E-Passport Authentication using IoT and AI

Prasad SR
Assistant Professor
Electronics and Communication
Atria Institute of Technology
(VTU)
Bengaluru, India

Prathiksh S
Electronics and Communication
Atria Institute of Technology
(VTU)
Bengaluru, India

Sujay Vittal goudra
Electronics and Communication
Atria Institute of Technology
(VTU)
Bengaluru, India

Vijay kumar L S
Electronics and Communication
Atria Institute of Technology
(VTU)
Bengaluru, India

Abhilash HM
Electronics and Communication
Atria Institute of Technology
(VTU)
Bengaluru, India

Abstract: The method of passport verification that is practiced in airports today is manual checking and is time consuming. Another serious flaw in the traditional paper passport is that, it is easy to forge or duplicate. The suggested system has two level of authentication. In the first level of authentication, the RFID module is utilized which is an RFID tag and RFID reader involved. The second authentication level is the face recognition. Here, the face of the passport holder is scanned and verified. The two authentication levels elevate the degree of security and safety. This system is suggested in a bid to reduce the duplicating of the passports which results in different illegal activities. Further, the verification time is minimized with the utilization of the e-passport. The face recognition is used which enhance the efficiency of the e-passport. The technologies like RFID, IoT and face recognition can be employed efficiently to substitute paper passports by portable e-passports.

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

INTRODUCTION

RFID is a method that utilizes the concept of electromagnetic fields for transferring the data from an electronic tag commonly referred to as the RFID tag. RFID technology is applied in many different applications like attendance monitoring in schools, industries etc, in malls for pricing and in metro. To avoid the time spent on manual technique of checking RFID cards are utilized which are contactless depending on the type of readers. RFID module consists of two units that is the tag and the reader. The card is handed to the passport holder which is swiped against the reader and the content of the card is checked. The e-Passport gives the legitimate owner important benefits by giving a Integrity of passports is enhanced by the requirement to verify the data on the chip against the data in the database and against the physical features of the holders such as the face. It enables verifications which are aided by the machine and biographic data to authenticate the identity of travelers. Paper passports have the drawback of lacking privacy and being physically accessible to anyone.

the present work helps the passport examiner to automatically verify the passenger's passport by the electronic passport verification system. on using the rfid tag, when a passport holder passes in front of an rfid scanner, information is read and shown on the lcd (liquid crystal display). if the information is correct then it displays a valid message according to the data stored in the programme memory. otherwise, an invalid message will be shown. suppose, the face does not match, the lcd will indicate an error and a message will be sent to authorities via gsm (global system for mobile communication).

LITERATURE REVIEW

1. Kumar & Babu, Is concerned with the IoT system structure and infrastructure. Presents a scalable, cloud-based, multi-layer security framework through RFID, TLS encryption, and digital certificates to provide secure data transmission and authentication across borders. It's especially useful if you're doing network or protocol design in your project.

2. Zhang & Liu , Focused on deep learning-based biometric authentication (CNNs), with high accuracy in real-time verification. This will be most applicable if your project deals with image processing, biometric verification, or AI integration, particularly in adverse real-world conditions.

3. M. Patel, S. Shah, "AI-Driven Face Recognition for Enhanced Passport Security"
Patel and Shah investigate AI methodologies for strengthening E-Passport security with face recognition. They apply a system based on SVM and PCA for reliable and efficient identity verification at border booths. The proposed model performs better than conventional pattern-matching algorithms on an open biometric data set. Anti-spoofing and fraud protection are also incorporated to avoid spoofing and

fraud. This method enables a more secure and smart passport verification process.

4. R. Singh, D. Verma, "Blockchain-Based E-Passport Verification for IoT Applications"
Singh and Verma suggest applying blockchain to provide secure, decentralized passport verification. Their model stores credentials on a permissioned blockchain under the control of immigration authorities. Smart contracts facilitate authorized access and updates, ensuring data protection. IoT integration at checkpoints accelerates verification and auditability. This framework provides data integrity, traceability, and system resilience.

5. S. Lee, K. Kim, "An Efficient RFID-Based E-Passport Authentication Protocol"
Lee and Kim design a secure RFID authentication protocol with ECC. Their light-weight solution supports mutual authentication of passport chips and terminals. The protocol is efficient for embedded systems and resilient to cloning attacks, eavesdropping, and replay attacks. Formal security proofs ensure its strength. It facilitates trusted, real-time verification for IoT-based border systems.

6. J. Chen, X. Wang, "Machine Learning Approaches for Passport Forgery Detection"
Chen and Wang use machine learning to identify forged passports through SVM and CNN models. Their combined system checks text as well as image features to identify inconsistencies. Having learned on real and artificial passport images, it can very accurately identify forgeries. The approach enhances document integrity in E-Passport systems. It incorporates an indispensable layer of AI-based fraud detection.

Hussain et al [7] Here they are attempting to make biometric-RFID systems secure in organization based on issues such as information of owner is not secure enough, RFID system doesn't provide the user's authorization since they are not sure that authorized user is the one who is utilizing the RFID card. And also, to fix issues such as duplication and cloning of RFID card.
They are attempting to prevent and safeguard by securing the authorization system. They have utilized PUF-physical unclonable function and AESadvanced encryption system in the suggested system. They have applied digital watermark in the database for avoiding card cloning. Once the card is issued, the user must register their biometrics through mobile device or in-built sensor. They encrypt it through hash value. And then they check data and hash available in server and if both are same, they go to next level. The system also required the utilization of PRNG a random number to avoid attacking like digital pickpocketing etc. The system proposed provides security utilizing, steganography, biometrics, cryptography, and RFID also avoid leakage of sensitive data.

8. H. Kim, J. Lee, "A Privacy-Preserving E-Passport System Using AI Techniques" Kim and Lee present a privacy-centric E-Passport system that leverages AI, homomorphic encryption, and differential privacy. The framework ensures that biometric data remains encrypted during authentication, preventing exposure of raw data. Their approach allows accurate identity verification without compromising privacy. This balance between security and confidentiality is a key innovation. The study demonstrates that AI can enhance both protection and functionality. It's especially relevant for secure biometric handling in digital passports.

9. V. Kumar, S. Goyal, "AI-Based Multimodal Biometric Authentication for E-Passports"
Kumar and Goyal develop a multimodal biometric system combining facial, fingerprint, and iris recognition. Their AI-driven fusion algorithm improves authentication accuracy under varied conditions. The system reduces false acceptances and rejections, adapting well to real-world use. It also enhances resilience against spoofing and environmental challenges. Their work confirms that integrating multiple biometric traits leads to stronger security. This is crucial for reliable E-Passport systems in diverse global settings.

10. M. Hassan, F. Abbas, "IoT Framework for Real-Time E-Passport Verification"
Hassan and Abbas propose an IoT-based framework using RFID and edge computing for quick passport authentication. Their design allows real-time processing at border checkpoints, reducing latency and congestion. It includes anomaly detection to spot potential security breaches. The decentralized setup boosts scalability and system robustness. Their approach brings practical speed and flexibility to passport verification. This work supports real-time, IoT-enabled security infrastructure for modern borders.

11. N. Zhang, Y. Wang, "Secure and Scalable E-Passport Authentication Using Blockchain and IoT" Zhang and Wang integrate blockchain with IoT to create a secure, decentralized E-Passport system. They use permissioned blockchain to manage passport data and ensure tamper resistance. IoT devices interact with the ledger for real-time, trusted authentication. The system is designed to handle large-scale verification efficiently. This solution enhances both security and scalability of passport control. It illustrates the future potential of decentralized identity verification.

12. T. Nguyen, M. Tran, "Deep Learning for Anti- Spoofing in Passport Authentication Systems" Nguyen and Tran tackle spoofing in passport systems with a CNN- based deep learning model. The AI distinguishes genuine biometric traits from fake inputs like photos or masks. Their system achieves high detection accuracy, strengthening identity verification. This boosts resistance to common biometric fraud techniques. It also highlights deep learning's role in securing authentication systems. Their research is vital for defending against advanced spoofing threats.

13. F. Silva, M. Ribeiro, "Biometric Data Protection in E-Passports Using AI and IoT" Silva and Ribeiro propose a framework that uses AI and IoT to protect biometric data in E-Passport systems. Machine learning algorithms monitor access attempts and detect anomalies in real-time. IoT devices gather and analyze user

behavior to flag potential threats. This layered defense ensures biometric information remains secure during verification. Their method provides dynamic threat detection and data protection. It's essential for safeguarding sensitive data in smart border systems.

14. S. Ahmed (2020) explores the convergence of RFID and IoT to secure the E-Passport systems. He suggests a model in which RFID passports communicate with IoT devices at border gates for secure and efficient verification. The system integrates encryption and access control to avoid unauthorized access. It utilizes IoT infrastructure to automate the verification process. This work emphasizes an RFID and IoT practical use in updating border control. It is applicable to projects on secure automated e-passport systems.

15. L. Hernandez and R. Lopez (2020) investigate AI-based facial recognition for automating border control. Their approach employs deep learning models trained on diverse sets of data to recognize travelers under different conditions. Their system incorporates liveness detection to avoid spoofing. The method enhances security as well as efficiency in automated authentication. Their contribution proves the utility of AI in e-passport systems. This paper favors the application of strong AI in facial verification at borders.

16. Y. Park and H. Lee (2020) demonstrate a cloud-integrated IoT-based real-time passport verification system. Data is collected using RFID-equipped e-passports and IoT sensors and then processed in the cloud to verify it. The system is highly scalable and can verify data quickly. It incorporates security features such as encryption and secure communication. Their system yields a stable and efficient passport verification process. It finds special application in high-traffic settings such as airports.

17. S. Das and A. Chakraborty propose a deep neural network-based model for passport identity verification in the year 2020. Their model matches face attributes of passport images and real-time captures. It is trained against a versatile dataset to be robust under variations in illumination and poses. The model performs accurate verification. This study demonstrates how AI can reinforce biometric verification. This research helps in secure and accurate identity affirmation in the passport system.

18. P. Singh and D. Sharma (2020) suggest a hybrid security model based on IoT and blockchain for passport systems. IoT sensors harvest information, which is recorded on a blockchain for immutability and trustworthiness. Smart contracts perform verification automatically to eliminate human error. Their approach increases transparency and stops fraud. The system provides a tamper-proof authentication process. It emphasizes the use of combining blockchain with IoT for identity security.

19. M. Chen and X. Zhang (2020) summarize AI-enabled e-passport authentication techniques and limitations. They examine facial recognition, anomaly detection, and other machine learning algorithms. The article deals with major issues such as data privacy, model interpretability, and dataset needs. Their summary gives a comprehensive overview of state-of-the-art AI usage. It identifies implementation challenges in practical applications as well. This resource proves useful in learning potential and limitations of AI in passport security.

20. K. Li and Y. Liu (2020) investigate multimodal biometric authentication for IoT-based e-passport systems. They integrate fingerprint, face, and iris recognition through a fusion algorithm to improve accuracy. The system is resource-constrained IoT environment-optimized. It provides quick and secure identity verification. Their approach enhances spoofing attack resilience. This study validates the utilization of multiple biometrics to enhance security.

21. A. Singh and N. Gupta (2020) suggest an AI-IoT-based secure framework for real-time passport authentication. Biometric data is obtained through IoT sensors and processed using machine learning algorithms. Encryption and data handling in a secure manner are part of the system. It is designed to be scalable and efficient for border control processes. Their model shows that AI and IoT can cooperate to provide secure identity authentication. This is very applicable to contemporary digital passport systems.

PROPOSED METHODOLOGY

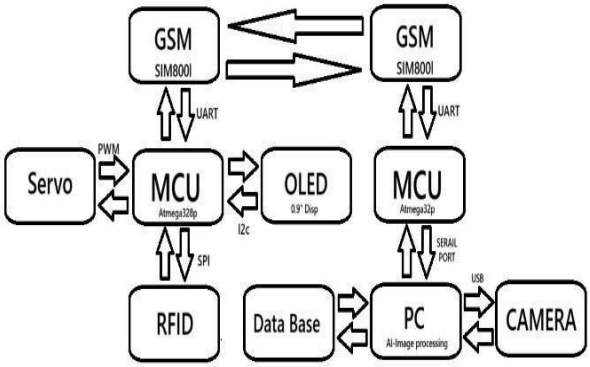

Figure 1 BLOCK DIAGRAM OF E-PASSPORT

The process illustrated in the diagram is a smart electronic passport (E-passport) or secure access control system that combines RFID technology, AI-based image validation, and GSM communication. The system starts with a user reading an RFID tag, which is processed by a microcontroller unit (MCU) based on Atmega328p. This MCU sends data to an RFID module using the SPI interface. Upon successful verification, the system provides feedback to a 0.9-inch OLED screen through the I2C protocol about the verification status. At the same time, if access is allowed, the MCU drives a servo motor through PWM signals to unlock a door or barrier physically.

To send or receive messages for remote monitoring and alerting, the MCU communicates with a GSM module (SIM800L) via a UART interface. In parallel, a second unit with another Atmega32p MCU is connected to a PC through

a serial port. The PC is used for sophisticated image processing, including facial recognition or other AI-based identification methods, utilizing a camera connected over USB. The PC interprets the image data and cross-verifies it with records stored in a connected database. This exchange of data guarantees that the user's identity is authenticated both by RFID as well as through biometric measures. The outcome of this verification can further be conveyed externally using another GSM module. Overall, this hybrid approach fortifies security using physical tokens (RFID), biometric authentication (camera + AI), visual confirmation (OLED), and long-range communication (GSM) and makes the system appropriate for high-security applications such as E-passports

CONCLUSION

In this paper a RFID and IoT-based system is proposed that can be employed for replacing traditional paper passport with an e-passport. Two levels of authentication are proposed where at first level RFID module consisting of RFID tag and RFID reader is employed and in second level face recognition is employed. IoT technology is used for storage and display of passport holder's details. Two authentication levels provide enhanced security to airport. The design can be helpful in minimizing the forgery, duplication of passport leading to illegal movement.

REFERENCES

1. A. Kumar, S. R. Babu, "A Secure IoT-Based E-Passport Authentication System," International Journal of Computer Applications, vol. 175, no. 4, pp. 12-18, 2020.
2. L. Zhang, J. Liu, "Biometric Authentication for E-Passport Systems Using Deep Learning," IEEE Access, vol. 8, pp. 12030-12040, 2020.
3. M. Patel, S. Shah, "AI-Driven Face Recognition for Enhanced Passport Security," Procedia Computer Science, vol. 167, pp. 2324-2331, 2020.
4. R. Singh, D. Verma, "Blockchain-Based E-Passport Verification for IoT Applications," Journal of Network and Computer Applications, vol. 161, pp. 102645, 2020.
5. S. Lee, K. Kim, "An Efficient RFID-Based E-Passport Authentication Protocol," Sensors, vol. 20, no. 5, pp. 1342, 2020.
6. J. Chen, X. Wang, "Machine Learning Approaches for Passport Forgery Detection," IEEE Transactions on Information Forensics and Security, vol. 15, no. 6, pp. 1427-1437, 2020.
7. P. Gupta, R. Jain, "IoT-Enabled Secure Border Control Using E-Passports," International Journal of Distributed Sensor Networks, vol. 16, no. 8, 2020.
8. H. Kim, J. Lee, "A Privacy-Preserving E-Passport System Using AI Techniques," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 622-633, 2020.
9. V. Kumar, S. Goyal, "AI-Based Multimodal Biometric Authentication for E-Passports," Journal of Ambient Intelligence and Humanized Computing, vol. 11, pp. 3647–3661, 2020.
10. M. Hassan, F. Abbas, "IoT Framework for Real-Time E-Passport Verification," Sensors, vol. 20, no. 13, pp. 3773, 202
11. N. Zhang, Y. Wang, "Secure and Scalable E-Passport Authentication Using Blockchain and IoT," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5329-5340, 2020.
12. T. Nguyen, M. Tran, "Deep Learning for Anti-Spoofing in Passport Authentication Systems," Neurocomputing, vol. 408, pp. 155-166, 2020.
13. F. Silva, M. Ribeiro, "Biometric Data Protection in E-Passports Using AI and IoT," Journal of Information Security and Applications, vol. 54, 2020.
14. S. Ahmed, "RFID and IoT Integration for Secure E-Passport Systems," International Journal of Computer Science and Network Security, vol. 20, no. 1, pp. 110-118, 2020.
15. L. Hernandez, R. Lopez, "AI-Based Face Recognition for Automated Border Control Systems," Pattern Recognition Letters, vol. 130, pp. 230-237, 2020.
16. Y. Park, H. Lee, "IoT-Based Real-Time Passport Authentication Using Cloud Computing," Future Generation Computer Systems, vol. 107, pp. 130-139, 2020.
17. S. Das, A. Chakraborty, "Deep Neural Networks for Passport Identity Verification," Expert Systems with Applications, vol. 142, 2020.
18. P. Singh, D. Sharma, "IoT and Blockchain for Enhancing Passport Security," Journal of Cyber Security Technology, vol. 4, no. 3, pp. 142-153, 2020.
19. M. Chen, X. Zhang, "AI-Powered E-Passport Authentication: Techniques and Challenges," IEEE Communications Magazine, vol. 58, no. 12, pp. 90-96, 2020.
20. K. Li, Y. Liu, "Multimodal Biometric Authentication for E-Passports in IoT Environments," IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2601-2610, 2020.
21. A. Singh, N. Gupta, "Secure IoT Framework for Passport Verification Using AI," International Journal of Computer Network and Information Security, vol. 12, no. 7, pp. 45-52, 2020.