ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Vol 10, Issue 9 September 2023

Power Theft Detection Using IOT

[1] R.Krishna Kumar, [2] Abinaya S, [3] Jayavarthini R, [4] Jeevitha J, [5] Priyanka R

[1] Assistant Professor, Department of Electrical and Electronics Engineering, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India

[2] [3] [4] [5] Student, Department of Electrical and Electronics Engineering, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India

Email: [1] kumaran23011991@gmail.com, [2] 19e101@kce.ac.in, [3] 19e119@kce.ac.in, [4] 19e121@kce.ac.in, [5] 19e126@kce.ac.in

Abstract— Monitoring electricity theft starts with analyzing losses in the electrical system. Losses occur at all levels, from generation to transmission and distribution, to consumers and meters. This usually happens at the distribution level where the most preventable losses occur. All power companies lose money to some degree. In this system, Blynk IOT software is implemented to transmit information about electricity theft to the Electricity Commission. The system is connected to the ARM cortex Pico Wi-Fi module and Node MCU, the current and voltage transformers are connected to the ARM cortex Pico to detect the load current and voltage.

Keywords- Power theft, IOT, Arduino IDE , Blynk application , LCD display , Current and potential transformers.

I. INTRODUCTION

Electricity theft is the most common problem in countries like India, which has a large population and is ultimately a very large consumer of electricity. Every year in India, there are more and more incidents of electricity theft from household electrical connections and industrial power sources, leading to frequent blackouts and load shedding in urban and rural areas to meet the needs in the country's electricity. There are also countless ways to steal, how the theft happened, we will never catch up, we need to solve this problem.

II. LITERATURE SURVEY

IoT Based Electricity Theft Detection (IJIET 2017) R Giridhar Balakrishna, P Yogananda Reddy, M L N Vital To prevent electricity theft, they use IoT system to detect electricity theft and usage of Arduino, GSM, LCD, ESP modules and current transformers. Of the two CTs, one is connected to the source side and the other is connected to the load side, and the signals from both CTs are supplied to the Arduino. The Arduino compares the data received from the source and load CTs. If a detected deviation is out of tolerance, it just means that a flight load is connected, then send this data to the substation using the iot and ESP module that works on the internet, if there is no internet the GSM module is not working. Used to send a message to the substation connected to the line where the stolen load was detected. In this system, detection of electricity tampering is performed using IoT and GSM. In the event of an IoT system failure, GSM will strive to eliminate network theft, a major global threat.

Electricity theft recognition using GSM technology Rhea Prakash, E. Annie Elisabeth Jebaseeli, YSU Sindhu Theft detection is performed using PIC microcontroller, sensors, a GSM module and an LCD screen. As we all know, electricity theft is mainly done through meter bypassing. The heart of the system is the Arduino controller as it consists of two microcontrollers. This project basically consists of two CTs, one connected to one side of a power pole and the other to the other side of the power pole, to study the voltage pattern in the area through the outputs of the two CTs to an Arduino controller to give When the voltage drop limit exceeds the allowed calculated value given by the utility, so it means that the flight load is connected to the system detected by the Arduino controller, which then uses the GSM module equipped with the kit Arduino to send a message to the utility. Use MATLAB to collect and analyse data provided by the Arduino and detect areas of theft and take action. In this project, theft is detected using real-time data without any human-machine interface.

III. PROPOSED METHOD

Our proposed project is an electricity theft detection system for automatic theft detection when transmission lines or meters are bypassed. In this method, current transformers and voltage transformers are used to sense the total amount of current and voltage consumed by the load. And we monitor voltage and current values in Blynk IOT app. Likewise, the LCD screen displays values and units of measurement. If taps are made or additional loads are introduced into the transmission line, the amount of current and voltage will be higher. At this time, the current and voltage values are measured by the WIFI module using the Blynk IOT app and the detected flight command is displayed on the app screen. This will prevent electricity theft. The current system offers the best solution to the existing problems of electricity theft and energy waste.

ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Vol 10, Issue 9 September 2023

IV. SOFTWARE IMPLEMENTATION

1. BLYNK APPLICATION

Control your Arduino board with your smartphone and Blynk via the Internet. This is my first time using the Blynk app to control an Arduino board. There is also a Bluetooth connection between the smartphone and the Arduino board, but it will not be presented in this book. Blynk can be downloaded from the Google Play Store (for Android). App Store (for Apple), which provides us with the dashboard and the connection to the Arduino (it's a virtual connection). Programming the Blynk is as simple as pushing and pulling widgets to form toolbars and assigning their pins on the Arduino board. For a project like this, a normal Arduino board, without an internet screen, connected to a computer and a smartphone with internet access can be used.The role of the computer is to ensure that the Arduino board is connected to the internet and to download the Arduino code. To do this, you need to install the Blynk library on your computer and perform some configuration. Blynk's Arduino code has the same structure as normal code, but includes specific sections for communicating with the Android device. I will give a simple example, taken from the internet and partially modified by me. As you can see, creating new code is almost similar to writing normal Arduino code.

Fig. 1 Software image

2. THINGSPEAK CLOUD PLATFORM

The Internet of Things (IoT) is a system of connected objects. Objects often contain embedded operating systems and the ability to communicate with the Internet or adjacent objects. One of the key elements of a general IoT system that connects various "things" is IoT services. An interesting implication of the “things” that make up an IoT system is that things cannot do anything on their own. They should at least be able to connect to other "things". But the real power of the IoT comes when things are connected directly or through other "things" to "services". In such systems, the service acts as an invisible manager providing capabilities ranging from simple data collection and monitoring to complex data analysis. The diagram below illustrates the place of IoT services in the IoT ecosystem: "ThingSpeak" is an IoT application platform that provides extensive analysis, monitoring and countermeasure capabilities. ThingSpeak is a platform that provides various services dedicated to building IoT applications. It provides real-time data collection, the ability to visualize collected data as maps, and create plugins and apps to collaborate with web services, social networks, and other APIs. We'll look at each of these features in detail below. The central element of ThingSpeak is the "ThingSpeak Channel". Channels store the data we send to ThingSpeak and consist of the following elements:

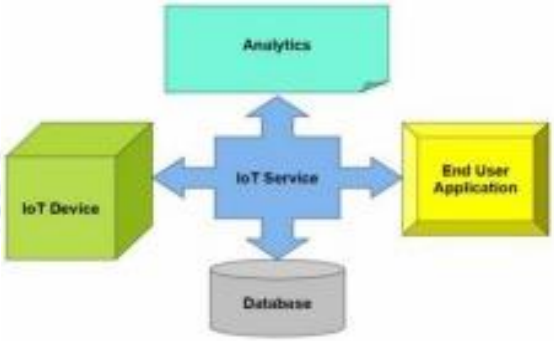

Fig. 2 Internet of things

1. 8 Fields to store any type of data this can be used to store data from sensors or embedded devices
2. 3 location fields can be used to store latitude, longitude and altitude. It is very useful for tracking mobile devices.
3. 1 status field short message describing the data stored channel.

The Internet of Things describes an emerging trend in which a large number of embedded devices (things) are connected to the Internet. These connected devices communicate with people and other objects, and often provide sensor data to storage and cloud computing resources, where the data is processed and analyzed to obtain critical in sights. This trend is fueled by cheap cloud computing power increased device connectivity. IoT solutions are specially designed for many vertical applications such as environmental monitoring and control,

ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Vol 10, Issue 9 September 2023

health monitoring, fleet monitoring, industrial monitoring and home automation. To use ThingSpeak, we need to log in and create a channel. Once we have a channel, we can send data, let ThingSpeak manage it, and retrieve it. Let's start exploring ThingSpeak by registering and setting up a channel.

V. BLOCK DIAGRAM

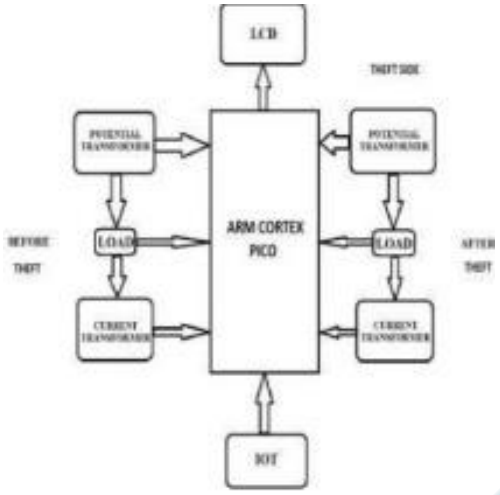

Fig. 3 Block diagram

VI. BLOCK DIAGRAM DESCRIPTION

First, supply regulated power to the circuit. The ARM cortex pico plays the main role in the circuit. We used four transformers, two current transformers and two voltage transformers. Connect the LCD display and the load to provide input to the transformer. The AC input is given from the primary side of the transformer, we cannot directly supply 12V AC to the cortex ARM board because we use a bridge rectifier to convert AC to DC.Converted 5V DC to the pico cortex ARM. Now, from the secondary side of the transformer, 5V DC is supplied to the pico cortex ARM and our load on the domestic/industrial side is activated. The WIFI module is connected to the ARM pico cortex, through this we can connect the IOT software application and see the voltage and current ratings in the application.

Then we enable the load on the domestic/industrial side, so the app can only show the current and voltage ratings on the screen. But when we

VII. CIRCUIT DIAGRAM DESCRIPTION

The main element of this circuit is an ARM pico cortex board. Initially, the four LCD power pins are connected to the (5,6,40,39)Th pins of the ARM pico cortex. The primary side terminals of the voltage transformer and the turn on the anti-theft charge, the rated voltage will become higher than the household/industrial side. Therefore, power is detected in this state and the app will display commands. Also current, voltage, unit and electricity cost will be displayed on the LCD. In this way, we detect the theft of domestic/industrial applications.

VIII. CIRCUIT DIAGRAM

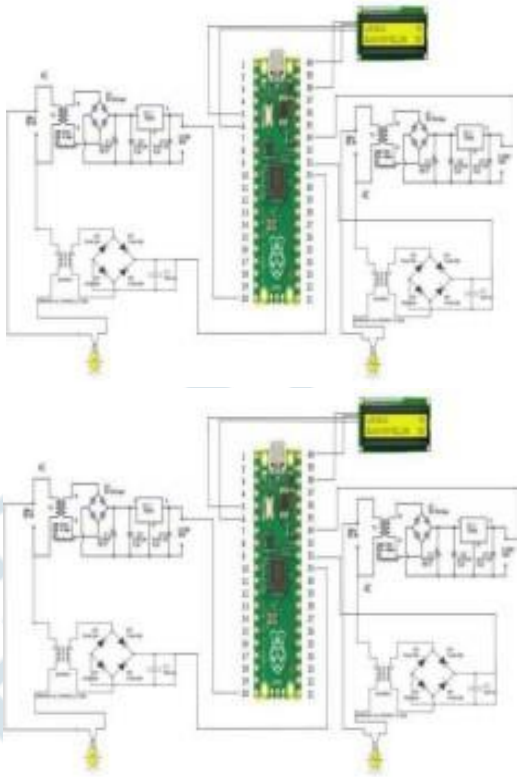

Fig. 4 Circuit diagram

ICs is to choose this "NodeMCU" circuit. We will introduce NodeMCU V3 in detail. It is an open source firmware and development kit that plays an important role in designing suitable IoT products using certain scripting rules. This module is primarily based on the ESP8266, a low-cost Wi-Fi chip that includes a full TCP/IP stack and microcontroller functionality. It is introduced by Expressive Systems manufacturer. The ESP8266 current transformer are connected to the load. And the secondary side of the transformer is connected to the bridge rectifier on both sides. 5V DC is supplied to the ARM cortex board via a bridge rectifier.

1. NODE MCU

Fig. 5 Node MCU

The best way to develop IoT applications with fewer NodeMCU is a complex device that combines some of the functionality of a classic Arduino board with the ability to be connected to the Internet.

ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Vol 10, Issue 9 September 2023

2. ARDUINO IDE

Arduino IDE is a Software Platform .In Arduino IDE we can easily write and dump the code in arduino.So that we can control the devices with the help of arduino.It is available in all Pcs, Macs and windows.

The environment is written in Java and based on Processing and other open source software. The Arduino development environment includes a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions, and a series of menus. It connects to Arduino hardware to download programs and communicate with it.

3. ARM CORTEX PICO

Fig. 6 ARM Cortex Pico

ARM cortex Pico is a microcontroller board based on the Raspberry Pi RP2040 microcontroller chip. It is flexible and inexpensive.It is operated using C++ or MicroPython. Pico provides minimal external circuitry to support the RP2040 chip (flash memory, crystal, power and disconnect connectors, and USB connector). Most of the pins of the RP2040 microcontroller are connected to the user IO pins on the left and right edges of the board. Four RP2040 I/Os are used for internal functions - driving LEDs, controlling power to the on-board switch-mode power supply (SMPS), and sensing system voltage.

4. LIQUID CRYSTAL DISPLAY

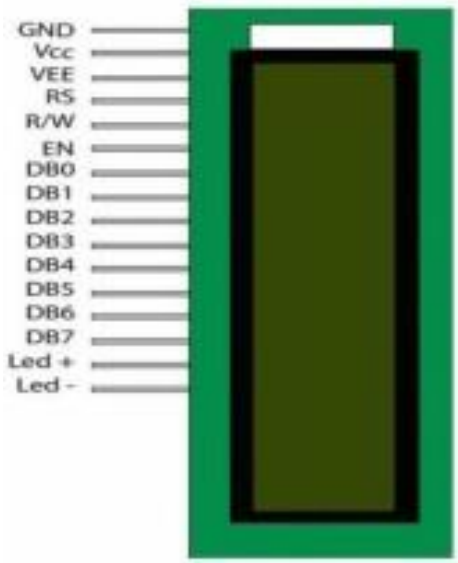

Fig. 7 LCD Display

The LCD (Liquid Crystal Display) is an electronic display module with a wide range of applications. The 16x2 LCD display is a very basic module which is very commonly used in various devices and circuits. These modules outperform seven-segment LEDs and other multi-segment LEDs.LCD have 8 data pins such as DB1 to DB7,1 enable pin,1 Read/Write pin.In this pin we can perform both read and write operation but we cannot perform both at meanwhile. A 16x2 LCD screen means it can display 16 characters per line, so we can display 32 characters. In this LCD, each character is displayed in a 5x7 pixel matrix. The LCD display has two registers, command and data.

5. RELAY MODULE

This circuit is intended to control loads. The load can be a car or any other load. The load is switched on and off by a relay. Activation and deactivation of the relay is controlled by a pair of switching transistors (BC 547). The relay is connected to the collector terminal of transistor Q2. A relay is an electromagnetic switching device consisting of three pins. They are very common, normally closed (NC) and normally open (NO).

The common pin of the relay is connected to the supply voltage. The normally open (NO) pin is connected to the load. When a high pulse signal (5 volts) is sent to the base of transistor Q1, the transistor turns on and shorts the collector and emitter terminals, and a zero signal (0 volts) is sent to the base of transistor Q2.So the relay is off.

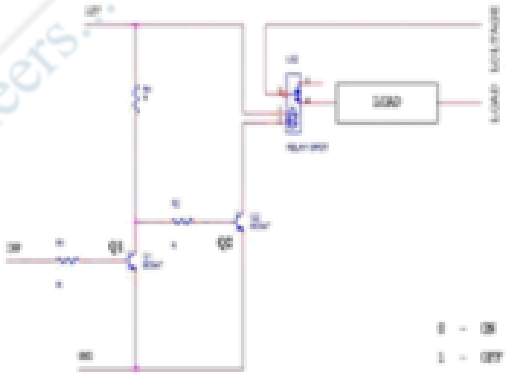

Fig. 8 Relay module

6. POTENTIAL TRANSFORMER

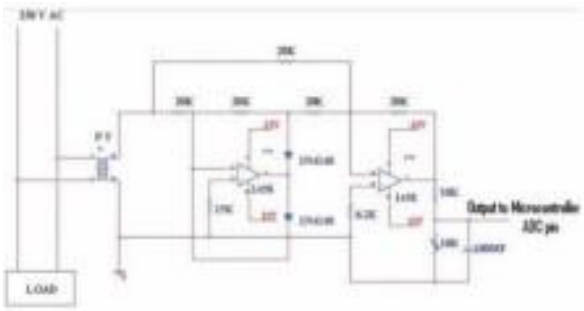

Fig. 9 Potential Transformer

ISSN (Online) 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)

Vol 10, Issue 9 September 2023

This circuit is designed to monitor the supply voltage. The mains voltage to be monitored is lowered by a voltage transformer. Usually we use 0-6v voltage transformer. The step-down voltage is rectified by a precision rectifier. A precision rectifier is a configuration achieved by using an operational amplifier, which causes the circuit to behave like an ideal diode or rectifier. A full-wave rectifier is a combination of a half-wave precision rectifier and a summing amplifier.A rectifier has two types of devices. Controllable and Uncontrollable device.

In here we are using diode (uncontrollable device).If the input voltage is negative the voltage across the diode also negative so the diode acts as an open circuit there is no current supplied to the load so no output voltage. If the input voltage is positive circuit it is amplified by the op amp and the diode is on. It acts as a closed circuit and the current supplied to the load and output voltage is equal to the input voltage due to feedback.

7. CURRENT TRANSFORMER

This circuit is designed to monitor the supply current. The supply current to be monitored is stepped down by a current transformer. Step-down current is converted to voltage using a shunt resistor. The converted voltage is then rectified by a precision rectifier. A precision rectifier is a configuration achieved with an operational amplifier that allows a circuit to behave like an ideal diode or rectifier.

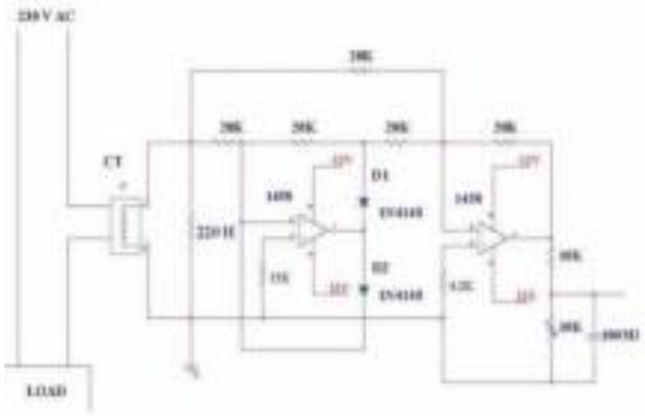

Fig. 10 Current Transformer

A full-wave rectifier is a combination of a half-wave precision rectifier and a summing amplifier. A rectifier has two types of devices.Controllable and Uncontrollable device.In here we are using diode(uncontrollable device).If the input voltage is negative the voltage across the diode also negative so the diode acts as an open circuit there is no current supplied to the load so no output voltage. If the input voltage is positive circuit it is amplified by the op amp and the diode is on. It acts as a closed circuit and the current supplied to the load and output voltage is equal to the input voltage due to feedback.

IX. PROJECT OUTCOME

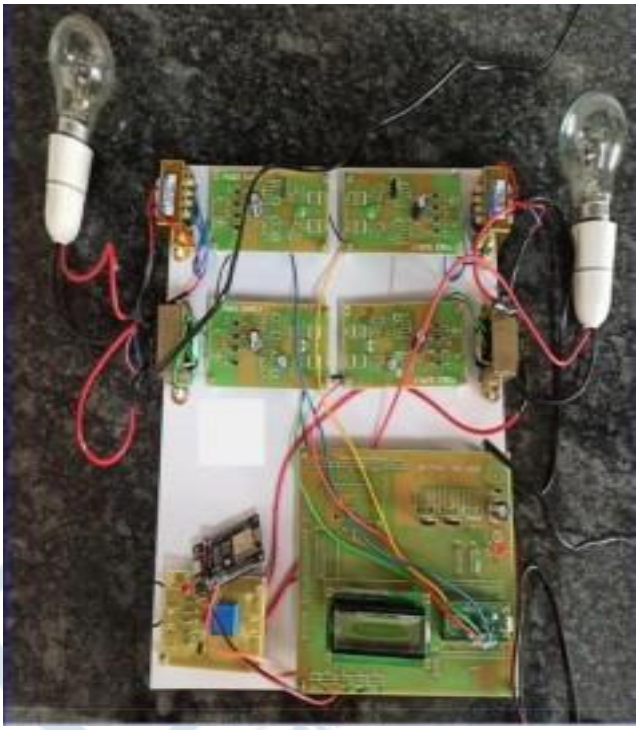

Fig.11 Outcome

X. CONCLUSION AND FUTURESCOPE

The Electricity Theft Detection System provides an effective and simple method to detect electricity theft. Using IoT, power theft detection kits have been implemented and help realize the many benefits of wireless communication. This approach reduces serious energy and revenue losses due to customer electricity theft. With this design, it can be concluded that electricity theft can be effectively combated by detecting where the electricity theft is occurring and immediately detecting illegal charges and notifying the authorities.

This concept is particularly suitable for cities and out backs. By minimizing electricity theft, high-quality power can be distributed even in rural areas. The system provides accurate and reliable measurement of energy consumption. Power theft detection and monitoring is designed and developed with proper hardware and software integration.

REFERENCE

[1]. Kumaran, K. "Power Theft Detection and Alert System using IOT." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.10 (2021):1135-1139.

[2]. Jeffin, M. J., et al. "Internet of Things Enabled Power Theft Detection and Smart Meter Monitoring System." 2020 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2020.

[3]. Leninpugalhanthi,P, et al. "Power theft identification system using IoT" 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). IEEE, 2019.

[4]. Yao, Donghuan,et al."Energy theft detection with energy privacy preservation in the smart grid." IEEE Internet of Things Journal 6.5 (2019): 7659-7669. [5] Meenal, R., et al. "Power Monitoring and Theft Detection System using IoT." Journal of Physics:Conference Series. Vol. 1362. No. 1. IOP Publishing, 2019.

[5]. Ogu, R. E., and G. A. Chukwudebe. "Development of a cost-effective electricity theft detection and prevention system based on IoT technology." 2017 IEEE 3rd international conference on electro-technology for national development (NIGERCON). IEEE, 2017.

[6]. Jindal, Anish, et al. "Decision tree and SVM-based data analytics for theft detection in smart grid." IEEE Transactions on Industrial Informatics 12.3 (2016): 1005-1016.

[7]. Sahoo, S., Nikovski, D., Muso, T., & Tsuru, K. (2015, February). Electricity theft detection using smart meter data. In 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) (pp. 1-5). IEEE.

[8]. Prashanthi, G. L., and K. V. Prasad. "Wireless power meter monitoring with power theft detection and intimation system using GSM and Zigbee networks." Journal of Electronics and Communication Engineering 9, no. 6 (2014).

[9]. Patil, Sagar, Gopal Pawaskar and Kirtikumar Patil. "Electrical power theft detection and wireless meter reading." International Journal of Innovative Research in Science, Engineering and Technology 2, no. 4 (2013):1114-1119.

[10]. Nikovski, Daniel Nikolaev, Zhenhua Wang, Alan Esenther, Hongbo Sun, Keisuke Sugiura, Toru Muso, and Kaoru Tsuru. "Smart meter data analysis for power theft detection." In Machine Learning and Data Mining in Pattern Recognition: 9th International Conference, MLDM 2013, New York, NY, USA, July 19-25, 2013. Proceedings 9, pp. 379-389. Springer Berlin Heidelberg, 2013.

[11]. Dlodlo, Nomusa, Thato E. Foko, Promise Mvelase, and Sizakele Mathaba. "The state of affairs in internet of things research." Academic Conferences International Ltd,2012.

[12]. Zhen, Yan, Xiangzhen Li, Yiying Zhang, Lingkang Zeng, Qinghai Ou, and Xiaohua Yin. "Transmission tower protection system based on Internet of Things in smart grid." In 2012 7th International Conference on Computer Science & Education (ICCSE), pp. 863-867. IEEE, 2012.