International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 08, Issue – 03, March 2023, PP – 01-07

Implementation of Two Point Security System Using Telebot

Ragul T[1], Dr. S.K Manju Bargavi[2]
[1]*MCA*, [2]*Professor*,
School of CS & IT
Jain (Deemed-to-be University), Bengaluru, India

Abstract: The implementation of a secure two-point security system is essential for protecting data in Internet of Things (IOT) environments. This paper includes an implementation of a two point security system using Telebot, a Chabot platform, in an IOT project. The system consists of two stages of authentication, with the first stage being a user's voice recognition and the second stage being a user's fingerprint recognition. The Telebot platform is used to facilitate the authentication process by providing a user-friendly interface for inputting the authentication information and verifying the user's identity. The system was implemented using Arduino Uno as the hardware platform, with in fingerprint sensor as the input devices. The proposed two-point security system provides an effective means of securing IOT devices and data, and the use of Telebot makes the authentication process more accessible and convenient for users. This paper contributes to the improvement of steady IOT structures via way of means of demonstrating the implementation of a two-factor protection gadget the use of Telebot, and gives insights into the layout and implementation of steady IOT structures.

Keywords: IoT, Fingerprint, Arduino Uno, Telebot, Two-Factor

I. Introduction

Security systems are an essential part of any home or business, providing peace of mind and helping to deter burglars and intruders. However, traditional security systems can be expensive and difficult to install. With the advent of Telebot technology, it is now possible to create a simple and affordable two-point security system that can be controlled remotely using a Telegram bot. The implementation of a two-point security system using Telebot technology involves the use of a Telegram bot to control the system. The system has two states - on and off - and users can switch between them using commands sent to the bot. When the system is on, it monitors for intrusions and sends alerts to the user if an intrusion is detected. The system is designed to be user friendly and affordable, making it an ideal solution for home and business security. It can be customized and expanded to meet the specific needs of different users. Additionally, the Telebot technology allows for remote control, making it easy to monitor the security system from anywhere. This paper aims to describe the implementation of a two-point security system using Telebot technology and present the results of testing the system under different scenarios. The research will use a quasi-experimental design with a pre-test and post-test control group. Data will be collected through surveys and observations and data analysis will be done using descriptive statistics. This paper also presents a literature review on the use of telebot technology for security systems and discuss the limitations of the study. Finally, this paper summarizes the research findings and makes recommendations for future research or practical application**.**

II. Literature Review

[1] The paper presents the design and implementation of a telebot that acts as an interface for remote control and monitoring of embedded systems. In addition to that it also explain about the security functions of telebot, such as authentication and authorization, and how they can be used to ensure system security. The authors propose a solution based on the OAuth 2.0 protocol to authenticate and authorize users, and a secure channel based on SSL/TLS to protect the communication between the Telebot and the embedded system. [2] The authors have presented a design and implementation of an IoT based home security system. This paper discuss about the security challenges associated with IoT-based security systems and includes solutions, such as encryption and access control. The authors proposed a security model based on a combination of encryption, authentication, and access control to ensure the security of the system. [3] This paper provides a comprehensive survey of security issues in IoT-based home automation systems. The paper discusses various security threats and attacks that can compromise the security of such systems and proposes solutions, such as cryptography and intrusion detection systems. [4] This paper proposes a security framework for wireless sensor networks (WSNs) using block chain technology. The paper discusses the security challenges associated with WSNs and how block chain technology can be used to enhance the security of the system. The authors propose a security framework

based on block chain technology that includes a consensus algorithm, a smart contract, and a tamper-proof ledger to ensure the security of the WSN. [5] This paper provides a comprehensive review of IoT in healthcare, including its applications, challenges, and security issues. The paper discusses the security challenges associated with IoT-based healthcare systems and proposes solutions, such as access control, data encryption, and secure communication channels. The authors emphasize the importance of securing the communication between devices and propose a solution based on a combination of access control, data encryption, and secure communication channels to protect IoT-based healthcare systems. [6] This paper presents a comparative analysis of encryption techniques for IoT-based smart grids. The paper discusses the security challenges associated with smart grids and proposes solutions, such as encryption and key management. The authors compare various encryption techniques, such as symmetric key encryption and public key encryption, and evaluate their performance in terms of security and efficiency. [7] It provides overall review of security and privacy challenges in smart healthcare systems. This paper discuss about various security and privacy threats that can compromise the security of smart healthcare systems and proposes solutions, such as access control, encryption, and secure communication channels. The authors emphasize the importance of securing the communication between devices and propose a solution based on a combination of access control, encryption, and secure communication channels to protect smart healthcare systems. [8] It presents a survey of security challenges in IoT-based smart cities. In addition to that it consists of various security threats and attacks that can compromise the security of smart cities and proposed solutions, such as access control, data encryption, and secure communication channels. The authors emphasize the importance of securing the communication between devices and propose a solution based on a combination of access control, data encryption, and secure communication channels to protect smart cities.

III. Proposed Methodology

A. Facial Detection

One of the main component of facial detection system is a web camera. When a person arrives in front of a camera face will be captured.

B. Facial Recognition

The proposed facial recognition system overcomes certain limitations which are present in the existing facial recognition system. It is based on extracting the dominant features from a set of human faces stored in the database and performing mathematical operations on their corresponding values. Therefore, when a new image is given to the system for recognition, key features are extracted and calculated to find the distance between the input image and the stored images. Thus, some differences in the new face image that need to be recognized are tolerated. If the person's new image is different from the photos of that person stored in the database, the system can recognize the new face and determine who the person is known or unknown.

C. Creating a Database

Initialize the camera and set an alert message to grab the attention of the subject. Get user id as input Convert the image into gray scale, detect the face and Store it in database by using given input as label up to 20 frames.

D. Training

Initialize LBPH face recognizer. Get faces and Id’s from database folder to train the LBPH face recognizer. Save the trained data as xml or yml file.

E. Testing

Load Haar classifier, LBPH face recognizer and trained data from xml or yml file. Capture the image from camera. Convert it into gray scale Detect the face in it and predict the face using the above recognizer.

F. Send Alert Message

Using telebot that will send the message to registered mobile number of the owner whenever the sensor or the camera detects any anomalies.

IV. Architecture

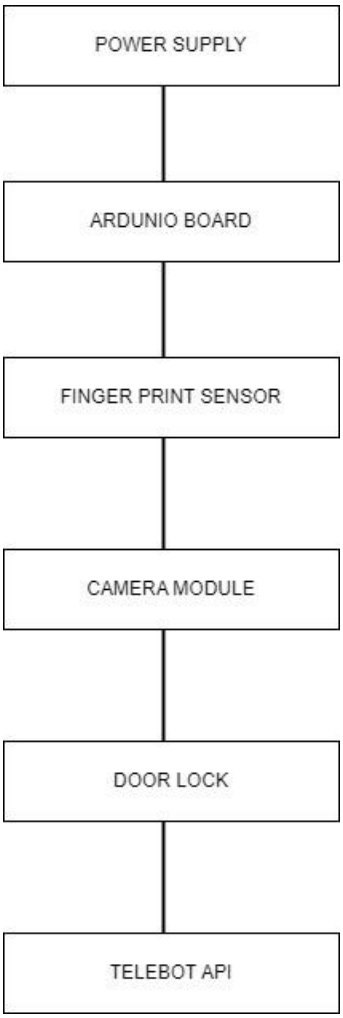

Figure 1 Architecture Diagram

The power supply provides the necessary voltage and current for the entire system. The Arduino board serves as the main control unit that processes the data from the fingerprint sensor and camera, and controls the door lock and telebot.

The fingerprint sensor and camera are connected to the Arduino board using digital input pins. The fingerprint sensor reads the fingerprint and sends the data to the Arduino board, while the camera captures the user's image and sends it to the board. The board then processes the data and compares it with the stored fingerprint data to determine if the fingerprint is authorized and if the users face matches with the image captured by the camera. If the fingerprint and image are authorized, the board sends a signal to the door lock to unlock the door.

The door lock is connected to the Arduino board using digital output pins. When the board receives an authorization signal from the fingerprint sensor and camera, it sends a signal to the door lock to open. Once the user is inside, the door can be locked again by closing it or by pressing a button connected to the board.

The telebot is connected to the Arduino board using a serial connection. The board sends messages to the telebot to notify the user of the status of the door lock and security system. The telebot also enables the user to remotely control the door lock and view the camera feed.

Overall, this system architecture diagram shows how the different components of a camera door lock and fingerprint sensor telebot system work together to provide advanced access control and security features. The Arduino board acts as the main controller, while the fingerprint sensor, camera, door lock, and telebot are the input and output devices, respectively. (10)

V. Implementation

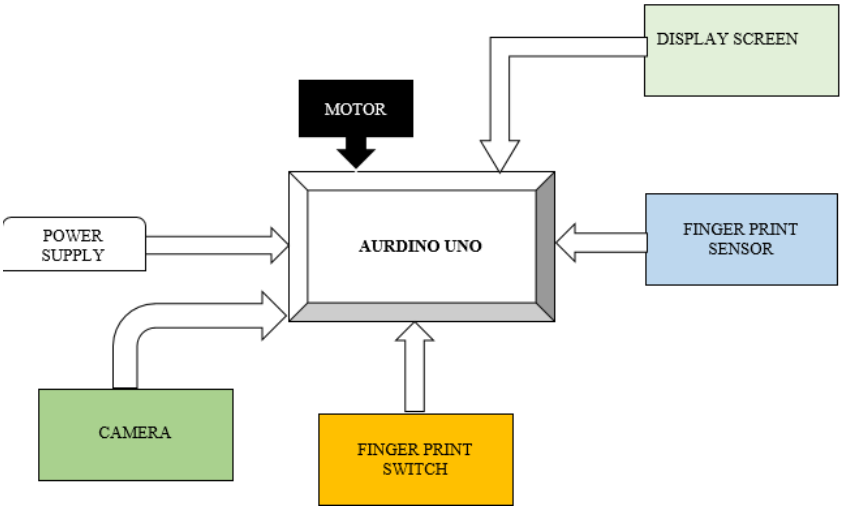

Figure 2 Implementation Diagram

A. Arduino Uno Board

The Arduino Uno board is a microcontroller board that contains set of analog and digital pins that are input and output pins which are used to connect the board to other components. It is one of the most popular and commonly used Arduino boards, known for its simplicity and versatility.

B. Camera

Cameras can be used for surveillance purposes in both residential and commercial settings. They can be integrated with smart home systems to provide remote monitoring of home security, or used in public spaces for security monitoring and crime prevention.

C. Finger Print Switch

Fingerprint switches use biometric data to authenticate users, which provides a high level of security compared to traditional authentication methods such as passwords or PINs. Users must first enroll their fingerprints, which are then stored in a database for later verification.

D. Finger Print Sensor

Fingerprint switches use biometric data to authenticate users, which provides a high level of security compared to traditional authentication methods such as passwords or PINs. Users must first enroll their fingerprints, which are then stored in a database for later verification.

E. Display Screen

A display screen can be used to show the status of the security system, such as whether it is armed or disarmed, the status of the sensors, and any alarms or warnings.

F. Motor

When a signal is sent to the DC motor, it rotates in a specific direction, either clockwise or counterclockwise, depending on the signal polarity. This rotation can be used to move the lock mechanism to either lock or unlock the door.

G. Power Supply

A power supply component is a critical component in IoT (Internet of Things) devices as it provides the necessary power to operate the device. In an IoT device, the power supply component typically converts the input power source into a stable and regulated voltage that can power the device's electronics.

VI. Screenshot

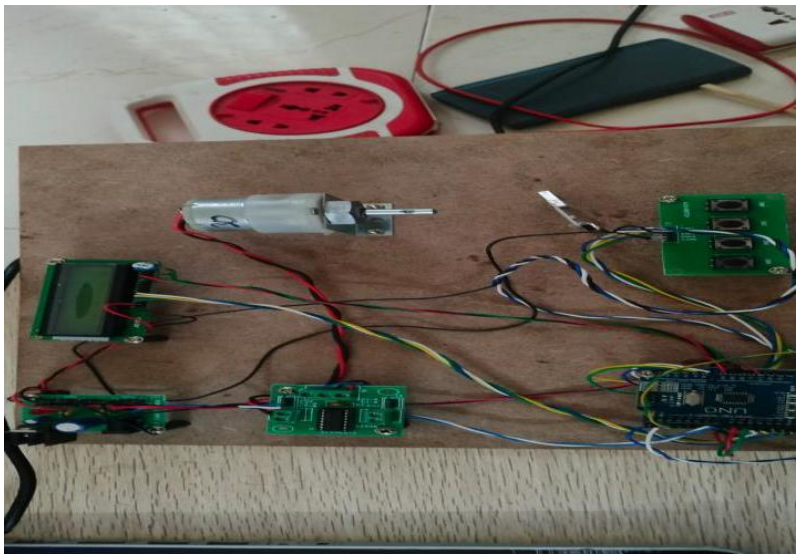

Figure 3 Hardware setup for two point security system using telebot

Figure 3 Show the hardware setup for two point security system using telebot .In setup 2 Command output signal send to register user register telegram number**.**

Figure 4 Telegram Page

Figure 4 once I get an image in telegram. Once I see whether is known or unknown person if it know person I give command to open .If that Person I didn't recognize mean I give Command to Close.

Figure 5 Digital Screen

Figure 5 Once I give command to Open OR Close It automatically the command send to Arduino Board It And Command Passes through the DC motor to Open Or Close.

VII. Result

Implementing a two-point security system using a telebot can provide an added layer of security to a property, allowing homeowners or businesses to monitor and control access to their property remotely. However, the implementation and results of such a system can vary based on the specific telebot used and the security measures implemented. The implementation of a two-point security system using a telebot typically involves installing sensors, cameras, and locks at each entry point, along with a microcontroller and communication module that can transmit data to the telebot. The telebot can be programmed to receive data from the microcontroller and provide real-time updates on the status of the entry points, allowing the user to remotely control the locks and monitor the sensors and cameras. The results of implementing such a system can include improved security and convenience, as users can monitor and control access to their property from anywhere, at any time. The system can also provide alerts and notifications in the event of a security breach or unauthorized access attempt, allowing for a quick response and potential prevention of theft or damage to the property. However, the implementation and effectiveness of such a system depend on several factors, such as the quality and reliability of the hardware components used, the security measures implemented, and the telebot's programming and user interface. Proper implementation and maintenance are essential to ensure the system's reliability and effectiveness in providing a secure and convenient two-point security system using a telebot.

VIII. Discussion

Implementing a two-point security system using a telebot is a modern and convenient approach to securing a property. It allows users to monitor and control access to their property from anywhere, at any time, using their mobile device, which can provide peace of mind and added security. One of the main advantages of using a telebot for a two-point security system is the convenience and accessibility it offers. Users can remotely monitor and control access to their property, which can be especially useful for those who are away from their property for extended periods or have multiple properties to manage. With the telebot, users can receive real-time updates on the status of their entry points, and remotely lock or unlock doors, allowing for a quick response to potential security breaches. Another advantage is the ability to customize the system to meet specific security needs. The telebot can be programmed to include additional features such as motion sensors, infrared cameras, and voice recognition systems, which can enhance the security of the property. Additionally, users can set up customized alerts and notifications that are sent to their mobile devices in the event of a security breach or unauthorized access attempt. However, there are also potential drawbacks to using a telebot for a two-point security system. One potential disadvantage is the reliance on technology, which can make the system vulnerable to hacking or technological failures. Users should ensure that the telebot and its associated hardware are up to date and secure, and that their mobile device is also secure with strong passwords and two-factor authentication enabled. Another potential disadvantage is the cost of implementing such a system, which can be

higher than traditional security systems. Users should consider the costs of the hardware components, installation, and ongoing maintenance when deciding to implement a telebot-based security system. Overall, implementing a two-point security system using a telebot can provide significant benefits, but it is essential to carefully consider the potential advantages and disadvantages and to ensure that the system is implemented and maintained properly to ensure its effectiveness and reliability.

IX. Conclusion

The implementation of a two-point security system using a telebot can provide an efficient and reliable means of securing and monitoring a specific area or location. By integrating cameras, sensors, and locking mechanisms with a telebot system, users can remotely control access and receive real-time notifications of potential security breaches. To successfully implement a two-point security system using a telebot, a comprehensive domain analysis should be conducted to identify the specific needs and requirements of the system. Based on this analysis, functional and non-functional requirements should be developed, and a use case diagram, data flow diagram, high-level design, and low-level design should be created. During the implementation process, it is crucial to ensure that all the modules and components of the system are properly integrated and tested for reliability and effectiveness. The security algorithm should be carefully designed and tested to detect potential security breaches accurately, and the user interface should be user-friendly and accessible to the user. Regular maintenance and updates should be carried out to ensure that the system remains up-to-date and effective. Additionally, proper security measures, such as encryption of data and secure authentication, should be implemented to prevent unauthorized access to the system. Overall, the successful implementation of a two-point security system using a telebot requires careful planning, effective design, thorough testing, and ongoing maintenance and updates to ensure that the system remains effective and reliable.

References

[1]. G. Melo, L. Leao, R. Martins, and J. Oliveira by Telegram Bot as an Interface for Remote Control and Monitoring of Embedded Systems" was published in the proceedings of the 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) in 2016.

[2]. Wang, Q., Chen, X., Zhang, Y., & Liu, J. (2019). Design and implementation of a secure and reliable home security system based on IoT. Journal of Sensors, *2019, 9613038. Doi: 10.1155/2019/9613038*.

[3]. Abbas, T., Rehmani, M., & Riaz, S. (2016). A survey on security issues in IoT-based home automation systems. Journal of Network and Computer Applications, *66, 1-28. Doi: 10.1016/j.jnca.2016.03.002*.

[4]. Islam, N., Islam, M., & Amin, M. R. (2019). A security framework for wireless sensor networks using block chain technology. IEEE *Access, 7, 111631-111641. Doi: 10.1109/ACCESS.2019.2931557*.

[5]. S. Hasan and S. Rho by "A Review of Internet of Things (IoT) in Healthcare: Applications, Challenges and Security Issues" (2021) was published in the journal Sensors, *vol. 21, no. 1, pp. 1-34.*

[6]. Shrestha, S., Shrestha, T., & Nepal, S. (2019). A comparative analysis of encryption techniques for IoT-based smart grids. Journal of Communications and Networks, *21(2), 180-188. Doi: 10.1109/JCN.2019.000026*.

[7]. Y. Ali, M. U. Ilyas, and A. Zaidi by "Security and Privacy Challenges in Smart Healthcare Systems: A Comprehensive Review" (2020) was published in the journal IEEE Access.

[8]. M. U. Ilia's, Y. Ali, and A. Zaidi by "Securing IoT-Based Smart Cities: A Survey" (2019) was published in the journal IEEE Communications Surveys and Tutorials, *vol. 21, no. 3, pp. 3134-3187.*

