Educational Administration: Theory and Practice
2024, 30(1), 4603 - 4610
ISSN: 2148-2403
https://kuey.net/

Research Article

Intelligent Access Control Using RFID and IoT Blynk Interface

Thejaswini S[1*], Rashmi N[2], Mamatha K R[3], Dr. Seema Singh[4], Dr. Girish H[5]

[1*]Dept. of ETE, B M S Institute of Technology and Management Bengaluru, Karnataka, India.
[2]Dept. of ECE, B M S Institute of Technology and Management Bengaluru, Karnataka, India
[3]Dept. of ECE, B M S Institute of Technology and Management Bengaluru, Karnataka, India.
[4]Professor (ETE), and Dean innovation and entrepreneurship. BMSIT&M, Bengaluru, Karnataka, India
[5]Professor, Department of ECE, Cambridge Institute of Technology, Bangalore, Karnataka, India.

Citation: Thejaswini S, et.al (2024), Intelligent Access Control Using RFID and IoT Blynk Interface, Educational Administration: Theory and Practice, 30(1), 4603 - 4610
Doi: 10.53555/kuey.v30i1.8289

ARTICLE INFO

ABSTRACT

This paper presents an Internet of Things (IoT)-based remote access security system that combines Radio Frequency Identification (RFID) technology with the capabilities of the Blynk mobile application for enhanced security and convenience. Built upon the foundational concept of IoT—interconnecting physical devices embedded with sensors, software, and network capabilities—this system enables real-time data exchange and remote control over secure access points via the Internet. IoT applications have already transformed our daily lives by facilitating smart city infrastructure and increasing the security of residential and commercial spaces. With this in mind, the current project leverages IoT to design a smart access system that can monitor and control entry points remotely. The system employs an EM18 RFID reader, NodeMCU ESP8266 Wi-Fi module, and software tools like Arduino IDE and Blynk. The NodeMCU, which serves as the central controller, interfaces with the RFID module and other components, handling data processing and communication with the Blynk app. The RFID reader scans authorized tags to authenticate users, and the Blynk app allows users to monitor and control the door lock status from anywhere in the world, providing real-time security monitoring and control through smartphones. This implementation of RFID-based access management not only improves security by restricting unauthorized entry but also offers convenience with remote accessibility. This paper details the system's design, implementation, and operation, highlighting the role of the Blynk app in managing device interactions and enabling user control through a user-friendly mobile interface. The proposed IoT-based security solution demonstrates the potential of integrating IoT, RFID, and mobile applications to create a secure, flexible, and scalable access control system suitable for residential and commercial environments.

Keywords— Node MCU, RFID, IoT, Blynk app andsurveillance.

I. INTRODUCTION

Securing personal spaces has always been a priority, and as reliance on technology grows, so does the demand for convenient and robust security solutions. With advances in IoT, individuals and organizations can now utilize connected devices to monitor and manage their spaces more effectively than ever before. Traditional locks and security measures, while still useful, no longer provide the flexibility, control, or remote monitoring that modern IoT-based systems offer. In this context, there is a clear need for a device that can enhance security while remaining user-friendly, versatile, and highly efficient.

To meet these demands, we have developed a smart access system that uses Radio Frequency Identification (RFID) technology integrated with a NodeMCU microcontroller. This RFID-based security system combines ease of use with advanced, reliable access control, ensuring that only authorized users can enter a secure area. The system operates by using RFID tags and an RFID reader module; each RFID tag contains a unique identifier (UID) that acts as a digital key for the user. These identifiers are programmed in the system's database using the Arduino IDE, allowing for accurate user recognition.

When an RFID tag is presented, the RFID reader module captures its unique ID, which is then sent to the NodeMCU controller. The controller checks this ID against its database of pre-registered IDs to determine if the user is authorized. If a match is found, the system grants access; otherwise, entry is denied. This process ensures that only users with verified IDs can enter the premises, offering enhanced security over conventional lock-and-key systems.

In addition to its core functionality, this system leverages IoT connectivity through the NodeMCU, providing remote control and monitoring capabilities. As IoT technology continues to evolve, this access system could be enhanced with Artificial Intelligence (AI) and Machine Learning (ML) to identify potential threats, detect unusual entry patterns, and further tighten security. By exploring the synergy between RFID and IoT, this system exemplifies how smart technologies can be integrated to create highly secure, scalable, and user-friendly access solutions for modern security needs.

II. Methodology

A. Hardware Requirement

Fig 1: NodeMCU ESP8266

With the advancements in automation and wireless technology, all household devices can now be interconnected, creating a seamless smart home environment. With the global shift towards digitalization, convenience and ease of use are becoming accessible to all age groups, from young adults to seniors. A Smart Home Automation Application powered by IoT enables remote control of basic household facilities, such as turning lights, fans, AC units, and water pumps on or off, as well as automating tasks like watering plants.

The system relies on the NodeMCU ESP8266 module, an Android application, and internet connectivity. This paper explores the functionality of the NodeMCU ESP8266, which can interface with various home appliances through coding and online hosting on a web server. Using the Blynk app, users can remotely manage and monitor these devices over the internet, offering full control of the connected home environment.

The NodeMCU ESP8266 microcontroller can connect up to eight devices, including sensors and appliances, depending on specific needs. RFID technology further enhances smart capabilities by supporting secure access and automation features. As illustrated in Figure 2, the NodeMCU is a Lua-based, open-source development board featuring the ESP-12E module, which contains an ESP8266 chip with a Tensilica Xtensa 32-bit LX106 RISC microprocessor. This processor supports RTOS and operates between 80MHz to 160MHz, with 128KB of RAM and 4MB of flash memory for data storage and program execution. The NodeMCU's robust processing power, integrated Wi-Fi/Bluetooth, and DeepSleep mode make it ideal for IoT applications, and it is powered via a micro-USB jack or an external VIN pin. It also supports UART, SPI, and I2C interfaces, enabling versatile connectivity for smart home automation..

1. EM18 RFID reader

Fig 2: EM18 RFID READER

Radio Frequency Identification (RFID) is a technology that uses radio waves to transfer data between a tag and a reader, allowing for automatic identification and tracking of objects. In an RFID system, digital data is encoded within RFID tags, which consist of a microchip that stores data and an antenna for transmitting this data. When an RFID reader, such as the EM18 reader module, detects a tag within its operating range, it

retrieves the encoded information through radio signals.
The EM18 reader module is specifically designed to read RFID tag information by capturing the unique identifier (UID) stored on each tag. The RFID tags in this system contain a 12-digit unique ID that distinguishes one tag from another. When the tag is brought within range of the reader, the EM18 module interprets this UID, allowing it to identify the specific tag accurately.

Operating at a frequency of 125 kHz, the EM18 reader relies on an internal antenna that generates a field to communicate with RFID tags. This frequency is ideal for close-range applications, typically providing a reading range of a few centimeters to a few inches. The module itself is compact and operates on a 5V DC power supply, making it easily integrable into microcontroller-based systems like the NodeMCU or Arduino. With its efficient design and reliable data interpretation, the EM18 RFID reader is widely used in access control, inventory management, and IoT applications, where it offers secure, rapid identification in a variety of settings

2. RFID tags

Fig 3: RFID Tags

In RFID-based identification systems, tags are attached to items to enable wireless tracking and data collection. Each tag includes an antenna or coupling element that transmits data, and in advanced tags, electronics such as microcontrollers and memory for data storage. There are two main types of RFID tags based on their power sources: active and passive.
Active RFID Tags: These tags are powered by an internal battery, enabling them to operate independently of the reader's energy. This allows for extended communication ranges, reaching up to 300 feet (approximately 91 meters), which is advantageous for applications that require long-range data acquisition, like large warehouse tracking. Active tags also typically include more storage capacity, often around 512KB, to support more extensive data logging, making them ideal for applications with high data storage needs.
Passive RFID Tags: In contrast, passive RFID tags don't contain an internal battery and rely entirely on power drawn from the reader's electromagnetic field. Although their range is limited (up to a few meters), passive tags are typically more cost-effective and easier to deploy in larger quantities, making them suitable for shorter-range applications like retail item tracking and automated checkout systems.
Development with Arduino and Other Vendor Boards: In the context of RFID and IoT applications, development boards like those from Arduino are widely used for prototyping. Programs written in the Arduino IDE are called "sketches." Each sketch is a code file that can be saved under different names with the .ino file extension. This flexible setup allows developers to implement various RFID functionalities and interact with different RFID tags and sensors using third-party cores, which expand the compatibility of the Arduino environment to support a range of third-party development boards.

This modular setup provides an accessible environment for developing RFID applications, from item identification and tracking to complex IoT integrations.

2.Blynk App

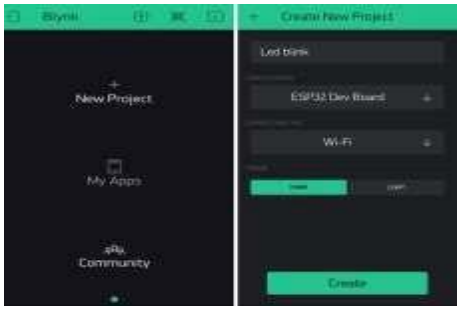

Fig.4 Blynk Application

Blynk App provides a platform to user for designing own app that is connected to the Blynk Server that provides

a path for transmission andreception between the developed project (kit) and user which is shown in Fig.4.

III. IMPLEMENTATION

B. Software Required

1. Arduino IDE

Fig.5 Arduino IDE

Arduino Integrated Development Environment (IDE)shown in figure 5, is a cross-platform program developed in C and C++ functions. It's used to createand upload programs to Arduino-compatible boards,

A. Block diagram

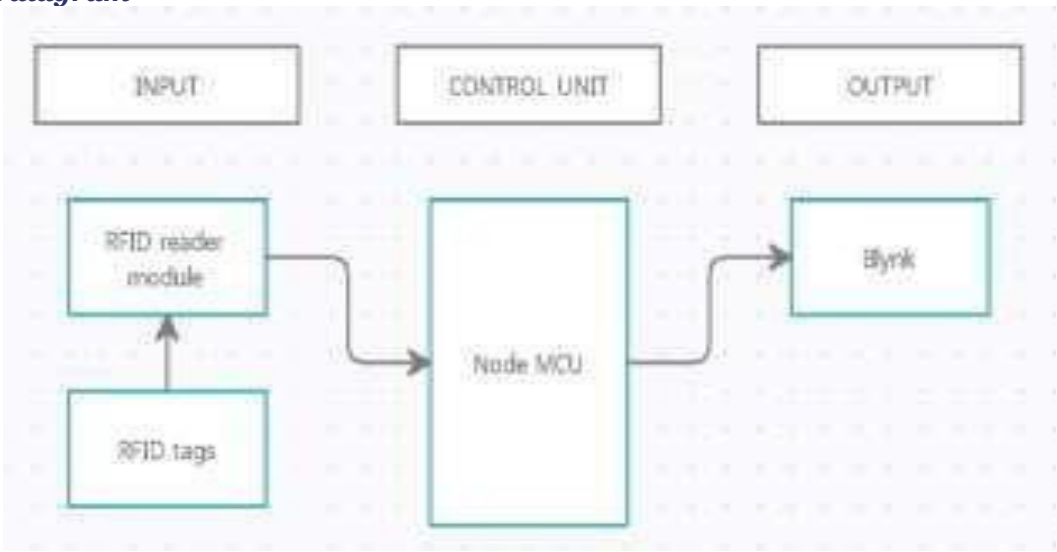

Fig.6 Block diagram

The above figure 6 represents the block diagram of the project IOT based secure system using RFID andBlynk. In this system, an RFID-based setup is used to verify user identity through a structured input-control-output process. Here's how each part works in detail:

Input

The input system includes an RFID reader module that interacts with RFID tags. Each RFID tag is embedded with a unique identifier (ID), which the system uses to recognize different users. When a tag comes within the RFID reader's range, the reader detects the unique ID on the tag. This unique ID, which is pre-assigned in the integrated development environment (IDE), represents each user. This means that in the code, each tag's unique ID corresponds to specific user data, allowing the system to verify user identities automatically. After

reading the ID from the tag, the RFID reader module sends this data to the NodeMCU microcontroller. NodeMCU is used here as the primary control unit for processing the ID data and handling the subsequent decision-making.

Control Unit

Upon receiving the ID from the RFID reader, the NodeMCU checks if the ID exists in its database. This database contains pre-approved IDs representing authorized users. The NodeMCU compares the received ID against this list to determine whether the user is authorized. If the received ID matches an entry in the database, the NodeMCU identifies the user as valid. Otherwise, the ID is marked as invalid. This step is crucial for security and helps in filtering unauthorized users from accessing the system. Once the verification process is complete, the NodeMCU decides the appropriate response. If the user is valid, the NodeMCU prepares to send a signal to the output system.

Output

When a valid user ID is detected, the NodeMCU generates a high signal to activate the output mechanism, effectively granting access to the user. This signal may, for example, unlock a door, activate a device, or allow the user to proceed with further actions. Simultaneously, the NodeMCU logs the successful access in the Blynk terminal. Blynk is a platform that connects IoT devices with a user interface, enabling real-time data viewing. By recording the user ID in Blynk, the system maintains a log of each access attempt, including details of authorized users who accessed the system. In this setup uses RFID tags and a reader module to verify users through a structured input-control-output process. The NodeMCU functions as a control unit, processing the IDs to grant access, while the Blynk terminal provides an interface for tracking access attempts in real time. This method ensures secure and efficient management of user authentication and access control.

B. Process Flow

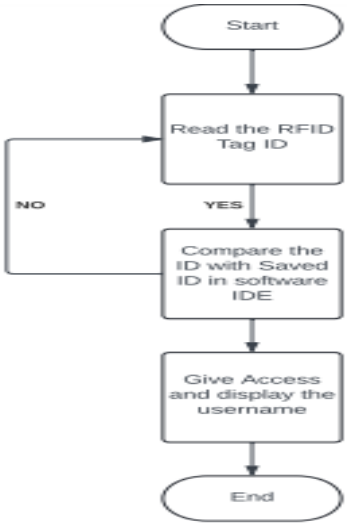

Fig.7 Flow chart

The above figure 7 represents the flow chart of the project IOT based secure system using RFID and Blynk. The input consist of a RFID reader module and the RFID tags. RFID reader tags consist of unique ID which can be assigned to the user in the IDE to identify them. The tags can be read by the RFID reader module sensor and the ID is passed on the Node MCU for the processing.

The data received from the RFID reader module is used to check the identity. ID received is processed to check the existence of the user in the database of Node MCU. If the ID is present and valid, the appropriate results are passed to the output.

A high signal is received as output from the processing unit i.e., Node MCU. The access is granted and the user ID is recorded in the Blynk terminal.

IV. RESULTS

The IoT-based security system was successfully tested and implemented, demonstrating its effectiveness in providing secure access management. Figure 10 presents the final setup of the system, showcasing the circuit connections and operational functionality. When an authorized user scans their RFID tag at the RFID reader, the LED indicator lights up, confirming successful identification and system response. This visual feedback is essential for users, as it clearly signals the status of each access attempt.

Figure 11 displays a screenshot of the Blynk app, specifically highlighting the terminal output section. Here, the names of authorized users appear in real-time each time their RFID tags are scanned, confirming their

access. This log not only serves as a record of entries but also provides the user with a transparent view of access events, making it easy to monitor who has gained entry.
The Blynk app's Remote Access feature offers flexibility and control, allowing the system administrator to manage permissions. Through this feature, the owner can remotely toggle access settings for registered users, enabling or disabling their ability to unlock the system as needed. This feature exemplifies the system's convenience and adaptability, especially in scenarios where immediate changes to access permissions are required. The results of the implementation show that the system is highly functional, responsive, and user-friendly, with practical applications in enhancing security for homes or small offices. The use of IoT technology, RFID identification, and remote management via Blynk successfully addresses the project's goals of providing both security and convenience.

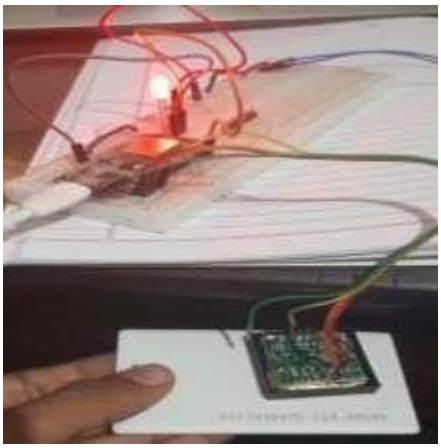

Fig 8: Final implementation

Fig 9: Blynk interface

V. CONCLUSION

The Internet of Things (IoT) connects the digital world of information technology with the physical world, enabling devices to communicate and operate together seamlessly. Technologies like RFID and sensors enhance convenience and comfort in our daily lives. This project, "IoT Secure Access System Using RFID and Blynk," demonstrates how IoT can provide accessible, secure entry management. In this system, each RFID tag's unique ID is registered in the Arduino IDE, linked to a username for straightforward identification. Registered users can simply scan their tags to gain access, with each entry logged in the Blynk application's terminal. Access permissions can be managed remotely via the Blynk app, allowing the owner to deny or permit access to registered users as needed. The RFID tags must be scanned within a 5cm range for accurate detection. Our IoT internship provided foundational knowledge that enabled the development of this secure access system and opened doors to other innovative IoT projects.

REFERENCES

[1] R. Colella, L. Catarinucci and L. Tarricone, "Improved RFID tag characterization system: Use case in the IoT arena," 2016 IEEE International Conference on RFID Technology and Applications (RFID-TA), 2016, pp. 172-176

[2] A. K. Gupta and R. Johari, "IOT based Electrical Device Surveillance and Control System," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-5

[3] H. Durani, M. Sheth, M. Vaghasia and S. Kotech, "Smart Automated Home Application using IoT with Blynk App," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 393-397

[4] Dr. GIRISH H et. al., "Design and Analysis of a Machine learning based Agriculture bot", Tuijin Jishu/Journal of Propulsion Technology ISSN: 1001-4055 Vol. 44 No. 6 (2023)

[5] Dr. GIRISH H et. al., "ROBOTIC INNOVATION IN E-DELIVERY SYSTEMS: A DESIGN AND MODELING APPROACH", The Seybold report ISSN 1533-9211, 2023.

[6] Dr. GIRISH H et. al., "Machine Learning based Agriculture Bot", International Conference on Smart Technologies, Communication and Robotics [ICSCR-2023] in association with IJSRSET Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com) doi : https://doi.org/10.32628/IJSRSET

[7] Dr. GIRISH H et.al., "A GSM-Based System for Vehicle Collision Detection and Alert". International Conference on Smart Technologies, Communication and Robotics [ICSCR-2023] in association with IJSRSET Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com) doi : https://doi.org/10.32628/IJSRSET

[8] H. Girish, T. G. Manjunat and A. C. Vikramathithan, "Detection and Alerting Animals in Forest using Artificial Intelligence and IoT," 2022 IEEE Fourth International Conference on Advances in Electronics, Computers and Communications (ICAECC), 2022, pp. 1-5, doi: 10.1109/ICAECC54045.2022.9716679.

[9] A. Devipriya, H. Girish, V. Srinivas, N. Adi Reddy and D. Rajkiran, "RTL Design and Logic Synthesis of Traffic Light Controller for 45nm Technology," 2022 3rd International Conference for Emerging Technology (INCET), 2022, pp. 1-5, doi: 10.1109/INCET54531.2022.9824833.

[10] S. Vaddadi, V. Srinivas, N. A. Reddy, G. H, R. D and A. Devipriya, "Factory Inventory Automation using Industry 4.0 Technologies," 2022 IEEE IAS Global Conference on Emerging Technologies (GlobConET), 2022, pp. 734-738, doi: 10.1109/GlobConET53749.2022.9872416.

[11] T G Manjunath , A C Vikramathithan , H Girish, "Analysis of Total Harmonic Distortion and implementation of Inverter Fault Diagnosis using Artificial Neural Network", Journal of Physics: Conference Series, Volume 2161, 1st International Conference on Artificial Intelligence, Computational Electronics and Communication System (AICECS 2021) 28-30 October 2021, Manipal, India. https://iopscience.iop.org/issue/1742-6596/2161/1

[12] GIRISH H , "Internet of Things Based Heart Beat Rate Monitoring System", © September 2022 | IJIRT | Volume 6 Issue 4 | ISSN: 2349-6002 IJIRT 156592 INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY 227

[13] Dr Girish H, Dr. Mangala Gowri , Dr. Keshava Murthy , Chetan Naik J, Autonomous Car Using Deep Learning and Open CV, PAGE NO: 107-115, VOLUME 8 ISSUE 10 2022, Gradiva review journal, ISSN NO : 0363-8057, DOI:10.37897.GRJ.2022.V8I8.22.50332

[14] Girish H. "Intelligent Traffic Tracking System Using Wi-Fi ." International Journal for Scientific Research and Development 8.12 (2021): 86-90.

[15] Girish H, Shashikumar D R, "Emission monitoring system using IOT", Dogo Rangsang Research Journal, UGC Care Group I Journal, ISSN: 347-7180, Vol – 8 Issue-14, No.6, 2020.

[16] Girish H, Shashikumar D R, "Display and misson computer software loading", International journal of engineering research & Technology (IJERT), ISSN: 2278-0181, Vol – 10 Issue-08, No.13, August 2020.

[17] Girish H, Shashikumar D R, "A Novel Optimization Framework for Controlling Stabilization Issue in Design Principle of FinFET based SRAM", International Journal of Electrical and Computer Engineering (IJECE) Vol. 9, No. 5 October 2019, pp. 4027~4034. ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp.4027-4034

[18] Girish H, Shashikumar D R, "PAOD: a predictive approach for optimization of design in FinFET/SRAM", International Journal of Electrical and Computer Engineering (IJECE) Vol. 9, No. 2, April 2019, pp. 960~966. ISSN: 2088-8708, DOI: 10.11591/ijece.v9i2.pp.960-966

[19] Girish H, Shashikumar D R, "SOPA: Search Optimization Based Predictive Approach for Design Optimization in FinFET/SRAM", © Springer International Publishing AG, part of Springer Nature 2019 Silhavy (Ed.): CSOC 2018, AISC 764, pp. 21–29, 2019. https://doi.org/10.1007/978-3-319-91189-2_3.

[20] Girish H, Shashikumar D R, "Cost-Effective Computational Modelling of Fault Tolerant Optimization of FinFET-based SRAM Cells", © Springer International Publishing AG 2017 R. Silhavy et al. (eds.), Cybernetics and Mathematics Applications in Intelligent Systems, Advances in Intelligent Systems and Computing 574, DOI 10.1007/978-3-319-57264-2_1.

[21] Girish H, Shashikumar D R, "A Survey on the Performance Analysis of FinFET SRAM Cells for Different Technologies", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 –

8958, Volume-4 Issue-6, 2016.
[22] Girish H, Shashikumar D R, “Insights of Performance Enhancement Techniques on FinFET-based SRAM Cells”, Communications on Applied Electronics (CAE) – ISSN: 2394-4714, Foundation of Computer Science FCS, New York, USA .Volume 5 – No.6, July 2016 – www.caeaccess.org
[23] Girish H, Shashikumar D R, “DESIGN OF FINFET”, International Journal of Engineering Research ISSN: 2319-6890) (online), 2347-5013(print) Volume No.5 Issue: Special 5, pp: 992-1128, doi: 10.17950/ijer/v5i5/013 2016.
[24] Dr. MANGALA GOWRI S G, Dr. SHASHIDHAR T M, Dr. SUNITHA R, SHYLAJA V, Dr. GIRISH H, “DESIGN OF 3-BIT CMOS WALLACE MULTIPLIER” , Seybold report, ISSN 1533-9211, Volume 18, Page No: 1260-1271 DOI: 10.5281/zenodo.8300481
[25] Dr. Mangala Gowri S G, Dr. Girish H, Ramesh N, Dr. Nataraj Vijaypur, “IOT based plant monitoring system and smart irrigation using new features” ResMilitaris, vol.13, n°2, January Issue 2023 https://resmilitaris.net/menu-script/index.php/resmilitaris/article/view/3312/2608
[26] Girish H.2023, Smart Theft Securityvehicular System Using Iot. Int J Recent Sci Res. 14(02), pp. 2881-2884. DOI: http://dx.doi.org/10.24327/ijrsr.2023.1402.0591
[27] Dr. Mangala Gowri S G, Dr. Girish H, Dr. Santosh Dattatray Bhopale, Weed Detection based on Neural Networks, International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211 Volume 11, Issue 3, March-2023, Impact Factor: 7.429, Available online at: www.ijaresm.com DOI: https://doi.org/11.56025/IJARESM.2023.11323351
[28] Shashidhara, K.S., Girish, H., Parameshwara, M.C., Rai, B.K., Dakulagi, V. (2023). A Novel Approach for Identification of Healthy and Unhealthy Leaves Using Scale Invariant Feature Transform and Shading Histogram-PCA Techniques. In: Shetty, N.R., Patnaik, L.M., Prasad, N.H. (eds) Emerging Research in Computing, Information, Communication and Applications. Lecture Notes in Electrical Engineering, vol 928. Springer, Singapore. https://doi.org/10.1007/978-981-19-5482-5_47