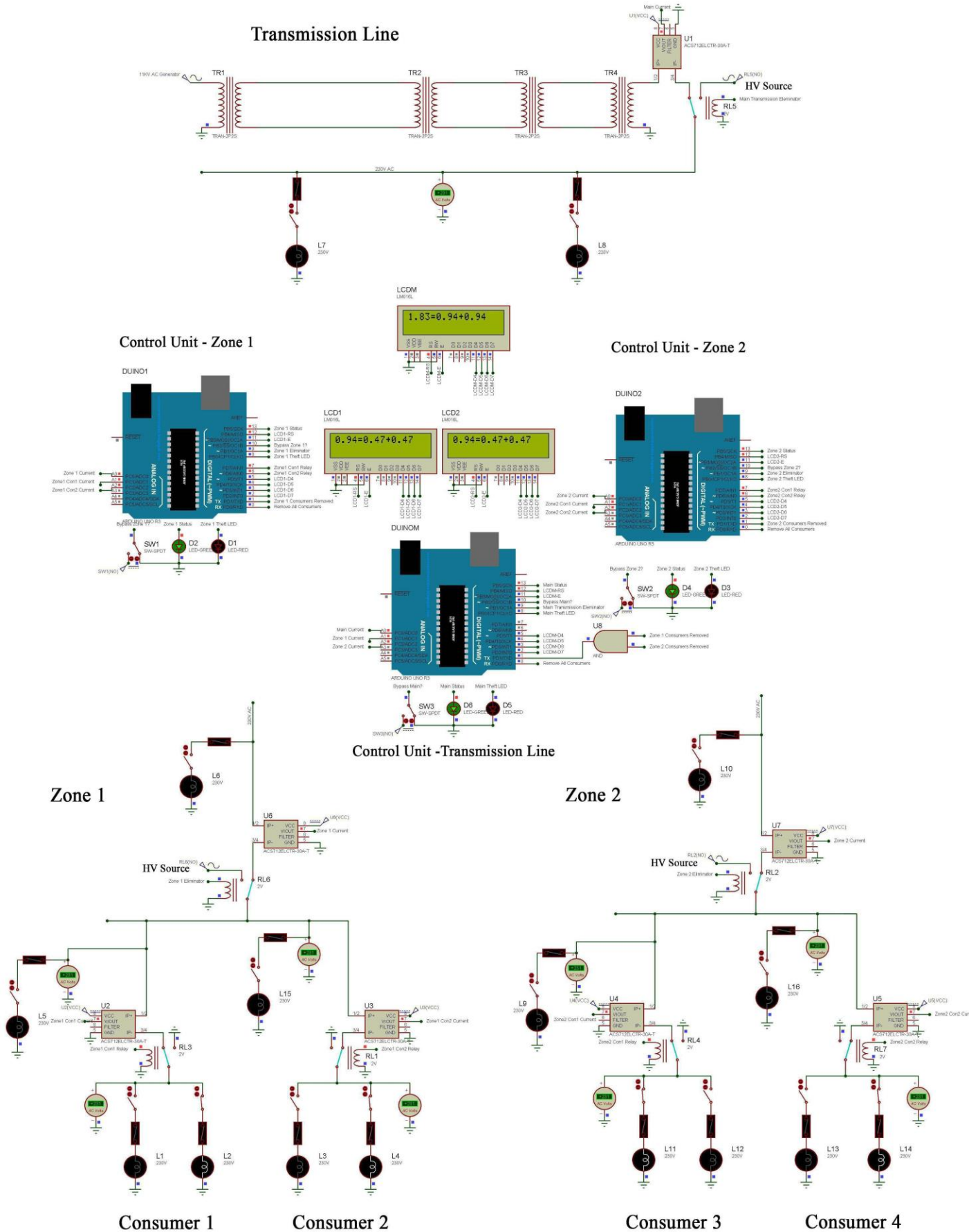


Fig 8

**VI. RESULT AND DISCUSSIONS**

The simulation work has been performed in Proteus 8.6 and the language used for programming Arduino is C. In this simulation work two zones have been delineated, but can be extended to N number of zones.

In this simulation work, the transmission line has been energized with 230V supply. There are two zones each covering two different consumers and each consumer has got two drawl points. In this case,

incandescent bulbs, each drawing a current of 0.47A arbitrarily, draw a total current of 0.94A. The LCD displays the consumed energy. For example, when two bulbs are switched on in the consumer side a total of 0.94A (0.47+0.47)A is expected to be displayed in the LCD. However, in case of any power pilferage, the sum total consumption of current is always greater than that consumed by two bulbs each of 0.47A (total is 0.94A). This aspect is clearly demonstrated by the data shown in Table II and Table III.

Capacity of bulb	The total number of the bulb.	Total Power Consumed (Displayed on LCD)
0.47	2	0.94

Table 2:- (Before Theft).

Capacity of bulb	The total number of the bulb.	Total Power Consumed (Displayed on LCD)
0.47	2	>>>0.94

Table 3:- (After Theft).

The process is so designed that the released high voltage from the source is restricted to the affected zone only, and under no circumstances, the same (high voltage) is leaked or transgressed to other adjoining zones. The latter design is more economical than the former owing to the fact that it is more cost effective because unlike the former design, only one high voltage source is able to cater to the need of power theft elimination in any of the zones.

Hardware for this operation has been designed considering two zones (The hardware video link is given in the footnote\*\*).The same can be extended to N number of zones.

In this simulated case study when theft is detected as discussed above, a high voltage to the tune of 400V-500V (due to the command received by the remote termination unit from Arduino) is automatically passed through the transmission line. This released high voltage instantaneously incapacitates or damages the devices pilfering the power. In this context, it is pertinent to mention here that while the respective Arduino (Control Unit), assigned for each zone, controls the functioning of that particular zone, the main Arduino (Control Unit) controls the functioning of all the zones put together. Additionally, it also helps eliminate theft, if any, nearby the distribution site.

**VII. ALGORITHM**

- Step 1: Initialize LCD and serial communication to all zones.
- Step 2: If requested for disconnection, disconnect the supply of all consumers and send success response until requested to reconnect.
- Step 3: Get the value of total input current to zone and the total current of individual consumers connected.
- Step 4: If current input to the zone is not equal to the sum of individual consumer's current, turn on theft LED.
- Step 5: If the bypass switch is off, disconnect consumers, otherwise go to step two. Also, if there is theft on the main zone send a disconnect signal to subzones until success response is received.
- Step 6: Switch to the high voltage supply for 1-5 seconds.
- Step 7: Switch to normal supply and check if sum of the individual consumer current is equal to the total input current. If yes, print successful and turn the theft LED off, else print unsuccessful.
- Step 8: Turn on consumer supply.

**VIII. ISOLATION OF ZONES**

The simulation diagram shown here involves separate high voltage sources for separate zones in order to eliminate power theft. However, one single high voltage source, as has been demonstrated further (The simulation video link is given to in footnote\*), is enough to eliminate theft taking place in any one or more of the interconnected zones.

\*[https://youtu.be/SKgurV\\_N93E](https://youtu.be/SKgurV_N93E); \*\*[https://youtu.be/ee-3uj\\_fpOg](https://youtu.be/ee-3uj_fpOg)

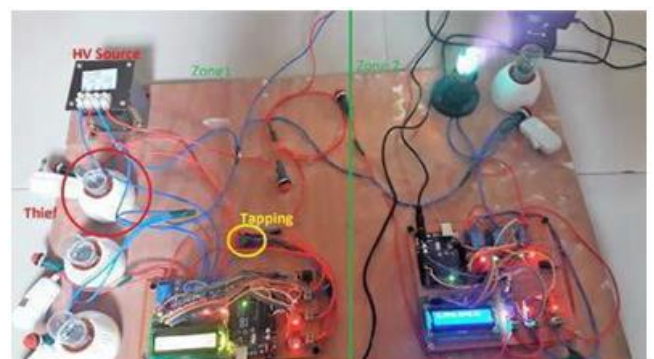


Fig 9:- Overall circuit Diagram of the system.

## IX. CONCLUSION

Up till now, innumerable methods are known for power theft detection. However, to the best of our knowledge, a limited number of methods are known for the detection and automatic elimination of power theft by a single system. Besides, as has already been mentioned, these methods are not quite effective in eliminating power theft. This prompted us to devise an effective technique for both detection as well as automatic elimination of power theft at any place. The method is simple, reliable and cost effective. In usual cases, the line is supposed to draw a specific load. However, in case more load is drawn than usual, the differential load registered by the Arduino (detection system) is a manifestation of definite theft somewhere as indicated by the LCD as well as LED display. The moment such theft is detected, a high voltage is automatically released in the transmission line (after disconnecting the normal supply to the consumers) which, in turn, damages the devices of the pilferers in the transmission line. This innovation as developed by us is recommended for use in detection and controlled elimination of power theft.

In order to make the method economically viable, it is ascertained that the cost of releasing high voltage into the system for elimination of theft should not exceed the cost of total power pilferage put together in that particular zone. The statistics of the cost of such pilferage can be gathered from the differential power consumption reading displayed on the LCD screen.

## FUTURE SCOPE

- As is evidenced by the experimental results presented in this paper, this novel technique may be adopted for rapid detection and elimination of possible thefts in the transmission lines.
- Once adopted, it would definitely save the appreciable loss of tax payer's money due to regular power theft.
- The system is designed in such a way that pilferers will automatically stop pilfering due to the scare of their instruments getting impaired.
- Thus, in future economic loss due to theft will automatically reduce.

## ACKNOWLEDGEMENT

The authors are thankful to Dr. Sandip Chanda, HOD-EE, NiT for his constant encouragement to do this project work.

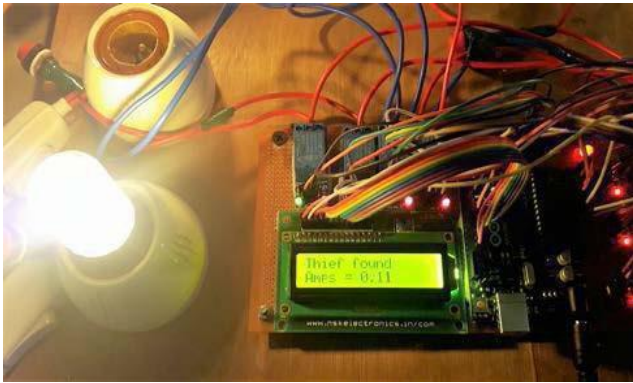


Fig 10:- Theft is detected.



Fig 11:- Theft is being eliminated.



Fig 12:- Theft has been eliminated successfully.

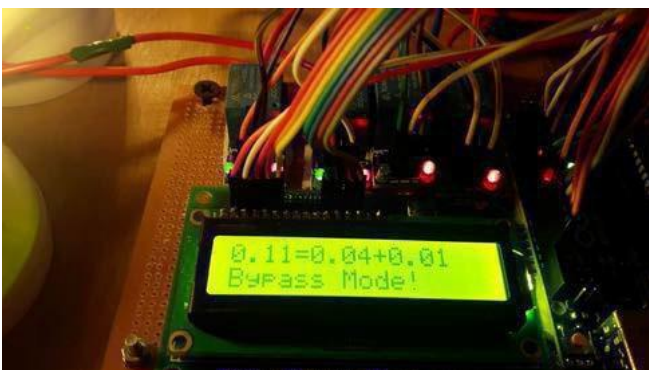


Fig 13:- Bypass Mode



## REFERENCES

of Engineering and Architecture), Turkey, vol. 32, pp. 121-130, September 2017.

- [1]. S.C. Yip, W.N. Tan, C. Tan, M.T.Gan, K. Wong, "An anomaly detection framework for identifying energy theft and defective meters in smart grids", *International Journal of Electrical Power & Energy Systems*, Netherland, vol. 101, pp. 189-203, October 2018. <https://doi.org/10.1016/j.ijepes.2018.03.025>
- [2]. M. Chakraborty, "Advanced Monitoring based Intrusion Detection system for Distributed and Intelligent Energy theft: DIET attack in Advanced Metering Infrastructure", *Transaction on Computer Science*, Berlin Heidelberg, vol. XXXI, pp. 77-97, January 2018. [https://doi.org/10.1007/978-3-662-56499-8\\_5](https://doi.org/10.1007/978-3-662-56499-8_5)
- [3]. R G. Balakrishnan, P Y. Reddy, and M N L. Vital, "IOT based power theft detection", *International Journal of Innovation in Engineering and Technology*, India, Vol. 8, pp. 111-115, June 2017. <http://dx.doi.org/10.21172/ijiet.83.016>
- [4]. H. Khandel, S. Pandey, D. Reynold, "A Review on IOT Based Power Theft Detection and Control System", *International Journal of Innovation Research in Electrical*, Electronics, Instrumentation and Control Engineering, India, vol. 5, pp. 161-163, September 2017. DOI10.17148/ IJIREECE.2017.5926
- [5]. L. Hinduja, M. Nivedha, B. Priyavadhan, B. Prema-latha, "GSM Based Electricity Theft Detection Using Arduino", *International Journal of Electronics, Electrical, Computational system*, India, vol. 7, pp. 472- 475, March 2018.
- [6]. A. Singhal, A. Tomar, N. Kumari, S.H. Kauser, S. S.C, "A Survey of IOT Power Theft Detection, Fault Identification and Location Tracking", *International Journal of Science, Engineering and Technology Research*, India, vol. 5, pp. 1662-1665, May 2016.
- [7]. S.S. Sayyed, R. Choudhari, P. Tribhuvan, S.S.A. Amte, "Theft Detection and Disconnection in Automated Electricity Energy Meter", *International Journal of Research in Applied Science & Engineering Technology*, India, vol. 6, pp. 2550-2554, January 2018.
- [8]. S.S. Mohammad, A.A. Dar, "Electricity Theft Prevention in Distributed System with Distributed Generation", *International Journal of Research in Science and Technology*, India, vol. 7, pp. 513-524, April 2018.
- [9]. S. Thangalakshmi, G.S. Bharath, S. Muthu, "Power Theft Prevention In Distribution System Using Smart Devices", *International Journal of Applied Engineering Research*, India, vol.10, pp.30841-30845, September 2015.
- [10]. P. Biswas, "Frequency Controlled Protection Scheme to Protect the theft of Electrical Power at Distributed End", *Journal of Electrical and Electronic Technology*, Romania, vol.5, pp. 60-67, May-June 2013.
- [11]. A. KARABİBER, "The Technical Revisions Required to Prevent Electricity Theft", *Çukurova Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi (Çukurova University Journal of the Faculty*