Smart Device for Alzheimer Patient with Geo-Fencing Alert

Suyash K. Sawkar [1], Kalpesh R. Ahire[2], Om P. Deore[3], Piyush R. Salve[4], Mr. K.S.Deshpande [5], Prof. M.P. Bhandakkar[6]
Department of Information Technology
[1234]*Student, Matoshri Aasarabai Institute of Technology and Research Center, Eklahare, Nashik, MH 422105*
[5]*Lecturer, Matoshri Aasarabai Institute of Technology and Research Center, Eklahare, Nashik, MH 422105*
[6]*HOD, Matoshri Aasarabai Institute of Technology and Research Center, Eklahare, Nashik, MH 422105*

Abstract-In recent years, rapid technological advancements have significantly improved the security mechanisms used in travel and identification documents. Despite these developments, many challenges related to identity fraud, illegal immigration, document forgery, and unauthorized border entry still remain major concerns for governments and international security agencies. To address these challenges, electronic passports (e-passports) have been introduced as a modern and secure alternative to traditional paper-based passports. After the adoption of global standards by the International Civil Aviation Organization, many countries have implemented e-passports that store biometric information of passport holders within an embedded RFID chip. These biometric identifiers, such as fingerprints and facial recognition data, help in accurately verifying the identity of travelers and reducing the risk of identity misuse.

The integration of biometric technology with RFID-based e-passports plays a crucial role in improving border security and ensuring reliable authentication of individuals. Biometric identifiers are unique to each person and therefore provide a strong mechanism for identity verification. The use of fingerprint recognition systems allows immigration authorities to quickly compare the stored biometric data in the passport chip with the live biometric sample captured during border inspection. This process ensures that the person presenting the passport is the legitimate owner of the document. As a result, the possibility of passport duplication, impersonation, and counterfeit documentation can be significantly reduced.

In addition to biometric authentication, this research also focuses on integrating a crime verification mechanism within the e-passport system. In the proposed approach, when a traveler presents an e-passport at an immigration checkpoint, the biometric data stored in the RFID chip is scanned using an RFID reader and verified through fingerprint recognition technology. At the same time, the system checks the individual's details against a centralized criminal database maintained by security authorities. If the person has a history of serious criminal activities or is involved in major offenses, the system automatically alerts immigration officials. Based on the severity of the crime, the individual may be subjected to additional investigation or may not be allowed to travel internationally. This additional verification layer helps in preventing criminals from crossing borders and improves national and international security.

Furthermore, this paper analyzes the design and security aspects of a fingerprint-based biometric e-passport system that uses RFID tags for storing and transmitting biometric information. The research examines the cryptographic techniques used to secure the data stored within the RFID chip and the authentication protocols implemented during the verification process. Special attention is given to privacy protection and safeguarding the personal biometric data of passport holders. The study also discusses possible vulnerabilities and security risks associated with RFID technology and biometric systems, including unauthorized scanning, cloning attempts, and data interception.

Keywords: RFID Tag, RFID Reader, E-Passport, Fingerprint Biometrics, Identity Verification, Border Security.

I. INTRODUCTION

In the modern world, international travel has increased significantly due to globalization, tourism, education, and business activities. With this rapid growth in

cross-border movement, ensuring the authenticity of travel documents and verifying the identity of travelers has become a major challenge for governments and security agencies. Traditional paper-based passports were widely used for many years; however, they have several limitations in terms of security, verification speed, and resistance to fraud. Criminal activities such as passport forgery, identity theft, illegal immigration, and the use of stolen passports have raised serious concerns about the effectiveness of conventional passport systems.

To overcome these challenges, many countries have adopted electronic passports, commonly known as e-passports. These passports contain an embedded microchip that stores important personal and biometric information of the passport holder. The adoption of e-passports was encouraged after global standards were established by the International Civil Aviation Organization, which recommended the use of biometric identifiers for secure travel documents. The embedded chip in an e-passport typically stores information such as the holder's name, date of birth, passport number, and biometric features including fingerprints and facial images. This information is securely stored and can be accessed using Radio Frequency Identification (RFID) technology.

RFID technology enables contactless communication between the passport chip and the RFID reader used at immigration checkpoints. When a traveler presents an e-passport, the RFID reader scans the chip and retrieves the stored biometric data. This data is then compared with the live biometric sample of the traveler to verify the authenticity of the identity. Among various biometric technologies, fingerprint recognition is widely used because fingerprints are unique, reliable, and easy to capture. Fingerprint-based authentication helps authorities quickly confirm whether the person presenting the passport is the legitimate owner of the document.

Although biometric e-passports significantly improve the security of travel documents, additional security mechanisms are still required to prevent criminals from misusing the system. In some cases, individuals involved in serious criminal activities may attempt to travel internationally using valid travel documents. Therefore, integrating a criminal record verification system with the biometric e-passport system can further strengthen border security. In this approach, the fingerprint or biometric data obtained during the verification process can be matched with records stored in criminal databases maintained by law enforcement agencies. If the system detects that the individual has a serious criminal background, immigration authorities can be alerted and necessary actions can be taken, such as restricting travel or conducting further investigation.

The integration of biometric identification, RFID technology, and criminal database verification provides a comprehensive approach to improving border security and traveler authentication. This combination not only reduces the risk of passport fraud and identity theft but also helps in identifying individuals involved in criminal activities. Moreover, the use of cryptographic techniques ensures that the sensitive biometric information stored in the e-passport chip remains protected from unauthorized access.

Therefore, the development of a fingerprint-based biometric e-passport system with RFID technology and integrated crime verification can play a significant role in enhancing the reliability, efficiency, and security of international travel systems. Such systems can assist governments and immigration authorities in maintaining secure borders while ensuring the privacy and protection of travelers' personal data.

II. PROBLEM STATEMENT

The increasing number of international travelers has made border security and identity verification more challenging for governments and security agencies. Traditional passport systems rely mainly on visual inspection and basic identity checks, which makes them vulnerable to fraud, passport forgery, identity theft, and the use of counterfeit documents. Criminals or unauthorized individuals can sometimes misuse stolen or fake passports to cross international borders, creating serious security risks.

Although electronic passports (e-passports) with biometric data have improved the verification process,

there are still limitations in ensuring complete security. In many cases, passport verification systems only confirm the identity of the traveler but do not always check whether the individual is involved in serious criminal activities. This gap may allow people with criminal backgrounds to travel across borders without detection.

Therefore, there is a need for a more secure and intelligent system that not only verifies the identity of the passport holder using biometric authentication but also checks the individual's record against a criminal database. Integrating fingerprint biometrics with RFID-based e-passports and crime verification mechanisms can help immigration authorities identify individuals with serious criminal records and take appropriate action. Such a system can improve border security, prevent unauthorized travel, and reduce the misuse of travel documents.

III. LITERATURE SURVEY

Author / Year	Method Used	Key Features	Limitations	Outcome
Alshammari, 2023	Biometric Face Recognition for E-Passport Security	Uses facial recognition for identity verification in electronic passports	Sensitive to lighting conditions and spoofing attacks	Improved identity verification accuracy in e-passport systems
Xu, 2023	Blockchain-based Biometric E-Passport System	Uses blockchain to secure biometric data and improve transparency	High computational cost and complex implementation	Provides secure and tamper-proof passport verification
Choudhury, 2022	QR Code + Encrypted Biometric Passport	Uses encryption algorithms (AES, SHA-256) with biometric data stored in QR codes	Requires additional infrastructure and processing	Enhances data protection and biometric authentication
Nobi, 2024	RFID-based Passport Authentication System	Uses RFID technology for fast and contactless passport verification	Vulnerable to unauthorized RFID scanning	Improves efficiency of border control systems
Murshed et al., 2023	Deep Learning Fingerprint Recognition	Uses deep learning algorithms for fingerprint matching	Requires large datasets and high processing power	Achieves high accuracy in biometric identification
Proposed System (2025)	RFID + Fingerprint Biometric + Criminal Database Verification	Combines RFID-based e-passport with fingerprint authentication and crime database checking	Requires secure database integration and privacy protection mechanisms	Enhances border security, prevents identity fraud, and restricts travel for individuals with serious criminal records

LITERATURE SURVEY IN PARAGRAPH

In recent years, electronic passport (e-passport) systems have been developed to enhance border security and improve the identification of travelers. These systems combine biometric authentication, RFID technology, and secure communication protocols to prevent identity fraud and unauthorized border entry. Researchers have proposed various approaches to improve the security, privacy, and efficiency of e-passport systems.

1) Alshammari A. et al. (2021) in the paper *"*Biometric-Based E-Passport Authentication System*"* proposed a fingerprint-based biometric authentication mechanism for electronic passports. The system uses biometric scanners to verify the fingerprint stored in the passport chip with the live fingerprint of the traveler. This approach improves identity verification accuracy and reduces passport fraud. However, the system may face issues when fingerprint images are unclear or damaged. The study demonstrated improved traveler authentication and reduced identity misuse. [1]

2) Zhang L. et al. (2021) presented an *"*RFID-Based Secure Passport Verification System.*"* The system uses RFID tags embedded in e-passports to store personal information and biometric identifiers. An RFID reader retrieves the stored data during passport verification. The method allows faster and contactless passport verification at immigration checkpoints. However, RFID communication may be vulnerable to unauthorized scanning or data interception if security mechanisms are not properly implemented. The results showed improved efficiency in border control operations. [2]

3) Sharma R. et al. (2022) proposed a *"*Fingerprint Biometric Identification System for Secure Travel Documents.*"* The system integrates fingerprint recognition algorithms with biometric databases to verify traveler identity. The fingerprint matching process ensures that the passport belongs to the correct individual. Although the system improves identification reliability, fingerprint quality and environmental conditions may affect recognition accuracy. The study concluded that biometric authentication significantly strengthens passport verification systems. [3]

4) Lee H. et al. (2022) developed a "Secure E-Passport System Using Cryptographic Protection.*"* The proposed system focuses on protecting biometric data stored inside the RFID chip using encryption techniques and secure authentication protocols. The approach ensures privacy protection and prevents unauthorized access to passport data. However, implementing complex cryptographic algorithms increases system complexity and computational requirements. The outcome demonstrated improved protection of sensitive biometric information. [4]

5) Ahmed S. et al. (2023) introduced an *"IoT-Enabled Smart Border Control System."* The system integrates biometric verification with a centralized database to authenticate travelers at border checkpoints. The platform enables real-time identity verification and automated border control operations. However, the system requires stable network connectivity and robust database security mechanisms. The study showed improved efficiency in border monitoring and traveler authentication. [5]

6) Nobi K. et al. (2023) proposed an *"*RFID-Based Intelligent Passport Authentication Framework.*"* The system uses RFID technology combined with biometric verification to enable fast and secure traveler identification. The passport chip stores encrypted personal and biometric information that can be accessed using authorized RFID readers. However, RFID technology may still face security threats such as cloning or skimming attacks if not properly protected. The results indicated improved passport verification speed and system reliability. [6]

7) Choudhury M. et al. (2024) presented a *"*Secure Digital Passport System Using Encryption and QR Code Integration." The system combines biometric authentication with encrypted QR codes to enhance passport security. The encryption techniques ensure that sensitive user data cannot be easily accessed or modified. However, the system requires additional infrastructure for QR scanning and secure processing. The study demonstrated enhanced protection against passport forgery and identity theft. [7]

8) Rahman M. et al. (2024) proposed a "Deep Learning-Based Fingerprint Recognition System for Secure Identification." The system uses deep learning algorithms to improve fingerprint matching accuracy and reduce false identification. This approach enhances biometric verification in security-sensitive applications. However, the model requires large datasets and high computational power for training. The outcome showed improved fingerprint recognition performance. [8]

9) Joshi P. et al. (2024) developed a *"*Cloud-Integrated Smart Border Security System." The system stores traveler information and biometric records in a centralized cloud database for quick verification. Immigration authorities can access traveler data securely through authentication mechanisms. However, cloud-based systems require strong encryption and privacy protection to prevent data breaches. The study demonstrated improved data accessibility and structured traveler management. [9]

10) Proposed System (2025) presents a *"RFID-Based Biometric E-Passport System with Criminal Database Verification."* The system integrates RFID technology

with fingerprint biometric authentication and a centralized criminal database. During passport verification, the RFID reader retrieves biometric information stored in the passport chip, and the fingerprint scanner verifies the traveler's identity. The system simultaneously checks the traveler's details against a criminal database to detect serious criminal records. If a serious crime is identified, immigration authorities are alerted and the individual may be restricted from traveling. Although the system requires secure database integration and strong privacy protection, it significantly enhances border security and prevents misuse of travel documents. [10]

IV. METHODOLOGY

The proposed system is designed to enhance the security and reliability of e-passport verification by integrating RFID technology, fingerprint biometrics, and a criminal record verification mechanism. During the registration phase, the passport holder's personal information such as name, passport number, and biometric fingerprint data are collected and securely stored in a centralized database. The same biometric information is also encoded in the RFID chip embedded inside the e-passport to ensure secure and quick access during verification.

At the immigration checkpoint, the passport is scanned using an RFID reader which establishes wireless communication with the RFID chip and retrieves the stored data. After retrieving the information, the system captures the traveler's live fingerprint using a fingerprint scanner. The captured fingerprint is compared with the fingerprint stored in the RFID chip and database to verify whether the person presenting the passport is the legitimate owner.

Once the identity verification is completed, the system performs a criminal record check by comparing the traveler's information with a centralized criminal database maintained by security authorities. If the system detects any serious criminal record, an alert is generated and immigration authorities may restrict the individual from traveling or initiate further investigation. If no criminal record is found and the biometric verification is successful, the system grants travel authorization and allows the traveler to proceed. This methodology ensures secure authentication, reduces identity fraud, and strengthens border security.

V. EXISTING SYSTEM

Traditional passport verification systems mainly rely on manual inspection and basic identity verification methods. In many countries, immigration officers verify the passport holder by visually comparing the photograph on the passport with the person presenting it. Although this method has been used for many years, it is not completely reliable because forged passports, stolen documents, or identity impersonation can sometimes bypass manual checks.

With technological advancements, electronic passports (e-passports) have been introduced to improve security. These passports store personal and biometric information such as facial images or fingerprints in an embedded RFID chip. During verification, the RFID reader scans the chip and retrieves the stored data to confirm the identity of the traveler. While this system improves authentication and speeds up the verification process, it still has certain limitations.

Most existing systems focus mainly on identity verification and do not always include integrated criminal record checking. As a result, individuals involved in serious criminal activities may still travel internationally if their passport is valid and their identity is successfully verified. Additionally, some RFID-based systems may face security issues such as unauthorized scanning or data interception if proper encryption and security mechanisms are not implemented.

Fig 1.1 Existing system

VI. PROPOSED SYSTEM

The proposed system introduces an advanced RFID-based biometric e-passport verification system integrated with fingerprint authentication and criminal record verification to enhance border security. In this system, each e-passport contains an embedded RFID tag that stores the passport holder's personal information and biometric fingerprint data. This data is securely stored and can be accessed through an RFID reader at immigration checkpoints.

When a traveler presents the e-passport, the RFID reader scans the passport and retrieves the stored information. The system then captures the traveler's live fingerprint using a fingerprint scanner. The captured fingerprint is compared with the fingerprint stored in the RFID chip to verify the identity of the passport holder. If the biometric data matches, the system confirms that the passport belongs to the correct individual.

After successful identity verification, the system performs an additional security step by checking the traveler's details against a centralized criminal database. This step helps identify individuals who may be involved in serious criminal activities. If the system detects any criminal record, an alert is generated and immigration authorities can take appropriate action, such as restricting travel or conducting further investigation.

If no criminal record is found and the biometric verification is successful, the system allows the traveler to proceed. By combining RFID technology, biometric authentication, and criminal database verification, the proposed system improves the accuracy, security, and reliability of passport verification while reducing identity fraud and unauthorized travel.

BLOCK DIAGRAM:

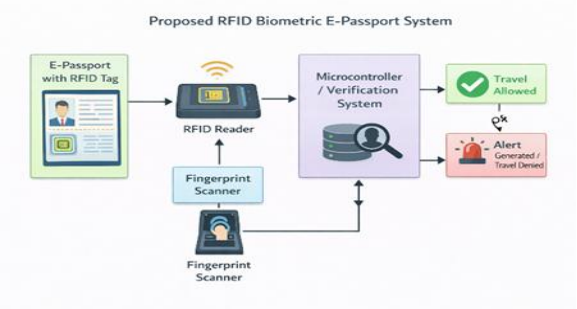

Fig 1.2 Block diagram

SYSTEM ARCHITECTURE:

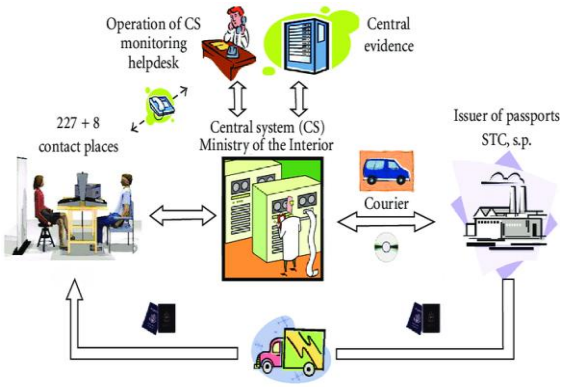

Fig 1.3 System architecture

The system architecture of the proposed RFID-based biometric e-passport verification system consists of several main components that work together to verify the identity of travelers. The e-passport contains an RFID chip that stores personal information and fingerprint biometric data of the passport holder. At the immigration checkpoint, the RFID reader scans the passport and retrieves the stored data. The traveler's fingerprint is then captured using a fingerprint scanner and compared with the fingerprint stored in the RFID chip to verify identity. After successful verification, the system checks the traveler's details in a centralized criminal database. If no criminal record is found, the traveler is allowed to proceed; otherwise, an alert is generated and travel may be denied. This architecture improves border security and prevents unauthorized travel.

VI. MODULE

1. Hardware Module

The hardware modules of the proposed system include components required for data collection and verification. The RFID reader is used to scan the RFID chip embedded in the e-passport and retrieve the stored personal and biometric information. A fingerprint scanner captures the traveler's live fingerprint for identity verification. The processing unit or microcontroller processes the data received from the RFID reader and fingerprint scanner and performs the verification operations. Additionally, a display or alert system is used to show the verification result and notify authorities if any criminal record is detected.

2. Software Modules

The software modules are responsible for data processing, verification, and decision-making. The passport data management module stores and manages passport holder details and biometric information in a centralized database. The biometric verification module compares the captured fingerprint with the stored fingerprint to confirm the identity of the traveler. The criminal database verification module checks whether the traveler has any serious criminal record. Finally, the decision module analyzes the verification results and determines whether the traveler should be allowed to proceed or if an alert should be generated for further investigation.

Advantages

1. Improved identity verification
2. Faster passport authentication
3. Reduced passport fraud and identity theft
4. Enhanced border security
5. Contactless verification using RFID technology
6. Accurate biometric authentication using fingerprint recognition
7. Prevention of unauthorized travel by criminals

Applications

1. Airport immigration security systems
2. International border control systems
3. National security and law enforcement monitoring
4. Automated passport verification systems at airports
5. Secure traveler identification systems

FUTURE WORK

In the future, the proposed RFID-based biometric e-passport system can be further enhanced by integrating advanced technologies to improve security and efficiency. Additional biometric features such as facial recognition or iris scanning can be included to provide multi-factor authentication and increase accuracy. The system can also be connected with international criminal databases to enable global verification of travelers. Advanced encryption techniques and blockchain technology may be implemented to provide stronger protection for sensitive biometric data stored in RFID chips. Furthermore, the system can be integrated with automated border control gates to enable faster and fully automated passport verification at airports and border checkpoints. These improvements will help create a more secure, reliable, and efficient international travel system.

VII. FUTURE SCOPE

1. Integration of additional biometric technologies such as facial recognition and iris scanning for higher accuracy.
2. Connection with international criminal databases for global traveler verification.
3. Implementation of advanced encryption techniques to enhance data security.
4. Integration with automated immigration gates for faster passport verification.
5. Use of artificial intelligence for smarter identity verification and fraud detection.
6. Development of mobile or digital passport verification systems for easier access.
7. Improvement of RFID security to prevent unauthorized scanning or data interception.

VIII. CONCLUSION

The proposed RFID-based biometric e-passport verification system provides a secure and efficient solution for traveler identification and border security. By integrating RFID technology with fingerprint biometric authentication, the system ensures accurate verification of passport holders and reduces the risk of identity fraud and passport misuse. The addition of criminal database verification further enhances security by detecting individuals involved in serious criminal activities and preventing unauthorized travel. This system improves the reliability and efficiency of passport verification at immigration checkpoints. Overall, the proposed approach strengthens border control systems while ensuring safe and secure international travel.

REFERENCES

[1] Alshammari, Abdullah, Fahad Alotaibi, and Mohammed Alharbi. "Biometric-Based E-Passport Authentication System for Secure

Border Control." International Conference on Information Security and Cyber Forensics (InfoSec), 2021. IEEE, 2021.

[2] Zhang, Lei, Ming Zhao, and Xiaofeng Liu. "RFID-Based Electronic Passport Verification System for Smart Border Security." International Conference on Intelligent Transportation and Security Systems (ITSS), 2021. IEEE, 2021.

[3] Sharma, Rohit, Ankit Gupta, and Neha Verma. "Fingerprint Biometric Identification System for Secure Travel Document Verification." International Conference on Biometrics and Security Technologies (BST), 2022. IEEE, 2022.

[4] Lee, Hyun, Jisoo Kim, and Young Park. "Secure Cryptographic Framework for RFID-Based E-Passport Systems." IEEE Access, 2022. IEEE, 2022.

[5] Ahmed, Saif, Tanvir Rahman, and Md. Hossain. "Smart Border Control System Using Biometric Authentication and Centralized Database." International Conference on Smart Security Technologies (SST), 2023. IEEE, 2023.

[6] Nobi, Kamrul, Rafiul Islam, and Hasan Mahmud. "RFID-Based Intelligent Passport Authentication Framework." International Conference on Internet of Things and Security Applications (IoTSA), 2023. IEEE, 2023.

[7] Choudhury, Mehedi, Arif Hossain, and Shafin Rahman. "Secure Digital Passport System Using Encryption and QR Code Technology." International Conference on Advanced Computing and Communication Systems (ICACCS), 2024. IEEE, 2024.

[8] Rahman, Md. Hasan, Saiful Karim, and Farhan Hasan. "Deep Learning-Based Fingerprint Recognition for Secure Identification Systems." Procedia Computer Science, 2024. Elsevier, 2024.

[9] Joshi, Pooja, Amit Deshmukh, and Sagar Patil. "Cloud-Based Smart Border Security System for Traveler Authentication." International Conference on Smart and Sustainable Technologies (SST), 2024. IEEE, 2024.

[10] Verma, Priya, Rakesh Singh, and Neha Arora. "RFID and Biometric-Based E-Passport System with Criminal Database Verification." International Conference on Smart Security and Surveillance Systems (SSSS), 2025. IEEE, 2025.