IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 1, January 2023

DOI: 10.17148/IARJSET.2023.10137

E-Passport Authentication using IoT and AI

Shamitha bijoor[1], Sinchana MN[2], Sushmitha S[3], Theerthana SR[4], Saleem S Tevaramani[5]

Student, ECE, KSIT, Bangalore, India[1-4]

Assistant professor, ECE, KSIT, Bangalore, India[5]

Abstract: The technique of passport verification which is currently used in the airports involves manual checking and it is time consuming. Another major issue with the conventional paper passport is that, it can be forged or duplicated easily. The proposed system consists of two level of authentication. In the first level of authentication, the RFID (Radio Frequency Identification) module is used which involves both RFID tag and RFID reader. The second level of authentication is the face recognition. In this the passport holder's face is captured and is verified. The two levels of authentication increase the level of security and safety. This system is proposed in order to decrease the duplicating of the passports which leads to various illegal activities. Also, the verification duration is reduced with the use of e-passport. The face recognition is implemented which increase the efficiency of the e-passport. The technologies such as RFID, IoT and face recognition can be used effectively to replace paper passports by portable e-passports.

Keywords: Authentication, e-passport, face recognition, IoT, RFID.

I. INTRODUCTION

RFID is a technique which makes use of the principle of electromagnetic fields for transferring the data from an electronic tag usually known as the RFID tag. The RFID technology is used in various applications such as monitoring the attendance in schools, industries etc, in shopping malls for pricing purpose and in metro. In order to save the time involved in manual technique of verifying RFID cards are used which are contactless based on the type of readers. RFID module comprises of two units that is the tag and the reader. The card is provided to the passport holder which is swiped against the reader and the contents of the card is verified. The e-Passport provides the legitimate possessor with significant advantages by offering a more advanced method of verifying identity. It authenticates the passport, if it is valid and belongs to the individual named on it, without putting privacy at risk.

The integrity of passports is improved by the need to match the information on the chip to the information stored in the database and to the physical characteristics of the holders like the face. It makes it possible for verification which is assisted by the machine and biographic information to confirm the identity of travellers. Paper passports have the disadvantage of having no privacy and being physically accessible by everyone.

The current study assists the passport examiner in automatically check the passenger's passport using electronic passport validation system. When the RFID tag is used, when a passport bearer approaches an RFID scanner, data is read from and displayed on the LCD (Liquid Crystal Display). If the information matches then it shows a valid message based on the data in the programme memory. Otherwise, an invalid message will be displayed. Suppose, the face does not match, the LCD will show an error and a message will be sent to authorities through GSM (Globally System for Mobile communication).

II. LITERATURE REVIEW

Vignesh et al [1] In this paper explains about the cutting-edge framework. The predominate risks in this framework is extra documentation and less security. The proposed system makes use of an eager card which has the name, date of birth, ethnicity and UID range for identify confirmation. The passenger's locations the cardboard into the cardboard peristerite UID is perused and later on checked. The advantages of the proposed framework is less documentation work, visa obstacle data is predicted appropriately, no compelling motive to deliver each one of the files .The proposed system eliminates the drawback of documentation overall performance of e- passport is increased.

Ayesha Sarwar et al [2] In the proposed study, biometric verification of passports is done using RFID. The study aims at increasing the security and privacy of a passport holder. It stores data electronically therefore avoiding forging of data and can also avoid illegal entry of travellers. They make use of an antenna, transponder and a transceiver which in turn uses radio waves to communicate with each other. When a transponder enters the zone, the RFID reader captures the information and sends it to the computer or any other host device.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 1, January 2023

DOI: 10.17148/IARJSET.2023.10137

Al-Ajeely [3] In this paper, verification of passport was done using Internet of things (IOT). The proposed system uses fingerprint as the biometric data for the verification. The fingerprint recognition was done by using fingerprint sensors which used to detect the fingerprints based on the level of surface. The fingerprint sensor used in this model was able to store memory of the fingerprints of about 3000 templates. This model was able to avoid forgery and manual work associated with verification of passport. It also updated the traveller's information constantly in the system.

Kumar el at [4] This model makes use of RFID chip which is integrated on the cover of passport This electronic passport provides privacy and eliminates the security risks. It can eliminate the problems of mismatched computer records and stolen identities. This study aims to find out to what extent the integration of biometric identification information into passports will improve their robustness against identity theft. Biometrics can never be forged as everybody will have unique identities like fingerprints, iris etc…

Nirmala.M el at [5] The proposed system focuses in avoiding the forgery and also the involvement of humans in passport verification. The e- passport is embed with RFID tag fingerprint sensor and also involves gsm for OTP. The system strengthens the security and aids in avoiding the fraud. The RFID tag works on the principle of electromagnetic fields for the transferring of the data from an electronic tag to identify an object or a person by means of Storing information electronically. As the passenger swipes the RFID tag that is red by the RFID reader and sends a signal to the board. The board identifies the ID of passenger. The gsm and the fingerprint sensor are used for identification and authenticates the details.

Deepthi M and dr U Eranna [6] In this study RFID, IOT and Cloud Technology was used for the purpose of identification and verification of a traveller. It was able to produce real time passport monitoring system that can be accessed by other parties. The traveller is given an RFID card that is integrated into the passport. The RFID card can process information just by modulating and demodulating the radio frequency. The details of the traveller are fed into the computer and a unique number is given to each traveller which is being imprinted on the RFID card. The reader reads the data and sends the information wirelessly using IOT and the receiver receives the information and sends the data to the microcontroller which compares the data and matches it with the right data.

Hussain et al [7] In this paper they are trying to secure biometric- RFID systems in organization based on problems like information of owner is not secure enough, RFID system doesn't give the authorization of the user as they are not sure that the authorized user is the one using the RFID card. And also, to rectify problems like duplication and cloning of RFID card. They are trying to prevent and protect by providing security to the authorization system. In the proposed system they have used PUF- physical unclonable function along with AESadvanced encryption system. Further they have used digital watermark in the database to prevent cloning of the card. after issuing card the user has to register their biometrics using mobile device or built-in sensor. They encrypt this using hash value. And then they verify data and hash present in server and when they both match, they proceed to next level. The system also needed the use of PRNG a random number to prevent attacking like digital pickpocketing etc. The proposed system gives security by using, steganography, biometrics, cryptography, and RFID also prevent leakage of sensitive information.

Khan and Junaid Moinuddin [8] In this paper, they have done the passport authentication using RFID technology and biometric information that is fingerprint. Here the person is provided with the RFID card issued by the authorities which consists of the information of the card holder. When the person enters the airport, he needs to present the RFID card where the RFID card reader reads the card, stores the information. In next step the person's fingerprint and verified with the one which stored in database and if it is valid then the person is let inside the airport.

Wimalasiri et al [9] this paper is based on RFID, encryption, signature verification, feature-matching, facial verification. This paper is trying to enhance and strengthen the existing security system of electronic passport. The proposed system methodology includes the first step by issuing passport for first time which includes data collection like user image, signature, name, gender, nationality DOB profession and other required details. The next step is facial image watermarking, this uses four-digit number to embed on the image to enhance security.

Also, next they generate RFID tag using AES algorithm. After generating tags, the required information will be saved in the database. the next step is passport verification which consists of collection of required details and storing them next is verifying the stored RFID information followed by image verification of face which is followed by signature verification. and they also recalculate the watermark and verity it from the database. The conclusion of this paper was they were able to achieve multi stage authentication system by meeting all the expected results.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 1, January 2023

DOI: 10.17148/IARJSET.2023.10137

V.Ravali et al [10] The proposed system mainly concentrates on the issues of paper passport booklets. The main issues are lack of privacy and the provision to reveal the identity to anybody with the physical access to the passport, also the risk of duplicating the passport led to frauds. The system uses RFID card, FID reader, FID module. The principle of this prototype enables details of the passport holder to be stored in the RFID card which is read by RFID reader for identification purpose. The module of RFID contains transmitter, receive recontrol unit and an antenna. The system can be implemented in real time systems like attendance record in company, industries etc.

Snehal Honade et al [11] The proposed system focuses on defining the technique of implementing the program in the system for generating a valid and the electronical identification. The electronic document consists of an attachment which is an electronic mark from the user. This document is also attached with a digital signature. The - passport can be seen as a legal form of authentication. This digital signature and mark are decrypted by an approving machine. This smart card provides easily handled for biometric data user public key and also the account. The system is embedded in RFID chip which makes use of cryptographic functionality. The main principle of this system is to acquire the details of the passenger through RFID and authenticate the person.

Verheul and eric R [12] Here in this paper, they have used RDE technology for the passport validation. This RDE technology works on three protocol that is Basic Access Control, Passive Authentication, Passive Authentication. Here the MRZ information of the card holder is read using MRZ reader and the information is shared with the authorities. After validating the information, a key is generated to the user which is compared with the key generated to the authorities. If it is matching then the person let inside the airport for future process.

[13] In this paper, they have used multiple biometric information like face recognition, iris recognition, palm print recognition, finger print recognition and the website are developed using ASP.NET. Initially the biometric information of the passport holder is verified with the biometric with is stored during issuing the passport. If it matches then then the passport holder should login to the website and should enter all the personal credentials like passport ID, name, DOB, phone number etc. Then this information is validated by the authorities. After verifying all the information, the passport holder is let inside the airport

Kumar et al [14] In this paper, they have discussed that along with biometric information even we can use RFID card in future. Some of the biometrics that can be used are eye, palm, finger print, iris, face etc which can be used for verification of the person. This biometric information which is stored during issuing the passport is compared at the time of travel. Along with this even RFID card can be used for verification.

Battaglia et al [15] This paper makes use of Face Recognition which is a multifactor authentication system for biometric identification with an encrypted RFID tag. It contains dual stage cascading classifier. This model avoids centralized database which is riskier and stores the sensitive data in the RFID. This model also minimizes the False Acceptance and False Rejection rate. The accuracy and speed are improvised and it works in almost real time. The overall cost and architectural complexity are also greatly reduced. The system is fully scalable as adding or removing a traveller from the data does not require any additional calculations or changes in the algorithm. This system also works faster with very low-resolution cameras which further decreases the cost of this model

Arulogun et al [16] In this paper, they have used the RFID technology for the student attendance. Every student is provided with the RFID card which contains his/her information. When he/her comes to school the RFID reader reads each student card. The information of the scanned student is share with the in charge. This is to ensure that he/she has come to the school and to provide attendance.

Kumar et al [17] This paper discusses about the different biometric e-passport design analysis such as face, palm print, fingerprint, and iris etc. It also gives cryptographic analysis of these different biometric e-passport. They are integrating the RFID tag in the passport which is capable of cryptographic functionality. In face recognition, it is commonly used to identify the unique features like eyes, nose, hair, mouth, etc. In face identification, the system first captures the face of the person and then compares it with the photo in the gallery. The type of comparisons made depends on matching algorithm and biometric used. Later the system gives the ordering of identities.

Bogari et al [18] in this paper they are using attach process modelling system to prevent risk by using a comprehensive risk strategy while using RFID card. This paper provides a brief information about the generations of e-passport which have used different mechanisms like passive and active authentication, basic access control, biometric in the first generation and second generation consists of, chip authentication, basic access control, terminal authentication biometric-face, fingerprint, iris print. this paper provides all the vulnerabilities which are both technical and non-technical factors

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 1, January 2023

DOI: 10.17148/IARJSET.2023.10137

in first and second generation. so, this paper acts as reference point for developing comprehensive risk management strategies. they have provided a systematic attack tree which includes data leak, origin authentication and spoofing for data leak they used random and static UID by reverse engineering and tracing. And for spoofing the replay technique for reader and chip. And for origin authentication they used replay to relay method

Belguechi et al [19]: In this paper they have addressed issues like personal biometrics tracking by cross-matching database of biometrics. And a crucial problem like this need's attention. they have presented the different mechanisms that exist. they have stored the finger print as DG3 information bio code which prevents stealing of data. After some time, the bio code will be regenerated with different random number following same steps mentioned above. They have also mentioned about the issues arising from this like key management. The bio code must be seeded before the process. from this they have concluded that it is very difficult to recover the original finger print code.

Sinha and Anshuman [20] The paper proposed discusses the idea of using optical character recognition for encoding the data such as the holder's name, date of birth and other identifying information. Discusses about the threats in the use of epassport which are forging, non- repudiations scheming eaves dropping, illicit verification, imposter, cloning. Makes use of three kinds of authentication that are passive authentication, active authentication and chip authentication. In passive authentication the hash of every data group is solved and stored in secured passport chip and hash verification is done the active authentication makes use of public key. The chip authentication is used in second generation e- passports. The system makes use of different algorithm

m Choi et al [21] : this paper is aiming for reducing demands and security weakness that occurs in electronic passport. they suggest a method for security based on authorization technique and safe key distribution. they have increased stability by using hash lock on reverse of a one-direction hash function to detect damaged electronic passport. They have also executed a kill tag method to block illegal information on server. First the reader has to authenticate the electronic passport by using previously registered key and produce new key and also has a meta-ID sent to the reader by passport using secret key. Now it compares the key sent by reader with the hash value and the meta-ID and provide the personal ID if they both match. Also, they have used super encryption to prevent wiretapping of e-passport.

Chawla et al [22] In this paper, they came up with the RFID technology for the verification of the person. Initially the person is provided with the RFID card issued by the authorities which consists of the information of the card holder. When the person enters the airport, he needs to present the RFID card where the RFID card reader reads the card, stores the information and compares the information which is previously stored in the database. If the information does not match then buzzer is beeped to alert the authorities.

III. PROPOSED METHODOLOGY

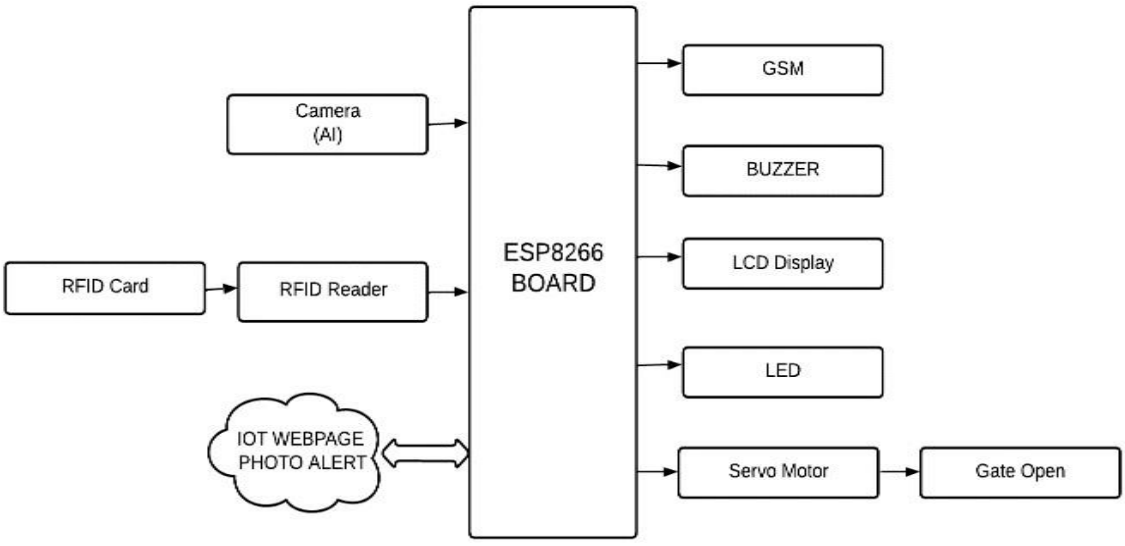

Figure 1 BLOCK DIAGRAM OF E-PASSPORT

DOI: 10.17148/IARJSET.2023.10137

ESP8266 is used as microcontroller board. In which WIFI module is inbuilt. The RFID card is read by the RFID reader, the unique code is stored in the database and the face of the passport bearer is captured using camera and stored in the database. The data is now compared with the database that is stored prior. This comparison process is done using image processing. If the passport bearer is valid then his details are displayed on the webpage and he is sent inside by opening the gates and green led is made to glow. If the passport bearer details doesn't match with the database, then an alert message is sent to the concerned authorities, the photo of the invalid person that is taken in the 2nd verification processes is sent to the concerned authorities. The gates are made to remain closed.

IV. CONCLUSION

In this paper a system based on RFID and IoT is proposed which can be used for replacing the conventional paper passport by an e-passport. Two levels of authentication are proposed where in the first level of authentication RFID module which comprises of RFID tag and RFID reader is used and in second level of authentication face recognition is implemented. IoT technology is implemented for storage and display of details of the passport holder. The two levels of authentication increase the security in airport. The design can be useful in reducing the forgery, duplicating of passport which can lead to illegal activity.

REFERENCES

[1] Vignesh, T., K. K. Thyagharajan, and R. Beaulah Jeyavathana. "An improved Epassport system with secured IoT and wireless communication technology." In *AIP Conference Proceedings*, vol. 2452, no. 1, p. 060001. AIP Publishing LLC, 2022.

[2] Prof. Snehal Honade, Ayesha Sarwar, Suyog Kanawade, Akshay Hawle," Electronic Passport using RFID", *International Journal of Innovative Science and Research Technology,* ISSN No: -2456 –2165, Volume 3, Issue 2, pp 610-613, February – 2022 [3] Al-Ajeely, Y. H. N. "Passport Verification System Development Via IOT Equipment." *Yanka Kupala State University of Grodno, Republic of Belarus*, ISSN No: 2349-6002 , Volume 7, Issue 2, pp 476-482,(2022).

[4] Kumar, VK Narendira, and B. Srinivasan, "Biometric passport validation scheme using radio frequency identification." *International Journal of Computer Network and Information Security* 5, no. 5 (2021): 30.

[5] Nirmala.M, Gayathri.R, Keerthana.R, Deepika.M," EPassport Verification System", *International Journal of Innovative Technology and Exploring Engineering*, ISSN: 2278-3075, Volume-9 Issue-6, pp 1775-1777, April 2020.

[6] Deepthi M, Dr U Eranna, "RFID and IoT Electronic Passport Verification System", International *Journal of Innovative Research in Technology,* ISSN No:2349-6002, Volume 7, Issue 4, pp 336-369, September 2020

[7] Hussain, Mohamed Arusham, Maen T. Alrashdan, and Qusay Al-Maatouk. "SECURE BIO-RFID SYSTEM IN ORGANIZATIONS." *International Journal of Management (IJM)* 11, no. 11 (2020).

[8] Khan, Junaid Moinuddin. "E-Passport Using RFID Tag and Fingerprint Sensor." *IEEE Transactions on Biomedical Circuits and Systems* 14, no. 5 (2020): 1088-1096.

[9] Wimalasiri, Bhagya, and Neera Jeyamohan. "An EPassport System with Multi-Stage Authentication: A Casestudy of the Security of Sri Lanka's E-Passport." *Global Journal of Computer Science and Technology* (2018).

[10] V.Ravali, P.Bhavani, D.Sampath Kumar, " PASSPORT VERIFICATION SYSTEM USING RFID", *Journal of Emerging Technologies and Innovative Research*, Volume 5, Issue 9, pp 106-113, September 2018.

[11] Prof. Snehal Honade, Ayesha Sarwar, Suyog Kanawade, Akshay Hawle," Electronic Passport using RFID", *International Journal of Innovative Science and Research Technology,* ISSN No: -2456 – 2165, Volume 3, Issue 2, pp 610-613, February – 2018.

[12] Verheul, Eric R. "Remote Document Encryptionencrypting data for e-passport holders." arXiv preprint arXiv:1704.05647 (2017).

[13] Kumar, VK Narendira, and B. Srinivasan. "Internet Passport Authentication System Using Multiple Biometric Identification Technology." IJ Information Technology and Computer Science 3 (2013): 79-89.

[14] Kumar, V. K., and B. Srinivasan. "Next Generation Electronic Passport Scheme using Cryptographic Authentication Protocols and Multiple Biometrics Technology." International Journal of Information Engineering & Electronic Business 5, no. 2 (2013).

[15] Battaglia, F., G. Iannizzotto, and L. Lo Bello. "A biometric authentication system based on face recognition and RFID tags.", *I.J Computer Network and Information Security,* Volume 5, pp 30-39, 2013.

[16] Arulogun, Oladiran Tayo, Adeboye Olatunbosun, O. A. Fakolujo, and Olayemi Mikail Olaniyi. "RFIDbased students attendance management system." (2013).

[17] Kumar, VK Narendira, B. Srinivasan, and P. Narendran, "Efficient Implementation of Electronic Passport Scheme using Cryptographic Security along with Multiple Biometrics." *International Journal of Information Engineering and Electronic Business* 4, no. 1 (2012): 18.

DOI: 10.17148/IARJSET.2023.10137

[18] Bogari, Eyad Abdullah, Pavol Zavarsky, Dale Lindskog, and Ron Ruhl. "An analysis of security weaknesses in the evolution of RFID enabled passport." In *World Congress on Internet Security (WorldCIS-2012)*, pp. 158- 166. IEEE, 2012.

[19] Belguechi, Rima, Patrick Lacharme, and Christophe Rosenberger. "Enhancing the privacy of electronic passports." *International Journal of Information Technology and Management (IJITM) Special Issue on:" Advances and Trends in Biometrics". Dr Lidong Wang (IF 0.727)* 11, no. 1/2 (2012): 122-137.

[20] Sinha, Anshuman. "A survey of system security in contactless electronic passports." *Journal of Computer Security* 19, no. 1 (2011): 203-226.

[21] Choi, Yong-Sik, Young-Jun Jeon, and SangHyun Park. "A study on secure protocol using the public key infrastructure approach in an epassport." In *2010 The 12th International Conference on Advanced Communication Technology (ICACT)*, vol. 1, pp. 458463. IEEE, 2010.

[22] Chawla, Vipul, and Dong Sam Ha. "An overview of passive RFID." IEEE Communications Magazine 45, no. 9 (2007): 11-17

