International Journal of Innovative Research in Engineering
Volume 7, Issue 2 (March - April 2026), PP: 85-89.
https://www.doi.org/10.59256/ijire.20260702011
www.theijire.com
ISSN No: 2582-8746

IOT Based Smart Parcel Receiving System

Saranya S[1], Vikram V[2], Yaseen VH[3], Santhosh Kumar S[4]
[1]*Assistant Professor Department of IT, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India.*
[2,3,4]*UG Students, Department of IT, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India.*

How to cite this paper:
Saranya S[1], Vikram V[2], Yaseen VH[3], Santhosh Kumar S[4], "IOT Based Smart Parcel Receiving System", IJIRE-V7I2-85-89.

Abstract: *e-commerce has rapidly expanded over recent years, and the volume of this particular type of commerce has contributed to a dramatic rise in the amount of parcel deliveries both to households and business premises. Nevertheless, a problem of missed deliveries, unavailability of receivers, and a chance of theft of a parcel are frequent issues in traditional methods of parcel delivery. These problems reveal the necessity of the safe and automatic system of parcel reception that can be stable without the constant control of a person. The project is dedicated to the design and implementation of a Smart Parcel Receiving System based on the Internet of Things (IoT) technology with the help of secure authentication methods. Proposed system combines ESP32 microcontroller, electromagnetic locking system, OTP verification system implemented in keypad and face recognition system to offer dual-level security system. The system helps deliver personnel to leave the packages safely via a one-time password (OTP), and the family members with authorization could access the parcel box both with face recognition and OTP authentication.*

Keywords: *Internet of things, Automated Pill Dispenser, ESP32, Remote Health Monitoring, Artificial Neural Network, GSM Communication*

I.INTRODUCTION

The boom of the e-commerce and online store business has led to the significant growth of the number of the parcels delivered to households and business sites. Although this has increased accessibility and convenience to the consumers, it has also come with a number of operational and safety problems. Incidences of missed deliveries, non-availability of the recipient, unauthorized access and theft of parcels has become more common especially in urban residential places. The traditional parcel delivery systems rely mostly on human verification and human presence which is not that reliable and secure.

To establish a secure and reliable parcel handling, this paper will suggest a smart parcel receiving system that employs IoT -based control and intelligent authentication mechanisms.

II.MATERIAL AND METHODS

A. System Architecture Design

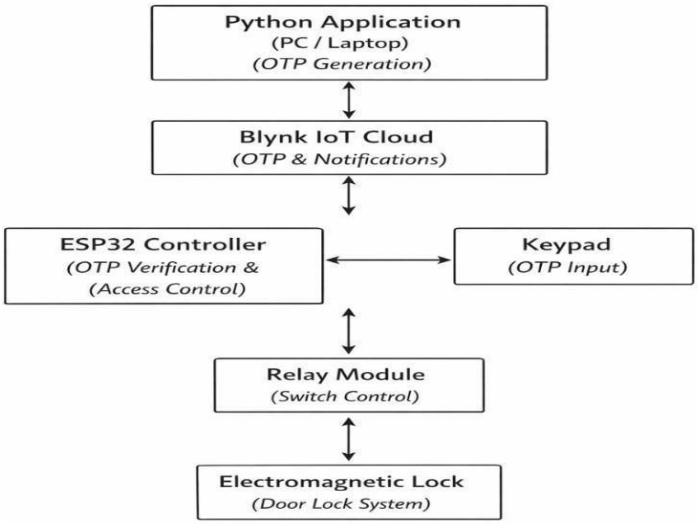

Fig 1. System Block Diagram

The proposed IoT-based Smart Parcel Receiving System uses its system architecture to provide secure user authentication and dependable system operation and continuous system surveillance through its hardware devices which connect to its cloud-based services. The overall architecture uses an ESP32 microcontroller together with input and sensing modules and cloud communication and an automated locking mechanism to create a system which enables controlled parcel delivery and retrieval.

The ESP32 microcontroller serves as the main processing unit which handles all data communication for the system architecture. It connects directly to the keypad module and relay module and electromagnetic lock while it maintains connection to the internet through its Wi-Fi capabilities. The ESP32 microcontroller checks user input and authentication data to determine who should be granted access.

B. Operational Workflow

The proposed smart parcel receiving system operational workflow will aim to present a secure, automated, and user-friendly parcel handling through the assistance of the IoT-based control and smart authentication. The system functions by having a synchronized collaboration between embedded hardware, cloud services, and authentication modules.

First, the system is in the idle monitoring mode and is constantly connected the cloud platform using Wi-Fi.In case of a scheduled delivery, a dynamic one-time password (OTP) is created with the help of the cloud application and safely sent to the registered user. The OTP received by the delivery person is typed in the keypad mounted on the parcel box. ESP32 microcontroller compares the OTP received with the stored value on the cloud and authenticates it. In case the test proves successful, the controller switches on the relay module, temporarily releasing the electromagnetic lock so that the parcels can be placed. After the specified time span, the lock is automatically re-locked so as to secure it.

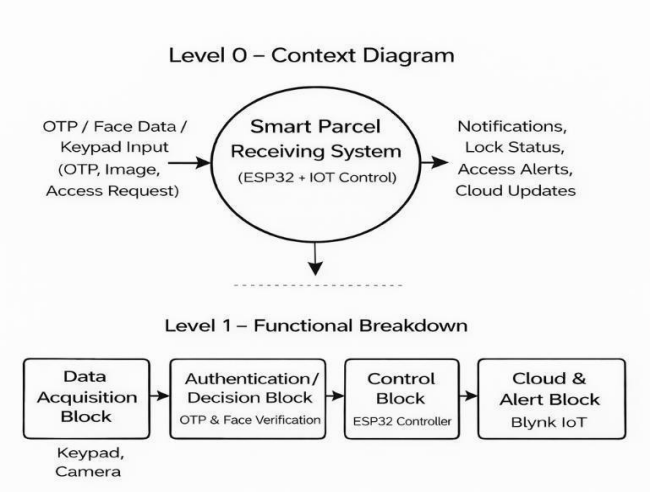

Fig 2. Workflow Diagram

C. Authentication and Access Control Logic

The smart parcel receiving system uses multi-factor verification to create controlled access which provides users with reliable and secure authentication through its access control system. The system supports two authentication modes—OTP-based verification and face recognition-based verification—depending on the type of user and access request. The ESP32 microcontroller functions as the central processing unit which assesses authentication data to manage physical entrance to restricted areas.

1. OTP-Based Authentication Logic

The system implements structured verification procedures to monitor parcel delivery and user access requests through OTP verification. The ESP32 transmits the keypad input to the cloud platform through a secure Wi-Fi connection when a user enters an OTP. The cloud system validates the received OTP by comparing it to the dynamically generated value which is linked to the delivery session.

The ESP32 activates the relay module to release the electromagnetic lock when the user enters a valid OTP which enables entry to the parcel compartment. The lock will automatically re-engage after the designated time period which returns the area to its secure state. The system immediately denies entry when the OTP fails authentication and it sends an alert notification through the cloud platform to the registered use

2. Face Recognition-Based Authentication Logic

The system has the ability to use the face recognition technology to achieve the system access by authorized users. When the user makes an access request that is detected by the camera, the facial image with user is captured and then passes the system sends on to the face recognition module via local connections. This algorithm of recognition matches the face image obtained against the facial templates of authorized persons in the database.

3. Multi-Factor Decision Logic

The system is implemented on a multi factor authentication system that allows access to the system leaving the information of the user safe. OTP authentication is the primary method used by delivery personnel and the option to use face recognition or OTP is open to authorized individuals. This authentication technique is employed in the system and it helps in reducing illegal access and waste delivery of packages.

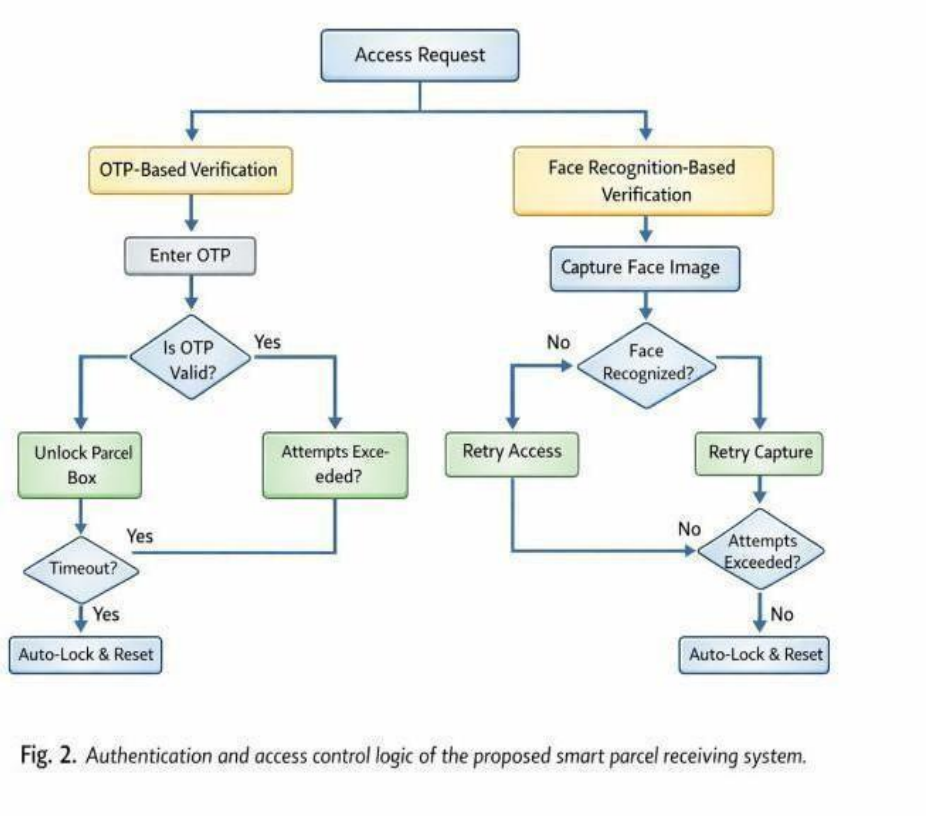

Fig. 2. *Authentication and access control logic of the proposed smart parcel receiving system.*

Fig 3. Authentication and Access

D. Experimental Setup

The experimental setup of the proposed Smart Parcel Receiving System is designed to validate secure parcel handling through IoT- based control and dual authentication mechanisms. The hardware and software components are integrated to ensure reliable operation, real-time monitoring, and automated access control under practical conditions.

The system has an ESP32 microcontroller as the heart of it because it has an inbuilt Wi-Fi and it requires low power to run. ESP32 is connected to a pin with a keypad device that has an option of one-time password (OTP) as an authentication method. Authorized users receive dynamically generated OTPs on the Blynk IoT cloud platform. The keypad enables the delivery personnel or users to key in received OTP which are verified by controller via cloud communication.

The face recognition-based authentication employs a camera module. The camera takes a picture of the faces of the users trying to open the parcel box and transfers the information to a face recognition system written in Python and executed on a processing unit connected to the camera. The recognition algorithm compares the Captured image with the stored authorized profiles and transfers the authentication result to the ESP32. This two-step system authentication process helps to increase the level of system security since it will be based on OTP and biometric authentication.

To guarantee the security of the parcel box, an electromagnetic lock is employed to assure physical access control. The relay module controls the lock using ESP32 interface. On successful authentication ESP32 opens the relay and opens the parcel box during a specific period. Once parcels have been placed or removed in a parcel suture, the lock is re- engaged automatically to curb illegal access. This time limitation lockout system provides control and safety of usage.

The regulated DC power supply powers the system to supply stable voltage to the ESP32, a relay module, and a locking mechanism. Wi- Fi will provide the means to establish a constant communication between the ESP32 and the Blynk IoT cloud, which sends notifications in real-time, establishes access alerts as well as the system status updates. The test was performed through experimental trials that were carried out under ideal indoor conditions to assess the accuracy in authentication, the response time, and the reliability of communication.

On the whole, the experimental platform shows that there is a smooth process of integrating embedded hardware, cloud computing, and intelligent authentication, which, in turn, proves the practicality of the suggested system related to the secure and automated management of parcels in residential settings.

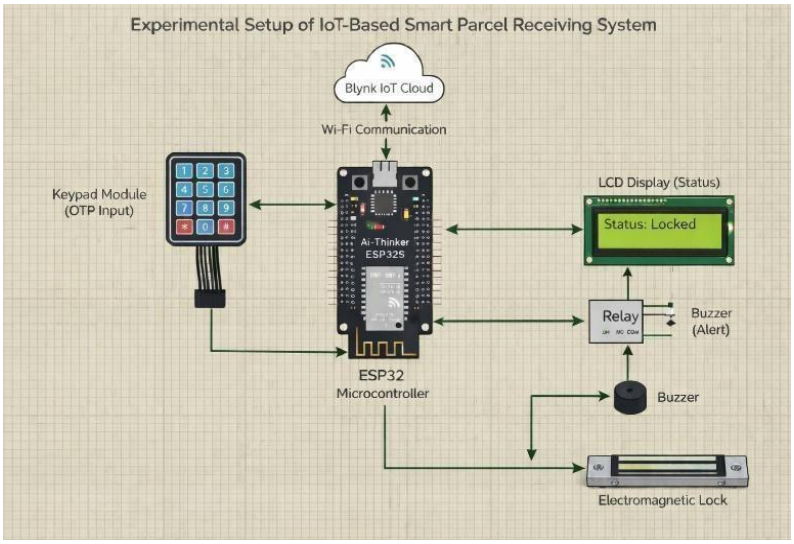

Fig 4. Circuit Diagram

III.RESULT

The proposed IoT-based Smart Parcel Receiving System was implemented and tested under controlled indoor conditions to evaluate its performance in terms of authentication accuracy, response time, and system reliability.

The OTP-based authentication mechanism demonstrated high accuracy, with all valid OTP entries being successfully verified through the Blynk IoT cloud platform. The average response time for OTP validation and lock activation was observed to be minimal, ensuring a smooth and efficient parcel delivery process.

The face recognition module, developed using Python, successfully identified authorized users with reliable accuracy under proper lighting conditions. The system was able to distinguish between authorized and unauthorized users, thereby enhancing the security of parcel access.

The electromagnetic locking system responded correctly to authentication signals. Upon successful verification (OTP or face recognition), the relay module activated the lock, allowing access for a predefined time duration, after which the lock was automatically re-engaged. This ensured secure handling of parcels without manual intervention.

Real-time notifications were successfully delivered to users through the Blynk IoT platform, providing updates on parcel delivery, access attempts, and system status. The system maintained stable communication between hardware and cloud services during testing.

Overall, the experimental results indicate that the system performs efficiently in providing secure, automated, and reliable parcel management, with minimal delay and high authentication accuracy.

IV.DISCUSSION

The proposed IoT-based Smart Parcel Receiving System demonstrates significant improvements over traditional parcel delivery methods by addressing key issues such as missed deliveries, unauthorized access, and parcel theft. The integration of dual authentication mechanisms, including OTP-based verification and face recognition, enhances the overall security of the system compared to existing solutions that rely on single-layer authentication.

The use of the ESP32 microcontroller enables efficient real-time processing and seamless communication with the Blynk IoT cloud platform. This ensures timely notifications, remote monitoring, and improved user awareness. The experimental setup confirms that OTP generation and verification occur with minimal delay, and the face recognition system provides reliable identity validation under controlled conditions.

Compared to earlier systems discussed in the literature, which mainly focus on either password-based or OTP- based access, the proposed system combines multiple technologies to provide a more robust and scalable solution. The addition of an electromagnetic locking mechanism further strengthens physical security, ensuring that access is granted only after successful authentication.

However, the system has certain limitations. Its performance is dependent on stable internet connectivity for cloud communication, and face recognition accuracy may vary under different lighting or environmental conditions. Additionally, system scalability in large residential complexes may require further optimization.

Overall, the discussion highlights that the proposed system effectively balances security, automation, and user convenience, making it a practical solution for modern parcel management in smart homes and residential environments.

V.CONCLUSION

The smart parcel receiving is a suggested system that offers a secure and reliable, automated system of controlling parcel deliveries in the suburban residential setting. As a result of the fast rise in e-commerce, the conventional methods of delivering goods have been in danger, leading to issues of lack of availability of people to receive their goods, unauthorized

access, and stealing of the parcels. The created system provides a solution to these problems since it will incorporate two aspects: Internet of Things (IoT) technology and intelligent authentication and automated access control and, therefore, will decrease the requirement of constant human control.

Substantiated is the system based on the ESP32 microcontroller and is around it, the core control element that coordinates the process of authentication, communications, and locking. A blend of one-time password (OTP) verification and camera-based face recognition provides the security mechanism of two layers. The Blynk IoT cloud platform is used to dynamically create OTPs and send them to authorize users and to authenticate a resident identity when accessing a parcel. This multi factor authentication method plays a tremendous role in strengthening system and avoids illegal acts in the delivery as well as retrieval of the parcel.

Generally, the smart parcel receiving system proposed can be seen as a successful approach to address popular issues in delivery by providing a low-cost, modular, and scalable solution. It is adaptable in nature and can be used in stand-alone houses and in apartment complexes and residential areas. The system forms a great base towards further development of more advanced analytics and better biometrics reliability and compatibility with wider smart home platforms as part of the continuing enhancement of intelligent and secure parcel management solutions.

References

1. J. O. Oughton and J. E. Gallagher, "Multispectral object detection and smart sensing for logistics applications," IEEE Access, vol. 10, pp. 112345–112356, 2022.
2. R. Patel and A. Singh, "Secure smart locker system for parcel delivery using IoT and OTP authentication," International Journal of Innovative Research in Computer and Communication Engineering, vol. 8, no. 6, pp. 1450–1457, 2020.
3. S. Kumar, R. Sharma, and V. Gupta, "Design and implementation of an IoT-based smart parcel locker system using embedded controllers," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 9, no. 4, pp. 112–118, 2020.
4. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347– 2376, 2015.
5. R. Want, B. N. Schilit, and S. Jenson, "Enabling the Internet of Things," IEEE Computer, vol. 48, no. 1, pp. 28–35, 2015.
6. A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.
7. M. Miettinen, S. Marchal, I. Hafeez, et al., "IoT SENTINEL: Automated device-type identification for security enforcement," in Proc. IEEE Int. Conf. on Distributed Computing Systems (ICDCS), 2017, pp. 2177–2184.
8. Y. Li, X. Chen, and H. Zhang, "Smart locker system for secure parcel delivery based on Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4631–4640, Jun. 2019.
9. A. Gupta and R. Kumar, "Design of an automated parcel delivery and locker system using IoT," International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 2, pp. 315–320, Dec. 2019
10. P. Sharma, S. Verma, and A. K. Singh, "Cloud-enabled IoT-based smart home security and access control system," International Journal of Internet of Things and Cyber-Assurance, vol. 4, no. 1, pp. 12–20, 2020.
11. J. Chen, L. Wang, and Z. Zhou, "Design of an intelligent access control system using biometric authentication," IEEE Access, vol. 8, pp. 145678–145687, 2020.
12. S. Ahmed and M. Rahman, "Secure IoT-based access control system with real-time monitoring," Journal of Network and Computer Applications, vol. 151, pp. 102–110, Feb. 2020. [15] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010