Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

Design of Internet of Things based Electricity Theft Detection using Raspberry PI

Oscar Famous Darteh*[1], Charity Oseiwah Adjei[2],
Raphael Anaadumba[4], Sajib Sarker[5], Goma T.F.J. Christian[6]
School of Computer Science and Software
Nanjing University of Information Science and Technology
Nanjing, China

Amo Samuel Blay[3]
Department of Electrical Engineering
Accra Technical University
Accra, Ghana

***Abstract*—The indicators of the size and development of an economy are dependent on its production and consumption of electricity, so electricity theft contributes to slow economic growth. Although few countries gain profit from electric power exportation, most production is for consumption. But recently, utility authorities are facing a considerable amount of losses. We can divide the losses into technical losses (TL) and non-technical losses (NTL). Technical losses are in-built in the network and are curbed to a considerable level; the remaining is due to the power dissipation of conductors and other equipment on in the distribution and transmission network. NTL happens due to inaccuracy of metering, electricity stealing or theft and energy unmetered. Detecting electricity theft is a nightmare most utility authority. It is against this draw-back that our paper seeks to deploy Internet of Things based Electricity theft detection Using Raspberry Pi. Researchers have predicted a volatile hike in the quantity of "things" or devices connected to the internet. The utility sector must take advantage of this technology to improve its losses. This research's design architecture is to detect any illegality that occurs between the utility serve and the energy meter at the customers' premises. The system could be monitored in real-time over the internet by the utility authority.**

Keywords— Internet of Things; Electricity Theft Detection; Raspberry Pi

I. INTRODUCTION

Internet of Things is a term used for a system where devices are given IP addresses, and everybody makes the device recognisable on the internet via that IP address. The web, which started with the internet of computers, is developing. Researchers have predicted a volatile increase in the number of sensors, devices or "things" connected to the internet. The product network is known as the Internet of Things (IoT) [1]. IoT has the propensity to alter people's lifestyles. People prefer to monitor things through automatic systems in today's world rather than through any manual system. The Raspberry Pi and the relay, together with the circuitry driving the system, are the main elements of the IoT-based electricity theft detection system introduced in this paper. The indicators of the size and development of an economy are dependent on its production and consumption of electricity, so electricity theft contributes to slow economic growth. Although few countries gain profit from electric power exportation, most production is for consumption. Although few countries gain profit from electric power exportation, most output in developing countries is for consumption. Most developing countries have suffered undesirable economic consequences to meet the demands of electricity for real estate and industrialisation due to electricity theft. According to the World Bank's development indicator collection, the percentage of distribution and losses due to transmission in Ghana was at 23% in 2014, gathered from officially recognised sources [2]. Reducing transmission and distribution losses is the greatest challenge to power utility authorities.

We can categorise the losses in to technical (TL) as well as non-technical (NTL) [3]. Technical losses are in-built in the system which is reduceable to an appreciable level; the remaining is due to power dissipated in equipment and conductions used to for the distribution and transmission lines[4]. NTL happens due to inaccuracy of metering, stealing or theft of electricity, as well as energy consumed but unrecorded by the energy meter [5]. Electricity theft is the energy consumed by a customer that is unaccounted for or not measured by the energy meter. Theft of electricity happens due to meter tampering, meter bypassing, and service lines tapping to the customers' premises. Due to the deficiencies in the metering system and the lack of transparency and accountability in billing customers of electricity in public utilities, customers take advantage to steal electricity to avoid paying the realistic tariff. Electricity theft causes a very high negative impact on the financial status of power distribution and utility companies, which puts pressure on the future investment of the power sector. The ripple effect is that the losses incurred due to the theft are passed as the cost to the paying consumers in either poor quality service and higher tariff [6]. Reports suggest 25 per cent of Ghana's current annual average losses are due to electricity theft [7]. However, the emergence of smart grid technologies has informed researchers to utilise the smart grid platform to detect and monitor electricity theft. Our research proposes a generalised IOT based design using raspberry pi to detect electricity theft by comparing the recorded values of current at the utility service intake to the recorded value of current at the energy meter intake. The result of the compared values is stored on the firebase server, which is accessible in real-time. The paper is structured as follows: Methods employed by fraudsters in electricity theft are described in section 3; Literature works on electricity theft detection is described in section 2; In chapter 4,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

our proposed detection system including the general design. Lastly, we present the conclusions with future related work in chapter 5.

II. RELATED WORKS

In this section, we review the existing and proposed designs for electricity theft detection.

A. Existing Designs

In [8], the theft detection system has two current transformers: one at the input and the other at the energy meter's output. Any difference in the input and output values of current transformers is considered as power theft by the user. The system was designed with the help of power line communication technology. Md. Umar Hashmi and Jayesh G. Priolkar's [9] anti-theft energy metering system explored advanced metering infrastructure (AMI) using PLC technology. A handshaking operation between the two AMI residential meters (M1 and M2) sends data to the central server at the utility authority's premises. The quantity recorded is the KWH value. The relationship is found by comparing the consumption between the two meters. The PLC communicates the frequency of the filtered signal between M1 and M2 to the server. Any distortion in signal means theft or illegal connection. Vinay N. and Shubham R [10]. proposed a microcontroller-based framework utilising ATmega32. Current sensor one records the transmitted source current, and current sensor 2 records the substantial load current. The slave transceiver of both transmits computerised information to the master transceiver of primary microcontroller atmega32, which persistently screen the information obtained from both the sensor and at the same time show it on LCD. If, perchance, that any undesirable load is found between any of the sensors, the current measured by sensor one will be more than the current measured by sensor 2. The master microcontroller detects this error, and the microcontroller commands the GSM modem to send an alarm message to the operator.

[11] proposed a power theft identifier using. Their system used an embedded microcontroller to compare the difference in energy consumption between two energy maters. The system calculates energy supplied by the distribution system on digital energy meter 1. The energy consumption on the residential side is also calculated and recorded by digital energy meter 2. For instance, if digital energy meter 2 is consuming eight units, this data is stored at a smart hardware microcontroller; this data is, however, compared with the energy reading at digital meter 1.

Fig. 1. *A Typical Distribution Service line*

If the digital meter 1 records say 15 units, then the smart grid two-way communication reports the theft of 5 units. A technical report published by [12] proposed a ZigBee-based electricity theft prevention system that uses a microcontroller to monitor any change in the resistance value of the energy meter and show its condition on the LCD. Other works carried out by [13] [14] [15] proposed various WSN based power theft control systems. A power theft detection and automated bill management system using the Arduino microcontroller and Electric Power theft detection and location Tracking using IOT were proposed by [16]-[17]. In order to find the power theft and automated billing system, they used a current sensor and voltage sensor.

III. METHODS EMPLOYED IN ELECTRICITY THEFT

In most cases, electricity is supplied from the utility distribution service lines to the energy meter installed at the customers' premises.

Fig.1 shows a typical distribution service line. The two leading electricity operators in Ghana, the Electricity Company of Ghana (ECG), introduced different types and versions of energy meters in its quest to reduce electricity theft. We can describe these meters as devices that calculate the quantity of electrical energy used by a customer of electricity or any powered electrically. Generally, we categorise the types of energy meters used in Ghana into two, namely, Whole Current meters (WC meters) and Transformer Operated (TO meters). Our research focuses on WC meters due to their percentage use. This section discusses these meters and the methods deployed by consumers to steal electricity.

A. Whole Current Meters

These type of meters are fixed directly at the intake of the customers' load—these meters are commonly utilised for residential and commercial customers who require low energy for operation. The WC meters, based on technology, are classified into Electromechanical and Electronic meters.

- The Electromechanical Meter's mode of operation is by counting the revolutions of an electrically conductive aluminium disc, which spins at speed equal to the meter records' quantity of energy. The number of spins counted is equal to the energy consumed. The voltage coil uses a little and moderately quantity of energy, generally in the area of 2 watts, which is unregistered by the energy meter. In the same manner, the current coil uses a little amount of energy which is equal to the current squared flowing through it, usually close to several watts at full capacity, which is recorded on the meter [18]. Fig.2 shows the electromechanical energy meter. To temper with this meter, fraudsters place large magnets at sides of the meter to lower the aluminium disc rotation, thereby drastically reducing the amount of electricity consumed. The other method is drilling a hole through the meter's plastic case and inserting a magnetic needle to stop or slow the rotating disc [19]. Another method is by meter bypassing and tapping of service lines to the customers' premises. Also, electricity thieves place sugar close to the rotating disc in the meter to attract ants, which slows the rate at which it rotates.
- The introduction of electronic meters curbed electricity theft until fraudsters found an alternative. These meters show the energy consumed on an LED or LCD screen, and others can also send readings to isolated places. These meters work by calculating impulses and therefore have impulse ratings per kWh, which is different from manufacturers. In addition to measuring consumed energy, electronic meters can also take account of other quantities of the load and incoming supply like

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

maximum and the minimum rate of consumption demands, reactive power, and amounts like voltage and power factor. They support, also time-of-night-and-day billing, for instance, reading the energy consumed during off-peak and on-peak hours[8]. Some use Smart ZIGB, and GPRS Technology with the system server positioned at the utility's premises. The energy charge is done by the server whenever the meter communicates to the system server, which informs the electricity customer via SMS. To additionally ensure security, they are locked-out with customised seals. However, these meters, even with security considerations, are basically tampered with by meter bypassing and tapping of service lines to the customers' premises. This is an organised crime mostly committed jointly by ECG /NEDCO field workers and the customer [19]. Some unscrupulous electricians have also developed a method that uses a contactor (an electromechanical device), which makes tapping into the service lines unnoticed by the utility operators even during an inspection, as shown in Fig.3. Finally, another general method employed in electricity theft is disconnecting the neutral line. In this condition, the meter cannot accurately calculate the voltage difference across the live wire and the neutral wire to the consumer distribution board. The result will be an unrealistic energy calculation of the meter.

Fig. 2.*Electromechanical Energy Meter*

This work has received funding from 5150 spring specialised (05492018012 , 05762018039), Major Program of the national social science Fun of China (Grant No. 17ZDA092), 333 high-level talent cultivation Project of Jiangsu province (BRA2018332), Royal society of Edinburgh, UK and China Natural Science Foundation Council (RSE reference:62967_LIU_2018_2) under their joint International projects funding scheme and basic research programs (National Science Foundation) of Jiangsu province(BK201913988)

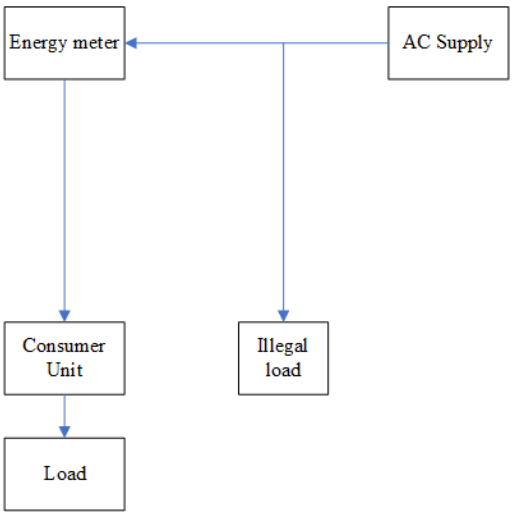

Fig. 3. *Illegal Tapping of Utility Service*

IV. THE PROPOSED SYSTEM

A We propose an IoT based electricity theft detection using Raspberry Pi.

A. System Design

1) Raspberry Pi: T The Raspberry Pi is a range of minicomputers, developed by the Raspberry Pi foundation. It is a United Kingdom-based company with one of their aims to encourage researchers and to encourage students to learn basic computer science and technology easy. They have developed free resources to aid learners to study computing and how computers work with devices alongside sensors. Launching of the ranges of Raspberry Pi started in 2006. Models A and B were announced on the 19th of February 2012. During July 2014, the Model B+ was announced. The Raspberry Pi, 3 Model B, was out doored on the 29th of February 2016 [20]. Raspberry pi is an inexpensive minicomputer. It is also capable of converting digital signals into text. PC Display, as well as Television, can be linked to Raspberry pi. You can attach Mouse and Keyboard to Raspberry pi. It consists of a central processing unit (CPU) and a chip-based graphical processing unit, all versions having Broadcom device on a chip. CPU velocities range from 700 megahertz to 1200 megahertz for the Raspberry Pi 3. The board has memory size ranges from 256megabytes to 1gigabytes of RAM. There is a stable digital card (SD) that stores operating systems and application memory. Practically, raspberry pi boards consist of several components, as shown in Fig.4.

a) Components

- 2Gigabytes, 4gigabytes and 8gigabytes LPDDR4-3200 SDRAM depending on medels.
- 2.4 gigahertz or 5 gigahertz IEEE 802.11ac wireless, bluetooth5.0, BLE.
- 2 universal serial bus 3.0 ports; 2 universal serial bus ports 2.0 ports
- Gigabit Ethernet

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

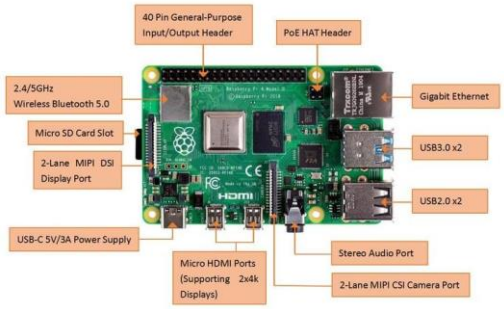

Fig. 4. *Raspberry Pi 4 Board*

- 40 pin standard GPIO header with fully backward compatibility.
- Supports 2 number of micro-HDMI ports up to 4kp60
- 2-channel MIPI DSI display port
- 2-channel MIPI CSI camera port
- 4-pole video and audio ports
- Decode of H.265 (4kp60), H264 (1080P60), 1080p30
- OpenGL ES 3.0 graphics
- Micro-SD card slot for loading operating system and data storage
- 5V DC via USB-C connector (minimum 3A*)
- 5VDC via GPIO header (minimum 3A)
- Power over Ethernet (PoE) enabled

2) NodeMCU ESP8266: The NodeMCU Development board is a firmware and development kit that is available freely. It plays a very critical role in an open-source firmware and development kit that plays an important role in using a few script lines to design a proper IoT application [21]. This allows explicitly flashing from a USB port. This incorporates characteristics of a WIFI entry point and deployed microcontroller. The module is primarily based on ESP8266, which is a low-cost Wi-Fi microchip with full TCP / IP stack as well as microcontroller capabilities. Due to the above features, WiFI networking with NodeMCU is very dominant. It aids downloading and uploading of data, hosting of a web server, can be possibly used as an access point or station. When fixed onto the Raspberry Pi allows the entire system to be connected to the internet for data fetch and upload.

Fig. 5. *NodeMCU ESP8266*

a) Components

- Analogue to digital converter (ADC)
- General-purpose input and output (GPIO) pin: NodeMCU has input pins of general use with its board. It aids the switching of LEDs to zeros and ones digitally. It is also capable of producing pulse width modulation.
- Serial Peripheral Interface (PI) Pins: NodeMCU based ESP8266 hardware has four-pins.
- SPI (HSPI) for SPI connectivity. It also has SPI pins for the contact with Quad-SPI. With this SPI interface, we can connect any device with NodeMCU enabled by SPI and make communication with it possible.
- Inter-integrated circuit (I2C) pins: On GPIO pins of the ESP8266, the NodeMCU has support for I2C functionalities.
- Universal asynchronous receiver transmitter pins: There are two interfaces, UART 0 and UART 1. The firmware and the codes are uploaded inboard by the UART0

3) Relay Module: The 4- channel relay interface circuit board that takes a supply voltage of 5V and a driving current of 15-20milliamps for every channel is used to control different types of large current equipment and appliances. It is manufactured with high current relays that woks with 250Volts, 10amps AC or 30Volts, 10amps DC. It has a standard microcontroller-controlled interface, as shown in Fig.6.

a) Components

- Maximum output of relay: 250Volts, 10Amps AC and 30Volts, 10 Amps DC
- 4- way relay module.
- Standard interface that can be operated by the Raspberry pi directly
- Isolation optocoupler for safety on high voltage and ground protection.

Fig. 6. *Block Diagram of Relay Module*

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

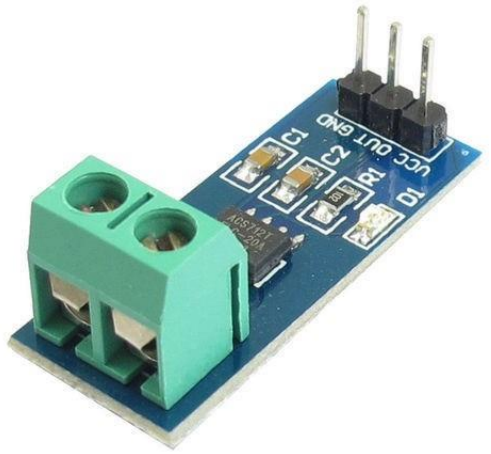

Fig. 7. *Current Sensor*

4) Current Sensor: ACS712 current sensor detects and generates an electrical signal proportional to the electrical current in a wire or network, whether it is high or weak. The current sensor records current and sends the signal to display the measured current on the comparator of the Raspberry Pi via the relay module for further analysis.

5) Firebase Server: Firebase, which is a Back-End -As-Services which started as a YC11, has been updated vigorously onto Google Could as the next-generation application development platform. Firebase frees developers to focus on building an excellent user interface. With firebase availability, we do not need to host servers. The firebase is its server, the application programming interface, and has its data store, that is written in such a generic fashion that it needs to be modified to suit most needs which allow data to be stored on GCloud. The storage of the firebase has a built-in security system to protect the Google Cloud bucket from intruders and at the same time giving authenticated customers detailed rights and privileges.

6) Utility Service Box (USB): The Utility Service Box house one of the relay module with a current sensor incorporated. It is mounted on the utility service pole and is accessible to only the utility authority staff.

B. System Architecture

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.

Initially, when the utility service feeder is energised, the value of the supply current will be measured by the current sensor incorporated in relay 1. The Raspberry Pi will fetch this measured current. In the same way, the current sensor integrated into relay two measures the source current at the energy meter intake point, which is then fetched by the Raspberry pi. The current signal recorded by the two current sensors is compared in the comparator of the Raspberry Pi. Any difference in the current recording will be registered as illegal and converted into text that will be saved onto the Firebase server via NodeMCU. The utility Authority will have the authorisation to monitor the condition in real-time.

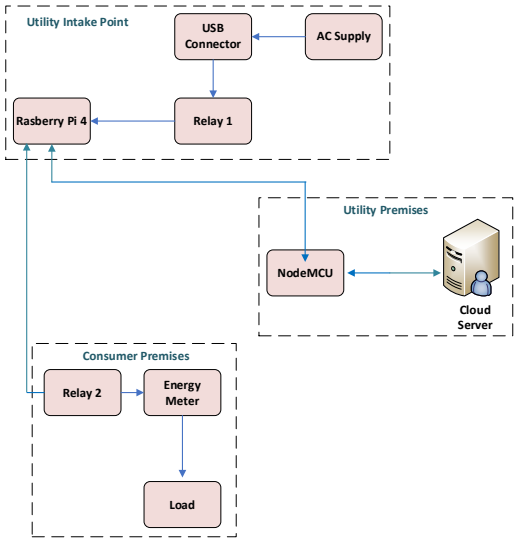

Fig. 8. *Activity flow diagram of IoT Based Electricity Theft Detection*

V. CONCLUSION

Internet of things based electricity theft detection using Raspberry Pi has been designed. The architecture deployed the use of a 4- channel relay interface circuit boards, incorporated with current sensors for measuring and recording current imbalance. The Raspberry Pi gives the utility authority the flexibility to monitor any theft between the energy meter and the USB in real-time. The design also incorporated NodeMCU that allows access to data stored on GCloud of the firebase server. It is envisaged that future works look at the construction of the system to establish this design's practicality.

REFERENCES

[1] N. Donald, The Internet of Things: Do-It-Yourself at Home Projects for Arduino, Raspberry Pi and BeagleBone Black, London: McGraw-HillTAB Electronics, 2015

[2] WORLD BANK, "Electric power transmission and distribution losses (% of output) – Ghana," World Bank, Ghana, 2018.

[3] J. Parmar, "Total losses in power distribution and transmission lines," Electrical Notes, vol. 1, no. 2, pp. 33-47, 2013.

[4] O. Eseosa and E. Promise, "Economic Effects of Technical and Non Technical Losses in Nigeria Power Transmission System," IOSR Journal of Electrical and Electronics Engineering Ver. I, vol. 10, no. 2, pp. 2278-1676, 2015.

[5] P. Navani, N. K. Sharma and . S. Sonal, "A Case Study Of Analysis Of Technical And Non-Technical Losses In Power System And Its Impact On Power Sector," International Journal Of Advances In Engineering Science And Technology (IJEAST), vol. 1, pp. 2319-1120, 2013.

[6] T. B. Smith, "Electricity theft: A comparative analysis," Energy Policy, vol. 32, no. 18, pp. 2067-2076, 2004.

[7] Ghanaweb, "ECG to fight power theft as it faults churches," Ghanaweb, the 2nd of March 2020. [Online]. Available: https://www.ghanaweb.com/GhanaHomePage/business/ECG-to-fight-power-theft-as-it-faults-churches-836506. [Accessed 06 08 2020].

[8] K. B. Amal, T. G. Alphy and N. K. Fathima , "HOME ENERGY MANAGEMENT SYSTEM BASED ON POWER LINE," International Research Journal of Engineering and Technology (IRJET), vol. 4, no. 4, p. 2532, 2017.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

[9] M. U. Hashmi and J. . G. Priolkar, “Anti-theft energy metering for smart electrical distribution system,” in 2015 International Conference on Industrial Instrumentation and Control, ICIC 2015, Maharashtra, 2015.

[10] S. N. Vinay and M. R. Shubham , “WSN-POWER THEFT CONTROL,” International Research Journal of Engineering and Technology (IRJET), vol. 04, no. 01, p. 1984, 2018.

[11] S. Thiruvalluvan, B. Swardheep and S. Arunachalam, “Power Theft Identification system using Power Line Carrier Communication (PLCC) technique in Distribution system based on Binary Search Algorithm,” International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC-2013), p. 978, 2013. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[12] S. Tshikomba, “How wireless electricity theft detection can assist in reducing electricity theft,” 26thAMEU Technical Convention, Tshwane, 201.

[13] S. Sardar and S. Ahmad, “Detecting And Minimizing Electricity Theft : A Review,” Peshawar, 2016.

[14] . R. V. P. Yerra, A. K. Bharathi and U. B. Desai, “WSN based power monitoring in smart grids,” in Proceedings of the 2011 7th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2011, Yeddumailaram, Medak, 2011.

[15] R. D. Aryadevi and M. V. Ramesh, “Wireless,” in Fourth International Conference on Sensor Technologies and Applications, India, 2010.

[16] “Power Theft Detection and Billing Using Arduino.” https://www.pantechsolutions.net/power-theft-detection-and-billing-using-arduino (accessed Jan. 25, 2021).

[17] A. Mahato, A. Nanda, A. K. Pal, and C. K. Singh, “Electric Power theft detection and location Tracking using IOT,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 4, no. 5, pp. 35–39, 2018.

[18] E. C. o. Ghana, “Meter Types,” Electricity Company of Ghana, Accra, 2020.

[19] O. Yakubu and N. . C. Babu, “Type And Nature of Electricity Theft: A Case Study Of Ghana,” International Journal of Mechanical Engineering and Technology (IJMET), p. 170–179, 2017.

[20] S. Bush, "Electronic Weekly," Electronic Weekly.com, 25 03 2011. [Online]. Available: https://www.electronicsweekly.com/market-sectors/embedded-systems/dongle-computer-lets-kids-discover-programming-on-a-2011-05/. [Accessed 20 09 2020].

[21] A. A. Dahoud and M. Fezari, “NodeMCU V3 For Fast IoT Application Development,” Notes, no. October, p. 5, 2018. I.S. Jacobs and CP Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.