

RESEARCH PAPER

An IoT-Based Smart Airport Check-In System Via Three-Factor Authentication (3FA)

Ashna Sahdi Ali¹, Dler Salih Hasan²

1Department of Computer Science and IT, College of Science, Salabaddin University-Erbil, Kurdistan Region. Iraq.

2Department of Computer Science, college of Science, Salahaddin University-Erbil, Kurdistan Region, Iraq

ABSTRACT:

The Internet of Things (IoT) has been taking over the globe, providing an interface where computer devices are connected to digital equipment, mechanical machines, and even individuals. This paper suggests a smart airport check-in system utilizing the Internet of Things. The system includes setting up a smart door to secure the passage to travelers at the airport, depending on the barcode boarding pass (BCBP). The door is designed and implemented by using Raspberry Pi 4B, and two cameras are installed. The first one is for scanning the BCBP, decoding a developed portable data file (PDF417)-based algorithm and processing the data. The second camera is to detect and capture traveler's faces in real-time video streaming among face alignment using Dlib and OpenCV-Python algorithms. A fingerprint reader is also attached to the system as biometric authentication. The system is monitored by using the KAA platform. When the data of a traveler is verified and matched, the door opens. If the data is not matched, the door remains closed and a Telegram notification will be sent to the airport security. The system was tested on 100 travelers. It resulted to obtain smooth, secure, and reliable check-ins. In terms of efficiency, our system has decreased maximum and minimum time to check-in for each passenger to a much larger extent comparing to the traditional check-in system.

KEY WORDS: IOT, BCBP, Smart AirPort Check-In, Raspberry Pi 4B, KAA, Dlib, 3FA, PDF417.

DOI: <http://dx.doi.org/10.21271/ZJPAS.35.4.01>

ZJPAS (2023) , 35(4);1-13 .

1.INTRODUCTION :

IoT, by definition, is connecting devices via sensors and an appropriate platform with the Internet (Hassan, 2018). Due to the cloud-based IoT services, it is possible at any time for the user to retrieve their data and monitor the systems via the Internet (Abdalla and Varol, 2019). There is an expansion of travel via airplane to a variety of locations worldwide due to recent improvements in airport infrastructure and technology. Therefore, the idea of an automatic security check-in door for airport arose. The proposed system is to establish a security door using a BCBP, fingerprint, and face detection of the traveler.

International Air Transport Association (IATA) started a project to launch Bar Coded Boarding Passes (BCBP) among those flight airlines who are their members to end magnetic boarding passes. This update allows the airlines to use more affordable boarding passes. It would also be more applicable for the other technologies such as web and mobile check-in. The BCBP standard defines QR and PDF417 codes can be used to encode the data from paper boarding passes (IATA, 2018). PDF417 (Portable Data File, or PDF-417) is a stacked linear [barcode](#) format theme that was introduced by Symbol Technologies as a high-capacity, highly secure symbology. PDF417 is classified as stacked, though each symbol character often consists of 4 bars and 4 spaces with a total width of 17 modules (hence the origin of 417 in the symbology's name) (Leopold, 2008). PDF417 can be applied in different fields of study and research such as in (automotive

* Corresponding Author:

Ashna Sahdi Ali

E-mail: ashna.s.ali@su.edu.krd

Article History:

Received: 30/10/2022

Accepted: 24/12/2022

Published: 30/08 /2023

industry), transport systems (e.g. for shipping labels), identification (e.g. driver licenses, passports) and document management. (Gounder & Sharma, 2021)

In this paper, an IoT security door is proposed to be implemented based on the use of Raspberry Pi 4B, which is a simple computing and networking miniature pc that tasks as a primary component of the IoT in this system; two webcams were used, one for scanning the barcode and the other for capturing the face of the traveler; also fingerprint sensor is attached to the system so that multi-biometric authentication is used.

A software is developed based on the PDF417 algorithm to decode BCBP data. Another software is developed by using Open-CV python, Dlib algorithm, to detect and recognize traveler's face images (Ismael et al.). The fingerprint sensor is programmed using a modified version of the Adafruit fingerprint library. When there is unmatched data of the traveler, the door stays closed.

The system is monitored through the Kdrive Acceleration Architecture (KAA) platform, which is a multifunctional middle layer platform for the IoT services that allows the applicators to complete the end-to-end IoT features, applications, and smart features. It shows check-in data utilized value, delivers notifications to airport staff by sending an SMS to Telegram, and the door is also tested in the real environment on 100 travelers.

The purpose of this paper is to provide an empirical analysis using Raspberry-pi 4B of an airport passenger operation and to improve its efficiency, and reduce the check-in time also to obtain maximum security by using face recognition and fingerprint of the passenger. An investigation was conducted to evaluate the quantitative and qualitative efficiency of the self-service check-in.

This paper's structure is as follows. In Section 2, relevant works are reviewed. Sections 3 and 4 illustrate the hardware requirement and system architecture of the research. Sections 5 and 6 explain the software requirement and system design. Section 7 discusses the results, and Section 8 explains the results.

2. LITERATURE REVIEW

International society is spending quickly on IoT devices and security issues nowadays. Especially in wealthy nations, there is a notable rise in intelligent automation systems. Emerging applications for smart door systems are thought to be derived from already installed smart door systems. The most recent academic literature reveals several developments and uses for various smart security setups. The following works demonstrated this and were utilized to support our suggested paradigm. A significant portion of the present literature is focused on smart security, which can be modelled more broadly for the suggested smart airport check-in system.

Liu, Li, Hu, & Sun proposed a new way of check-in identification system based on face recognition. This system included three main processes. First, face images were captured by web cameras. Second, the PCA algorithm was performed on normalized images to extract features. Thirdly, a database including the basic information of participants was created, and each image was associated with corresponding information in the database. The system can serve as an efficient and accurate way of check-in (Liu, Li, Hu, & Sun, 2018).

Jahnavi and Nandini designed smart door locking system to make the facial recognition and detection systems previously used to open doors more secure. The LBP technique was used to fully detect the facial image, which was taken by using the Raspberry Pi camera. For the dimensional reduction, a Principal Component Analysis (PCA) approach was employed. A face was eventually found and compared to the original programming. When a match was used to unlock the door, access was prohibited in the absence of a match, which set off an alarm to notify the homeowner. This work used just one authentication factor, but it is obvious to use a more authentic factor can increase the security and accuracy levels of the system (Jahnavi and Nandini, 2019).

Pinjala and Gupta designed an intelligent door lock which can be continuously managed and

observed remotely via a smartphone application. The Raspberry Pi HD camera was made to turn on when a visitor rang the doorbell and sent a text message to the user to let them know. In addition, IoT capabilities were used to transmit the visitor's live stream to the owner. They even demonstrated how the app could be used as a doorbell over a cloud server in real time and how the door could be opened from the app using a pre-programmed password. However, there is also a lack of using many authentication factors (Pinjala and Gupta, 2019).

Kumar et al. developed a Smart Door Lock system using Raspberry Pi that successfully integrated a camera motion sensor with e-mail. The motion sensor and webcam were handled and managed by Raspberry Pi for sensing and monitoring. The Raspberry Pi gadget would start streaming the webcam whenever motion was detected and send the owner a notification through e-mail to his registered mail ID (Kumar et al., 2019).

Husni et al. intended to strengthen and increase security by using electronic key to open, close, and control the door via an android smartphone, which is used with an electronic key to open and close doors. In order to open or close the door, the Arduino Global System for Mobile communication (GSM) receives commands from the server via the Raspberry Pi, and a webcam captures images of the surrounding area for documentation. This research applied a different factor for authentication, but the system should consider an alternative way in case of failure to receive the electronic keys (Husni et al., 2019).

Rahaman et al. (2021) have proposed door access security system that can operate different lighting and identify faces from various angles using Raspberry pi. Moreover, it triggers the security alarm when unauthorized travelers try to check in and their faces data do not match with the stored data inside its database and using Haar Cascade Face detection process, to perform the face recognition system (Local Binary Pattern (LBP)) Algorithm has been applied (Rahaman et al., 2021).

Baluprithviraj et al. effectively integrated safety and facial recognition in order to ensure that householders were contacted safely. They demonstrated how to unlock doors only when a

mask-covered face was seen in order to guarantee that residents may be visited safely in the COVID-19 period. Researchers demonstrated how their system could recognize people without masks and integrated with a clever application to notify the homeowner. They used a new technique for recognizing a person even wearing a mask, but this work also ignored alternative ways to recognize the person in case the system is not able to recognize the trusted person via their face, such as using fingerprints as an alternative technique for authentication (Baluprithviraj et al., 2021).

Prathapagiri and Kosalendra suggested a door security system application that would employ an ESP32 CAM Wi-Fi Door Lock and IoT technology to manage the door, check its state, and send an alert to the owner's phone along with a picture of that person. Additionally, they showed how it might be used to unlock the door from a mobile device after scanning the image; as in other studies in this area, the proposed system did not consider the alternative authentication factors. For example, due to some technical issues, the systems will not recognize the authorized person correctly, or in some cases, the system may allow opening the door with a trusted person; the best way to solve this issue is using various authentication factors (Prathapagiri and Kosalendra, 2021).

Prity et al. suggested that an RFID-based safe door lock system attempts to leverage its many benefits over conventional door security systems in order to boost security. For example, a wireless technology called radio frequency identification (RFID) enables the creation of flexible, scalable control systems. However, tag collision happens when too many tags confuse an RFID reader by transmitting data simultaneously, which is one of the major RFID vulnerabilities (Prity et al., 2021). Elechi created a facial recognition security system that could easily integrate into an intelligent home system utilizing the Raspberry Pi. For feature extraction, Eigen face was applied, and Principal Component Analysis (PCA) was used to classify data. The facial recognition algorithm's result was linked to the Relay circuit that manages a door-mounted magnetic lock. Overall, the outcomes were facial recognition accuracy of 90% very significant (Elechi, 2022).

Mishra et al. demonstrated a smart home technology component that utilizes Bluetooth in a mobile device to facilitate and improve user efficiency. Additionally, it is based on the open-source, free Android and Arduino platforms. The development of a mobile application based on Bluetooth for locking and unlocking door is discussed first, followed by hardware design and software development (Mishra et al., 2022).

Jeong created a door lock which can reduce the user's fingerprint trail and complement the shape of the existing door lock that is visible from the outside. Additionally, a technique of fingerprint recognition by image processing and a random pattern number arrangement is used to reinforce security. The effectiveness of this sort of door lock was tested in an experiment, and the detection was partially damaged. Additionally, fingerprints were verified (Jeong, 2022).

The paper is based on door security system using Raspberry-pi 4B of an airport passenger operation to improve its efficiency, reduce duration of check-in and queue time, also to obtain maximum security by using BCBP, face recognition and fingerprint of each passenger.

3. Hardware Requirements

This section explains the required hardware for designing the proposed system.

3.1. Raspberry Pi 4B

Raspberry Pi 4B is a single-board computer with a 64-bit quad-core ARM8 Broadcom (BCM2711) 1.5 GHz Central Processing Unit (CPU), 4GB Low Power Double-Data Rate Fourth-generation (LPDDR4) Random-Access Memory (RAM), an extensible Micro secure digital (SD) card, and a conventional 40-pin General Purpose Input/output (GPIO) port. Along with inbuilt wireless networking, Bluetooth, and Gigabit Ethernet, Raspberry Pi 4 has these features, as shown in Figure 1. The Raspberry Pi is the optimal choice for IoT applications because it is simple to set up for remote communication when combined with Wi-Fi and Internet connectivity (Chaudhari et al., 2020). Therefore, this microcontroller is used in the suggested system.

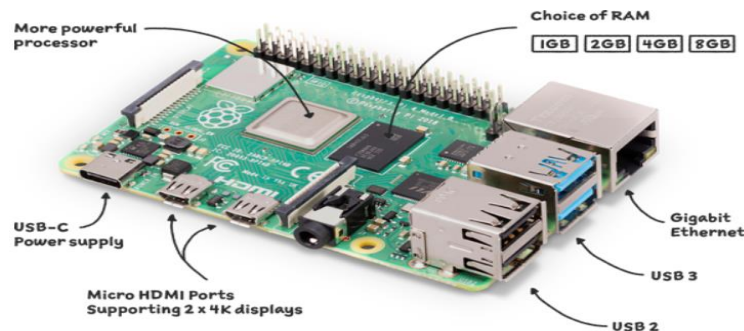


Figure 1: Raspberry Pi 4B

3.2. Webcam Sensor

A Joyaccess webcam with Auto Light Balance is a type of camera used in this system that sends live video or still photos over a USB cable with a resolution of HD 1920 x1080p that allows you to record and share colorful, vivid, high-definition quality videos, with its focus range from 5cm to infinity as shown in Figure 2 (Anwar et al., 2022).

Two webcams are used in the proposed system;

the first webcam was used to scan the BCBP, then encrypted by a decoding algorithm. The second webcam was used to capture a face image of the traveler.



Figure 2: Joyaccess webcam

3.3. Fingerprint

The R307 fingerprint sensor module used in the system for detecting and verifying traveler is a high-powered DSP chip with low power consumption, low cost, small size, excellent performance, professional optical technology, precise module manufacturing technics. Good image processing capabilities can successfully capture an image up to resolution 500 dpi Finger detection function(Arun et al., 2018), as shown in Figure 3.



Figure 3: R307 Fingerprint device

3.4. Servo Motor

A two MG90S micro servo motor is used in the system to control both door sides. Despite its low-

cost, metal gear radio control (RC) servo with 1.80kg.cm holding torque (at 4.8V) and tiny size and lightweight, it has powerful output. The advantage of servo motor over the brush motor is the ability to control its rotation angle (Gaponcic et al., 2021), as shown in Figure 4.



Figure 4: Servo Motor MG90S

4. System Design and Architecture

Traveler's BCBP, fingerprint, and face are the key points of this study; thus, the system applies three-factor authentication (3FA) for verification. The flowchart shows the main steps which the passage follows in the check-in process. A GUI for the check-in process is designed for passengers. The first phase is to scan the BCBP barcode. The acquired data from BCBP is compared with the airport database; if verification occurs, biometrics phase (fingerprint and face) will be processed. When both biometric data are confirmed, the door will open. The verification process is tested under neutral condition and works excellently. The proposed system software is shown in Figure 5.

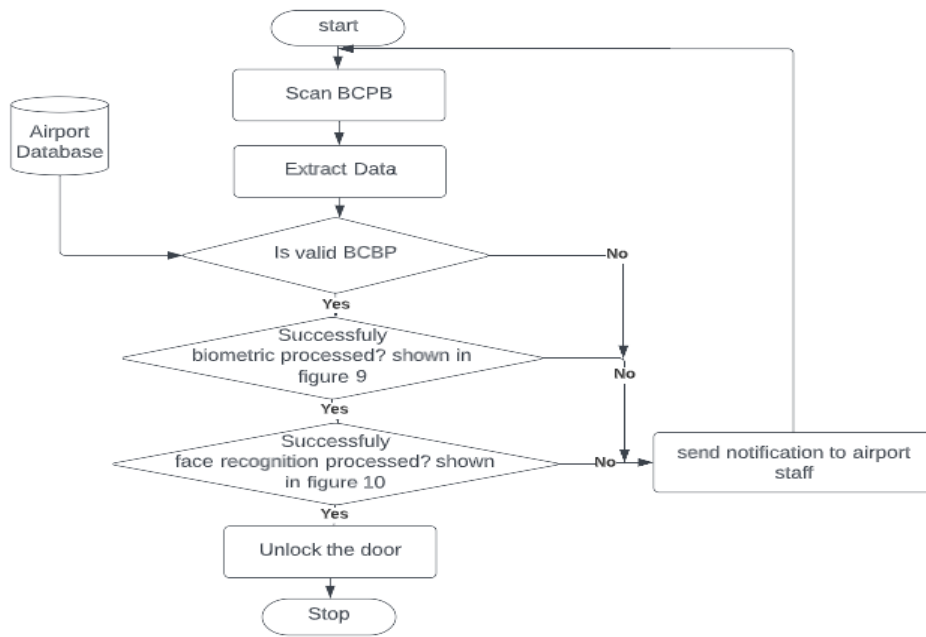


Figure 5: The flowchart of the proposed system

Our system protocol is consisted of a motherboard, three sensors two motor and a monitor. The sensor, motor and monitor are lined through the motherboard. The sensor includes two cameras and one fingerprint. One camera is used to scan BCBP and the other is used to capture the face. Fingerprint sensor is used to record the passenger fingerprint of the thumb. After having

accurate data process confirmation, the two motors are used to open the door. And the monitor connected through Wi-Fi is used to display the data. Figure 6a shows the schematic architecture design of the proposed system and the connection between hardware parts and Raspberry Pi microcontroller, and Figure 6b shows the prototype design of the system.

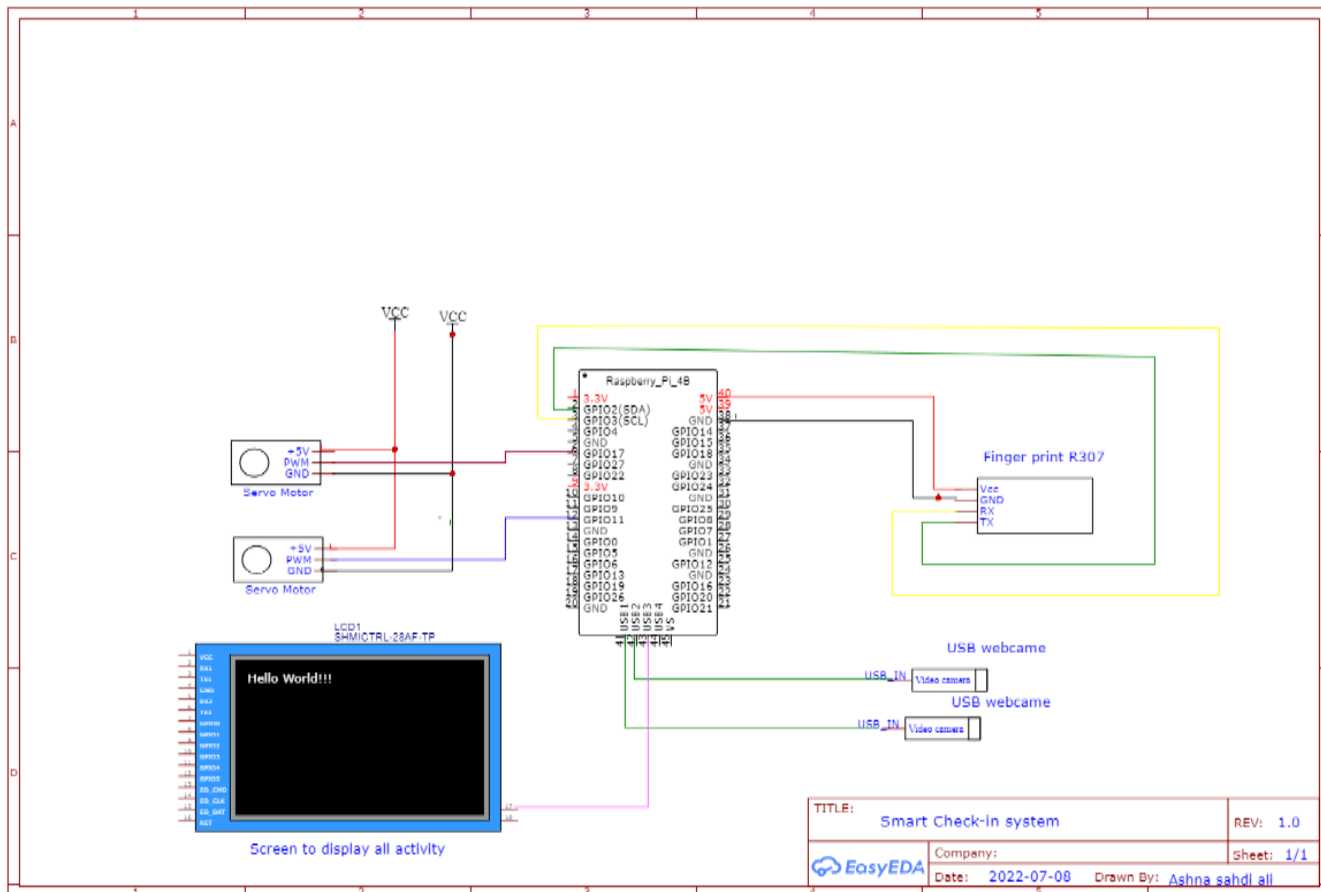


Figure 6a: The hardware components schematic of the smart door system




Figure 6b: prototype design of the system

5. Software requirements

The hardware components, for reading barcode, fingerprint, and facial detector, require programming for them to work properly. The software development includes three different libraries which are discussed below, where two of the libraries are ready-made. However, pdf417 library for reading the barcode needed to be customized.

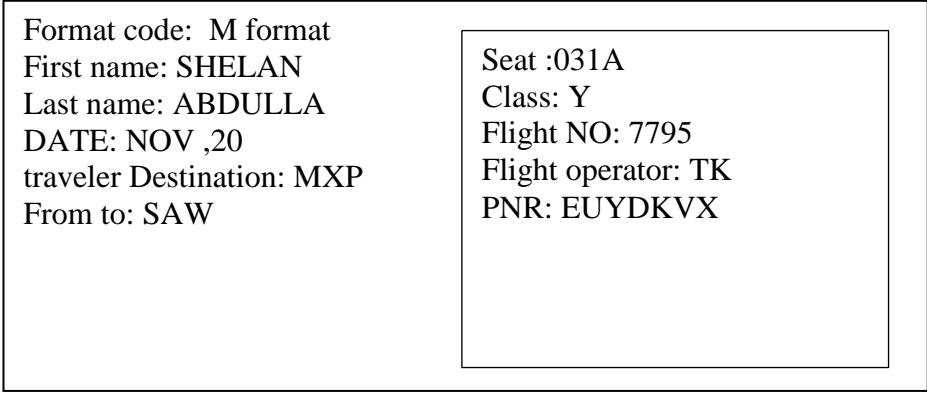
5.1. Barcode detection and reading process

After having the barcode scanned, the barcode capture through open cv will be converted into a string of codes through python program and is designed based on the PDF417 library. The string array will be compartmentalizing into different indexes; each index represents specific data. For instance, the second index coded as (EUYDKVX) indicates PNR (Passenger Name Record), the third index specifies the to/from airport, and stored inside the MySQL database, as shown in Figure 8.



```
M1ABDULLAH/SHELAN EUYDKVX MXPSAWTK 7795 324Y031A0093
15E>518
```

Figure 7: encrypted data obtained from webcam



```
Format code: M format
First name: SHELAN
Last name: ABDULLA
DATE: NOV ,20
traveler Destination: MXP
From to: SAW

Seat :031A
Class: Y
Flight NO: 7795
Flight operator: TK
PNR: EUYDKVX
```

Figure 8: Real traveler data obtained from modified PDF library

5.2. Fingerprint Process

The fingerprint process depends on the traveler's barcode; the system checks the status of the barcode and decides on one of the following situations:

- 1- Unchecked barcodes (new barcodes): for unchecked barcode the system search for a traveler's fingerprint in the database, if there is a fingerprint match, the system will proceed directly to face process. If otherwise (first time system user), the system saves the traveler's fingerprint and proceeds to face process.

- 2- Checked barcodes (barcode used previously): for checked (used) barcode the system search for a traveler's fingerprint in the database, if there is a fingerprint match, the system will proceed directly to face process. If otherwise, it means a fake person uses previously registered barcode; immediate telegram notification will be sent to airport staff.

The flowchart represents the fingerprint process for the traveler check-in system shown in Figure 9.

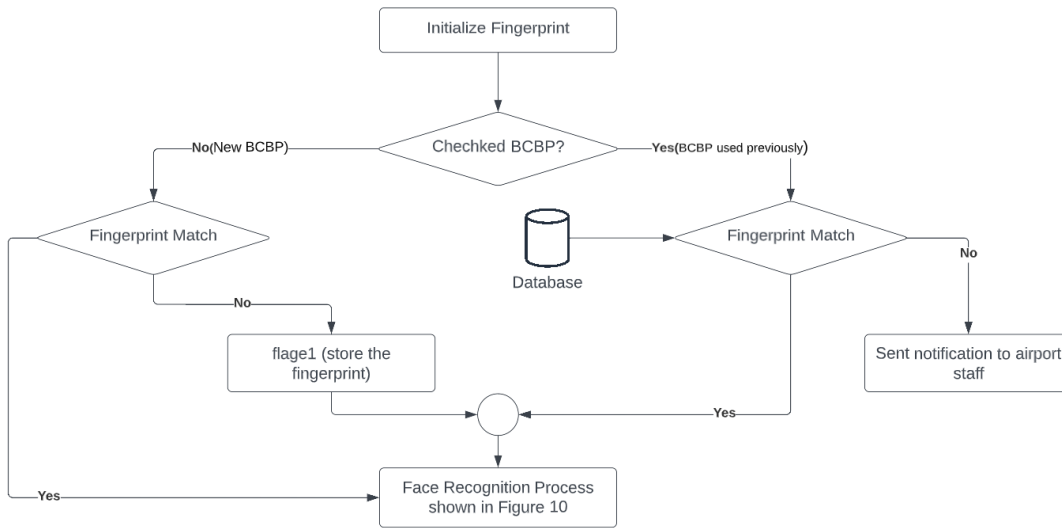


Figure 9: fingerprint process for the traveler check-in system

5.3. Facial Detection and Recognition Process

After face is detected as shown in Figure 11, the camera will capture the face. Open CV haar cascade and Dlib library are ready-made package and they are used for detection and recognition of the face; Figure 10 shows the flowchart for face detection and recognition process for the traveler check-in system.

After the face detection process, there will be two cases:

- 1- Unrecognized face of new traveler: When the face of the traveler is not recognized in the database and if no fingerprint is detected in the database, the user will be registered as a new record, the door is

unlocked. Otherwise, the person is fake and a Telegram notification will be sent to the airport staff that indicates the same barcode is used by two different persons.

- 2- Recognized face: When the traveler's face is recognized, it means he/she used the system before and if there is a match of the fingerprint on the database, the face is updated and the door is unlocked. If otherwise (face not matched with face), the person is fake and a Telegram notification will be sent to the airport staff.

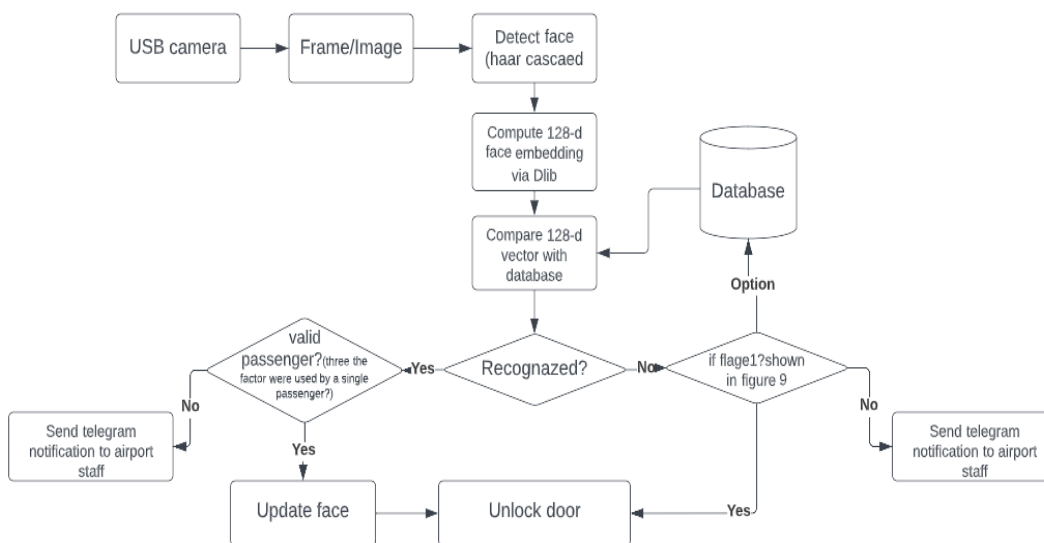


Figure 10: face detection and recognition Process for the traveler check-in system

5.4. KAA platform for User Authentication

KAA is the enterprise IoT platform for data collection and visualization. The system is continuously monitored through the KAA platform. Furthermore, the KAA platform is also used for statistical purposes.

6.Results and Discussion

In this study, an IoT security door is proposed and implemented based on the use of the Raspberry Pi 4B, where two webcams were used. One of them is for scanning the barcode and the other for capturing the face of the traveler, also an Adafruit fingerprint sensor is attached to the system.

Themes multi-biometric authentication can also be used.

Testing the system with the real-time traveler check-in progresses smoothly and securely. A Pdf417 algorithm decodes the BCBP barcode very effectively. The screen in Figure 11 shows the scanned barcode (BPBC) and the captured data from the barcode. A fingerprint sensor is programmed with a modified version of the Adafruit library tested for 100 travelers and they were satisfactorily authenticated.

The software is developed by using Open-CV python, dilb algorithm, and haar cascade to detect and recognize live stream of the traveler faces; while testing among the travelers, it was able to authenticate the authorize their check-in processes.

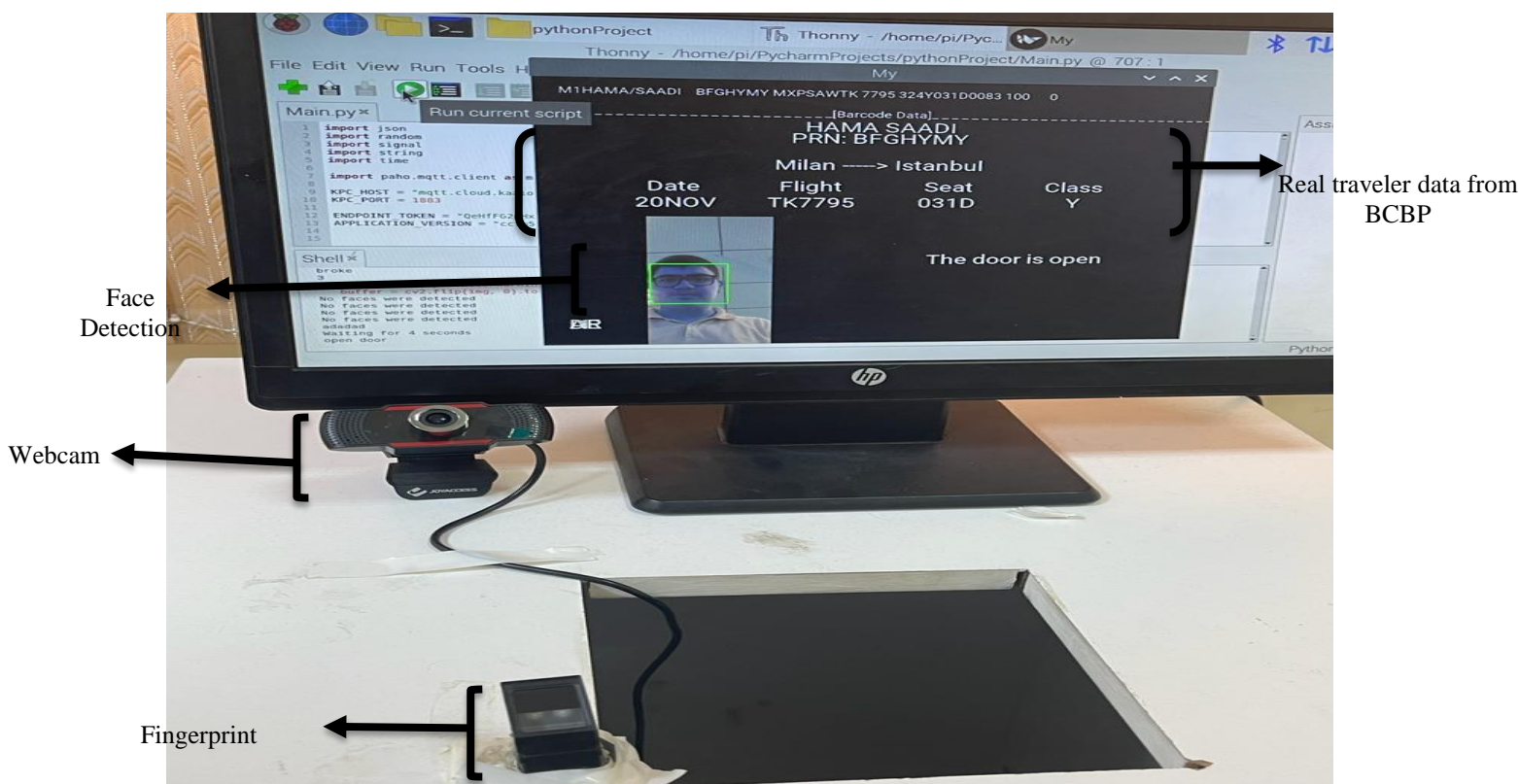


Figure 11: check-in process of a traveler

The status of the check-in process is monitored in real-time with the KAA platform, as shown in Figure 12. The Y-axis represents the number of

the passed travelers and the X-axis represents time of the check-in.



Figure 12: Real time check-in process IoT KAA platform

Table 1 shows the time per passenger in our system and traditional system. As it is shown, our newly designed system takes much lesser time to check-in comparing to the traditional one. The

minimum time for check in per passenger is 40 seconds and its maximum is 80 seconds, while in the traditional systems it takes 60 seconds and 120 seconds per person, respectively.

Table 1: check-in time per passenger

check-in style	minimum time for check in	maximum time for check in
traditional check-in	60 sec	120 sec
our system	40sec	80 sec

A comparison of our proposed system check-in is made with the traditional check-in as seen in Figure 13. The bar-graph shows the number of passengers processed (Figure 13a) and average processing time per passenger (Figure 13b) and average queue time per passenger (Figure 13c). It can be seen that our system has a higher total number of passengers processed in 15 minutes than traditional check-in.

is true that our system has a lower Average Queue Time (AQT) than traditional check-in. Our system, with an AQT of 12 secs, is superior to traditional check-in. This shows that a passenger checking-in with our system spends less time in the queue than a passenger checking-in with traditional check-in system. This proves the superiority and efficiency of operating with our system.

Moreover, our system has a lower APT (Average Processing Time) of 48 sec. than traditional system which has an APT of 100 sec. This means that our system is able to process passengers faster than traditional check-in system. What is more, it

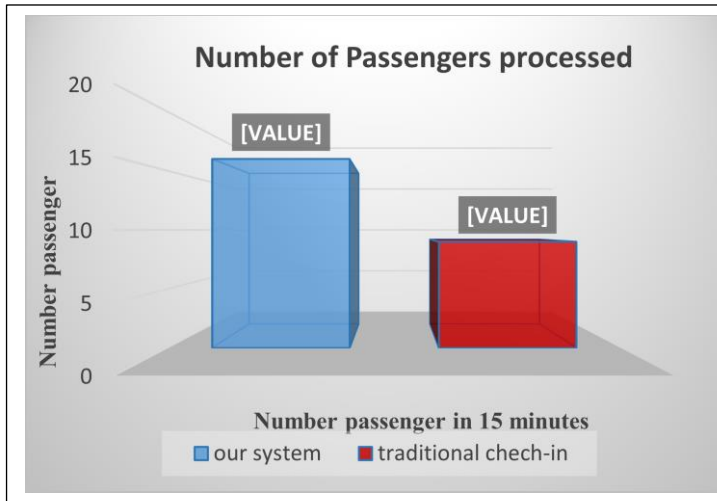


Figure 13a: Number of Passengers processed in 15 min

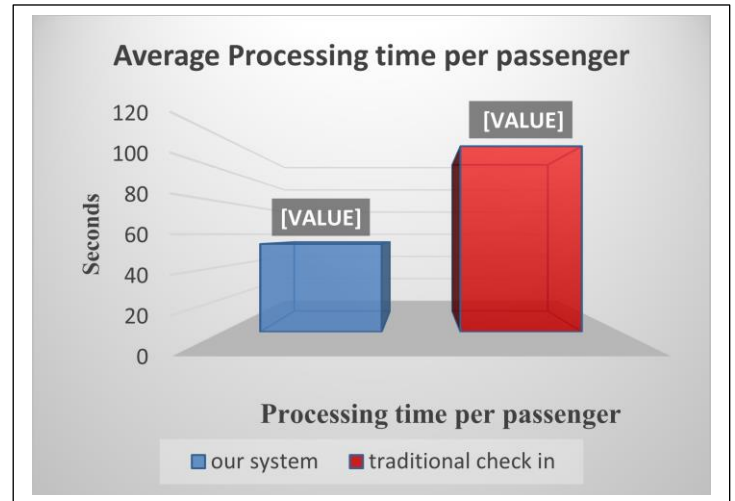


Figure 13b: Average Processing time per passenger in sec

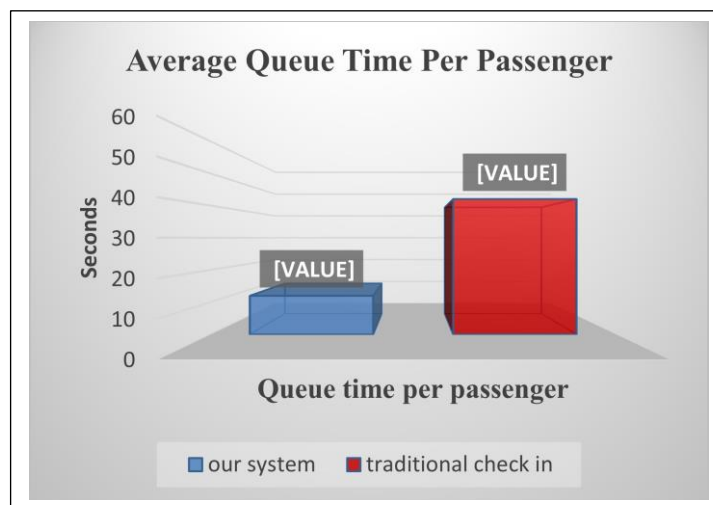


Figure 13c: Average Queue Time Per Passenger in sec

Figure 13: Comparison between the traditional check-in and our system in airport

7. Conclusion

This paper offers an implementation of a low-cost computing system for the check-in system. It simplifies the traveler's experience and reduces the airport check-in hassles. The system stores the history of the travelers at the airports to enable accessing the required information when needed including the number of flights, the destination of travel, and the date and time of travel and return. The paper shows the integration of OpenCv library, dlib algorithm, and Adafruit algorithm with Raspberry Pi to build IoT applications.

The proposed system forms a secure airport check-in system to control the check-in system using three authentication factors, which are face,

fingerprint, and barcode inputs. As shown above, this newly designed system has the ability to perform much more efficiently and accurately comparing to traditional check-in system. On the other hand, the system can also reject unauthorized travelers to pass from the airport with informing the airport staff. The system can also recognize travelers who have travelled before. It uses the requested biometrics, face and fingerprint, against the stored data in the database that assists the airports to control every travel.

References

ABDALLA, P. A. & VAROL, A. ADVANTAGES TO DISADVANTAGES OF CLOUD COMPUTING

- FOR SMALL-SIZED BUSINESS. 2019 7TH INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY (ISDFS), 2019. IEEE, 1-6.
- ANWAR, S., RISKIAWAN, H., HARIONO, B., SETYOHADI, D., KURNIASARI, A. & HAKIM, M. AUTOMATIC SECURITY SYSTEM ARCHITECTURE FOR SMART GREENHOUSE USING FACE RECOGNITION APPROACH. IOP CONFERENCE SERIES: EARTH AND ENVIRONMENTAL SCIENCE, 2022. IOP PUBLISHING, 012058.
- ARUN, P., PALAKKAD, K. & NAMBOODIRI, S. 2018. FINGERPRINT BASED SECURITY SYSTEM FOR VEHICLES. *INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY*, 4, AVAILABLE-ONLINE, AT: [HTTPS://WWW.IJARJIT.COM/MANUSCRIPTS/V](https://www.ijarjit.com/manuscripts/v).
- BALUPRITHVIRAJ, K., BHARATHI, K., CHENDHURAN, S. & LOKESHWARAN, P. ARTIFICIAL INTELLIGENCE BASED SMART DOOR WITH FACE MASK DETECTION. 2021 INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE AND SMART SYSTEMS (ICAIS), 2021. IEEE, 543-548.
- CHAUDHARI, U., GILBILE, S., BHOSALE, G., CHAVAN, N. & WAKHARE, P. SMART DOORBELL SECURITY SYSTEM USING IOT. INTERNATIONAL CONFERENCE ON SCIENCES AND TECHNOLOGY (NO. 4228), 2020.
- ELECHI, P. 2022. FACIAL RECOGNITION BASED SMART DOOR LOCK SYSTEM. *FUPRE JOURNAL OF SCIENTIFIC INDUSTRIAL RESEARCH*, 6, 95-105.
- GAPONCIC, D., FILIPESCU, M., COTELNIC, E. & BUGAIAN, P. 2021. SMART LIGHT MANAGER.
- GOUNDER, M. P., & SHARMA, N. A. (2021). CONTACT TRACING APPLICATION FOR AVIATION- A DIGITAL INOCULATION. 2021 *IEEE ASIA-PACIFIC CONFERENCE ON COMPUTER SCIENCE AND DATA ENGINEERING (CSDE)*, 1-8 DOI: 10.1109/CSDE53843.2021.9718447.
- HASSAN, Q. F. 2018. *INTERNET OF THINGS A TO Z: TECHNOLOGIES AND APPLICATIONS*, JOHN WILEY & SONS.
- HUSNI, M., CIPTANINGTYAS, H. T., HARIADI, R. R., SABILLA, I. A. & ARIFIANI, S. J. T. 2019. INTEGRATED SMART DOOR SYSTEM IN APARTMENT ROOM BASED ON INTERNET. 17, 2747-2754.
- IATA. (2018). *BAR CODED BOARDING PASS (BCBP) IMPLEMENTATION GUIDE*. CANADA: INTERNATIONAL AIR TRANSPORT ASSOCIATION.
- ISMAEL, Y. S., SHAKOR, M. Y. & ABDALLA, P. A. DEEP LEARNING BASED REAL-TIME FACE RECOGNITION SYSTEM.
- JAHNAVI, S. & NANDINI, C. SMART ANTI-THEFT DOOR LOCKING SYSTEM. 2019 1ST INTERNATIONAL CONFERENCE ON ADVANCED TECHNOLOGIES IN INTELLIGENT CONTROL, ENVIRONMENT, COMPUTING & COMMUNICATION ENGINEERING (ICATIECE), 2019. IEEE, 205-208.
- JEONG, S. J. I. J. O. I. V. 2022. DESIGN ON NOVEL DOOR LOCK USING MINIMIZING PHYSICAL EXPOSURE AND FINGERPRINT RECOGNITION TECHNOLOGY. 6, 103-108.
- KUMAR, J., KUMAR, S., KUMAR, A. & BEHERA, B. REAL-TIME MONITORING SECURITY SYSTEM INTEGRATED WITH RASPBERRY PI AND E-MAIL COMMUNICATION LINK. 2019 9TH INTERNATIONAL CONFERENCE ON CLOUD COMPUTING, DATA SCIENCE & ENGINEERING (CONFLUENCE), 2019. IEEE, 79-84.
- LIU, Q., LI, H., HU, Y., & SUN, L. (2018). A CHECK-IN SYSTEM LEVERAGING FACE RECOGNITION. *IEEE CONFS ON INTERNET OF THINGS, GREEN COMPUTING AND COMMUNICATIONS, CYBER, PHYSICAL AND SOCIAL COMPUTING*, 412-418.
- LEOPOLD, E. J. I. A. R. 2008. BAR CODED BOARDING PASSES (BCBP). 12.
- MISHRA, S., MOHITE, O. & KHARAT, S. 2022. SMART DOOR LOCK SYSTEM USING ARDUINO. *INTERNATIONAL RESEARCH JOURNAL OF MODERNIZATION IN ENGINEERING TECHNOLOGY AND SCIENCE*
- PINJALA, S. R. & GUPTA, S. REMOTELY ACCESSIBLE SMART LOCK SECURITY SYSTEM WITH ESSENTIAL FEATURES. 2019 INTERNATIONAL CONFERENCE ON WIRELESS COMMUNICATIONS SIGNAL PROCESSING AND NETWORKING (WISPNET), 2019. IEEE, 44-47.
- PRATHAPAGIRI, D. & KOSALENDRA, E. 2021. WI-FI DOOR LOCK SYSTEM USING ESP32 CAM BASED ON IOT. *THE INTERNATIONAL JOURNAL OF ANALYTICAL EXPERIMENTAL MODAL ANALYSIS*, XIII.
- PRITY, S. A., AFROSE, J. & HASAN, M. 2021. RFID BASED SMART DOOR LOCK SECURITY SYSTEM. *AMERICAN JOURNAL OF SCIENCES ENGINEERING RESEARCH*, 4.
- RAHAMAN, M. F., AL NOMAN, M. A., ALI, M. L. & RAHMAN, M. 2021. DESIGN AND IMPLEMENTATION OF A FACE RECOGNITION BASED DOOR ACCESS SECURITY SYSTEM USING RASPBERRY PI.