

Electronic Passport Verification System using IOT

K.Pooja¹, K.L.S.M.Likhitha², K.Ujwala³, B.Vamsy Krishna⁴

^{1, 2, 3} U.G Student, Department of Electronics and Communication Engineering, SR Gudlavalleru Engineering College, Andhra Pradesh, India.

⁴Assistant Professor, Department of Electronics and Communication Engineering, SR Gudlavalleru Engineering College, Andhra Pradesh, India.

Abstract - In the Past, verification of passport control at airports involved manual checks and was time-consuming. Another disadvantage of this type of passport verification is that it is very easy to duplicate or forge. The proposed system helps to verify passports using an electronic passport validation system. This type of verification helps reduce duplicate passports that can lead to illegal activities. The overall time consumption can be reduced and the efficiency of the e-passport can be increased. This e-passport technology using Internet of Things (IOT) provides wireless identification using different tags for authorized and unauthorized persons. This system is used to verify the identity of passport holder. This avoids the forgery of data and manual work with respect to the traditional passport verification system. Passport control checks the passenger's passport using an embedded e-passport with a QR scan. These electronic passports serve to enhance security and help airport authorities to identify the troublemakers or the persons who are performing anti-social elements.

Keywords: Raspberry-pi Pico, ESP 32 Camera, Red LED, Green LED, Buzzer.

1. INTRODUCTION

A digitized file that integrates security measures to verify the identity of the passport holder is an e-passport. Biometric passports are intended to strengthen border security, boost privacy protection against identity fraud and theft by ensuring authentication of the document bearer [1]. The system for issuing this biometric type of passports has been operationalized in several European countries. It is the responsibility of the ICAO to define the criteria and rules along with regulations that are to be followed by biometric passports [2]. The criteria incorporate biometric features such as facial image, fingerprint, an iris image, and other biometrics with the RFID technologies to be applied and the Public Key Infrastructure (PKI) [3]. The demand for more reliable authentication methods must be deployed since the level of protection and authentication imposter has been raised. The new standardized biometric includes biometric features for instance facial, fingerprint, and iris recognition strengthen the safety mechanisms. While an electronic passport with biometrics is a very advanced method of authentication, it can extend to many privacy issues and threats. RFID is a system that transfers identifying

information from an electronic tag by applying radio waves. It is prone to remote attacks as the information stored in the RFID chip is transmitted wirelessly. A passport is an official travel document issued by a government that contains a given person's identity. It provides the benefit of travelling to different countries. In general, this passport certifies the personal identity of the holder along with their nationality. The standard passports contain the user data i.e their full name along with photograph, date of birth, location, signature of holder, and the expiration date of the passport. In general the passports are given by national government itself. However certain subnational governments are proposed to issue the passports to the holders who are present with in their areas as residents. A passport holder is can be allowed inside the country where they have received the passport, though some holders may not be the full citizens of that particular nation. A passport itself does not create any individuals rights in the country or oppose the rights that are issuing by the country in any manner. Some passports which is provided to the holder having a passport related status as either diplomat or other official, entitled to the rights such as having immunity against prosecution or any arrests. Many nations planning to issue electronic passports which can be machine-readable and is difficult to theft the data. Currently, there are an approximate of 150 jurisdictions present which are issuing electronic passports. Previously issued passports will get expired based on expiry date which is given by government authority.

1.1 Background

In the past years, the passport holder will have the passport which consisting of overall data about the holder. This information include full name, date of birth, nation, expiry date of the passport, signature etc. However, as the increase in technology is producing several problems to the humans. This is one of the problem among them where the individual data is being theft by the frauds and the data is using by them for various criminal activities. In order to overcome those fraudulent activities e-passport verification system is being implemented. However manual testing can also be decreased.

1.2 Aim of the Project

The aim of the project is to reduce the illegal activates that are performing by the passengers. The Electronic passport is

an enhanced version of older passport to provide stronger security to individual identity authentication. This provides the security by elimination of duplicate passports and can eliminate data tampering and it is easy for the border control authorities to monitor the incoming and outgoing passengers.

1.3 Methodology

The system process for the verification of each passport holder will be provided with some QR codes for authentication purposes and to protect the passport holder's data. When the holder checks in near the airport, he should scan his QR'S and if the QR code matches the codes of the embedded system, then the passenger is marked as an authorized holder. Therefore, the green LED lights up for identification. If the QR code does not match the built-in QR, the red LED will light up along with the alarm buzzer. Therefore, it is said that these are unauthorized users; the relevant department will take strict action against them.

1.4 Significance of the work

This proposed system can be an excellent tool to keep yourself along with the data safe and serves as a helpful tool for protecting your data. This e-passport verification is used to validate the passport holder in easy manner. This avoids forgery and manual work associated with traditional passport verification system.

These are some of the main reasons for accepting e-Passports over the general passport :

- a. Security and protection of information stored in passport.
- b. Lesser chances of theft of individual data.
- c. Enhanced features compared to older passport.
- d. Privacy protection and Minimum chances of forgery.

2. LITERATURE SURVEY

To improve safety and protection at every country border, several countries have adopted biometric passports in compliance with the ICAO electronic passport guidelines during the years 2004-2005 [1]. The biometric passport evolves on the basis of the ICAO standard has shown that it strengthens the biometric passports system with the consolidation of the MRTD biometric Wireless Microchip. An e-passport is an important requirement used for travelling to international countries by almost all individuals. It is created by binding a electronic passport to RFID system known as an electronic microchip. This chip acknowledges the information recognized by the electronic biometric passport and helps to read the data by an appropriate e-passport readability system built at the border control point [7]. This electronic biometric passport defines the option of facial recognition to be exchanged for machine-assisted validation internationally through biometric technology. Because of

these factors, the technological and practical consideration of implementing the biometric technique in MRTDs is favored. It also considers the possibility that states can opt to carry supplements in order to identification and verification the iris, the fingerprint, the palm print, and face recognition. Due to global interconnectivity, the significance of national defense, border protection, and security has evolved rapidly from a national security perspective. To distinguish and safeguard against illegal immigrants, implementation includes the necessary authentication of the traveler. The importance of incorporating new e-passport components, such as biometric data to find an authorized person has been introduced [6]. In the government sector, biometric technologies are evolving more rapidly in terms of higher precision and citizens' security in both verification and identification [2]. Bill Gates projected that the use of the biometric system

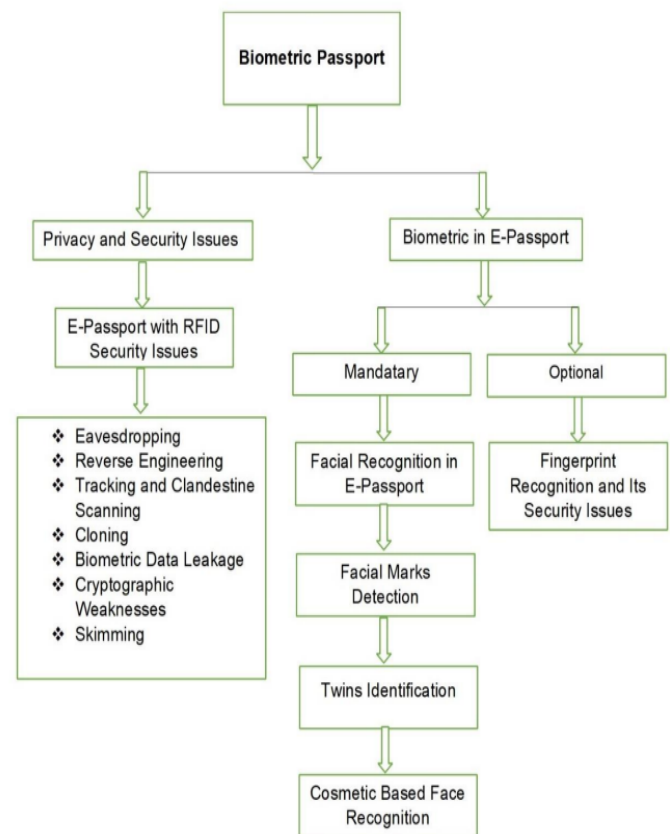


Figure 1: E-passport and its security issues

For human characteristics, such as fingerprint, voice, and face recognition will be the most significant development in the successive decades of IT during the PC Week online on October 8, 1997. The European Union submitted an electronic passport that was conceived to be the most required feature of IT in the European countries in August 2006. Privacy, confidentiality, identity, and data are the methods suggested by Achilles Heel that lead to potential misapplication. A major biometric safety report, 2B or not

3. BLOCK DIAGRAM

From Fig 2, we can understand that the overall setup is required to verify the holder is an authorized person or unauthorized person. Here each component has its operation to perform and in order to produce the result

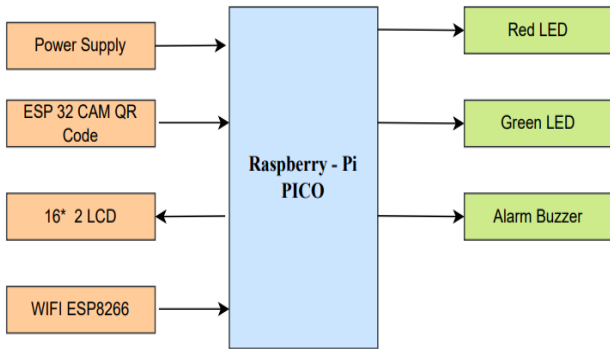


Fig 2: Block Diagram

4. FLOW CHART

Fig3 indicates the operation which is happening by using the system, After QR scan the results are displayed on screen. Hence the authorized and Unauthorized persons can be identified and further actions can be taken based on the data

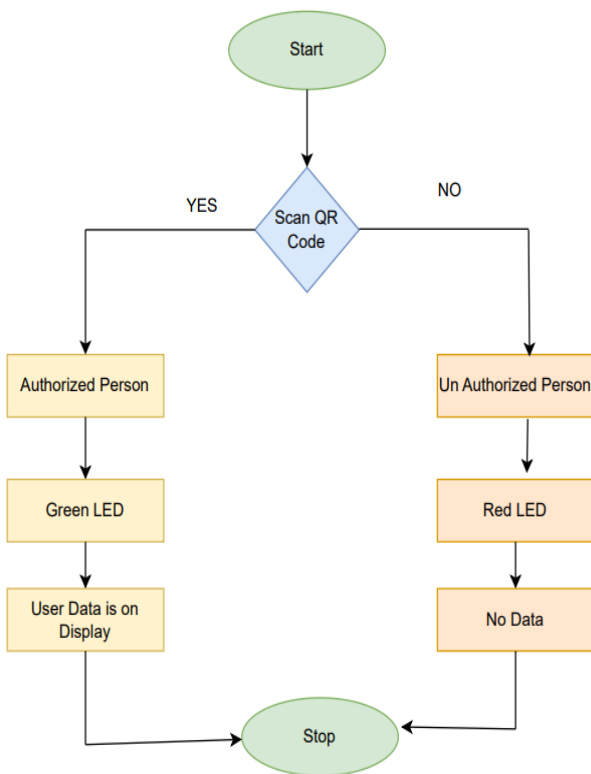


Fig 3: Flow Chart

5. RESULT AND ANALYSIS

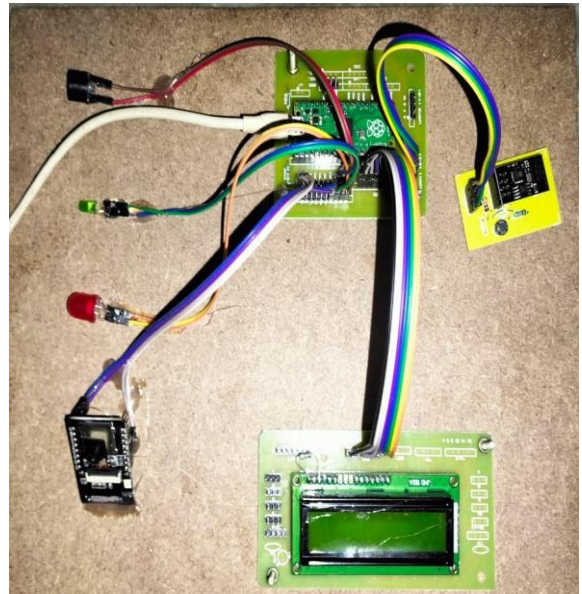


Fig 4: Electronic Passport Verification System using IOT Initial Setup

Figure 4. represents the overall implementation of the system. This system detects the authorized and unauthorized users and give appropriate alerts based on identification.



Fig 5: Circuit Implementation after Power supply Turn on

From Figure 5, we can understand that the LCD displays e-passport verification system and wi-fi module searching for a wi-fi connection. Now the system is ready to scan QR codes.

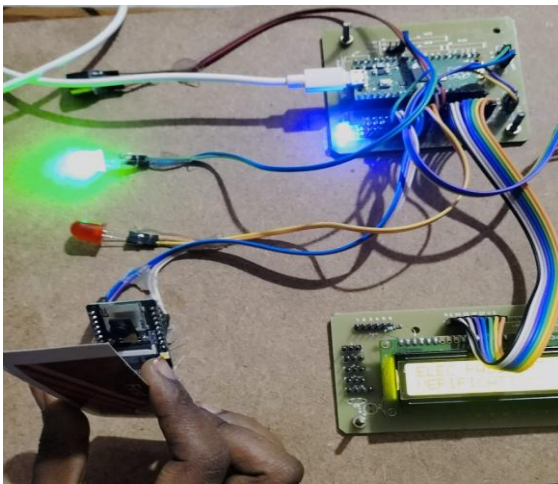


Fig 6: QR Scan glows green LED for Authorized Passport Holder

From Figure 6. we can understand that when we scan QR which is given to the user we can identify whether they are authorized or not. The above figure indicates green Led turned on. Hence, it displays the person as an authorized Holder.

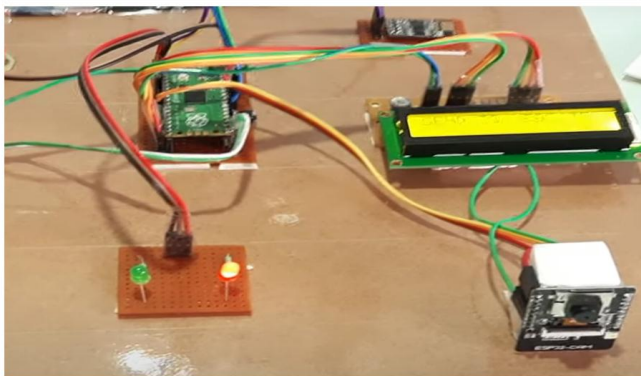
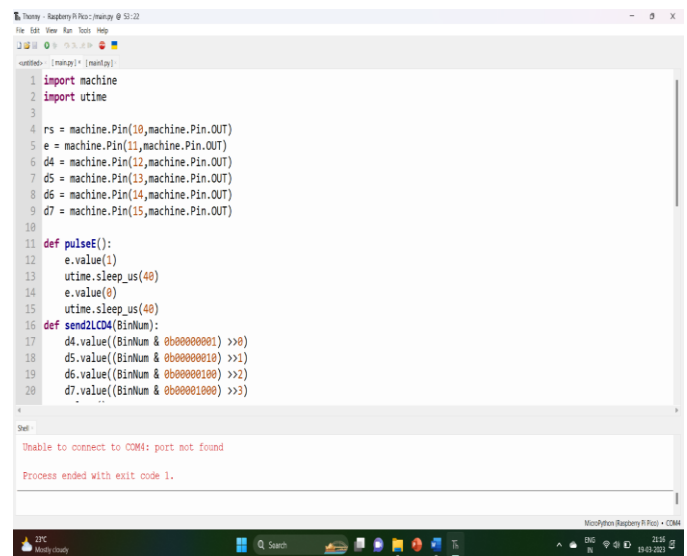


Fig.7: QR Scan glows Red LED for Unauthorized passport Holder

From Fig 7, we can understand that when we scan QR which is given to the user we can identify whether they are authorized or not. The above figure indicates Red Led turned on. Hence, LCD will display person as an unauthorized Holder.

5.1 SOFTWARE RESULTS



```

1 import machine
2 import utime
3
4 rs = machine.Pin(10,machine.Pin.OUT)
5 e = machine.Pin(11,machine.Pin.OUT)
6 d4 = machine.Pin(12,machine.Pin.OUT)
7 d5 = machine.Pin(13,machine.Pin.OUT)
8 d6 = machine.Pin(14,machine.Pin.OUT)
9 d7 = machine.Pin(15,machine.Pin.OUT)
10
11 def pulseE():
12     e.value(1)
13     utime.sleep_us(40)
14     e.value(0)
15     utime.sleep_us(40)
16 def send2LCD4(BinNum):
17     d4.value((BinNum & 0b00000001) >>0)
18     d5.value((BinNum & 0b00000010) >>1)
19     d6.value((BinNum & 0b00000100) >>2)
20     d7.value((BinNum & 0b00001000) >>3)
    
```

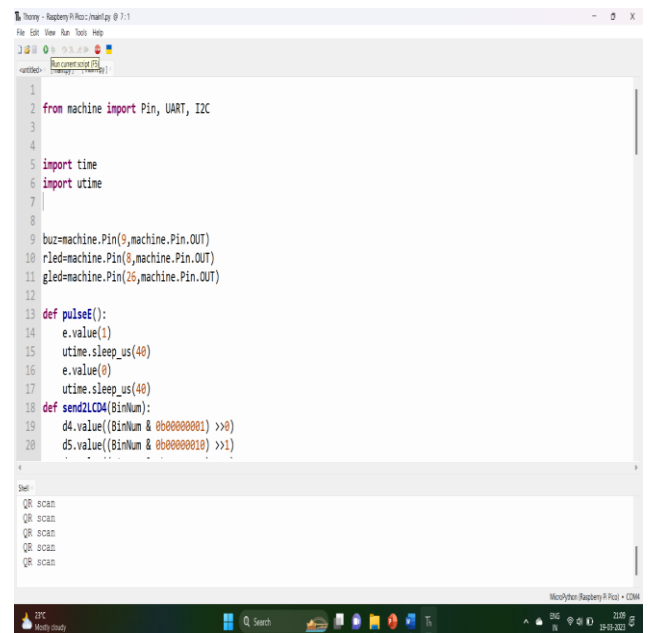
Shell

```

Unable to connect to COM4: port not found
Process ended with exit code 1.
    
```

Fig 8: Initial Setup

Above Figure 8, indicates the results that are obtained we click run button in thorny python IDE before the wi-fi module is connected. We can see that Unable to connect to COM4: port not found error occur.



```

1
2 from machine import Pin, UART, I2C
3
4
5 import time
6 import utime
7
8
9 buz=machine.Pin(9,machine.Pin.OUT)
10 r1ed=machine.Pin(8,machine.Pin.OUT)
11 g1ed=machine.Pin(16,machine.Pin.OUT)
12
13 def pulseE():
14     e.value(1)
15     utime.sleep_us(40)
16     e.value(0)
17     utime.sleep_us(40)
18 def send2LCD4(BinNum):
19     d4.value((BinNum & 0b00000001) >>0)
20     d5.value((BinNum & 0b00000010) >>1)
    
```

Shell

```

QR scan
QR scan
QR scan
QR scan
QR scan
    
```

Fig 9: Setup after Wi-Fi Module connection

From figure 9, We can understand that after connecting wi-fi module to the hotspot of our mobile. The system will run the code and provide the data as QR Scan on the LCD to scan the respective QR's of the holders to identify the authorized and unauthorized users.

6. CONCLUSIONS

Now a days, this is used in many of the applications such as transportation, healthcare, industry, etc. This type of technology along with Internet of Things (IOT) ease wireless identification using QR codes provided by passengers. This project works with the electronic passport verification system to verify the identity of passport holder. This avoids the forgery and can reduce the manual work associated with the traditional passport verification system. This system makes it clear that all passport data will be stored electronically, reducing the risk of forgery, identity duplication or identity theft, which are the main problems presented by the traditional paper passport booklet. The system also proved to continuously update the cardholder information in the system without any problems. They can enter the electromagnetic field zone by showing QR and within a fraction of a seconds, the details of the card will be on the system monitor. The system thus saves time and provides better border control.

6.1 Future Scope

This project can be further customized by adding biometrics and fingerprints related to passport holder. In this way, the safety of passport holder can be further increased. With increased security, there will be less chance of falsifying the passport holder's details. To reduce the time required for passport verification and validation.

7. REFERENCES

- [1] Kundra, Shivani, Aman Dureja, and Riya Bhatnagar. "The study of recent technologies used in E-passport system." 2014 IEEE global humanitarian technology Conference-South Asia Satellite (GHTCSAS). 26-27 Sept. 2014, IEEE, Trivandrum, India, 2014, pp. 141-146. DOI: 10.1109/GHTCSAS.2014.6967573.
- [2] Ntungwe, Vera Njeng. "ILO Convention 185 on seafarers' identity document thirteen years after entering into force: analysing implementation challenges and future outlook." Master's Thesis, World Maritime University, Malmö, Sweden, 2018.
- [3] Caviedes, Alexander. "European integration and the governance of migration." *Journal of Contemporary European Research*, Vol.12, no. 1, 2016, pp. 552-565.
- [4] East African Community. "Ministry of East African Community Affairs in Conjunction with the Directorate of Citizenship and Immigration Control M of IA." East African Community, Kampala, Uganda, 2012.
- [5] Morosan, Cristian. "Customers' adoption of biometric systems in restaurants: An extension of the technology acceptance model." *Journal of Hospitality Marketing & Management*, Vol. 20, no. 6, 2011, pp. 661-690.
- [6] Pons, Alexander P., and Peter Polak. "Understanding user perspectives on biometric technology." *Communications of the ACM*, Vol. 51, no. 9, 2008, pp. 115-118.
- [7] Miltgen, Caroline Lancelot, Aleš Popovič, and Tiago Oliveira. "Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context." *Decision Support Systems*, Vol. 56, 2013, pp. 103-114. 113
- [8] Ng-Kruelle, Grace, Paul A. Swatman, J. Felix Hampe, and Douglas S. Rebne. "Biometrics and e-Identity (e-Passport) in the European Union: End-user perspectives on the adoption of a controversial innovation." *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 1, no. 2, 2006, pp. 12-35.
- [9] Habibu, Taban, Edith Talina Luhanga, and Anael Elikana Sam. "Evaluation of Users' Knowledge and Concerns of Biometric Passport Systems." *Data*, Vol. 4, no. 2, 2019, pp. 1-17. doi:10.3390/data4020058
- [10] ICAO. Machine Readable Official Travel Documents – MRtds with Machine Readable Data Stored in Optical Character Recognition Format. Technical Report, Doc 9303, Volume I, 3rd edition, Part III, 2008.
- [11] ICAO. Machine Readable Passports – Passports with Machine Readable Data Stored in Optical Character Recognition Format. Technical Report, Doc 9303 Part I, Volume I, 6th edition, Montreal, Canada, 2006.
- [12] ICAO. Machine Readable Passports. Technical Report, Doc 9303, Part I, Volume II, 6th edition, Montreal, Canada, 2006.
- [13] ICAO. Request for Information (RFI) 2007/2008. Technical report, Technical Advisory Group on Machine Readable Travel Documents, Canada, March 2007.
- [14] Davida, George I., and Yvo G. Desmedt. "Passports and visas versus IDs." In *Workshop on themApplication of Cryptographic Techniques and related theory*, pp. 183-188. Springer, Berlin, Heidelberg, 1988
- [15] Davida, George I., and Yvo G. Desmedt. "Passports and visas versus IDs." *Computers & Security*, Vol. 11, no. 3, 1992, pp. 253-258.