International Journal of Modern Science and Technology *Vol. 2, No. S1, 2017. Page 76-82.*
http://www.ijmst.co/ ***ISSN: 2456-0235***.

Research Article

Hardware Architecture for IoT Based Smart Power Management System

S. Kiruthiga, G. Balasubramanian, R. Malarvannan

Department of Electrical and Electronics Engineering, Arasu Engineering College, Kumbakonam - 612501. India.

Corresponding author's e-mail: keerthilakshmi251193@gmail.com

Abstract

The paper presents IOT based smart power management system. The system principally monitors and controls electrical parameters such as voltage and current and subsequently calculates the power consumed. The main goal of this project is to develop a newly equipped well designed prototype for consumers to provide secured power. The innovation of this system is controlling mechanism implementation. For controlling parameters, it sends a intimation to the user when the parameter exceeds their predefined values. The controlling process of electrical parameters that can be programmed using a ATMEGA32 controller and monitor even via mobile phone or PC from anywhere in the world. . To provide more confidentiality to the consumer, Trust Security Privacy (TSP) algorithm is used. To provide a high degree of security user or authenticator id is given by server to consumers. Due to that users only access their corresponding loads. Also, the proposed system is a user authentication, economical and easily operable. The system is a flexible and low cost and accordingly can save electricity outflow due to that we can save electricity expense of the consumers. To avoid a power theft, Power Theft Detection Algorithm (PTDA) was proposed and simulations are carried out in proteus software. Thus, the real-time monitoring of the electrical parameters can be observed over a website.

Keywords: Internet of Things; Power Theft Detection Algorithm; Trust Security Privacy; Sensors; Proteus software.

Introduction

Improvements in power electronics technologies and utilization of renewable energy sources for power generation have given rise to the use of distributed generation and create concept of smart grids and micro grids to overcome rapid increase in the demands for electricity and depletion of conventional energy sources. Monitoring of power system parameters like voltage, current and power at distribution level is crucial for efficient functioning of smart grid [1]. Monitoring of the power system essentially has two main modules: communication module which is the backbone and the sensor module for sensing the different parameters like voltage, current and power [2]. With support of information and communications technology, smart meters can be controlled and monitored remotely over the wireless broadband public network. Therefore, smart meters are vulnerable to cyber-attacks due to connectivity and communication through the open space [3]. The system has low-cost design, user-friendly interface, and easy installation in home or multi-purpose building. Using this technology, the consumer can reduce the wastage of electrical power by regular monitoring of home appliances or the proper ON/OFF scheduling of the devices [4].

The term Internet of Things (IoT) is an intelligent network, that promptly achieving ground in the context of modern wireless telecommunications. The IoT has recently become universal to highlight the vision of a global structure of interconnected physical objects. The prime purpose of this concept is the universal presence around us of a variety of things or objects. This includes Radio-Frequency Identification (RFID) tags, smart meters, sensors, actuators, smart phones, etc. These objects or things, are able to interact with each

Received: 10.04.2017; Received after Revision: 15.05.2017; Accepted: 16.05.2017; Published: 19.05.2017

other through unique addressing schemes, and cooperate with their neighbours to achieve common goals [5]. IoT technology is a new information processing and acquisition method, including radio frequency identification technology, sensor technology, smart technology, nanotechnology and other technologies [6].

It has been considered as the third wave of the information industry after computer, Internet and mobile communication network. Now it has been widely used in intelligent transportation, industrial monitoring, environmental monitoring, defense and military, digital family and other fields. Internet of Things is an important technical mean to promote the development of smart grid [7]. The project proposes an efficient implementation for IoT used for monitoring and controlling the appliances via World Wide Web. They can communicate with home automation network through an Internet gateway, by means of low power communication protocols like ZigBee, bluetooth etc [8].

IoT is an emerging field and IoT based devices have created a revolution in electronics and IT [9]. The communication architecture of IoT is divided into three layers, the first layer is called sensor layer, which is composed by sensors, on-line monitoring terminals and wireless routers, the sensors are responsible for sensing the physical information, the on-line monitoring terminals are responsible for gathering the monitoring data from the sensors, and the wireless routers are responsible for building the multi hop wireless network, through which the monitoring terminals can exchange data; the second layer is called fiber communication layer, the fibers in the OPGW cable are used as the communication path, the data gathered by monitoring terminals is send to the sink terminal connected to the OPGW by wireless router, and transfer to the datacenter; the third layer is the composed by GPRS network and the Beidou (COMPASS) navigation satellite system (CNSS), it is used in those place where there is no OPGW or the OPGW does not work well, in this layer the data gathered by monitoring terminals is send to the sink terminal equipped with GPRS module and CNSS module, the GPRS module is the priority choice for data transfer and the CNSS module only work when the GPRS module can't work as normal, module only work when the GPRS module can't work as normal[10].

The basic ZigBee communication architecture is simple and the actual network topologies can be very diverse and depend mostly on the field-level network. ZigBee based WSN are proven to be more reliable in packet delivery due to mesh based multi-hop networking [11]. ZigBee Functionality Test Result This process is for checking the functionality and testing how far the ZigBee transmitter can connect with ZigBee receiver. The communication system is responsible for transmitting and receiving data amongst these controllers. This communication system is based on ZigBee technology, which is a low cost and low power consumption device. However, its main limitation is the low data transfer rate [12].

Electricity is vital for our everyday life and a backbone for the industry. Therefore, the concept of the future networks (smart grids) aims to increase the reliability, quality and security of supply for the future. In order to do so, this will also require more information about the operation and the distribution networks [13]. Electricity theft is a major concern for the utilities. In India, energy theft causes about six million rupees losses to utility companies every year. With the smart grid being proposed to modernize current power grids, energy theft may become an even more serious problem since the "smart meters" used in smart grids are vulnerable to more types of attacks compared to traditional mechanical meters. Therefore, it is important to develop efficient and reliable methods to identify illegal users who are committing energy theft [14].

Although some schemes have been proposed to detect energy theft, they all require users to send their private information, e.g., load profiles or meter reading certain times, which invades users' privacy and raises serious concerns about privacy, safety, etc. With the advent of smart meters, the frequency of collecting household energy consumption data has increased, making it possible for advanced data analysis, which was not possible earlier. To the best of our knowledge, we are the first to investigate the energy theft detection problem considering users' privacy issues. We have proposed a theft predictive model which uses

smart meter data and data from distribution unit to detect electricity theft in system [15].

Proposed System

The proposed system is based on wireless communication networks, depend on the far of distance the communication will be chosen. For a small distance ZigBee communication is enough to transfer the data. When a distance is increased, we go for IoT which extends upto worldwide. For this, the block diagrams are drawn individually for simulation and hardware, which are shown below Fig. 1, 2, 3 and 4 respectively. An AC supply is fed to the three phase step down transformer and current transformer (Fig. 3).The current and voltage transformer is used to sense the current and voltage values. Here signal conditioning is done.

Signal conditioning

In electronics, signal conditioning means manipulating an analog signal in such a way that it meets the requirements of the next stage for further processing. Most common use is in analog-to-digital converters. In control engineering applications, it is common to have a sensing stage (which consists of a sensor), a signal conditioning stage (where usually amplification of the signal is done) and a processing stage (normally carried out by an ADC and a micro-controller). Operational amplifiers (op-amps) are commonly employed to carry out the amplification of the signal in the signal conditioning stage.

Amplification

Signal amplification performs two important functions: increases the resolution of the input signal, and increases its signal-to-noise ratio. For example, the output of an electronic temperature sensor, which is probably in the millivolts range is probably too low for an analog-to-digital converter (ADC) to process directly. In this case it is necessary to bring the voltage level up to that required by the ADC. Commonly used amplifiers on signal on conditioning include sample and hold amplifiers, peak detectors, log amplifiers, antilog amplifiers, instrumentation amplifiers and programmable gain amplifiers.

ATMEGA32 Board

A microcontroller requires separate power supply to ON. It's about 5volts. An ATMEGA32 consists of 40 pins. It is very fast IC when compared to other microcontrollers. It is four times better than PIC and eight times better than 8051 IC. For a continuous monitoring of the system, it supports very well and helps to provide a secured power to users.

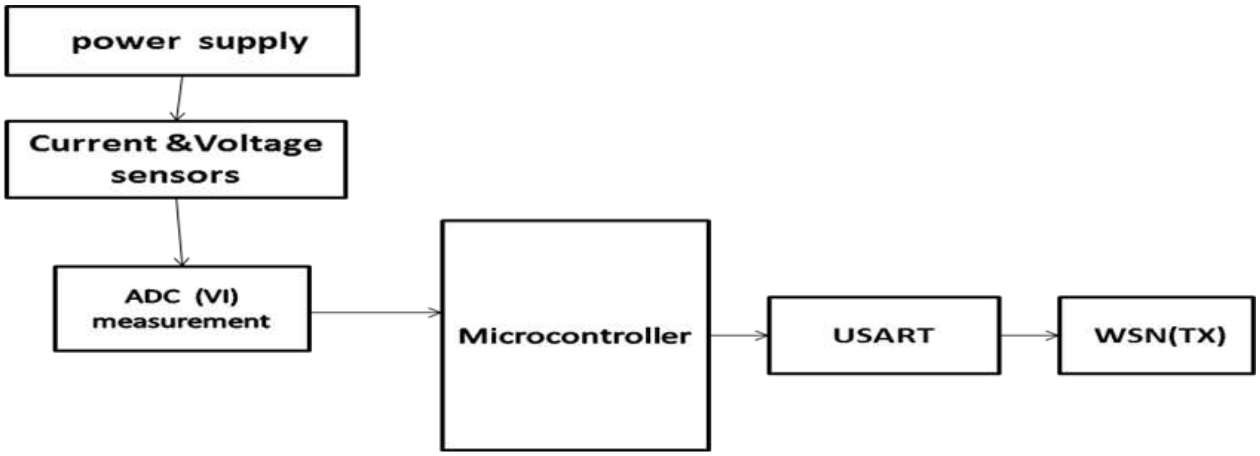

Fig. 1. Transmitter section

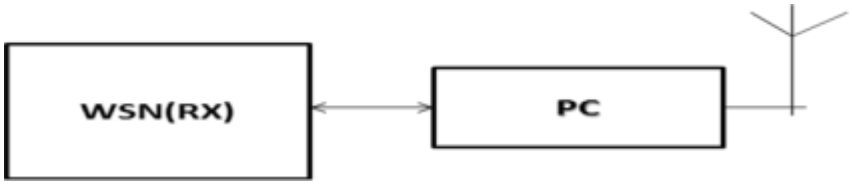

Fig. 2. Receiver section

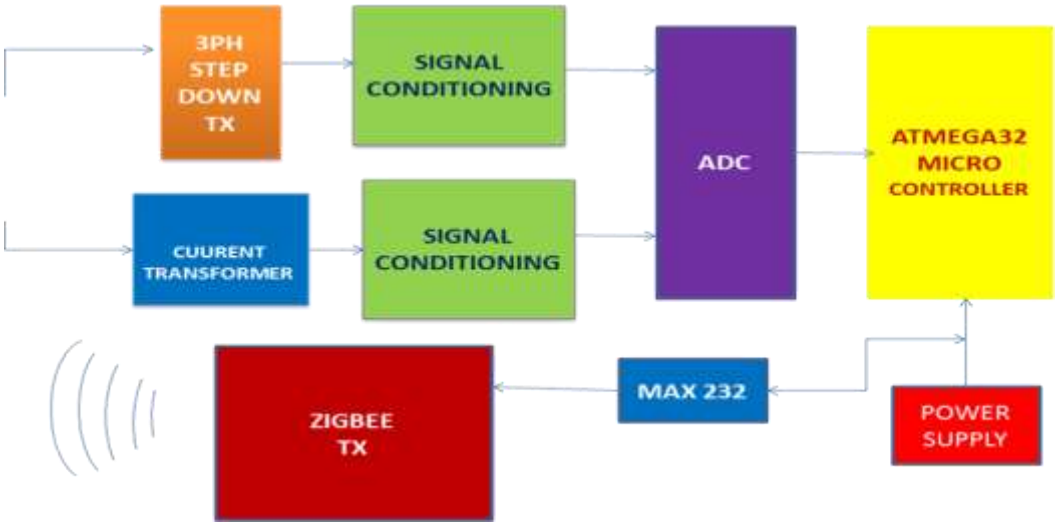

Fig. 3. Transmitter section

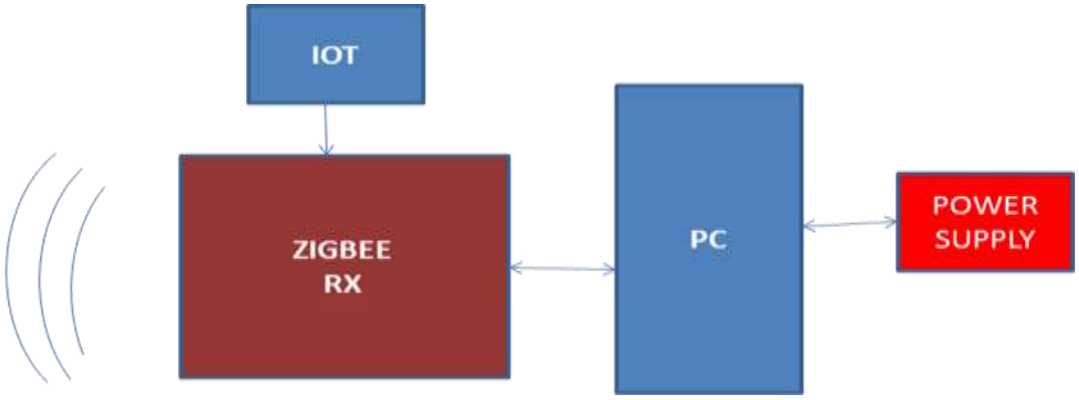

Fig. 4. Receiver section

The AVR ATmega32 Development Board can be used to evaluate and demonstrate the capabilities of AVR ATmega32 microcontroller. The MCU socket on board provides support for 40 pin DIP package of AVR ATmega32 controller. The board is designed for general purpose applications and includes a variety of hardware to exercise microcontroller peripherals. It is a fantastic tool for code debugging, development and prototyping. Due to the nature of non-technical loss during transmission of electrical energy, it is very difficult for the utility companies to detect and fight the people responsible for energy theft. The unique challenges for energy theft in AMI call for the development of effective detection techniques.

By using USART (Fig. 1), it is send to the WSN terminals in simulation part, which provides a better output. An USART is nothing but Universal Synchronus/Asynchronus Receiver Transmitter. It has two modes one is synchronus mode and another one is asynchronus mode. The synchronus mode requires both data and clock signals. For a periodic transmission of data is well suited. The asynchronus mode requires only a data signal. Here we use asynchronus mode. Because, depend upon on the demand of consumers, the data transmission will be changed that is it doesn't a periodic process. When the data reached a wireless sensor network (Fig. 2), then it goes to the corresponding consumers.

In hardware, USART is replaced by the MAX232 cable which is act as inter-mediator between the microcontroller and wireless communication. Through the MAX232 (Fig. 3) the data are reached the communication terminal. If the communication range is small, then ZigBee is used to pass information to consumers. When a communication range is extended then IoT (Fig. 4) is used to display the data about the system.

Simulation Results

Extensive simulations are carried out using circuit diagram shown in Fig. 5 and the results shown (Fig. 6 to 13) that the proposed algorithms can efficiently and successfully identify the fraudulent users in the system. To provide a secured power to the consumers, power theft detection algorithm is used for loads. The simulations are done in proteus software. Here, five loads (namely A, B and C) are connected to five users.

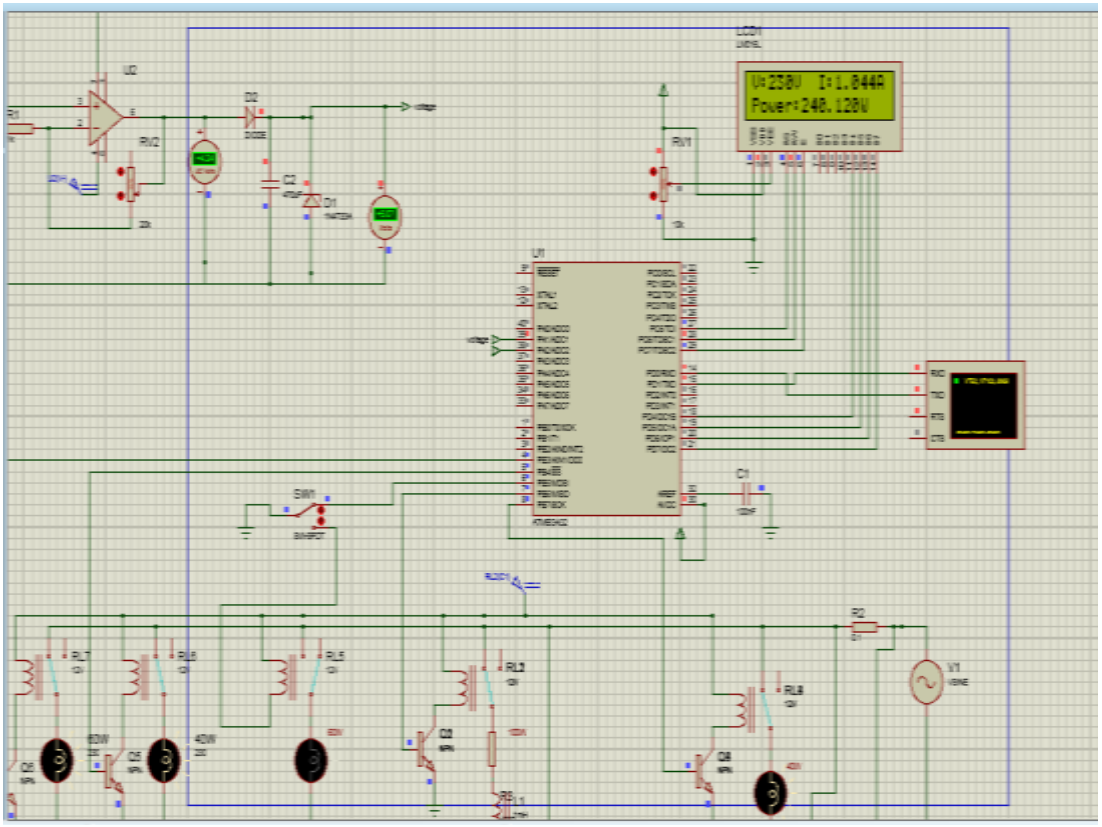

Fig. 5. Circuit diagram for simulation

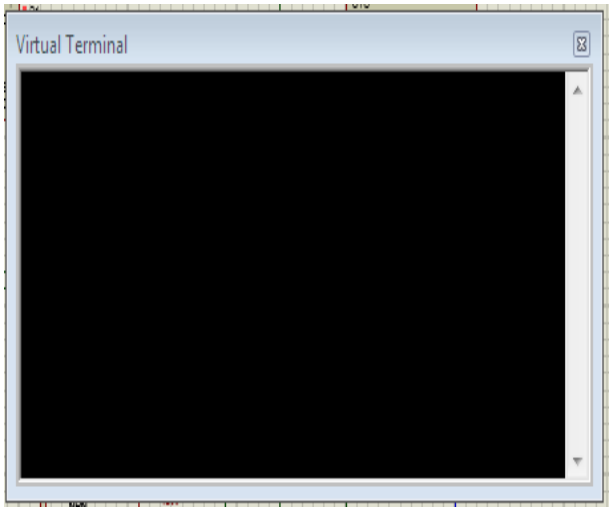

Fig. 6. Virtual terminal for initial state

When load A is turned on its voltage, current and power are displayed in virtual terminal and corresponding graph shows the values of voltage and current flow. For simulation only, it is considered as a virtual terminal, when this project is done in hardware it is replaced by website. Similarly, all of these loads are governed by the wireless sensors. When some snoopers tried to snoop a power, it sends intimation to corresponding consumer. It is showed in load E which is assumed as a theft load. The graph represents the corresponding voltage and current of each load. Due to this process, we can able to provide a secured power to all users. The values for current, voltage and power for three loads are tabulated in Table 1.

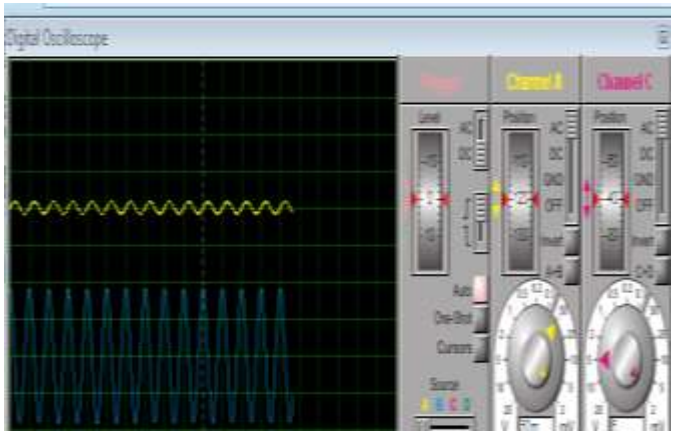

Fig. 7. Waveform for initial state

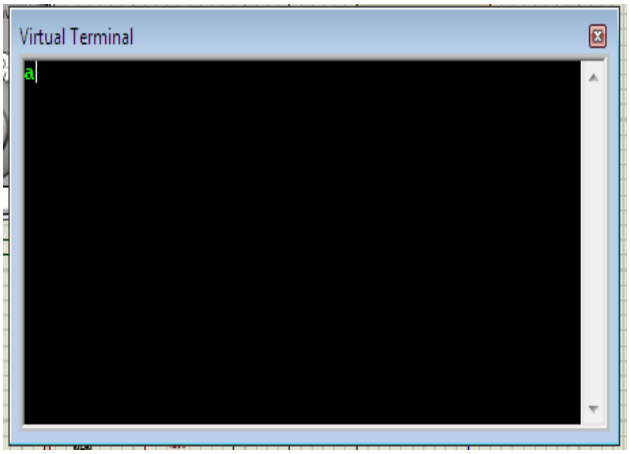

Fig. 8. Virtual terminal for load A

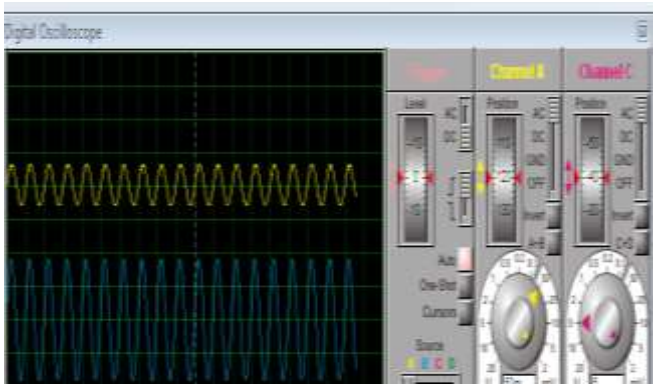

Fig. 9. Waveform for load A

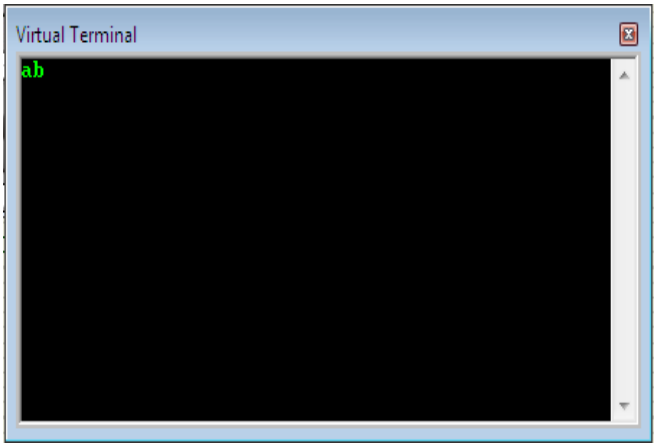

Fig. 10. Virtual terminal for load B

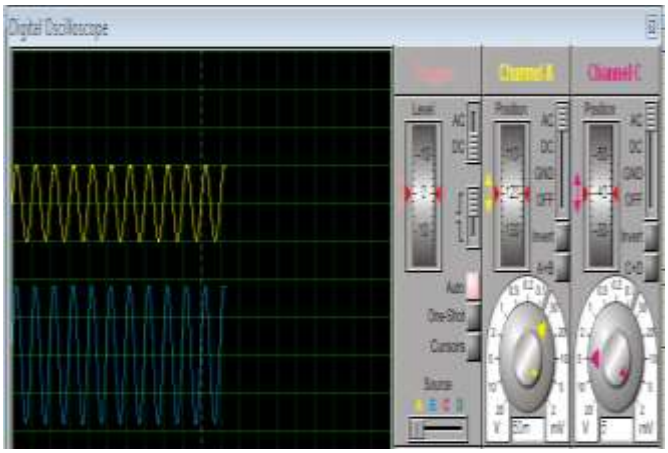

Fig. 11. Waveform for load B

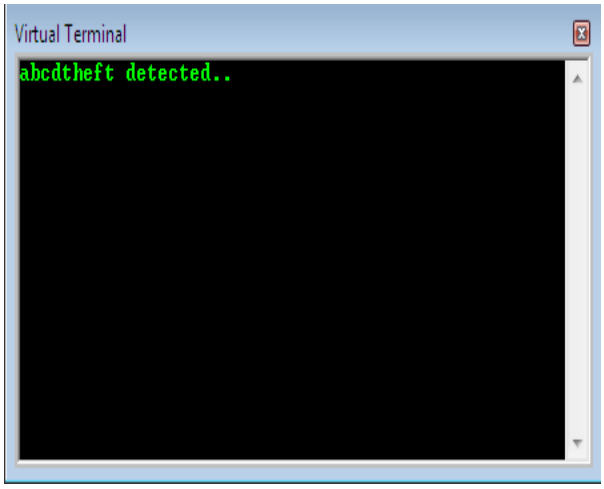

Fig. 12. Virtual terminal for theft detection

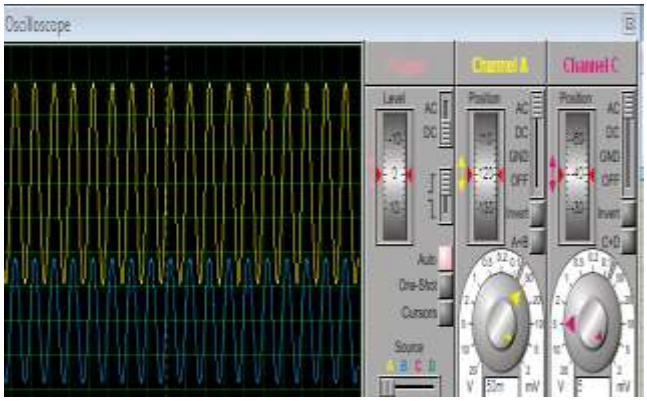

Fig. 13. Waveform for theft identification

Table 1. Outputs for load A, B and C (Theft)

S. No	Load	Current (Ampere)	Voltage (volts)	Power (Watts)
1	A	0.26	230	60.030
2	B	0.435	230	100.050
3	Theft	0.522	230	120.060

Conclusions

The real-time monitoring of the electrical appliances can be viewed through a website. The processed voltage, current values are displayed on LCD screen, which can be controlled through application. A proteus is software for microprocessor simulation, schematic capture, and printed circuit board design. It is developed by Lab center Electronics. The sensor networks are programmed with various user interfaces suitable for users of varying ability and for expert users such that the system can be maintained easily. The current and voltage of a transformer is monitored continuously using wireless sensors. When the hacker tries to theft a load it sent a message notification to a customer. The simulation is carried out in Proteus software and simulations are showed. The results of

implementation and experimentation has shown the proposed system and platform can provide more IoT application possibilities daily life.

Conflict of interest

Authors declare there are no conflicts of interest.

References

[1] Prasad Yerra RV, Bharathi AK, Rajalakshmi P, Desai UB. WSN Based Power Monitoring In Smart Grids, Seventh International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2011.

[2] Sachan A. GSM based automated embedded system for monitoring and controlling of smart grid. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering 2013;7(12):1748-1752.

[3] Almakrami H. Intrusion Detection System For Smart Meters National Grid-SA, Saudi Arabia.

[4] Praveen Kumar, Umesh Chandra Pati. Iot based monitoring and control of appliances for smart home. IEEE International Conference on Recent Trends In Electronics Information Communication Technology, India, 2016.

[5] Maninder K, Sheetal K. A Review on Iot based smart grid department of computer science. International Journal of Energy, Information and Communications. 2016;7:11-22

[6] Liu H, Zhang J, Lin F. Internet of Things technology and its applications in smart grid. Indonesian Journal of Electrical Engineering. 2014;12:940-946.

[7] Pavithra D, Ranjith B. Iot based monitoring and control system for home automation" Proceedings of Global Conference on Communication Technologies, 2015.

[8] Al-Ali AR, Aburukba R. Role Of Internet Of Things In The Smart Grid Technology. Journal of Computer and Communications. 2015;3:229-233.

[9] Sanket T, Akshay S, Vikas T, Prakash Y, Keerthi U. Implementation of an energy monitoring and control device based on Iot. Electronics and Telecommunication Engineering. F.C.R.I.T., 2016.

[10] Shao-Lei Z, Dong-Sheng Z, Zhen W, Yi Z. Research of communication technology on Iot for high-voltage transmission line. International Journal of Smart Grid and Clean Energy. 2012;1(1):87-90.

[11] Kun-Long C. Yan-Ru C, Yuan-Pin T. A novel wireless multifunctional electronic current transformer based on zigbee-based communication. IEEE Transactions on Smart Grid. 2016;PP(99):1-1.

[12] Setiawan MA, Shahnia F, Rajakaruna S. Zigbee-Based communication system for data transfer within future Micro Grids. IEEE Transactions on Smart Grid. 2015;6(5):2343-2355.

[13] Kadurek P. Blom J, Cobben JFG. Theft detection and smart metering practices and expectations in the Netherlands. Proceedings of the Innovative Smart Grid Technologies Conference Europe, 2010.

[14] Sergio S, Li M, Li P. Privacy-preserving energy theft detection in smart grids: a p2p computing approach. IEEE journal on Aelected Areas in Communications/Supplement. 2013;31(9): 257-267.

[15] Sanujit S, Censio B, Daniel N. Electricity theft detection using smart meter data. MA, USA. 2015.

****

