International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

ELECTRONIC PASSPORT SYSTEM USING NODE MCU

B Sreelatha[1], D Venkata Rami Reddy[2], M Sowjanya[3]

[1,2,3] *Geethanjali College of Engineering and Technology, Hyderabad, India*

ABSTRACT

Physical passport verification is time-intensive and error-prone. This paper explains the process of eliminating forgery and time wastage in confirming passports. RFID tags contain a unique code with special coding designed to access the user's knowledge of the information.

An electronic passport, often known as an "E-Passport," is an identification document that contains biographic or biometric data about the holder. It is included within the Radio Frequency Identification Tag's chip, which is capable of incorporating cryptographic technique. The passport offices are currently issuing E-Passports, which equates to more than 50% of all passports being issued worldwide. The successful implementation of biometric techniques in documents such as E-Passports aims to strengthen border security by reducing the possibility of a copy or fake passport and establishing without hesitation the identity of the documents' holder. The primary aim of this paper is to use RFID technology to access a passport holder's passport information. An RFID card is provided to the authorized person for this function. This card includes a built-in circuit used for storing data. As a result, the information stored in this card is referred to as the person's passport details.

Keywords: Biometric data, Cryptographic technique, E-Passport, fake passport, RFID

1. INTRODUCTION

An “E-passport” is a passport which features microchip technology. An integrated circuit stores the data that is essential in verifying the identity of the passport holder. This data include the personal data found on the data page of the passport, the biometrics of the passport holder, and the unique chip identification number. Electronic passports have an integrated chip, generally embedded in the cover page of the document that contains personal information of the document owner. a contactless (or RFID) technology has been chosen for the inspection process. An E-passport, or a digital passport, is a combined paper and electronic passport that contains biometric information that can be used to authenticate the identity of travellers. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or canter page, of the passport. Electronic passports include contactless chip which stores personal data of the passport holder, information about the passport and the issuing institution**.**

There are many cases where forgery passports are processed illegally without government authorization, and this illegal activity is carried out by private consultancies where they process the passport that looks like the original passport that is published by the central government. The main purpose of this technology is to reduce the use of forgery passports, as well as the use of paper passport booklets, and to shorten the waiting time. So,

the actual procedure is that the government issues the RFID card which contains the biographic as well as biometric information of the passport holder and the data is stored in the cloud. The RFID card consists of unique ID. This unique ID is generated because we can have same names and sometimes same initials, so to differ from person to person; we use unique IDs, user name, address, contact details and biometric information such as fingerprints for verification. First, we will read the RFID card so that the details are displayed on the LCD screen which is visible to the user for verifying purpose and we use RFID reader which is use to read the data present inside the RFID chip and this data is verified with the data present in the database. and it asks the user to place the finger within the time limit, and it verifies the details with those present in the database. If the fingerprint and unique ID match, a message is displayed on the screen stating that access is granted as the user is using an authorised passport. We used a servo motor to replace an airport gate; if access is granted, the gate rotates, indicating the gate is opened, and after a certain time limit, the gate closes, indicating that the user has successfully completed the verification. If the details do not match, then the user is using a fake passport, and a message is displayed on the screen stating that access is not granted.

2. PROPOSED TECHNOLOGY

- The RFID card is read using an RFID reader, which sends the information to Node-MCU.
- The details are displayed on the LCD Screen.
- If the unique Id matches, it asks you to place your finger for two-factor authentication.
- As a two-factor authentication, we used a fingerprint sensor. Permission is granted and the user is allowed to pass through the gate if both the unique ID and fingerprint matches with the details in the database.
- If the unique Id does not match, then it denies the permission and displays that the user is using a fake passport.
- The collected information is stored in the Firebase.

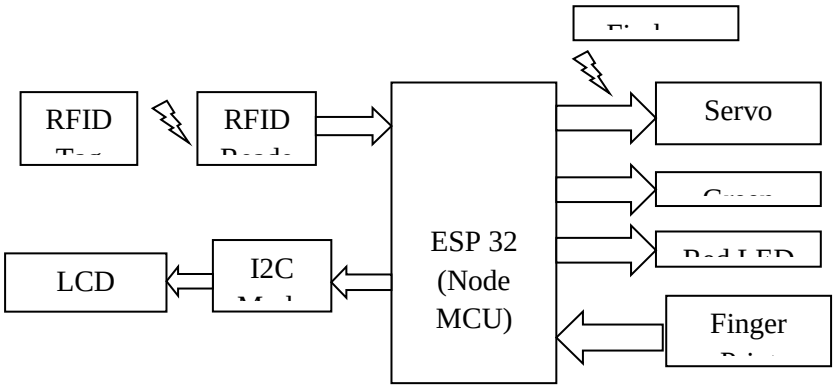

Fig 1: Block diagram

International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

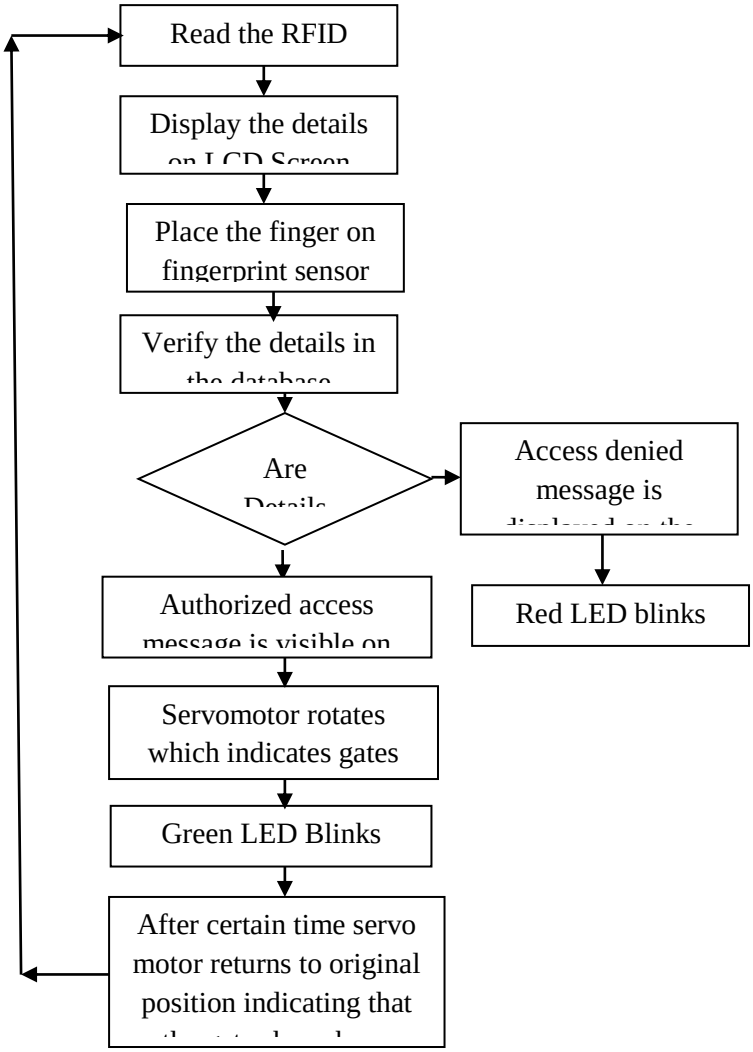

Fig 2: Flow Chart

3. APPLICATIONS

This technique can be used in airports, colleges and government offices. Japan, United States of America, Norway, and Spain, incorporate RFID tags into passports to store information (such as a photograph) about the passport holder and to track visitors entering and exiting the country.

4. LIMITATIONS AND ADVANTAGES

4.1 Advantages

- It reduces threat of identity fraud by increasing security features in it.
- It embeds biometric information such as fingerprint, iris and face. This information helps to identify individual carrying e-passport.

- It helps in detection of counterfeit documents.
- It makes it very difficult to alter the e-passports. Hence it restricts admission of unauthorized individuals to any country on fake documents.
- It protects privacy of the citizens.
- Tempering of the chip is notified to the system which results into passport authentication failure.
- It can be scanned in few seconds which avoids long wait for passengers.

4.2 Disadvantages

- Contactless RFID embedded chips can be read using radio frequency from few centimetres away. Unprotected chips are subject to clandestine scanning or eavesdropping.
- E-passports use standard ISO 14443 which generates unique chip ID during protocol initiation. Using this unique chip ID, e-passport holder can be tracked by unauthorized parties.
- Digital signatures used in e-passports do not bind data to any particular chip used on passport. Hence it does not offer any defence for passport cloning.
- E-passport supports automation which can lead to biometric data-leakage and consecutively weakens human oversight.

5. CONCLUSION

This paper gives a clear idea about the electronic passport system, which is much more beneficial for airports and universities. It also reduces the documentation burden and the time consumption. We analyzed the potential uses of RFID in identifying documents. The most important feature of this project is security, which will make the system centralized. The security of the system can be further increased by adding more biometric information, such as a palm scan, an iris scan, a digital signature, and other active authentication methods to the passport system.

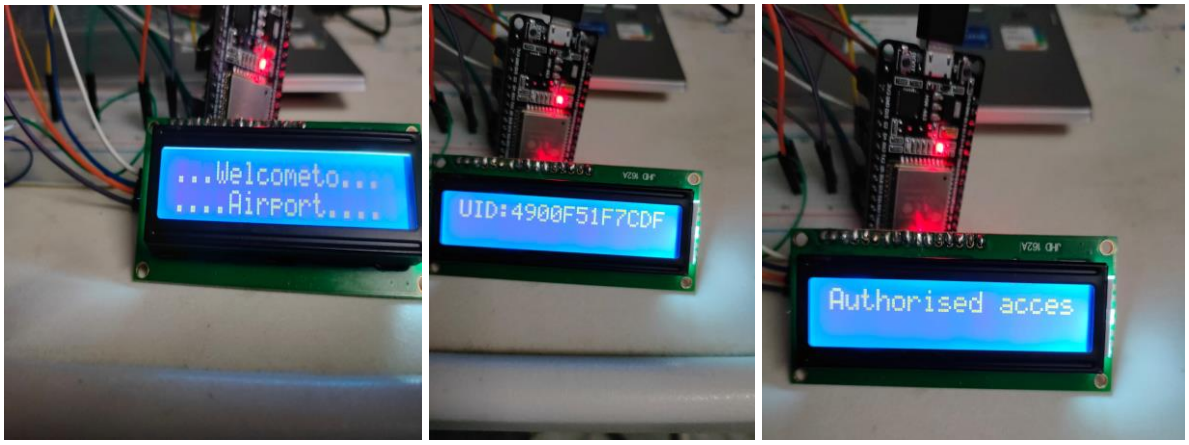

Fig 3: Outcomes on LCD Screen

6. FUTURE SCOPE

One card Policy throughout country and also the security of the system can be further increased by adding biometric information such as fingerprints, palm scan, iris scan, digital signature and other active authentication

ISSN: 2454-9665

in the passport system. We can even implement iris identification or face detection using open cv so that there is more security and there would be less chance of processing of fake passports and everything will be digitalised in future.

REFERENCES

[1]. G. Matthew Ezovski, Steve E. Watkins, The Electronic Passport and the Future of Government-Issued RFID-Based Identification 2007 IEEE International Conference on RFID Gaylord Texan Resort, Grapevine, TX, USA March 26-28, 2007

[2]. Rima Belguechi, Patrick Lacharme, Christophe Rosenberger, Enhancing the privacy of electronic passportsˆ, International Journal of Information Technology and Management (IJITM), Vol.11, No. (1/2), pp.122 ˆa 137, 2012.

[3]. Marci Meingast, Jennifer King, and Deirdre K. Mulligan," Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond," Journal of Communications. 2, no. 7, pp. 36-48, 2007.

[4]. Nikita Maria, RFID chips and EU e-passports: the end of privacy? International conference on information law and ethics 2012, Ionian University-INSEIT, June 29-30, 2012.

[5]. Kumar, V. K. Narendira; Srinivasan, B. Design and Development of e-passports using Biometric Access Control System International Journal of Advanced Smart Sensor