IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12647

Two Factor Authentication using RFID and Biometric sensor – A Progressive Review

Sanjay S Tippannavar[1], Yashwanth S D[2], Eshwari A Madappa[3]

Student, Department of Electronics and Communication Engineering, JSS Science and Technology University, Mysuru, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, JSS Science and Technology University, Mysuru, India[2]

Assistant Professor, Department of Electronics and Communication Engineering, JSS Science and Technology University, Mysuru, India[3]

Abstract: Identity identification is often carried out via traditional authentication methods using biometric data, such as fingerprints, or user information verification, such as inputting a password. When using simply these authentication techniques, there are security hazards. Everyone considers security to be a big problem while they are apart from their family. There is currently no satisfactory solution for the aforementioned problem. Here, an electronic security architecture is introduced. Security has always been a worry in our homes, offices, stores, etc., and it continues to be so today. Everyone worries about someone breaking into their house or workplace without their permission. For instance, it may be difficult to tell if the person typing the password is authorised if the password has been hacked. The development of a two-factor RFI and biometric fingerprint authentication-based security scheme is described in this work. It can offer effective control facilities to prevent entry of an unauthorised user at any workplace, posing risks and disrupting work-flow. Passive approaches, communication alerts, the Internet of Things, machine learning, and database management systems have all been explored in relation to various technologies. This initiative focuses on protecting customers against unauthorised use of products, thefts, and constant notification for the benefit of society.

Keywords: Fingerprint sensor, RFID, Signal Processing, Micro-controller, Data Acquisition, Communication,Machine Learning,

I. INTRODUCTION

The technique of employing radio frequency waves to transfer data is known as RFID. RFID is a wireless, non-contact wave. By adding RFID tags to items, users may instantaneously and uniquely identify commodities and assets. Automatic product identification is accomplished using RFID, a radio frequency-based technology. The RFID system's two primary components are. The error was made. If the RFID-tagged item was still within the RFID reader's range, the reader would have returned with input. RFID scanners and antennas are powered by RF frequency power, whereas passive RFID tags are uncontrolled. The signal transmitted by the readers and antenna, which also reflects the reader's energy back, controls the tag [1].

In this research, we present the design of a two-factor RFID-based security door authentication mechanism that may offer effective control capabilities to prevent access of an unauthorised door user. The RFID unit, a microprocessor, and a synchronous motor are the main components of the system that has been built. In order to indicate the card user's status while the alarm system alerts the public to an intruder, multiplexers made up of integrated circuits were used in conjunction with liquid crystal displays. Discussion and presentation of the experimental findings. Aluminium sheet measuring (50 cm × 30 cm) was used to create the prototype security door system. Hard board was used to cover the object [2].

The majority of individuals today struggle to preserve their personal belongings like jewels, important documents, and money kept at home since theft occurs in homes, businesses, and organisations as well. Because of this, most homeowners employ safe-keeping lockers and atlases to safeguard their priceless valuables. They however persisted in using a manual lock and key system, providing the user with no notification when a theft took place by breaking them. As a consequence, efforts have been made to develop a sophisticated alert home security system that uses fingerprint and password verification to open or shut the door system and also sends messages in the event that any miss activities will be carried out by others using GSM Technology with smart mobile. All kinds of residences may benefit from the greater security

DOI: 10.17148/IJARCCE.2023.12647

provided by the present system, which is also widely available and reasonably priced. Our lives and our movable goods are protected by security. To prevent using theft as an unlawful form of defence against intruders and to ensure the safety and security of individuals and their valuables while at home. Most individuals in both urban and rural regions now consider safety to be a top priority. Things will attempt to defraud or steal property, putting the safety of their possessions, such jewellery, critical papers, and money, at risk at their homes, offices, and residences. The majority of individuals will install several locks or shutting devices to combat this security danger. However, mechanical locks that are simple to bypass with modern equipment make robberies more commonplace nowadays. We thus tried to create a sophisticated home security system that uses soft password and fingerprint authentication. Additionally, using GSM technology as a low-cost alternative to the current process to send alarm messages about a home locker that will be more secure than others [3].

This endeavour aims to protect vehicles against unauthorised use and theft. The vehicle's biometric fingerprint security technology allows only authorised people to start it. It shields the automobile. The usage of security systems is growing and is being demanded more and more everywhere. In companies, buildings, and schools, biometrics like fingerprints are often used. The security of vehicles is a focus of this project, which led to the creation of an automobile anti-theft system utilising the ATmega328. An in-vehicle fingerprint sensor is utilised to find the fingerprint. Utilising the pre-assigned data, the fingerprint sensor data reading from the ATmega328 is examined. When the individual is identified as the owner of the vehicle or another authorised fingerprint user with authority over the vehicle, the ignition system for the engine fires up. The engine won't start if there is an intrusion. While other security systems are vulnerable to hacking, this one uses a fingerprint as the key since each person's fingerprint is unique, increasing security. The ignition of the automobile was also controlled by an RFID sensor. In the event that the fingerprint sensor malfunctions, the RFID tag may still be scanned to start the vehicle. This code will be kept in his or her RFID tag in case the fingerprint sensor malfunctions [4].

Identity identification is often carried out by traditional authentication methods using user information verification (such as inputting a password) or biometric data (such as fingerprints). However, using only these authentication techniques poses security problems. It may be difficult, for instance, to tell if a user is genuine if the password has been hacked. It confirms the user's password first, and then locates the biometric traits of the authorised user. As a result of the coupling effect between tags, any modification to a tag signal brought on by a user's touch will also alter other tag signals simultaneously. Since each user's fingertip impedance varies, each contact will result in various alterations to the tag signal. The tag array will thereby enable unique user identification by integrating biometric data. With an average recognition rate of 93.8%, the evaluation's findings demonstrate that RF-Ubia delivers high authentication performance. The coupling effect causes the signals of the other eight tags to change when a tag is touched, in addition to changing the signal of the touched tag. The body impedance of the user is closely associated with these signal variations. The average impedance of a human body is between 300 and 1000. There are variations in the body impedance of various users, which affects how the phase signal of the tags fluctuates. When combined with user biometric data, it is possible to identify between distinct users who submitted the same password [5].

When we are away from our family, security is a vital concern shared by everybody. The aforesaid problem still hasn't found an appropriate solution as of right now. An electronic security system that uses Arduino as the preparation unit is presented here. Microcontroller board Arduino, which is part of the Uber family, is used there. The instrument is simple and open source. It can filter, store, and operate applications as well as detect them. Using an Arduino Mega 2560 board, the entrance's access control is completed. Using a predetermined PICTURE secret key and OTP, this exercise illustrates a keyless architecture for locking and opening purposes. By delivering an OTP and a picture password to the administrator, who must be contacted in order to receive them, access is prevented by unauthorised individuals. The 2.8" TFT touch screen, which displays all UI messages and accepts user inputs, is used to enter the information. When a user is authorised, the system uses a fingerprint sensor to verify their identity before sending an OTP or PICTURE password to the user's registered cell phone number stored in the database (local SD card) via SIM using a GSM module. This lets them to open the door. When a password is entered, the door will automatically open if it matches. If not, a notice indicating an erroneous password will appear on the TFT display, and a warning to the owner that a security breach attempt was made. With readily accessible components, this hardware project offers three layers of protection while using less electricity. Three degrees of protection are available in our fingerprint lock system, and any two of the levels may be used to unlock the system by the user. This creates a high level of protection where, on the first try itself, the admin receives notification if someone attempting to unlock without authorization. The system uses OTP, or one-time password, image password, and fingerprint authentication. This door locking method is different from others. Out of three levels of security, the system processes two levels of security. With the aid of the admin, a visitor must navigate two levels of security in this system. To access the gadget via a mobile phone or the internet, the market's current approach includes IOT, pin, and fingerprint authentication. In certain devices, the system is unlocked by creating an OTP through GSM (the worldwide standard for mobile), which is then used to modify the password rather than a set password. If the system has a set password, a hacker or other unauthorised individual may open it using different attacks such as brute force attacks. A duplicate fingerprint imprint may be created in the fingerprint module, which is a security risk for fingerprint technology. When a person isn't paying attention to their surroundings, a pin or password-based security lock may be assaulted via brute force or live monitored [6].

The use of ATMs to withdraw cash has grown in the modern world. In addition, there have been more instances of theft and robbery, which highlights the need for more secure ATMs with added security measures. The goal of this effort is to create a security-based smart ATM with access controlled by fingerprint and RFID technology. The user's RFID number and fingerprint information are collected, and then the recognised card number, authorisation status, and access location are sent to be verified with database information. The appropriate account holder receives a message indicating whether or not the authorisation is legitimate once the information has been verified using the database details that have been obtained. The account holder is also alerted of the access's location, time, and date. By installing vibration and flame sensors that instantly alert in case of fire and breaking, this also improves security. In order to establish total security, a camera within the machine records the user's face as well as the time and date of the access, which may be used as evidence in the event of a suspicion [7].

On standard doors, locks that may be opened with a separate key may be placed. This approach may be replaced by another, such as the lock's password or pattern system, both of which have the potential to be broken and unlock the lock. A door lock and biometric combination might thus be a fix for these problems. Biometric verification is any method that assesses a person's identification by one or more unique biological traits. In addition to fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures are further distinguishing characteristics. The security risk of unauthorised people entering into our homes, stores, workplaces, etc. may be significantly reduced by using a fingerprint as the key to door locks since duplicating such a key is impossible. Due to the fact that each person's fingerprints are unique, we shall utilise them in this case for biometric verification. Furthermore, if this system is used in lieu of traditional locks, key loss problems won't arise since we won't need to carry keys about with us. So, using the Arduino platform, we will try to build the system with characteristics that will increase the level of security [8].

When used in a variety of fields, including manufacturing, healthcare, agriculture, and more, radio frequency identification (RFID) technologies have achieved notable success. RFID technology uses passive or active tags with the appropriate scanners to make automated item detection and tracking simpler. the development of electronic learning paradigms in comparison to conventional methods and the accessibility of nearly all material through the information superhighway (Internet). Due to its many advantages, RFID-based applications have grown in popularity in recent years. In this project, a student database system using RFID and FINGERPRINT technology has been created. It contains student papers that may activate, authenticate, and verify the user. This article presented an RFID-based student information system that would let students access and retrieve their data via RFID cards and fingerprints. Since its present cheap cost and developments in other computer domains that expand its potential application areas, RFID is not technically a new technology; it has just lately attracted increased attention. RFID is a smart system that combines radio frequency and microchip technology that may be used to identify, monitor, secure, and inventory objects. At its most basic, RFID systems employ small chips called "tags" that broadcast identifying data to an RFID reader, a device that can communicate with computers [9].

The development of precise positioning systems and Internet of Things technologies, which have already made it possible for site-specific applications, resource management that is sustainable, and linked gear, are what are driving the growth of smart farming. Farm-internal connectivity of agricultural tools and equipment is now made possible by so-called Farm Management Information Systems (FMISs), which also make it possible to coordinate cooperative agricultural activities and share field data. During the course of a job, machine data is often immediately recorded. Additionally, the connectivity between farms, agricultural contractors, and market centres facilitates cooperation. However, user authentication is a specific weakness of contemporary FMISs in terms of security. In this article, we offer a security architecture for a decentralised, open-source FMIS that is not tied to any one manufacturer. The continuous user authentication based on Radio Frequency Identification (RFID) is given particular focus since it significantly enhances the security and authority of automated documentation while still maintaining usability in the real world. In this article, we propose a thorough authorization framework that assures data sovereignty together with a security architecture for the ODiL platform that covers private communication between individual actors. We provide an easy-to-use RFID-based method for the necessary hardware initialization of the various platform components. Additionally, using ODiL's FMIS as an example, we provide a practical and affordable method for continuous RFID-based user identification that is exemplarily tested to authenticate users on agricultural equipment and significantly aids traceability inside FMISs 10].

DOI: 10.17148/IJARCCE.2023.12647

IoT development has spread to a number of industries. IoT device production is expected to reach 75 billion units by 2025 if it keeps growing. Security advancements do not, however, follow the proliferation of IoT devices. As a result, IoT devices might turn into entry points for cyberattacks including brute force and sniffer attempts. To prevent assaults, authentication measures might be utilised. It is difficult to install authentication procedures for IoT devices, nevertheless. Constraint devices with little computational power are up the majority of IoT devices. Therefore, using traditional authentication methods is not recommended. RFID and fingerprint two-factor authentication may be a way to provide an authentication method. An RFID and fingerprint two factor authentication system has been suggested in earlier investigations. Previous studies, however, did not consider message exchange security concerns or provide mutual authentication. This study suggests a MQTT-based secure mutual authentication system that uses two-factor RFID and fingerprint authentication. The registration procedure and authentication are the two steps that help the authentication process. The suggested protocol is put to the test using biometric security by calculating the fingerprint's false acceptance rate (FAR) and false rejection rate (FRR), as well as brute force and sniffer attacks. At the 80% threshold, the test results produced the best FAR and FRR. In addition, this study suggested employing RFID and fingerprints in tandem with two-factor authentication to carry out safe mutual authentication—RFID serving as the first factor and fingerprint serving as the second. The three steps of handshaking, proving, and verifying are used to accomplish reciprocal authentication. Requests for the verifier to start the authentication process are made during the handshaking phase. The proofreading phase is used to assess the legitimacy of the customer. The verifying step is also used to confirm that the client is in communication with an authorised verifier. Additionally, the fingerprint is evaluated to determine the user verification threshold. The security was tested via a brute force attack by sending out random characteristics. The sniffing attack was then carried out to assess the communication transmitted across the network [11].

Several illegal activities are seen by the traffic authorities when they go through the documentation. The crime will be committed by both the people and the police. To assist in resolving this problem, the traffic police are given a second portable fingerprint sensor module. The licencing data is stored on the internet of things, which is connected to this module. If the person places their finger on the sensor, the device will let you know whether or not they have a licence. This is made feasible by linking the IOT with the data from the car. The bulk of the suggested system is made up of the IOT, fingerprint sensor, RFID, Arduino UNO board, LCD display, buzzer, and power supply. The vehicle's number, registered owner's name, insurance policy number, licence number, expiry date, and information from the government's RC BOOK are all recorded by a clever reader that is installed. The information gathering through IOT is subsequently sent to the government. The server has easy access to the database. This concept allows for efficient traffic management. Since the fingerprint sensor is used to identify a specific person's licence, the traffic police can simply find a person regardless of whether they have a licence. The information above is connected to the IOT [12].

Building a complex voting system is difficult since there are so many requirements that must be met. The privacy of a poll should be protected. It should not be made public which candidate earned a certain vote via the voting process. The researchers in this study employed an authenticated voting machine in the college elections to simplify the process and boost transparency. The concept has to be developed further in order to become stable and conceptually sound. To provide safety, the model uses radiofrequency recognition and fingerprint recognition. The major components of the automated voting machine that is the focus of this research are the two-one AVM unit and an extra User Interface (UI). The Internet of Things (IoT) components that make up AVM, which are assembled on a breadboard and run Python programmes, include an Arduino Mega Board, a fingerprint scanner, an RFID reader, a WiFi interface, a buzzer, a tiny LCD display, and momentary push buttons [13].

II. METHODOLOGY

A. Biometric and rfid based authentication using IoT Technology:

The main block diagram of the system is shown in Fig. 1. The whole system is composed of an RFID reader, fingerprint scanner, RF transceiver, display, electric lock, and WiFi transceiver. A signal is delivered to an RFID tag when it is positioned near to an RFID reader. It is recognised by the tag when it gets it, and it then returns the signal reader. The microcontroller should obtain the reader since it is an electronic device. Using a 12 V DC motor, the lock's integrated mechanism is unlocked. A motor drive is utilised because the microcontroller's output voltage is too low and inadequate to power a motor. A Piezo Electric Plate is used to send a warning to the board if someone tries to open the box. The controller receives the user's information once the fingerprint sensor reads it. The controller compares the data to data that has been stored [1]. For instance, in a farm network, a company's whole resource base—including its machinery, personnel, and warehouses—is connected to a farm server. All farm-internal data management duties are managed by these servers, which are referred to as Home Nodes (HNs) in the context of ODiL, and they provide an API for Representational State Transfer (REST) communication.

DOI: 10.17148/IJARCCE.2023.12647

They use encryption and strict access restrictions to turn connected resources into a "Trusted Data Space" (TDS); see Fig 2. Different user groups may also gather, evaluate, visualise, and (knowingly) share farm data with other users or ODiL actors via a Graphical User Interface (GUI) [6] [10][11].

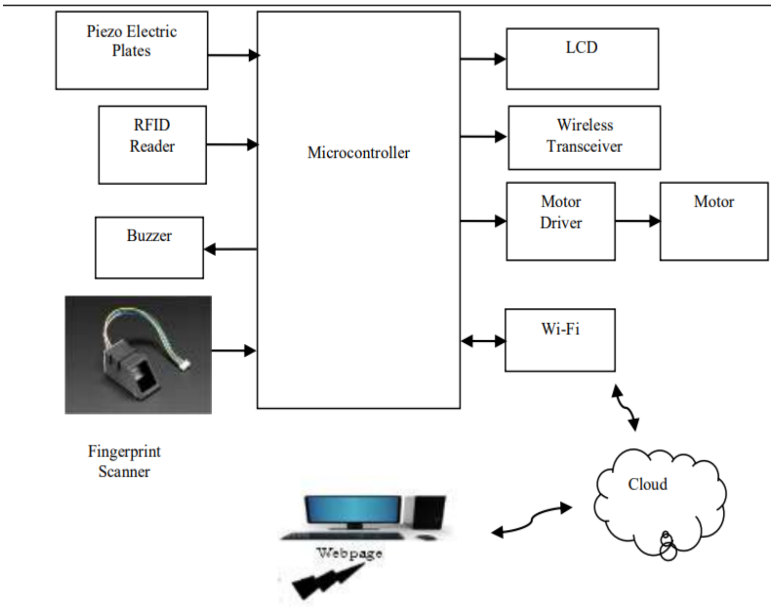


Fig. 1: Block diagram of the proposed system [1]

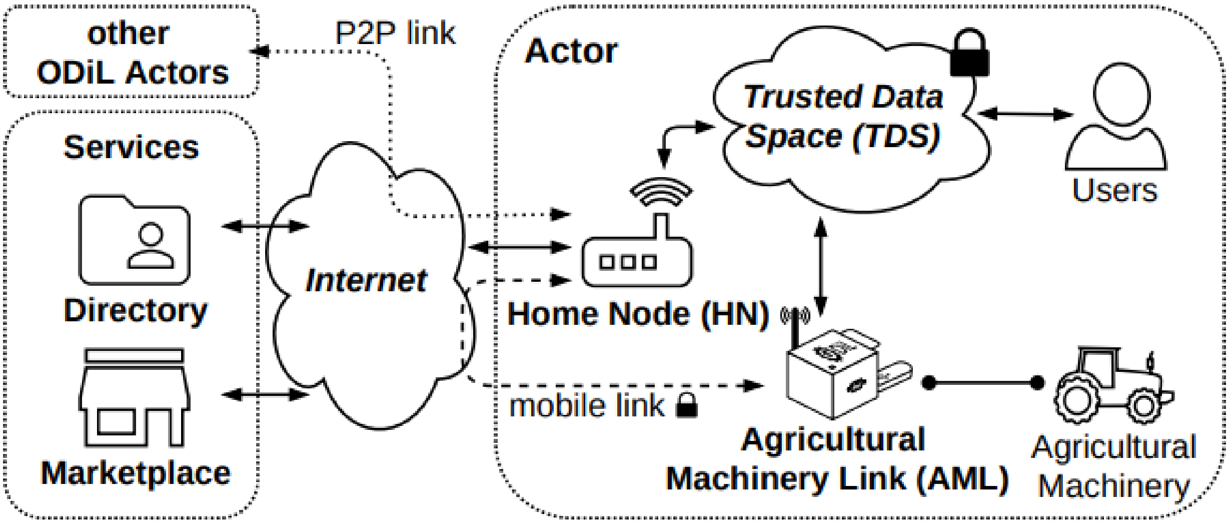


Fig. 2: Overview on the overall ODiL framework [10]

B. Authentication based on GSM using Arduino:

As illustrated in Fig 3, the created RFID-based security system proposed in this research uses a two-factor (tag and pin code) authentication method. The intended circuit's current threshold led to the selection of IN4001 diodes for D1 through D6, and a 167 resistance for the 12V relay coil. Aluminium with measurements of (50 cm x 30 cm) was used to construct the experimental security door system. A hard board served as the structure's covering. It was possible to identify the different parts used in the circuit construction [2-3]. All of the security flaws in the current system are fixed by the proposed method, which offers excellent security and productivity. The bother of a lost or stolen key or an unauthorised access may be avoided with this ideal and flawless solution. The locking system's three level security, which requires the user to unlock the system by passing through any two levels of protection, is its key benefit.

DOI: 10.17148/IJARCCE.2023.12647

This method solves the issues that the current systems had. The proposed method is used to give great security to homes, offices, stores, etc. since, as was already said, every password generated by the existing system may be cracked [6][8][12].

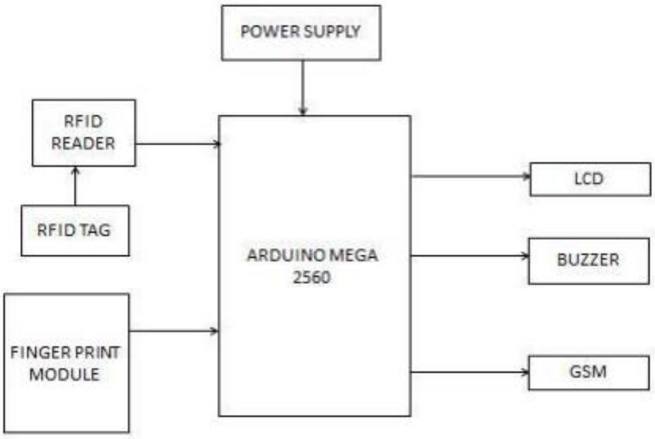


Fig. 3: Block diagram based on GSM using Arduino [3]

C. Authentication based on Machine Learning:

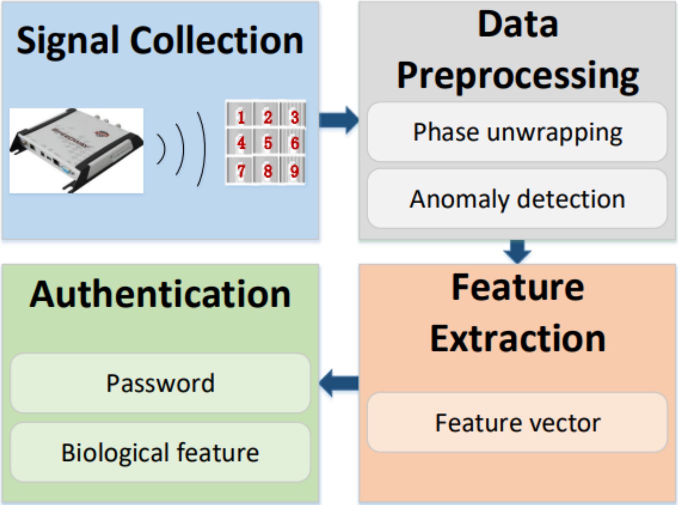


Fig. 4: Working of RF-Ubia system

The technology makes use of passive tags, which don't have their own power source and get their working electricity by reflecting the carrier signals that the reader emits. An antenna and a chip are the two main components of an RF tag. The antenna's primary jobs are to receive the radio frequency signal that the reader emits, transfer it to the chip for processing, and then communicate the chip data back to the reader. The antenna is a conductor structure made specifically for coupling electromagnetic radiation that is emitted. The operational efficiency and radiation impedance of an antenna often decrease with decreasing size. In this section, we provide a quick overview of the four processes involved in putting the RF-Ubia system into practise. Hardware Configurations. We must first organise nine RFID tags into a 3x3 arrangement in order to implement RF-Ubia's password function. The tag array is then fixed to stop signal alterations brought on by the relative mobility of the tags from impacting the outcomes of user authentication. Identification of the tag. The reader first transmits a signal to activate each of the nine tags in the array before doing a preliminary identification using the EPC of the tag. Once the reader has the signal from a valid tag, it waits for the user to touch the appropriate tag before collecting the signal data. Processing data. The goal of this stage is to process the tag data that the reader has obtained in order to get rid of the periodic signal surround and inverted phenomena (also known as phase unwrapping). Then, we extract the necessary characteristic data and determine the user's password sequence. User identification. The system initially assesses whether the detected password sequence is a legitimate password. The second round of verification will take place if the user's password sequence is really recorded in the system. The system checks the user's legitimacy in the second step to stop an unauthorised attacker from obtaining the password sequences of authorised users [5].

DOI: 10.17148/IJARCCE.2023.12647

D. Passive Authentication with Database Management systems:

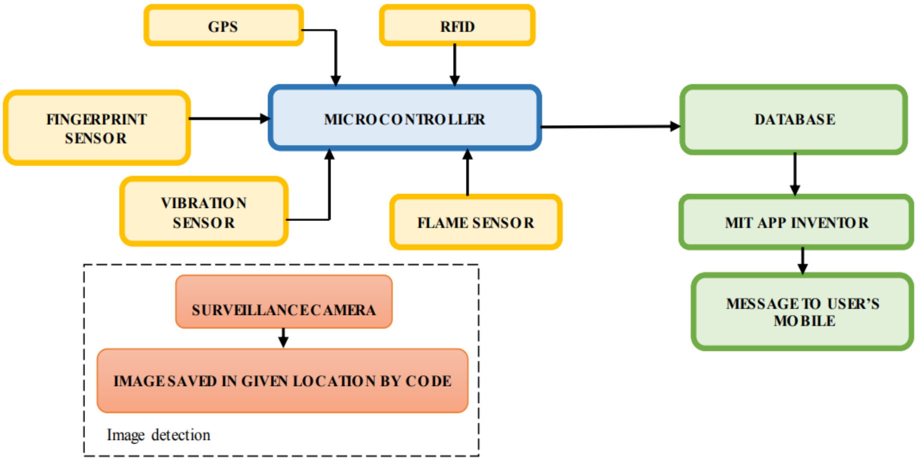


Fig. 5: Block diagram of the Passive Authentication with Database management system [4].

First, 230V AC power is provided to the step-up transformer, a 0-12V transformer. The step-up transformer lowers the output current so that the input and output power of the system stay equal. The LCD display then displays the ignition system for the car. There has been use of the UP/DOWN, ENROL, D/T, and OK buttons. These four buttons [4] allow us to store and delete fingerprints. The proposed system is a microcontroller-based ATM that replaces conventional cards with RFID cards that include the card number of the user. Instead of using a PIN, the user's fingerprint is used for authorization. As a result, when a user approaches an ATM, the RFID scanner scans his or her card, and the system waits for a genuine fingerprint from a matching card. The phone number connected to the card will get a message saying "The access is granted" if the ATM's fingerprint sensor recognises a valid fingerprint. However, if the wrong fingerprint is discovered, the connected card's user will get a message that says, "Access not authorised! There has been an attempt to access this card. The cardholder also learns if the access was approved as well as the time, date, and location of the access. A camera is used to take pictures of the people within the ATM and save them in a database, limiting the storage of extraneous video feed and aiding the appropriate bank and the cardholder in the case of ATM theft. The recommended system sends a message with the ATM's GPS position to the fire station, alerting them immediately to an ATM fire. Additionally, the system immediately alerts the police station to any ATM break-in attempts and provides them with a message that includes the ATM's essential GPS location. Thus, the recommended solution includes a number of crucial components that help the bank and maintain ATM security. [7]. The author has maintained a student database including student papers. The 28-pin dual inline package microcontroller ATMEGA 328P is connected to the PC via a Serial to USB converter module. All that is required of an authorised user to read a document is for them to scan their RFID tag with the RFID scanner module that is connected to the microcontroller. In order to operate a database system employing RFID and fingerprint technologies, students have built a microcontroller that first confirms the user's authorization. If the user is approved, they will have access to any information that is similar to what the students provided in the data. We now provide a fingerprint module for further security and authentication. With the help of the fingerprint module, an authorised user may access his information from the database kept on the computer. When an RFID or fingerprint scanner scans the tag, the buzzer activates [9].

III. RESULTS & DISCUSSIONS

A. Biometric and RFID based authentication using IoT Technology:

When an RFID tag is placed close to an RFID reader, a signal is sent to the tag. When the tag receives it, it recognises it and sends the signal reader back. The reader is electronic, and The microcontroller should get it. To unlock the lock embedded mechanism, a 12 V DC motor is employed. Since the microcontroller's output voltage is very low and insufficient to operate a motor, a motor drive is used. When somebody attempts to open the box, a Piezo Electric Plate is utilised to transmit a warning to the board. The fingerprint sensor reads the user's data and transmits it to the controller. The data is compared by the controller to information that has been saved. A wireless transceiver will provide the precise position of the item, however GPS will only give the latitude and longitude of a certain border region. When it comes to security, if someone scans the incorrect RFID tag or fingerprint, the system will notify the user through a cloud interface. [1].

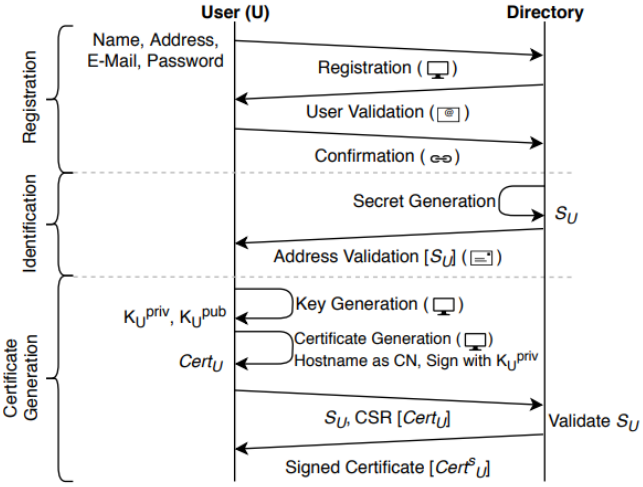


Fig. 6: Authentication and Account creation process [1].

The overall architecture for a decentralised, open service delivery system in agricultural situations has been outlined in this article, with a focus on security and data sovereignty utilising well-established technologies. Using certificates issued by a PKI incorporated into the systems service architecture, TLS is used to encrypt communication channels both worldwide and inside the autonomous, self-sufficient actor networks. OAuth2 is also utilised to provide a user-friendly RAC mechanism for devices and users. The user authentication on agricultural equipment is given particular attention since it hasn't been incorporated in the FMIS systems and machine terminals that are currently in use. Due to the unique requirements in the provided situation, an HF RFID-based solution was chosen, prototypically developed, and tested in field testing after comparing and assessing several alternative processes. This system guarantees use while significantly enhancing security and enabling traceability in agricultural practise [10]. Data and communications may be kept safe with the use of a secure authentication system. However, it might be difficult to install authentication procedures for IoT devices. Constraint devices with restricted computational power dominate the IoT device market. Conventional authentication mechanisms become inappropriate for usage. In order to provide an authentication method for IoT constrained devices, two-factor authentication combining RFID and fingerprint may be a solution. A two-factor authentication system employing RFID and fingerprint has been suggested in earlier investigations. But prior study did not take into account security as a whole. Data transmission security on networks was not a focus of earlier study. Furthermore, no mutual authentication method was offered in earlier experiments. In this paper, a secure mutual authentication system utilising RFID with two-factor authentication and MQTT fingerprinting is proposed. The registration procedure and authentication work in tandem to facilitate the authentication process. From the client to the authentication server, RFID and fingerprint data are securely registered throughout the registration procedure. The next step in the authentication process is to securely verify the client's RFID and fingerprint data [11].

B. Authentication based on GSM using Arduino:

The next step was to evaluate the system's performance once the system had been fully developed. The test was run to verify the created system's operational performance. According to what was seen, the experimental findings varied somewhat from the theoretical values; these changes are ascribed to either the instrument's low battery and percentage error, which cannot be completely removed, or both [2]. The created system is evaluated and put into use in our lab as an Advance Alert Home Locker safety and security system employing FINGERPRINT, SOFT PASSWORD, and GSM. We also discovered that the systems function well. The systems have cutting-edge capabilities, such as standalone, portable, and reasonably priced systems [3]. The security concerns in the current scenario may be resolved by the suggested solution. The system's three levels of protection may aid the user in getting precise security. The primary goal of the suggested system is to safeguard the user's home, workplace, or area where they store their valuables and papers. As a result, individuals can understand this initiative and carry out future work [6]. In this essay, we attempt to address the issue of door security by integrating the idea of biometrics with the door lock. Therefore, to achieve that goal, a device to lock or unlock a door is implemented utilising finger prints as a special key. We have explained the various Arduino components that we would need to construct our project, and we have provided the necessary hardware and software [8]. The RFID Reader portion and the Fingerprint sensor section each make up one element of the project. The RFID reader part was operational. When the RFID tag is installed on the car, we can readily identify the information of the vehicles, such as RC BOOK, Pollution Certificate, and Insurance, with the use of an RFID reader. Using this strategy, the burden of those who are carrying the papers with them is finally lightened. It also increases the nation's digitalization while reducing corruption [12].

DOI: 10.17148/IJARCCE.2023.12647

C. Authentication based on Machine Learning:

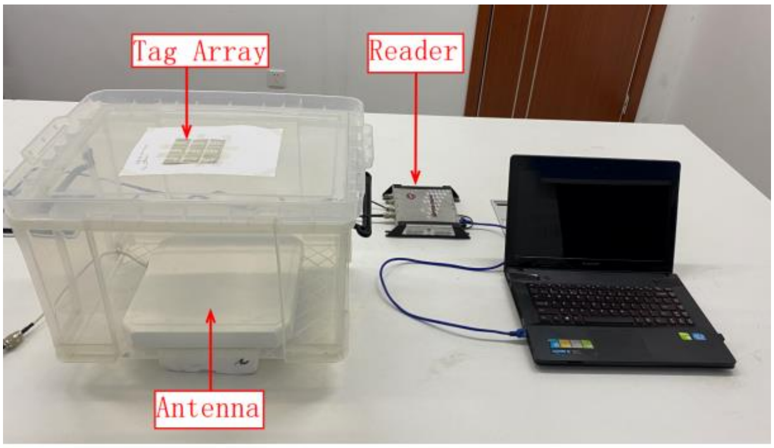
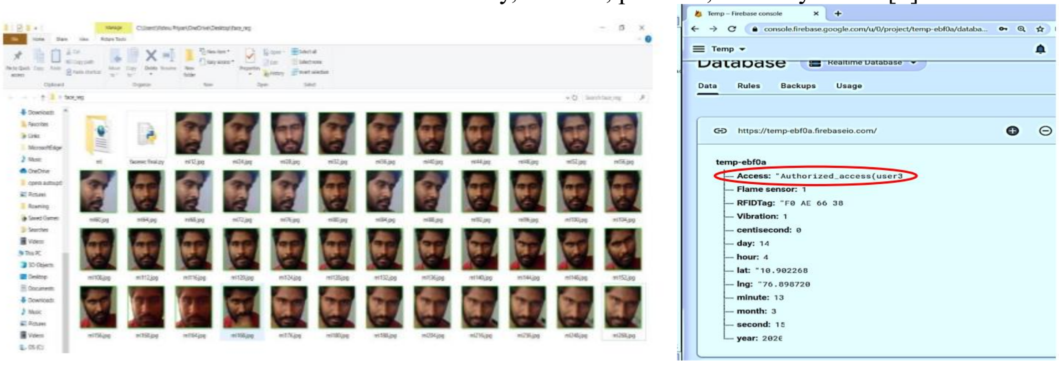


Fig. 7: Working Environment of RF-Ubia System [5]

The recommended user authentication approach combines user information with biometric data to provide good user identification accuracy even when just a simple password is employed. Even so, there are certain drawbacks. For instance, we still need to use passwords, which is inconvenient for people who often forget them, such as the elderly with poor memory and those who do not regularly use the authentication system. We must also test several experimental scenarios in order to strengthen the system's resilience. Our tests revealed that RFID signals are sensitive to dynamic environmental changes (such as a person moving), but since the typical bandwidth of typical human finger movements is between 3 and 5 Hz, it is possible to counteract these effects by using low-pass filters (like Butterworth filters). Other normal human movements fall within a 0–18 Hz frequency range. We might use state-of-the-art signal processing techniques (such empirical pattern decomposition) to filter out noise with overlapping frequencies [5].

D. Passive Authentication with Database Management systems:

This paper's main emphasis is on sensor-assisted vehicle ignition, which will be useful to users in a number of contexts. Real and registered users may be verified via the usage of fingerprint sensors. The car's ignition was also controlled by an RFID sensor. The RFID tag may be used to start the automobile by just scanning it if the fingerprint sensor stops working. This code will be kept in the RFID tag he or she is wearing in the event that the fingerprint sensor malfunctions. Automotive Fingerprint Sensor for Ignition The safety and portability of the present version of this framework might be improved with a number of additions or functions. The system won't let the user start the car if the registered user's finger is damaged, coloured, or defiled. In our suggestion, the project is divided into two modules, one of which has an LCD crystal display that shows and displays the value and the other of which has a fingerprint sensor that receives input from the user side [4]. A signal processing method for photographing the face of the person entering the ATM is utilised to keep track of them. The CCTV picture stored within the ATM requires extra storage capacity. Python was used to monitor the photos of the faces of different ATM users in order to save storage space. The ATM's built-in camera keeps tabs on everyone using it. The Python "OpenCV" package is used to do this. based on Haar features The object identification technique in the code used to identify items in an image or a video employs a cascade classifier. When the programme is run, the camera looks for faces using the classifier and the facial attributes. The face is reversed, altered, and highlighted after it has been identified. The face is outlined in a rectangular box and added to the database [7]. Through the "Student database system using RFID and fingerprint module" project, it was discovered that RFID base tracking produces a cost-effective and accurate solution that is hardware that is tiny, flexible, portable, and easy to use [9].



```
https://temp-ebf0a.firebaseio.com/

temp-ebf0a
├─ Access: "Authorized_access(user3
├─ Flame sensor: 1
├─ RFIDTag: "F0 AE 66 38
├─ Vibration: 1
├─ centisecond: 0
├─ day: 14
├─ hour: 4
├─ lat: "10.902268
├─ lng: "76.898720
├─ minute: 13
├─ month: 3
├─ second: 15
└─ year: 202€
```

Fig. 8: Database of users accessing the ATM [7]

TABLE I. COMPARISON OF METHODOLOGIES BASED ON VARIOUS PARAMETERS.

Citation Number	Methodology (Dataset/Realtime)	Advantages	Disadvantages	Accuracy	Error
1	RT	Better Security, Remote Monitoring	Power consumption is high, Incurring GSM costs	68%	32%
2	RT	RFID along with LCD interfaced with Arduino for better performance.	Delay increased as the microcontroller is old, slow processing. This work doesn't have any alerting features, No cloud interface.	70%	30%
3	RT	State-of-Art board Raspberry Pi is utilised to reduce delay and increase efficiency.	Power consumption is high and not regulated as the system is on at all times.	75%	25%
4	RT	Arduino is used to accomplish the task.	Better board could be used. Also, lacks alerting features with on-site monitoring only. Doesn't support Remote Monitoring.	60%	40%
5	DT	ML utilised to monitor the proposed work. Low-cost features along with utilization of Random Forest Classifier in Weka.	Requires a PC at all times, Bulky design and increased power consumption.	92%	8%
6	RT	More features covered under a single work.	Load on the low-cost Arduino board increased, delay increased, hence the feasibility of the work reduced in real-time.	60%	40%
7	RT	More sensors, along with Geotagging enabled in this work.	Not feasible as the board "ESP8266" increase delay. Unceratainity of the work exists as the model is dependent of internet for functioning. Also, it doesn't contain an inbuilt camera and requires the PC to be used externally.	70%	30%
8	RT	Door unlocks via biometric enable din this work.	This system doesn't work at all conditions, during rainy weather. If the fingerprint entered has dust particles, then the system is redundant and not preferred. Also Arduino increases delay in computation.	70%	30%
9	RT	RFID based data authentication and data collection	Data isn't secured in the DBMS, no alerting system utilised incase of break-in to the Database Management systems.	60%	40%
10	RT	State-of-art work done with usage of IoT in Smart Farming.	Increased cost with increase in power consumption. Complexity of the system is high and requires more time and effort to debug during any faults.	80%	20%
11	RT	Two Factor Authentication using RFID & Fingerprint achieved along with tests for Sniffing and cyber-attacks.	Cost to keep the system on at all times increases, not feasible as the system is required to be turned on only during usage. Additional cost add with WiFi. High Complexity.	80%	20%
12	RT	Two Factor Authentication Achieved using Arduino.	Increased delay to process the data, no interface to cloud reducing the usage and data security. No protocols used for alerting the owner of the vehicle of data breach.	82%	18%
13	RT	Cloud interface for alerts has been achieved for Electoral Voting systems.	Two separate boards have been used to accomplish the tasks adding to the cost. For a voting system, RFID isn't required as it requires for all to use an RFID card at all times for voting, high incurred cost along with delay increased as the data processing takes place on Arduino.	80%	20%

IV. CONCLUSION

The primary goal of this study is to examine previous studies that have used different techniques and boards for data collecting and processing in the areas of RFID and biometric identification. In the twenty-first century, the usage of biometric-based technology has increased exponentially. This is as a result of the enormous advancements made in this area, which enabled them to reduce their pricing. Biometrics is swiftly becoming into a cutting-edge security system technique. For important operating systems like ATMs, mobile phones, cars, laptop computers, workplaces, and other things that need authorised access, biometrics are employed to offer secure access. Nowadays, strong levels of security are required for safety reasons in homes, businesses, stores, and banks. An introduction of a smart lock system is made to give security for these fields. To lock and unlock the system, several cutting-edge smart door locks have been developed. These have a fingerprint reader, RFID card, pin, password, or IOT that requires a mobile phone to open the system. These systems have similar benefits and drawbacks, and this category of security locks has any given degree of security that may be used to open the system. These locking systems require the user to unlock the device with a pin number, fingerprint, or RFID card.

Physical attacks on IoT devices are the most common. Future research will examine whether cloning constitutes a direct physical attack. Additionally, methods for producing a sufficient and secure random number will be investigated, including the use of a physical unclonable function (PUF). From this review research, it can be inferred that using appropriate micro-controllers is essential to assist and make up for the delay in signal processing, and that having effective methods of communication to notify staff is crucial to avoiding risks in daily life. Instead of only serving as a convenience for later use, biometrics are intended to be tested and utilised in real time. Additionally, biometric data security is crucial in order to guarantee that customer data is always treated with the utmost confidentiality and privacy.

REFERENCES

[1]. Roseela, Ann & Godhavari, T.. (2020). Biometric and RFID based authentication system for exam paper leakages detection using IoT technology. Indonesian Journal of Electrical Engineering and Computer Science. 20. 1271. http://doi.org/10.11591/ijeecs.v20.i3.pp1271-1277

[2]. Emakpor, S., & Esekhaigbe , E. (2020). Development of an RFID-based security door system . Journal of Electrical, Control and Technological Research, 1, 9 - 16. https://doi.org/10.37121/jectr.vol1.112

DOI: 10.17148/IJARCCE.2023.12647

[3]. Leekongxue, Sialee & Li, Li & Page, Tomas. (2020). Smart Door Monitoring and Locking System using SIM900 GSM Shield and Arduino UNO. International Journal of Engineering Research and. V9. https://doi.org/10.17577/IJERTV9IS040011

[4]. Sawant, N., Sutar, S., & Ghumare, G. (2021). FINGERPRINT BASED CAR IGNITION SYSTEM USING ARDUINO AND RFID. https://doi.org/10.51319/2456-0774.2021.5.0048

[5]. Huang, Y.; Fu, B.; Peng, N.; Ba, Y.; Liu, X.; Zhang, S. RFID Authentication System Based on User Biometric Information. Appl. Sci. 2022, 12, 12865. https://doi.org/ 10.3390/app122412865

[6]. N. Meenakshi, M. Monish, K. J. Dikshit and S. Bharath, "Arduino Based Smart Fingerprint Authentication System," 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, 2019, pp. 1-7, https://doi.org/10.1109/ICIICT1.2019.8741459

[7]. S. Gokul, S. Kukan, K. Meenakshi, S. S. V. Priyan, J. R. Gini and M. E. Harikumar, "Biometric Based Smart ATM Using RFID," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 406-411, https://doi.org/10.1109/ICSSIT48917.2020.9214287

[8]. Sarma, M., Gogoi, A., Saikia, R., & Bora, D. J. (2020). Fingerprint based door access system using Arduino. Int. J. Sci. Res. Eng. Manage.(IJSREM), 4(8), 1-5.

[9]. Shaikh, A. R., Sahane, D. S., & Wagh, P. V. (2020). RFID and FINGERPRINT based Students Database System, IRJET.

[10]. A. Bothe, J. Bauer and N. Aschenbruck, "RFID-assisted Continuous User Authentication for IoT-based Smart Farming," 2019 IEEE International Conference on RFID Technology and Applications (RFID-TA), Pisa, Italy, 2019, pp. 505-510, https://doi.org/10.1109/RFID-TA.2019.8892140

[11]. R. R. Pahlevi, V. Suryani, H. H. Nuha and R. Yasirandi, "Secure Two-Factor Authentication for IoT Device," 2022 10th International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 2022, pp. 407-412, https://doi.org/10.1109/ICoICT55009.2022.9914866

[12]. S. Prema, M. R. V. S. Deen, M. V. P. Krishna and S. Praveen, "Vehicle And License Authentication Using Finger Print," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 737-740, https://doi.org/10.1109/ICACCS.2019.8728402

[13]. Poornima, K. G., Rajeshwari, M., & Prasad, K. K. (2020, December). Arduino Based Authenticated Voting Machine (AVM) using RFID and Fingerprint for the Student Elections. In Journal of Physics: Conference Series (Vol. 1712, No. 1, p. 012004). IOP Publishing.

[14]. S. S. Tippannavar, V. Mishra, Y. S D, R. R. Gowda, S. H R and A. M, "Smart Transformer - An Analysis of Recent Technologies for Monitoring Transformer," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-11, https://doi.org/10.1109/ICRTEC56977.2023.10111875

[15]. S. S. Tippannavar, Y. S. D, C. M. B. N and P. K. M. S, "IoT enabled Smart Car with V2X Enhanced Comunication and Safety Alert system," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-5, https://doi.org/10.1109/ICRTEC56977.2023.10111919

[16]. S. S. Tippannavar, S. N and Y. S. D, "Smart Gloves — A tool to assist Individuals with Hearing difficulties," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-5, https://doi.org/10.1109/ICRTEC56977.2023.10111927

[17]. S. S. Tippannavar, M. P. M. Sudan, R. M. Sudan, V. S. Athreya and S. D. Yashwanth, "SISR - Smart Indoor Surveillance Robot using IoT for day to day usage," 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, 2022, pp. 01-05, https://doi.org/10.1109/ICERECT56837.2022.10059670

[18]. S. S. Tippannavar, S. B. Rudraswamy, S. Gayathri, S. P. Kulkarni, A. Thyagaraja Murthy and S. D. Yashwanth, "Smart Car - One stop for all Automobile needs," 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2022, pp. 54-59, https://doi.org/10.1109/ICCCIS56430.2022.10037715

[19]. Sanjay S Tippannavar, Yashwanth S D. Madhu Sudan M P (2023). Design,Modelling and Optimization of an electric Vehicle (EV) and comparison of performance for different drive cycles using MATLAB & SIMULINK. IJIRAE, Volume 10, Issue 03 of 2023 pages 58-66 https://doi.org/10.26562/ijirae.2023.v1003.03

[20]. Sanjay S Tippannavar, Yashwanth, Rishitha, Mohammed, Pilimgole (2023). OAOF-Obstacle Avoidance using Optical Flow Algorithm for Unmanned Aerial Vehicles. International Journal of Innovative Research in Advanced Engineering, Volume 10, Issue 02 of 2023 pages 33-39 https://doi.org/10.26562/ijirae.2023.v1002.04

[21]. Sanjay S Tippannavar, Shashank Gowda, Gayathri S (2023). Analog Data Logger for Remote Monitoring of Control Systems. IJARCCE. 12. 1103-1115. https://doi.org/10.17148/IJARCCE.2023.124191