iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42846

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

E-Passport System

Dhanashree Wadnere[1], Shravani Belgi[2], Rutuja Devkute[3], Sakshi Jadhav[4], Bhavika Rathod[5]
[1, 2, 3, 4, 5]*Department of Computer Science & Engineering, Sandip Polytechnic, Nashik, India*

Abstract: ***The Electronic passport is the digital version of the paper passport to provide stronger identity authentication. Passport verification and checking which a very time-consuming process. To be ease identity checks, lessen the amount of human errors, protect against manipulation of travel documents and improve border security issues hence, new passport turned out to be much more intrusive than the traditional one. The proposed system simplifies this process with RFID card where the unique identification number is stored which corresponds to the information of the person. The information includes the name, nationality, address etc. along with attach the copy of the required certificates required according to the application. The information is transferred to computer with the help of RF transceiver. It may also include some other features such as buzzer for audio visual indication and system to lock the door. This proposed system uses Radio Frequency Identification (RFID) is a technology that uses wireless communication for identification purposes. The key characteristic that differentiates one RFID application from another is the purpose of identification.***

Keywords: RFID Radio Frequency Identification, E-Chip Electronic Chip

I. INTRODUCTION

Advancements in technology have created the chance of larger assurance of correct travel document possession, however, some issues relating to security and effective- ness stay unaddressed. Electronic passports have notable a good and quick readying all around the world since the International Civil Aviation Organization the globe have adopted standards whereby passports will store biometric identifiers. The em- ployment of life science for identification has the potential to create the lives easier, and therefore the world folks board a safer place. The aim of biometric with RFID Tag suggests that e-passports are to stop the misappropriated entry of a person into a selected country and limit the employment of counterfeit documents by a lot of correct identification of a person. This paper analyses the fingerprint biometric e- passport style. These papers concentrate on the privacy and private security of bear- ers of e-passports, the particular security profit countries obtained by the introduction of e-passports victimization fingerprint recognition systems. The research worker analyzed its main crypto graphical features; the fingerprint life science presently used with e-passports and regarded the encompassing procedures. Research worker- centered on vulnerabilities since anyone willing to bypass the system would select a constant approach. On the contrary, only wishing on them could create a risk that didn't exist with previous passports and border controls. The paper conjointly pro- vides a security analysis of the e-passport victimization fingerprint biometric with RFID tags that are supposed to produce improved security in protective biometric info of the e-passport bearer.An E-Passport is an ID document that possesses connected biometric data of its bearer. It's embedded in the RFID tag that is accomplished by crypto graphical practicality. The triple-crown implementation of biometric techniques in documents like E-Passports aims to the strength of border security by decreasing the chance of the document's holder. The e-passport additionally offers substantial edges to the rightful holder by providing a lot of refined suggests that of confirming that the passport belongs thereto person which it's authentic, while not privacy.

II. PURPOSE AND MOTIVATION

In the case of normal passports which are we using nowadays, to establish a positive match between the travel document and the person who presents it, there are four typical applications:

1) Each time a traveller enters or exits a State, his identity can be verified against the image created at the time his travel document was issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any advance passenger information (API) system.
2) Two-way check The travellers current captured biometric image data and the biometric template from his travel document (or from a central database), can be matched to confirm that the travel document has not been altered.
3) Three-way check The travellers current biometric image data, the image from his travel document and the image stored in a central database can be matched (by constructing biometric templates of each) to confirm that the travel docu- ment has not been altered. This technique matches the person with his pass- port and with the database recording the data that was put in that passport at the time it was issued.

©IJRASET: All Rights are Reserved

4) Four-way check A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the three-way check with the digitised photo- graph on the data page of the travellers passport.

In the second case application for an ePassport there are two basic applications:

a) The end users biometric data, generated by the enrolment process, can be used in a search of one or more biometric databases (identification) to determine whether the end user is known to any of the corresponding systems (for ex- ample, holding a passport under a different identity, having a criminal record, holding a passport from another State).

b) When the end user collects the passport or visa (or presents himself for any step in the issuance process after the initial application is made and the biometric data is captured) his biometric data can be taken again and verified against the initially captured biometric data.

The primary reasons for worldwide acceptance of e-Passports over the conventional passports are:

- Secure Identification of the passport holder.
- Minimal chances of forgery of biometric information stored in the passport.
- Enhanced privacy protection.
- Greater protection against identity theft.

III. MODELING AND ANALYSIS

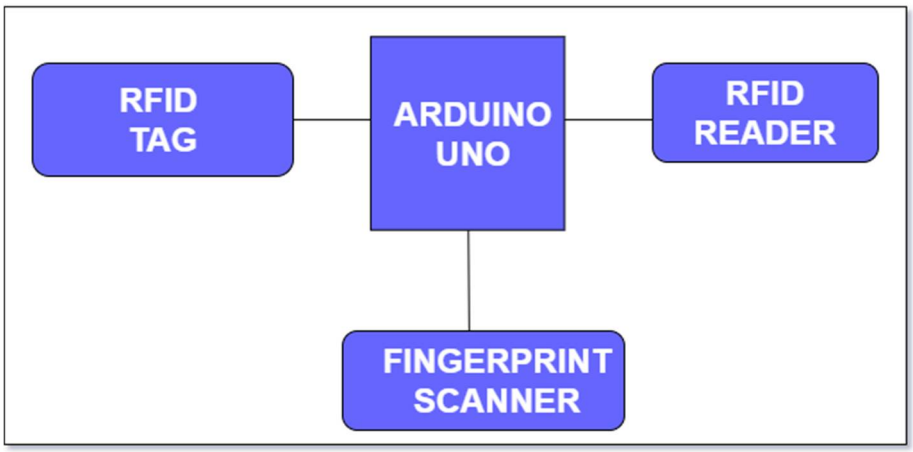


Figure 1: Block Diagram

IV. BACKGROUND

A passport is an official travel document issued by a government that contains a given person's identity. It enables its holder travel to and from foreign countries and to access consular assistance while overseas. The document certifies the personal identity and nationality of its holder.[1] Standard passports contain the full name, photograph, place and date of birth, signature, and the expiration date of the passport. While passports are typically issued by national governments, certain subnational governments[a] are authorized to issue passports to citizens residing within their borders.

Many nations issue (or plan to issue) biometric passports that contain an embedded microchip, making them machine-readable and difficult to counterfeit. As of January 2019, there were over 150 jurisdictions issuing e-passports. Previously issued non-biometric machine-readable passports usually remain valid until their respective expiration dates.

A passport holder is normally entitled to enter the country that issued the passport, though some people entitled to a passport may not be full citizens with right of abode (e.g., American nationals or British nationals). A passport does not of itself create any rights in the country being visited or obligate the issuing country in any way, such as providing consular assistance. Some passports attest to the bearer having a status as a diplomat or other official, entitled to rights and privileges such as immunity from arrest or prosecution.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

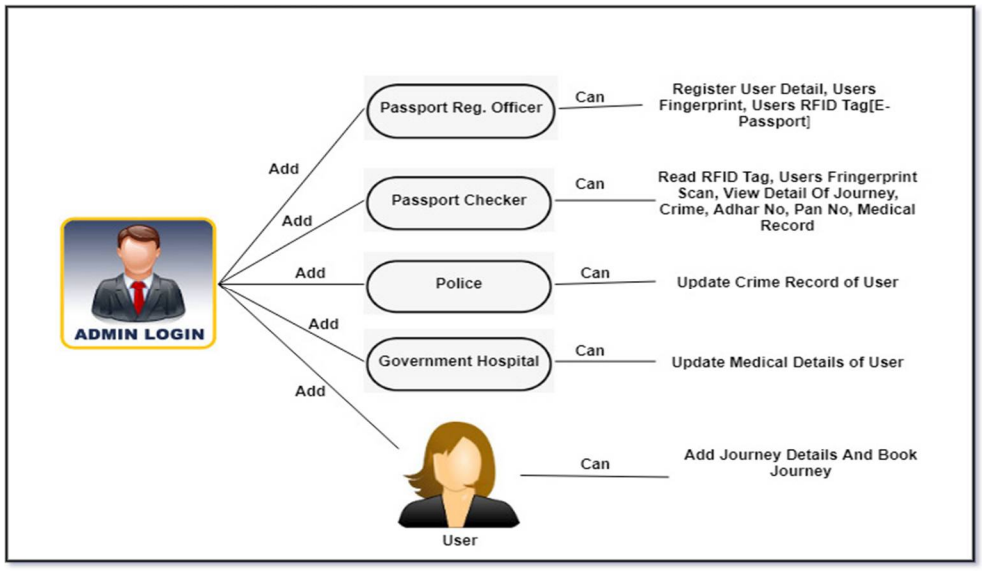


Figure 2: Use case Diagram

V. DISCUSSION

This project is based on java. This project supports all types of web browsers.Active internet connection. The system gives advice or alerts user immediately.The System gives accurate results.Interactive, minimal delays, safe info transmission

VI. RESULT

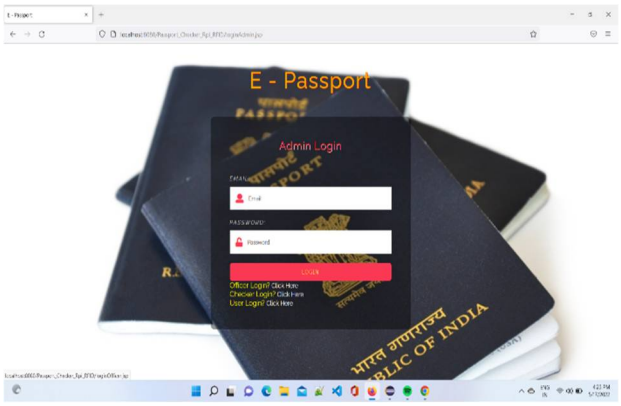




Figure 3: Output

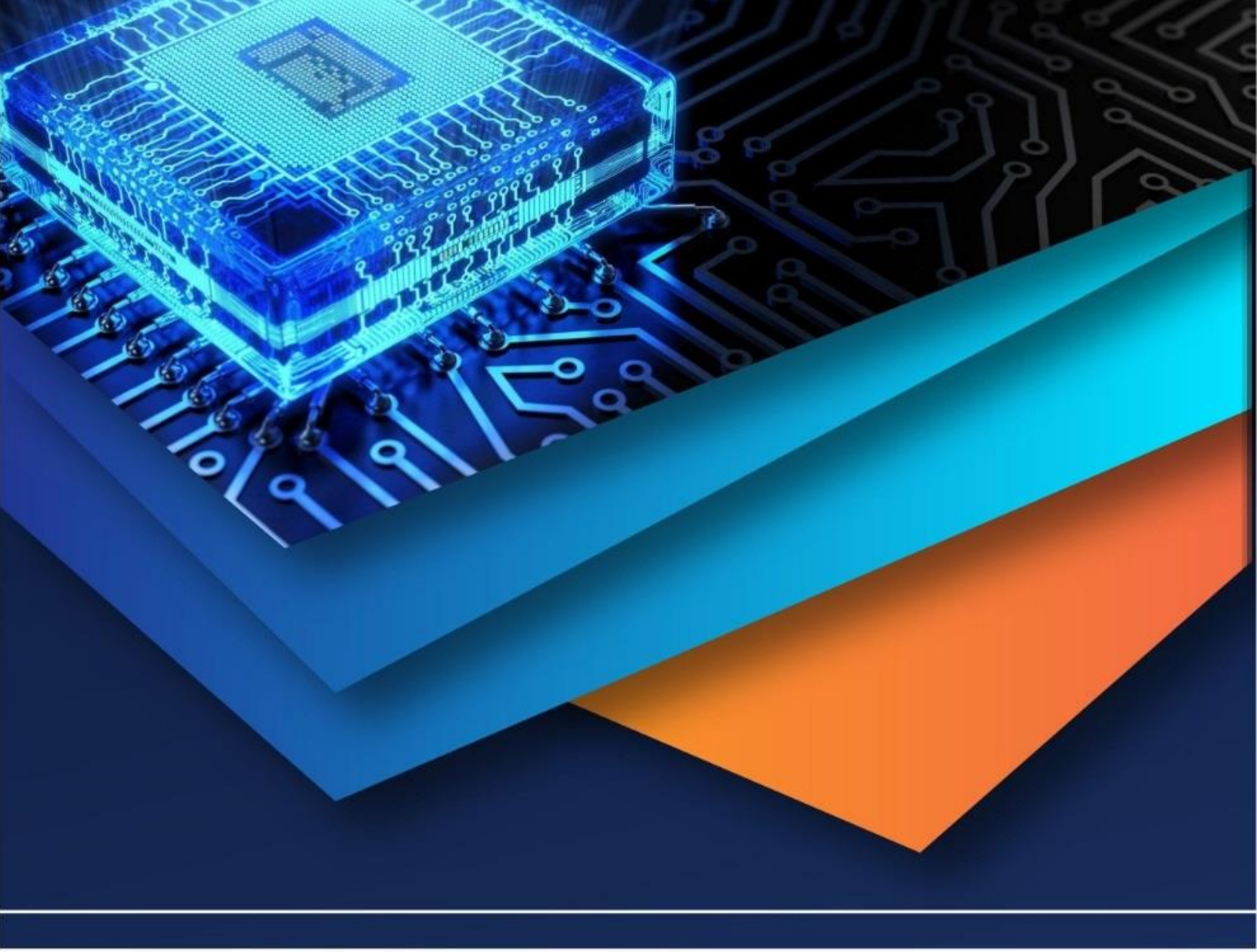
VII. CONCLUSION

The project has analyzed the major current and potential uses of RFID in identifying documents. The important feature of this project is secu- rity and time wastage involved in validation of passports. Inclusion of RFID technology into machine readable documents will improve their robustness against identity theft.

REFERENCES

[1] Keerti Srivastava, Amit K. Awasthi and R.C.Mittal Biometric based RFID tag mutual authentication protocol defending against illegitimate access -2018, Malaya Journal ofMatematik[102-106].
[2] Gualberto Aguilar, Gabriel Sanchez, Karina Toscano, Moises Salinas, Mariko Nakano, and Hector Perez. 2007. Fingerprint Recognition.In Proceedings of the Second International Con- ference on Internet Monitoring and Protection(ICIMP '07). IEEE Computer Society, Washington, DC, USA, 32-. DOI: https://doi.org/10.1109/ICIMP.2007.18
[3] Y. A. Badamasi, The working principle of an Arduino," 2014 11th International Conference on Electronics, Com- puter and Computation (ICECCO), Abuja, 2014, pp. 1-4.URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?
[4] Ivanov, Vladimir I. and John S. Baras. Authentication of fingerprint scanners. 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). (2011): 1912-1915.
[5] S. Kundra, A. Dureja and R. Bhatnagar, The study of recent tech- nologies used in E-passport system, 2014 IEEE Global Humanitarian Technology Conference - South Asia Satellite (GHTC-SAS), Trivan- drum, 2014, pp. 141-146.
[6] M. Arapinis, T. Chothia, E. Ritter, and M. Ryan, "Untraceability in the applied pi-calculus," in Proceedings of the 1st Int. Workshop on RFID Security and Cryptography., 2009, to appear.
[7] Piotr Porwik, "The Biometric Passport: The Technical Requirements and Possibilities of Using", Biometrics and Kansei Engineering, International Conference - ICBAKE on 2009, pp. 65.
[8] Dr Albert B. Jeng, Elizabeth Hsu, And Chia-Hung Lin Sponsor: "Should and How CC be used to evaluate RFID based Passports‖
[9] K. Nohl and D. Evans, "Privacy through noise: a design space for private identification," in Annual Computer Security Applications Conference (ACSAC 2009), 2009.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)