OTP-Based Smart Door Opening System

P. Srinivasan, R. S. Sabeenian, B. Thiyaneswaran, M. Swathi, and G. Dineshkumar

Abstract The idea of this project is to improve the security performance in houses and safe places by using Arduino and GSM. In this project, we are going to make an OTP-based door opening system using Arduino and GSM. The method we have developed will generate a one-time password that helps you unlock the door. This method will enhance the security level further, which is much safer than the traditional key-based system. In the traditional key-based system, we used to face the problem of what to do if I miss the key somewhere or what to do if the key gets stolen. We do not have to worry about it since the password is automatically generated on your mobile phone and you can enter it and unlock the door.

Keywords Arduino · Global system for mobile communication · Liquid crystal display · One-time password · Servomotor · Door opening and closing · Key panel

1 Introduction

Arduino Microcontrollers are bound to play an undeniably significant part in altering different enterprises and affecting our everyday lives more firmly than one can envision. Since its development in the mid-1980s, the microcontroller has been perceived as a broadly useful structural block for computerized frameworks. It is being discovered utilizing different regions, beginning from basic kids' toys to exceptionally complex rockets. Due to its flexibility and many benefits, the application area has spread in every possible way, making it universal. As an outcome, it has produced a lot of interest and excitement among understudies, instructors, and rehearsing engineers, making intense training a necessity for bestowing the information on

P. Srinivasan (✉) · R. S. Sabeenian · B. Thiyaneswaran · M. Swathi · G. Dineshkumar
Electronics and Communication Engineering, Sona College of Technology, Salem, India
e-mail: srinisamy2004@gmail.com

B. Thiyaneswaran
e-mail: thiyanesb@yahoo.co.in

G. Dineshkumar
e-mail: dineshkumar.18ece@sonatech.ac.in

G. Rajakumar et al. (eds.), *Intelligent Communication Technologies and Virtual Mobile Networks*, Lecture Notes on Data Engineering and Communications Technologies 131,
https://doi.org/10.1007/978-981-19-1844-5_7

microcontroller-based framework planning and improvement. It identifies the critical elements responsible for their massive impact, the intense instructional need created by them, and provides a brief overview of the significant application area.

2 Literature Review

As security is a main issue these days, existing innovations such as straightforward keys are not idiot-proof any longer. Our shrewd entryway lock framework expects proprietors to set a pin each time the premises are leased to another visitor. The visitor needs only to open an entryway utilizing the one-time secret word (OTP), which is advantageous for both the proprietor of the spot and the visitor leasing the spot. The one-time secret key (OTP) and SMS handling are used to create a safe and simple to use smart entryway lock in lodgings and premises [1].

The investigation will also shed light on the advantages and disadvantages of the various entryway lock frameworks and the innovation used in the various frameworks. The investigation will include conventional entryway lock frameworks, RFID-based frameworks, signal-based frameworks, Bluetooth and GSM innovation-based frameworks, and other advances used in entryway lock security frameworks. The development in innovation each day can assist us with going over different advancements that can be utilized in the entryway lock security framework [2].

We planned and fostered a total framework, including an Android cell phone application, utilizing cryptographic calculations for secure correspondence and programmable equipment with sensors and actuators to control unapproved access. This crypto lock ensures our assets are behind the entryway and secures our information which is being sent throughout the organization. It gives simple remote access, controls unapproved access, and gives a total feeling of safety [3].

In the rapidly evolving mechanical world, “Home Security” stands out enough to be noticed in everyday life. The test to creating different home security gadgets is not just guaranteeing the security and well-being of clients and their homes, but also making gadgets advantageous and smart. Work on the convenience of the clever may lock framework as the main entry. This paper proposes a clever, shrewd entryway lock framework and the board framework. The framework’s design fundamentally embraces the possibility of a secluded plan, partitioning the entire framework into distinct mark module, RFID module, secret word module, show module, rest module, correspondence module, and customer module, among other sub-modules [4].

This module’s password is entered and compared to the original password stored in the EPROM, and additional instructions are given if needed. The touch screen, the micro controller, and the GSM module are the three primary functional elements in the design. The touch screen module serves as an input device for using a password or pattern lock system to gain entry to the door [5].

We frequently forgot to deliver the key to our house. Or, in contrast, at times, we emerge from our home and the entryway lock closes unintentionally. In these cases, it is truly hard to get inside the house. This task will help in the keyless section and, simultaneously, will be safer. This concept will reduce overall costs by utilizing Bluetooth rather than GSM (which charges for support) [6].

In this paper, the first person to register the username and password as well as their mobile phone number is the winner. If the username and password are the same, then the finger of the person will receive and keep an ID. If the ID found is the same. The four-digit code will then be sent to the authorized cell phone to open. As a result, biometric and Bluetooth security systems outperform other systems [7].

A password-protected electronic key includes a keypad for input, an LCD display as an output device, and a small controller as a control unit. The lock system is protected by a user-set password. The lock only opens when the correct password is entered. In contrast, the option to change the password is somewhat more secure, which only an authorized person can do [8].

This assists with keeping away from unapproved admittance to the storage space. When the client is inside, they need to demonstrate their certifications and enter the secret phrase given for the client's protected box. The secret phrase is handled by the microcontroller, and if it matches, it conveys the message to the engine, which opens the safe [9].

This work depends on the idea of DTMF (double tone multi-recurrence) innovation. When all the numeric buttons on the keypad of a cell phone are squeezed together, an interesting recurrence occurs. These frequencies are decoded by the DTMF decoder IC at the less than desirable end, which is taken care of by the microcontroller. In the event that these decoded values, for example, code squeezed by the client, coordinates with the secret phrase put away in the microcontroller, and then, at that point, the microcontroller starts a system to open the entryway through an engine driver interface [10].

With the development of a digital lock system, even after knowing the unlock code, the system sends an SMS to the office and the landlord's cell phone. The program should be activated by the owner simply by pressing the "0" key found on the hex keypad and leaving it. Every time an unauthorized person tries to press even the first key to the full unlock code, the UART-based FPGA is activated and activates the GSM module to send an SMS to the owner's cell phone [11].

The cell phone present in the framework utilizes the auto-answer capacity to take the call. When squeezed, each key on the cell phone communicates two tones with various frequencies. The sent frequencies are decoded utilizing a DTMF decoder, and the decoded esteem is taken care of as a contribution to the microcontroller, which thusly works the stepper motor, which controls the open and close of the door [12].

A model for this framework was created, coordinating elements like guest validation utilizing face acknowledgment, voice ordering, dubious movement recognition utilizing sound alarms, and perceiving unsafe articles guests which might convey utilizing article and metal recognition. This proposed framework will diminish the reliance of outwardly weakened individuals and provide them with a sense of self-appreciation adequacy while reinforcing security at home [13].

The system includes an Android phone that acts as a signal transmitter, a Bluetooth communication module that acts as a signal receiver, an ARDUINO microcontroller that acts as a CPU, servomotors, and light emitting diodes that act as outputs [14].

In this study, we provide an encryption approach suitable for clinical picture sharing that effectively combines the benefits of the two procedures. This model employs a cloud server and blockchain to ensure that the data provided is recognizable, critical, and unaltered. Furthermore, it eliminates the processing and capacity limitations of the blockchain [15].

This technology proposes remote monitoring of transformer maintenance. It uses an IoT-based monitoring system and is connected to the Internet for data transmission and reception via a Wi-Fi module [16].

This technique proposes iris recognition utilizing Eigen esteems for Feature Extraction for Off Gaze Images and investigates various Iris recognition and recognizable proof plans known to produce remarkable outcomes with extremely fewer mistakes [17].

This paper proposed a Raspberry Pi framework for catching face recognition of students' attendance. The framework included a local binary pattern histogram and a convolution neural network strategy for face recognition. The Apache web server gives the Application Programming Interface to send off MySQL information databases, which will keep up the attendance log of students. This framework will give great exactness [18].

In this article, a succession of confirmation levels enables the information stockpiling and recovery to be protected by combining block chain technology with keyless signature technology that is used with various marks to check and certify the information preserved in the cloud. According to the acceptance of the system introduced using the Apache J Meter, the proposed procedure's cost and reaction time were more convincing than the current solutions for distributed storage [19].

This paper presents a template matching mechanism that generates a matching score using AND-OR rules. Over multiple efforts, the efficiency has been examined using several benchmark performance measures [20].

Along with an overall model of OFE, an outsider who is responsible and clear is supplied. The proposed engineering relies on a variety of cryptographic calculations all around to achieve all security measures. The three classes of responsibility are defined in this work just to capture the fundamental requirements of a conscious OFE, and any OFE convention should meet the traits in accordance with the qualities [21].

In this research work, automated warehouse logistics uses sensor networks to collect data on the quantity of things entering and exiting the warehouse, and artificial intelligence to correctly handle them inside the storehouse [22].

3 Existing Method

Various years earlier, when security was less significantly a concern in the overall population, our progenitors peacefully used direct resting mats to cover the doorways of their huts. They were not disturbed at all by any event of a robbery attack since they had a system that would not allow that to happen. Everyone knew their neighbors and essentially every other individual in the town. Nowadays, it has gotten all things considered hard to achieve that kind of mental adequacy and in this manner distinctive contraptions have been used over time to shield the lives and properties of its owners. This new gadget is a lot more secure than the customary key-based framework and electronic remote lock framework. In case you are yet utilizing the key-based framework, you are probably going to land in a major issue if your key gets lost or taken. The electronic remote lock framework is not protected by the same token. You may fail to remember the secret phrase, and there is additionally a high danger of being hacked.

4 Proposed Method

Considering the situation we have all been going through these years, we came up with the idea of an "*OTP-based system.*" We will be sending you the OTP to your registered mobile number; you use that to unlock your door. We will give the input to the system, which includes your name, mobile number, and government ID number (Aadhaar number). First you must enter your government ID number (Aadhaar number), then the system will automatically display your number. After displaying your name, you will be sent an OTP to your registered mobile number. You can enter the OTP and unlock the door. If you have mistakenly entered the wrong number, there will be a beep (high-pitched) sound for 3 s, and you can redo the procedure after the beep sound.

4.1 Block Diagram

The block diagram depicts how the project operates in a simplified manner. At first, the secret phrase is known. When the gadget is turned on, it resets the servo point to lock the entryway. Presently, the client is prompted to enter the secret word. The client enters the password through a keypad, which is perused by the Arduino. Presently, the entered secret key is checked with the known secret key. On the off chance that the secret phrase matches, then, at that point, the servo engine diverts, and the entryway opens for 10 s, or else the bell blares, showing the deficiency of the secret key. The proprietor gets the data too, about the locking and opening of the entryway, through SMS shipped off his cell phone by GSM modem. It asks for OTP and Aadhaar Card

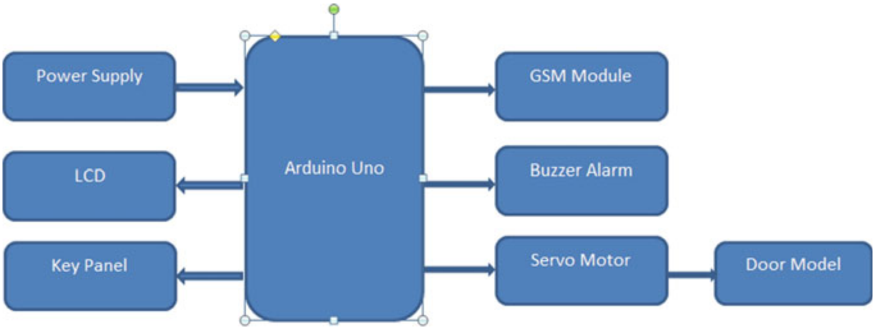


Fig. 1 Block diagram of proposed system

numbers to confirm the information and requests to enter OTP. When the framework gets locked, the secret word cannot be entered through the keypad. Presently, only the proprietor can open or lock the entryway with the secret key he knows (Fig. 1).

4.2 Flowchart

The above flowchart shows the algorithm of how the OTP-based door opening system works. To send messages to the appropriate person, the GSM (Global System for Mobile Communication) is used. After the GSM initialization, we have to enter the Aadhaar number. After entering the Aadhaar number, an OTP will be sent to the respective person's mobile number, and we have to enter the OTP sent. If the entered OTP is valid and a correct one, the door will open automatically. If the entered OTP is invalid and incorrect, the buzzer will alarm, and we will have to redo it (Fig. 2).

4.3 Arduino

Arduino is a free and open-source electronics platform with simple hardware and programming. Arduino sheets can translate inputs like light on a sensor, a finger on a button, or a Twitter post into actions like starting a motor, turning on a light, or broadcasting anything on the Internet. By sending a set of instructions to the board's micro regulator, you may control it. To do so, you will need to use the Arduino software (for Processing) and the Arduino programming language (for Wiring) [23] (Fig. 3).

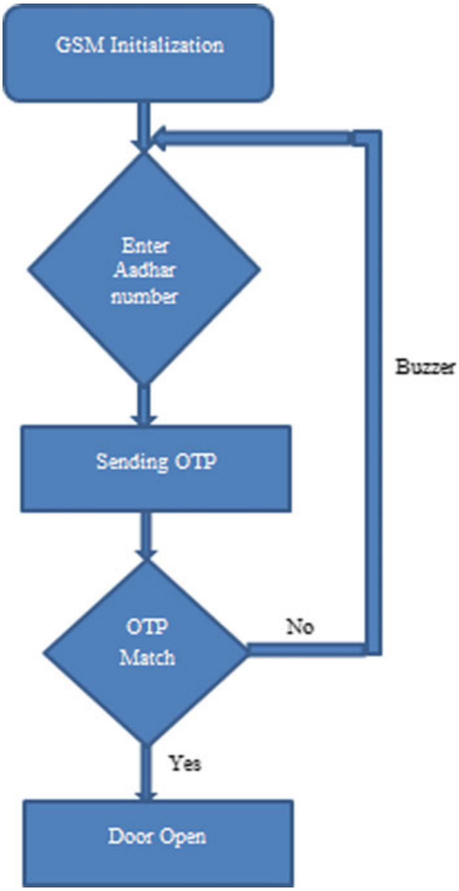


Fig. 2 Flowchart for door opening system

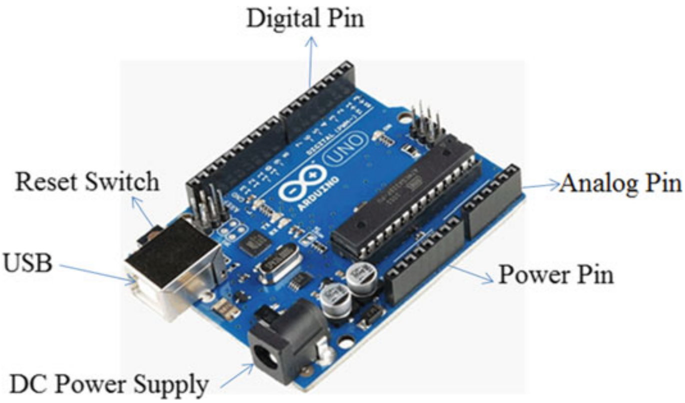


Fig. 3 Arduino board

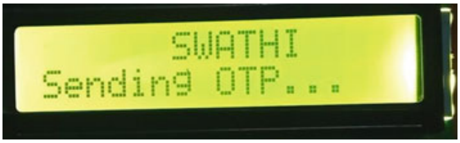


Fig. 4 LCD display

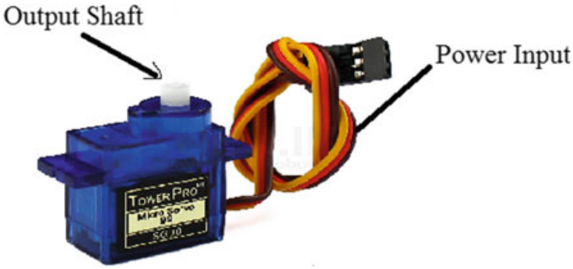


Fig. 5 Servomotor

4.4 LCD Display

A liquid crystal display (LCD) is a low-power, flat-panel display that is used in a variety of digital devices to display numbers or graphics. It is composed of a liquid sandwiched between glass and plastic filtering layers with crystals that are touched by an electric current. When an electric current is passed through the material, the molecules of the "liquid crystal" twist, reflecting or transmitting light from an external source (Fig. 4).

4.5 Servomotor

A servomotor is a spinning or straight actuator that permits accurate or direct position, speed, and acceleration to be controlled. It is made up of an appropriate engine and a position tracking sensor. It also demands a more complex regulator, which is usually a separate module built exclusively for servomotors (Fig. 5).

4.6 Hardware Specifications

Arduino

Microcontroller: ATmega328P
Operating voltage: 5 V
Clock speed: 16 MHz
LED_BUILTIN: 13

Key Panel

Connector: 8 pins, 0.1″ (2.54 mm) Pitch

5 Result and Discussion

This venture is useful in providing sufficient security if the secret phrase is not shared. Later, this “secret phrase-based door lock system” can be given the greatest security by the above improvements to totally fulfill the client’s needs. Consequently, an average person can afford to purchase such a locking framework at a negligible expense to keep their assets secure with next to no concerns. The security level can be expanded by adding a biometric unique mark scanner. We can interface sensors like fire, LPG, and PIR movement finders to microcontrollers if there should be an occurrence of a mishap with the goal of the entryway opening naturally. We can interface a camera to the microcontroller so it could catch the image of the criminal who is attempting to penetrate security. This basic circuit can be utilized at places like homes to guarantee better security. With a slight change, this venture can also be utilized to control the exchanging of burdens through passwords. It can also be used by organizations to ensure admission to highly sought-after locations (Figs. 6, 7, 8, 9, and 10).

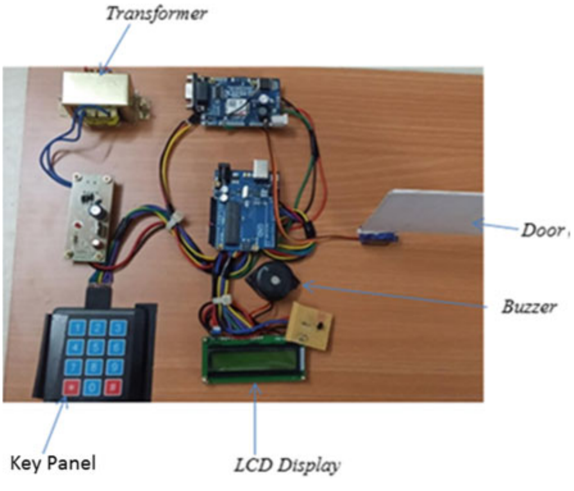


Fig. 6 Prototype model of door opening system

Enter Aadhar NO:

Fig. 7 LCD display of Aadhaar number authentication

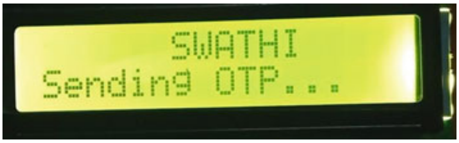


Fig. 8 Displaying the process of sending OTP

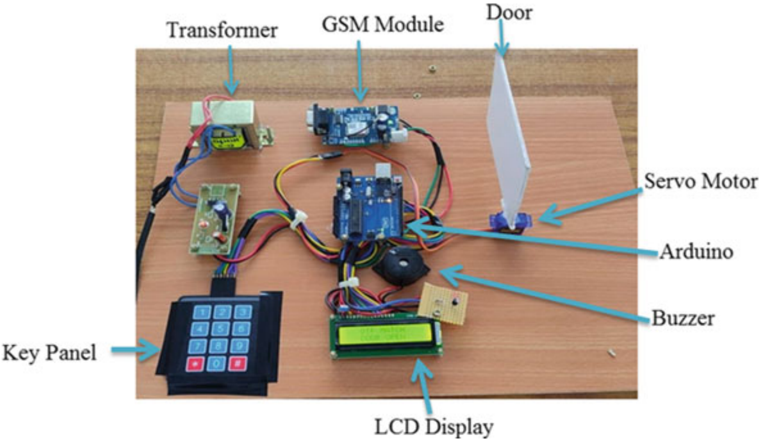
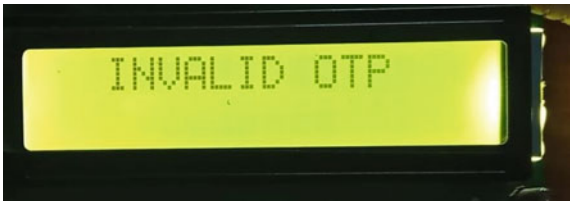


Fig. 9 OTP matched on LCD display and door opening

Fig. 10 Displaying invalid OTP



This shows the hardware setup of the OTP-based door opening system, which is attached to the keypad, door model, buzzer, key panel, GSM, Arduino, and LCD display.

If the entered OTP is incorrect, then it will be displayed as “INVALID OTP.”

6 Conclusion

This straightforward circuit can be utilized at private spots to guarantee better well-being. It could be used by organizations to ensure access to highly restricted areas. With a slight alteration, this project can be utilized to control the exchanging of burdens through secret phrases. This undertaking gives security. Power utilization is lower, and we utilized usually accessible parts. It is a low-reach circuit, i.e., it is beyond the realm of possibility to expect to work the circuit from a distance. In the event that we fail to remember the secret phrase, it is beyond the realm of possibility to expect to open the entryway.

References

1. Daegyu S, Hanshin G, Yongdeok N (2015) Design and Implementation of digital door lock by IoT. KIISE Trans Comput Practices 21(3):215–222
2. Nehete PR, Rane KP (2016, June 21) A paper on OTP based door lock security system. Int J Emerg Trends Eng Manag Res (IJETEMR) II(II). ISSN 2455-7773
3. Supraja E, Goutham KV, Subramanyam N, Dasthagiraiah A, Prasad HKP (2014) Enhanced wireless security system with digital code lock using Rf&Gsm technology. Int J Comput Eng Res 4(7)
4. Oommen AP, Rahul AP, Pranav V, Ponni S, Nadeshan R (2014) Design and implementation of a digital code lock. Int J Adv Res Electr Electron Instrum Eng 3(2)
5. Deeksha P, Mangala Gowri MK, Sateesh R, Yashaswini M, Ashika VB (2021) OTP based locking system using IOT. Int J Res Publ Rev 2(7)
6. Manish A (2017) Secure electronic lock based on bluetooth based OTP system. Elins Int J Sci Eng Manag 2(1)
7. Pooja KM, Chandrakala KG, Nikhitha MA, Anushree PN (2018) Finger print based bank locker security system. Int J Eng Res Technol (IJERT) NCESC 6(13)
8. Rahman MM, Ali MS, Akther MS (2018) Password protected electronic lock system for smart home security. Int J Eng Res Technol (IJERT) 7(4)
9. Prajwal D, Naaga Soujanya N, Shruthi N (2018) Secure bank lockers using RFID and password based technology (embedded system). Int J Sci Dev Res 3(5)
10. Jadhav A, Kumbhar M, Walunjkar M (2013) Feasibility study of implementation of cell phone controlled, password protected door locking system. Int J Innov Res Comput Commun Eng 1(6)
11. Gaikwad PK (2013) Development of Fpga and Gsm based advanced digital locker system. Int J Comput Sci Mobile Appl 1(3)
12. Panchal S, Shinde S, Deval S, Reddy V, Adeppa A (2016) Automatic door opening and closing system. 2(5)
13. Thiyaneswaran B, Elayaraja P, Srinivasan P, Kumarganesh S, Anguraj K (2021) IoT based air quality measurement and alert system for steel, material and copper processing industries. Mater Today: Proc ISSN 2214-7853. https://doi.org/10.1016/j.matpr.2021.02.696
14. Dewani A, Bhatti S, Memon P, Kumari V, Arain A, Jiskani A (2018) Keyless smart home an application of home security and automation 11(2):107–114
15. Joe CV, Raj JS (2021) Deniable authentication encryption for privacy protection using blockchain." J Artif Intell Capsule Netw 3(3):259–271
16. Sharma RR (2021) Design of distribution transformer health management system using IOT sensors. J Soft Comput Paradigm 3(3):192–204
17. Sabeenian RS, Lavanya S (2015) Novel segmentation of iris images for biometric authentication using multi feature volumetric measure. Int J Appl Sci Eng Technol 11(4):347–354
18. Sabeenian RS, Harirajkumar J (2020) Attendance authentication system using face recognition. J Adv Res Dyn Control Syst 12, 1235–1248
19. Kumar D, Smys S (2020) Enhancing security mechanisms for healthcare informatics using ubiquitous cloud. J Ubiquitous Comput Commun Technol 2(1):19–28

20. Manoharan JS (2021) A novel user layer cloud security model based on chaotic amold transformation using fingerprint biometric traits. J Innov Image Proces (JIIP) 3(1):36–51
21. Satheesh M, Deepika M (2020) Implementation of multifactor authentication using optimistic fair exchange. J Ubiquitous Comput Commun Technol (UCCT) 2(2):70–78
22. Pandian AP (2019) Artificial intelligence application in smart warehousing environment for automated logistics. J Art Intell 1(2):63–72
23. Srinivasan P, Thiyaneswaran B, Jaya Priya P, Dharani B,Kiruthigaa V (2021, March) IOT based smart dustbin. Ann Rom Cell Biol 25(3)