IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10589

POWER THEFT IDENTIFICATION SYSTEM IN SMART GRID USING IOT

Harshitha T S[1], Sathwik M S[2], Shamitha K R[3] ,Dr Sharath Kumar Y H[4], Dr Pushpa D[5]

Student, Department of Information Science, Maharaja Institute of Technology Mysore, India[1]

Student, Department of Information Science, Maharaja Institute of Technology Mysore, India[2]

Student, Department of Information Science, Maharaja Institute of Technology Mysore, India[3]

Professor & Head, Department of Information Science, Maharaja Institute of Technology Mysore, India[4]

Associate Professor, Department of Information Science, Maharaja Institute of Technology Mysore, India[5]

Abstract: The Internet of Things (IoT) is a rapidly emerging field of technologies that delivers numerous cutting-edge solutions in various domains including critical infrastructures. Thanks to the IoT, the conventional power system network can be transformed into an effective and smarter energy grid. In this, we are going to review the architecture and functionalities of IoT-enabled smart energy grid systems. Specifically, we focus on different IoT technologies including sensing, communication, computing technologies, and their standards for the smart energy grid. Based on recent surveys and literature, we observe that the security vulnerabilities related to IoT technologies have been attributed as one of the major concerns of IoT-enabled energy systems. Therefore, the existing threat for IoT-enabled energy systems and summarize mitigation techniques for those security vulnerabilities. Finally, we highlight how advanced technologies (e.g., blockchain, machine learning, and artificial intelligence) can complement IoT-enabled energy systems to be more resilient and secure and overcome the existing difficulties so that they become more effective, robust, and reliable in operation. This will help understand the framework for IoT-enabled smart energy systems, associated security vulnerabilities, and prospects of advanced technologies to improve the effectiveness of smart energy systems.

Keywords: Smart grid, IoT, audio labelling, ESP8266, Blynk.

I. INTRODUCTION

Electricity is considered to be the heart of modern social and economic development. Technology advancements tempted us to use electricity-driven elements in every aspect of our life from the commercial to the domestic sector to make our lives more comfortable. The Internet of Things (IoT) is a rapidly emerging field of technologies that delivers numerous cutting-edge solutions in various situations, the IoT has appeared to be an empowering set of technologies for the smart energy grid system with substantial perspective due to its multi-dimensional advantages in various sectors. The smart grid is built on advanced infrastructure that supports a variety of technologies and components. such grids can sense the transmission lines, and detect and react to changes in the network.

Power theft is a blatant problem in electric power systems, which causes great economic losses and leads to irregular electricity supply. Power theft can be briefly defined as the usage of power without the knowledge of the supplier. It has become a major problem in India and it is a crime. Overall, India has the highest losses about 16.2 billion dollars. Power theft can happen in many ways one such way is that registered customers steal either by bypassing the meter connecting around the meter to a live cable on a company side of the meter or tampering with the meter to make the meter read less or no consumption. To eradicate power theft, it has to be identified. In this project, the Arduino is fixed with threshold voltage and current whenever the voltage level gets decreased, power theft is detected. The proposed system will also provide the faults and energy consumption. IoT can be used for various applications for energy monitoring and saving it helps in demand side management and various area of energy production. Power systems may face many losses in their way of producing power, mainly the operational losses that occur in the generation of power and distribution of power. but the losses that occurred in the generation process can be technically defined but the losses that occurred in the distribution may not be evaluated by using sending end information. This lets us know the usage of unspecialized techniques in the transmission and distribution of power.Power theft technically affects the economy of the nation and it is one of the non-ignorable crimes. so power theft is a crime and it is a social evil that has to be fully eradicated. The power generated must be utilized most coherently by the way of closely examining the consumption and losses of power.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10589

This proposed system is used to prevent the theft of electricity. Due to technological development, IoT is used to prevent the theft of electricity without the intervention of humans. Due to this implementation, more consumers in highly populated countries such as India, and China will consume electricity as it saves a large amount of electricity. Electricity theft can be defined as the usage of electrical power without any valid contract with the supplier. This power theft also can be reduced in many ways such as benefiting companies that should appreciate consumers to report the power theft. power theft is frequently caused when there is a disconnection in the transmission lines. so the lines should be checked periodically. The government must take the initiative to provide awareness about theft and enforcement of law among the consumers. In case of any negative value occurring in the system power theft can be identified by using IoT. So, this power theft system will overcome the problems faced before. This system helps us to save energy and distribute power equally.

II. ORGANIZATION

The 1st section of this paper gives an introduction to the technological trends and need for IoT in the field of electric transmission. In the 3rd section, we discuss the survey on various related works. 4th section provides a problem statement.5th section hardware, various tools and the libraries used for implementation. 6th section provides the design and implementation of the system followed by the conclusion and future enhancements and references used.

III. LITERATURE SURVEY

A. M J Jeffin's paper describes IoT-based power theft detection and a smart meter monitoring system that uses a linear regression-based approach to detect power theft. The proposed system works when all the smart meters at individual consumer premises and the smart meter equipped near the distribution transformer reads the power flow parameters and send them to the server. [1]

B. Saurabh Singh Rajawat collectively proposed theuse of the RP-3 model with the PIR sensors and RP-3 camera for intelligent observance function. Once somebody enters its selection, the PIR detector is employed to spot movement. RP-3 camera activates and displays an image once the PIR detector detects the movement. This image can then be saved within the theme and located on OpenCV and Python for a personality's face. [2]

C. For overload detection, LDR is connected along with the LED of the energy meter. The pulse rate of energy is 3300 imp/kwh resulting in approximately 5 LED blinks per minute for 100 watts of load connected for 1 minute. Thus, the rate of LED blink is directly proportional to the amount of load connected. When the blinking increases the prescribed limit due to overload, the overload signal is sent to Arduino and an overload alert is issued through IOT and GSM. [3]

D. Ms Achal Punwatkar proposed an IoT solution model to detect power theft and monitor power, pair of current sensors and a controller is going to use. This current sensor provides the current status of the power value from the ac source. There will be two pairs of current sensors and controllers going to use. One pair will use at the distributor box (meter at AC source) and one pair will be connected to the usage meter to monitor the actual current and current consumed by the user.[4]

E. Goma T.F.J. Christian explains the advantage of this architecture is that it will be able to detect any illegal connection done between the USB and the energy meter, which supersedes the existing architectures that aimed to detect the illegality between the energy meter and the consumer unit. .[5]

IV. PROBLEM STATEMENT

An electric power system can never be 100% secure from theft. Power theft is a major problem faced by global power utilities. Though difficult to quantify electricity theft, is a major contributor to power deficit Legitimate customers bear the cost of illegal electricity. Reducing theft delivers tangible financial benefits (increased revenue, revenue recovery and reduced cost of energy). Technology can enable innovative solutions, to reduce and overcome power theft significantly. The economic benefit of electricity theft reduction would make a good case for technology implementation.

This project identifies challenges and issues such as detecting energy theft without engaging any man powers by developing a cost-effective and efficient system. In such a situation, it is primarily essential to identify and discuss these kinds of barriers to overcoming deployment concerns, including consumer acceptance. In this project, such major challenges and issues for SG implementation have been encapsulated like energy theft.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10589

V. REQUIREMENTS

A. *ESP8266 NodeMCU:*

TABLE I: TECHNICAL SPECIFICATIONS

Microcontroller	ESP-8266 32-bit
NodeMCU Model	Amica
NodeMCU Size	49mm x 26mm
Carrier Board Size	n/a
Pin Spacing	0.9" (22.86mm)
Clock Speed	80 MHz
USB to Serial	CP2102
USB Connector	Micro USB
Operating Voltage	3.3V
Input Voltage	4.5V-10V
Flash Memory/SRAM	4 MB / 64 KB
Digital I/O Pins	11
Analog In Pins	1
ADC Range	0-3.3V
UART/SPI/I2C	1 / 1 / 1
Wi-Fi Built-In	802.11 b/g/n
Temperature Range	-40C - 125C

B. *Sensors:*

TABLE II: SENSOR REQUIREMENTS

S No	Name	Description
1	Relay	Turn it on and off
2	Voltage sensor	Voltage difference detection
3	Current sensor	To measure the flow of current in an electric circuit

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10589

C. Arduino IDE:

The Arduino integrated development environment (IDE) is a cross-platform application (for Microsoft Windows, macOS, and Linux) that is written in the Java programming language. It includes a code editor with features such as text cutting and pasting, searching and replacing text, automatic indenting, brace matching, and syntax highlighting, and provides simple one-click mechanisms to compile and upload programs to an Arduino board. It also contains a message area, a text console, a toolbar with buttons for common functions and a hierarchy of operation menus. The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension .ino. The editor has features for cutting/pasting and searching/replacing text. The message area gives feedback while saving and exporting and also displaying errors.

D. Blynk:

Blynk is a popular Internet of Things (IoT) platform that allows users to easily create custom dashboards and manage their IoT activities via mobile apps. Blynk provides a user-friendly interface to create and configure virtual dashboards called dashboards that can be accessed and controlled using the Blynk mobile app. Platform, Arduino, Raspberry Pi, ESP8266 etc. It supports various hardware platforms such as With the Blynk app, users can create personalized dashboards by adding widgets such as buttons, sliders, graphics, and instructions that can be linked to the body of their IoT project. It provides a mobile app that allows users to control and monitor connected hardware devices remotely. we can create custom mobile apps for iOS and Android devices without writing complex code. The platform provides a drag-and-drop interface to design the app's user interface and control elements. You can then link these elements to your hardware devices using Blynk's cloud infrastructure.

VI. METHODOLOGY

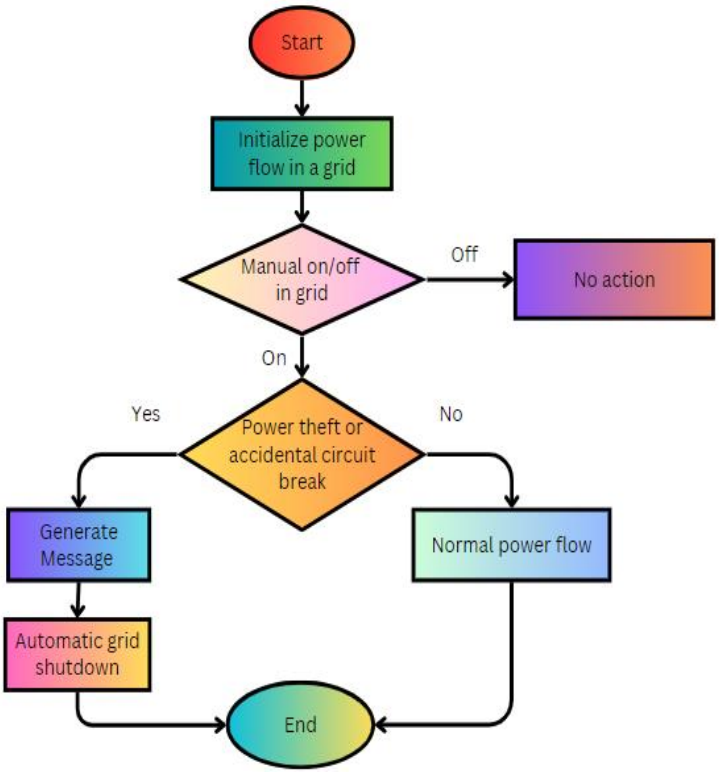

Fig 1. Block Diagram of Proposed System for IoT-enabled Smart Grid

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10589

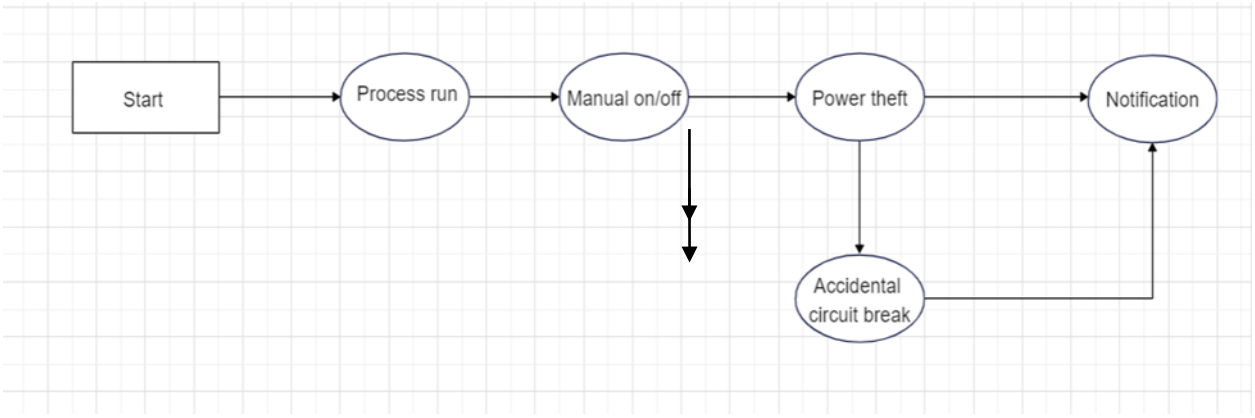

Fig 2. Use Case Diagram for Smart grid

Working Principle:

First, the circuit connections are made between the ESP8266 NodeMCU board and all the available sensors. The ESP8266 consists of 11 digital i/o pins and 1 analog input pin and also consists of the 4 ground pins and TX and RX pins each. 1 Vin where the voltage is supplied to the MCU board .3 3.3V pins. The sensors have 3 pins, they are GND, Data, and Vin Pins. The pins of the sensors are connected to the corresponding MCU board pins. The board is connected to a constant power supply to run the components.

The configured circuit is connected to the grid to convert it into IoT-enabled. The next step is to configure the Arduino IDE to work with the ESP8266. Programming is done to read the data from the sensors and make the relay effectively work. The next step is to configure the Blynk dashboard or the Android app. This is done by logging onto the Blynk website by providing the credentials and selecting the ESP8266 board and respective ports in the further process. Once the initial configuration has been done, templates must be addedto give the interface for the admin/user to remotely monitor just by pressing the buttons and also track information through the dashboard and app. Since NodeMCU provides WiFi module capabilities, one should change their hotspot name and the password to the one that has been fed in the IDE program so that the device can be accessed from anywhere if it is power supplied.

Clearly define the objectives and requirements of the power theft identification system. Identify the specific features you want to implement, such as detecting unusual power consumption patterns or unauthorized connections. Gather the necessary hardware components. This may include an Arduino Uno board, current sensors (such as Hall effect sensors or current transformers), voltage sensors, a GSM module (for sending notifications), an LCD (for real-time information), and relays (for controlling power supply). design a circuit diagram for connecting the components. Ensure proper connections between the Arduino Uno board and the sensors. You may need additional circuitry to interface the sensors with the Arduino. Connect the current and voltage sensors to measure the power consumption. The current sensor should be placed in series with the power line to monitor the current flowing through it. The voltage sensor should be connected in parallel to measure the voltage level. Use the analog or digital input pins of the Arduino Uno to read the sensor values. The current and voltage sensor outputs can be processed using suitable signal conditioning techniques, such as amplification or filtering if required. The Arduino's built-in ADC (Analog-to-Digital Converter) can be used to convert analog signals to digital values. Develop an algorithm to analyze the sensor data and detect power theft. This can involve comparing the measured values with predefined thresholds or implementing pattern recognition techniques. Determine the criteria for identifying power theft, such as sudden changes in power consumption or exceeding a specific threshold for an extended period.

When power theft is detected, activate an alarm or buzzer to alert the user or nearby authorities. Additionally, you can use a GSM module to send SMS notifications or connect to a network to generate email alerts. Utilize an APP display to provide real-time information about power consumption, status, and detected anomalies. This allows users to monitor the system's performance. Integrate relays with the Arduino to remotely control the power supply. This enables authorized personnel to disconnect the power in case of theft detection or other emergencies. Thoroughly test the system to ensure its accuracy and reliability. Simulate different scenarios to verify the system's ability to detect power theft accurately.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10589

VII. RESULTS

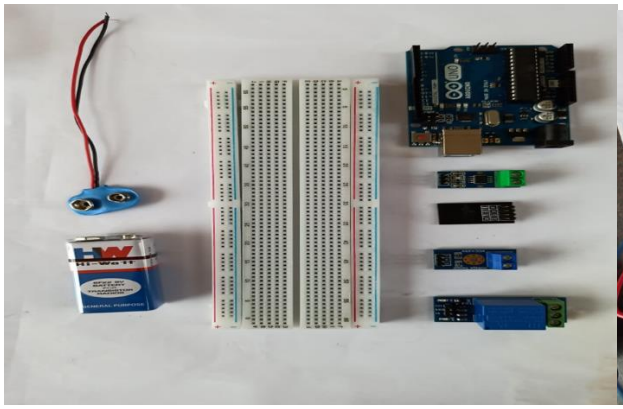

Fig 3a: Power theft identification system home page

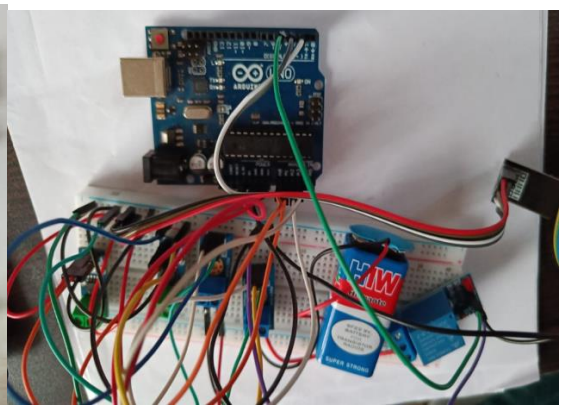

Fig 3b: Arduino main board with complete connection

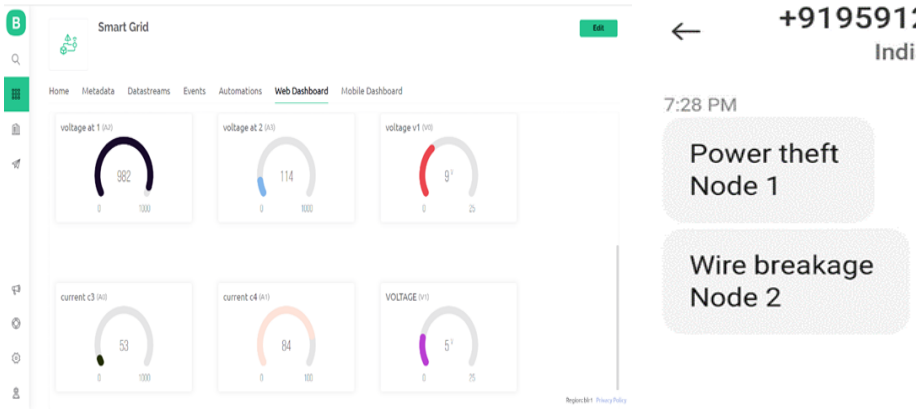

Fig 4: Blynk and Message notification

VIII. CONCLUSION

This system enables accurate and efficient detection of power theft incidents, ensuring fair distribution of electricity and reducing financial losses for utility companies. The use of Arduino Uno provides a cost-effective and flexible solution for monitoring and analyzing power consumption patterns. By comparing real-time data from various meters, the system can identify irregularities and deviations that may indicate power theft. This allows for prompt action to be taken, preventing further losses and ensuring that legitimate consumers receive their fair share of electricity. The integration of smart grid technology enhances the effectiveness of the power theft identification system. Through the implementation of advanced communication protocols and data analysis algorithms, the system can detect and report suspicious activities in real time.

IX. FUTURE ENHANCEMENT

The future of technology is always evolving and changing for the better needs of the people. Thus it is possible to combine artificial intelligence and machine learning algorithms with the smart grid. As an enhanced version, in future, this system can be implemented for various types of grids like centralized, circular or mesh structures. And more effective devices and sensors can be used to detect theft, especially in AC grids.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10589

REFERENCES

[1]. Mrs. A. Preethi Vinnarasi M.E 1, Bhuvanesh P2 Eugine Prince S3, Daniel Vinnarasan A4 Power Theft Identification System Using Iot. 2021 5th International Conference on Advanced Computing & Communication Systems (ICACCS).

[2]. kadala, S. K., Rajagiri, A. K., Ajitha, A., & Thalluri, A. K. (2021). Development of an IoT-based solution for Smart Distribution Systems. 2021 International Conference on Sustainable Energy and Future Electric Transportation (SEFET).

[3]. Jaya Deepthi, B., Ramesh, J., & Chandra Babu Naidu, P. (2019). Detection of Electricity Theft in the Distribution System using Arduino and GSM. 2019 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC).

[4]. Leninpugalhanthi, P., R, J., s, N., RV, M., I, K., & Senthil Kumar, R. (2019). Power Theft Identification System Using Iot. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS).

[5]. Barman, B. K., Yadav, S. N., Kumar, S., & Gope, S. (2018). IOT-Based Last Meter Smart Grid With Energy Theft Detection. 2018 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE).

[6]. S S Nagendra Kumar, S Koteswara Rao, M Suresh Raju, S Trimurthulu, K Sivaji, T Ram Manohar Reddy (2017). IoT-Based Control and Monitoring of Smart Grid and Power Theft Detection by Locating Area.

[7]. Ogu, R. E., & Chukwudebe, G. A. (2017). 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).

[8]. Choudhary, P., & Bera, J. N. (2020). SMS-Based Load Flow Monitoring and Analysis for Theft Location Detection in Rural Distribution Systems. 2020 IEEE Calcutta Conference (CALCON).

[9]. Sultan, Z., Jiang, Y., Malik, A., & Ahmed, S. F. (2019). GSM-based smart wireless controlled digital energy meter. 2019 IEEE 6th International Conference on Engineering Technologies and Applied Sciences (ICETAS).

[10]. Kamatagi, A. P., Umadi, R. B., & Sujith, V. (2020). Development of an Energy Meter Monitoring System (EMMS) for Data Acquisition and Tampering Detection using IoT. 2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONNECT).

