IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15386

RFID And Fingerprint Based Digital Passport For Cross Border Authentication

Mr. H.M. Gaikwad[1], Mr. S.V. Waghmare[2], Saili Borse[3], Krutika Bhamare[4],

Vidhi Daryani[5], Darshana Kothari[6]

Sr. Lecturer in AIML, K K Wagh Polytechnic, Nashik[1]

Lecturer in AIML, K K Wagh Polytechnic, Nashik[2]

Third Year Students of Artificial Intelligence and Machine Learning, K K Wagh Polytechnic, Nashik[3-6]

Abstract: Advancements in technology have improved the verification of travel documents through the use of electronic passports (e-passports). These passports follow International Civil Aviation Organization standards and store biometric identifiers such as fingerprints. Biometric technology combined with RFID tags enhances identity verification and reduces the use of counterfeit documents. Fingerprint-based biometric e-passports help simplify travel processes while improving global security. They also focus on protecting the privacy and sensitive biometric data of passport holders. However, certain security challenges and vulnerabilities still exist in the system. This study analyzes the cryptographic features, biometric techniques, and security protocols used in e-passports. It also examines possible risks where individuals may attempt to bypass the system. In the proposed AI/ML-based crime monitoring system, registered crimes are analyzed and categorized by severity. If a serious crime is detected, the information is used during passport verification to evaluate the applicant's criminal background before allowing travel[1].

Keywords: RFID Tag, RFID Reader, E-Passport.

I. INTRODUCTION

Advancements in technology have improved the reliability of travel document verification, though some security and efficiency challenges still remain. Electronic passports (e-passports) have been widely adopted following the standards of the International Civil Aviation Organization (ICAO), which require passports to store biometric identifiers [4]. By integrating biometric data such as fingerprints with RFID tags, e-passports help prevent unauthorized entry and reduce the use of counterfeit documents through more accurate identification[4][5]. This technology enhances border security while also making travel processes faster and more convenient for legitimate passport holders.

Fingerprint-based biometric e-passports also focus on protecting the privacy and personal security of passport holders through cryptographic mechanisms[1]. The system allows authorities to verify both the authenticity of the passport and the identity of the traveler. However, researchers also highlight possible vulnerabilities, as individuals attempting to bypass the system may exploit predictable weaknesses. Despite these challenges, the global adoption of e-passports now representing more than half of passports issued worldwide has significantly strengthened national and international security[2][3] by enabling automated verification of biometric and personal data.

II. LITERATURE REVIEW

Vignesh et al. (2022)[1] – Enhanced IoT-Based E-Passport System
Vignesh et al. (2022) proposed an enhanced E-Passport system integrating secured IoT and wireless communication technology. They highlighted the vulnerabilities of existing E-Passport systems, including security risks and limited data storage capacity. The authors suggested a novel approach using IoT-enabled RFID tags and wireless communication protocols to ensure secure data transmission and storage. Their system utilizes advanced encryption methods and biometric authentication to prevent unauthorized access and identity theft. The proposed system aims to improve the efficiency and security of identity verification processes, enabling seamless and reliable travel experiences. This study contributes to the development of a more robust and secure E-Passport system, addressing the limitations of existing solutions.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026
DOI: 10.17148/IJARCCE.2026.15386

Honade et al. (2022[2]) – RFID-Based Electronic Passport System
Honade et al. (2022) presented a comprehensive study on the development of an electronic passport using RFID technology. They explored the benefits of integrating RFID in passports, including enhanced security, increased data storage capacity, and improved identity verification processes. The authors discussed the components of an RFID-enabled passport, including a microprocessor, memory, and antenna, and highlighted the use of encryption algorithms to ensure secure data storage and transmission. They also examined the advantages of RFID passports over traditional paper-based passports, such as reduced counterfeiting risks and faster processing times. The study provided a foundation for the development of a secure and efficient electronic passport system using RFID technology, emphasizing its potential to revolutionize international travel and border control processes.

Al-Ajeely (2022) [3]– IoT-Based Passport Verification System
Al-Ajeely (2022) proposed a passport verification system using IoT equipment, aiming to enhance the security and efficiency of identity verification processes. The author designed a system integrating IoT devices, such as RFID readers and sensors, to authenticate passports and verify holder identities. The system utilizes a cloud-based database to store and manage passport data, enabling real-time verification and reducing the risk of counterfeiting. Al-Ajeely highlighted the benefits of IoT-based passport verification, including improved accuracy, reduced processing times, and enhanced security. The study demonstrated the potential of IoT technology in revolutionizing passport verification, ensuring reliable and efficient identity verification for international travel and border control applications.

III. METHODOLOGY

The proposed E-Passport verification system integrates RFID technology and biometric authentication to ensure secure and reliable identity verification[4][6]. Initially, the passport registration officer collects the user's personal information and captures the fingerprint of the passport holder. An RFID tag is then assigned to the user and linked with their biometric data and personal details in the system database. The RFID tag embedded in the E-Passport stores essential information that can be read wirelessly using an RFID reader[2][6]. This process ensures that each passport is uniquely associated with its holder and reduces the possibility of document forgery or duplication.

During verification at border control or checkpoints, the passport checker scans the RFID tag using an RFID reader to retrieve the stored passport data. The traveler is then required to place their finger on a fingerprint scanner, which captures a live biometric sample. The system processes the fingerprint image, extracts unique features, and compares it with the stored biometric template in the database[4]. If the fingerprint matches the stored data, the identity of the traveler is confirmed; otherwise, the system generates an alert indicating a verification failure or potential fraud.

After successful authentication, the system retrieves additional information related to the passport holder, such as journey details and criminal or medical records if available. Authorized personnel such as police officers and government hospital representatives can update these records in the database when required. Based on the verification results and retrieved data, the system generates a final decision regarding travel authorization. All verification activities are logged in the system for monitoring, auditing, and future reference, ensuring transparency, accountability, and enhanced security in the E-Passport verification process.

1.SYSTEM DESIGN AND ARCHITECTURE

The design of the RFID and biometric fingerprint-based digital passport system ensures secure data handling, efficient module interaction, and reliable decision-making for improved border security.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15386

System Architecture:

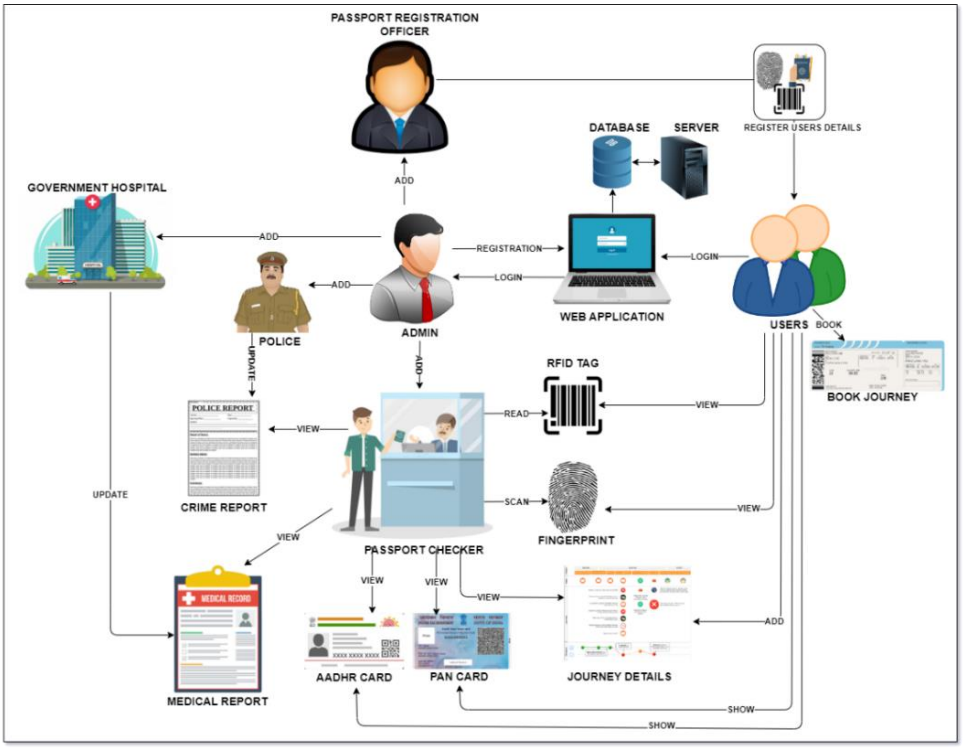

Fig 1:System Architecture

Overall architecture of the RFID and fingerprint-based digital passport verification system, illustrating interaction between the RFID reader, fingerprint sensor, Arduino Nano, database, and verification modules.

A. Overall Architecture

The system consists of:

i RFID Reader and RFID Tags
ii Fingerprint Biometric Sensor
iii Arduino Nano

2. Hardware Design

A. Arduino Nano Board

Arduino Nano is a small microcontroller board based on the ATmega328P[6], used in embedded and IoT projects. It supports easy programming using C/C++.

It includes 14 digital I/O pins, 8 analog pins, a 16 MHz crystal, USB interface, reset button, and ICSP header. It can be powered by USB or external power and is ideal for compact prototyping applications.

B. Fingerprint Scanner

To scan biometrics we are using fingerprint scanner. Fingerprint scanners have unique patterns that can be used to distinguish one scanner from another one. The pattern, which we call scanner pattern, stems from the variability of device characteristics at silicon level and is caused by imperfections of the conversion from the input to the scanner.

C. RFID Scanner/Reader

The RFID reader is also known as an interrogator[2], it provides the connection between the tag data and the software that needs the information.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15386

Circuit Diagram Of The Project:

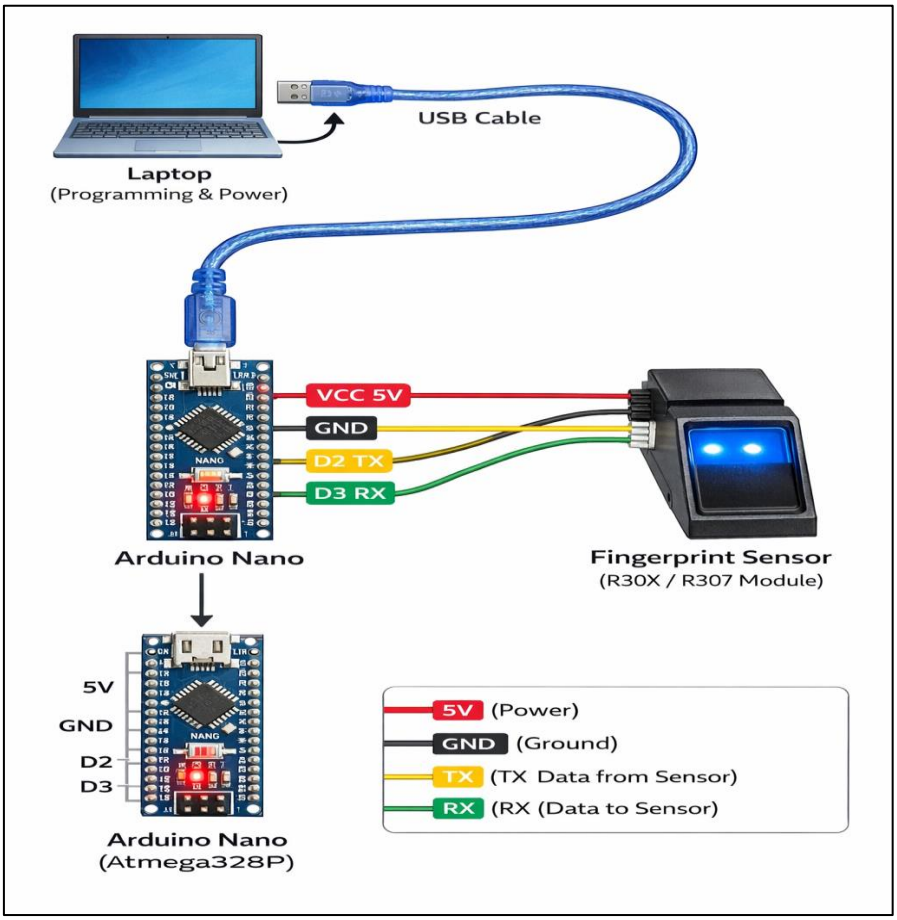

Fig 2: Circuit Diagram

Arduino Nano acts as the central controller connecting all hardware components. The RFID reader module is connected to the Arduino through power (VCC), ground (GND), and communication pins used for transmitting RFID tag data. The fingerprint scanner is also connected to the Arduino using VCC and GND for power supply and TX/RX pins for serial communication. When the RFID tag is scanned, the reader sends the tag information to the Arduino. The fingerprint scanner captures the biometric data and sends it to the Arduino for comparison and verification in the system.

IV. RESULT AND DISCUSSION

The developed E-Passport system successfully integrates RFID technology and fingerprint biometric authentication for secure identity verification. During testing, the RFID reader was able to scan the RFID tag and retrieve passport data quickly. The fingerprint scanner captured the user's fingerprint and compared it with the stored template to verify the identity of the passport holder.

The results show that the system improves the accuracy and reliability of passport verification. By linking biometric data with RFID tags, the system helps prevent identity fraud, passport duplication, and unauthorized access[4][5]. The secure database also allows authorized officials to access necessary user information when required.

The system also improves the efficiency of border control operations. RFID scanning and biometric matching reduce manual verification and speed up the authentication process. This helps in faster immigration clearance and better monitoring of travelers.

Overall, the proposed system provides enhanced security, faster verification, and improved data management. It demonstrates that combining RFID and biometric technologies can make passport verification more reliable and effective.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15386

RFID reader detecting the passport RFID tag and retrieving stored identification data

Fig 3:RFID Scanning

RFID tag detection process where the reader wirelessly scans the passport tag and retrieves the stored identification number linked to the database

RFID tag data received and processed by the verification system

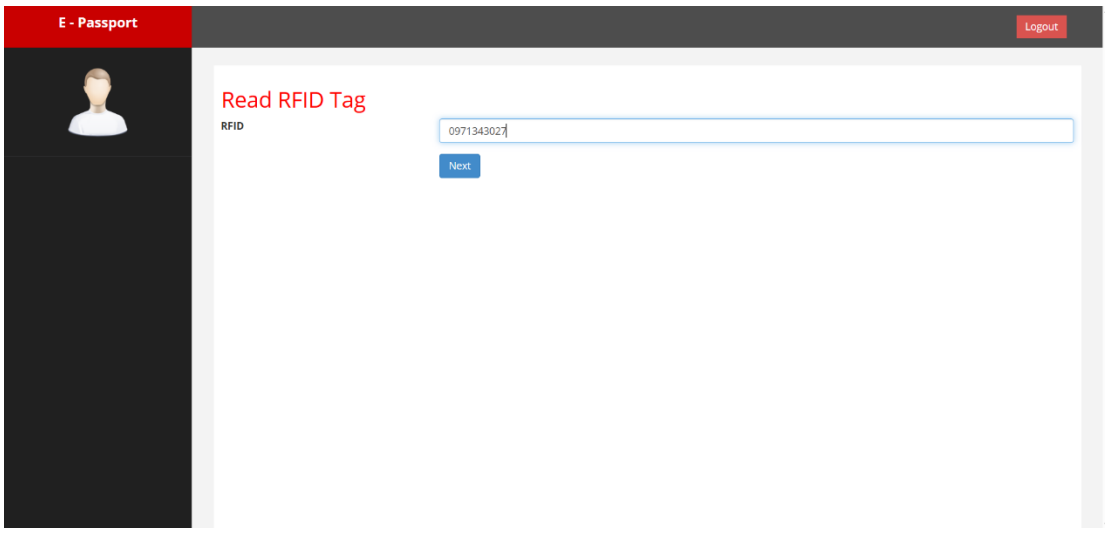

Fig 4:RFID Input

Captured RFID tag data transmitted to the system for processing and verification with stored passport holder information.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15386

Authentication failure generated when fingerprint or passport data does not match or crime is registered.

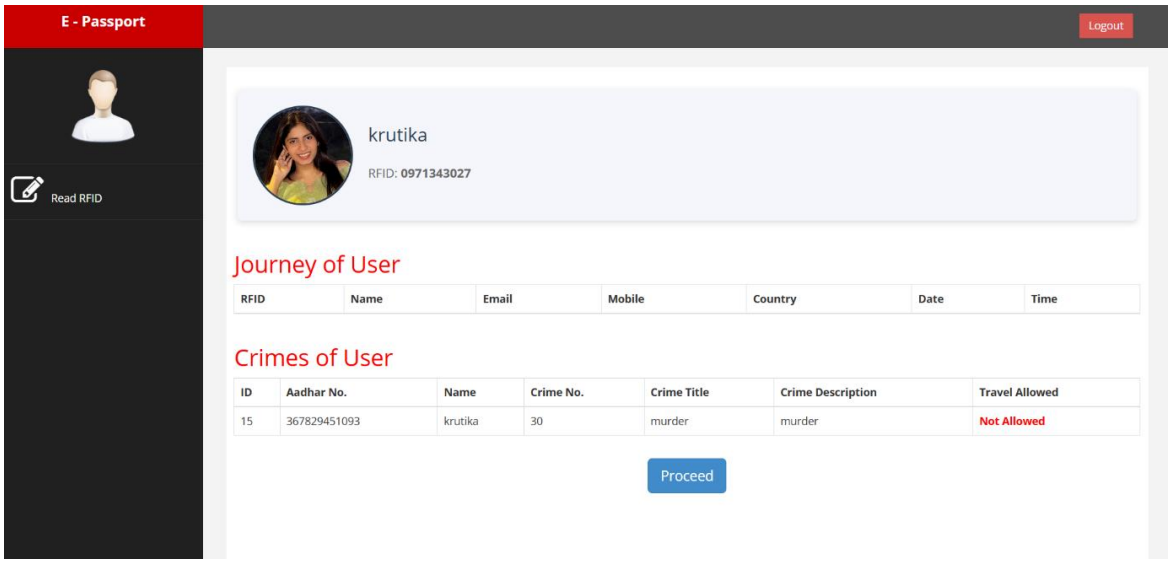

Fig 5: Final output(Negative Response)

System response generated when authentication fails due to fingerprint mismatch, invalid RFID data, or unauthorized access attempt.

Successful authentication after matching RFID data and fingerprint template.

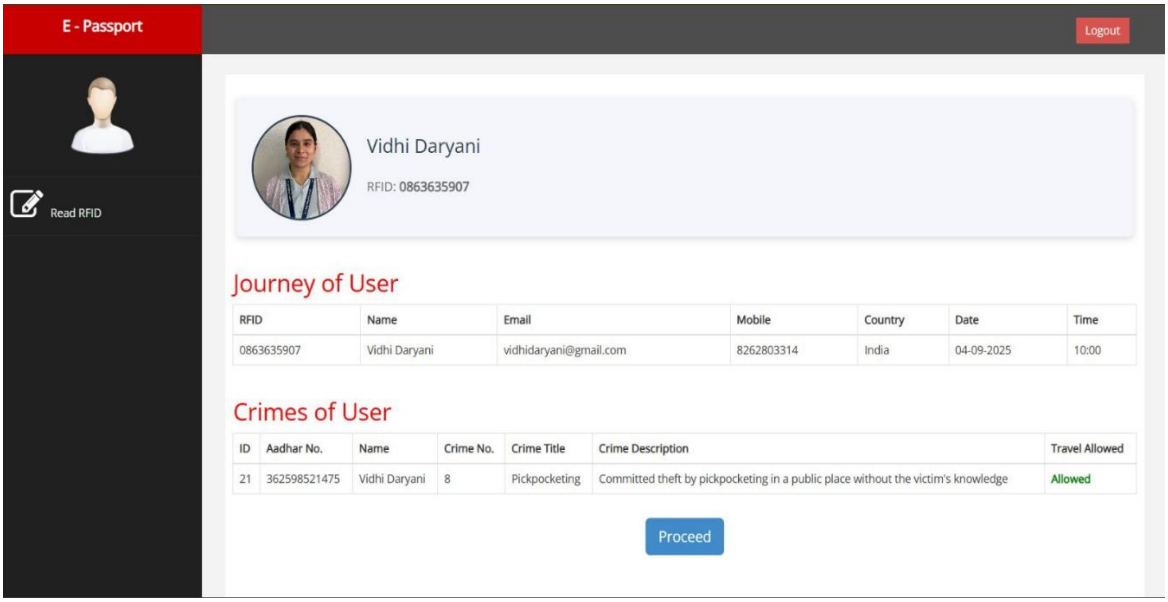

Fig 6: Final output(Positive Response)

Verification result confirming successful authentication after matching RFID information with the fingerprint biometric data stored in the system.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15386

V. APPLICATIONS

1. Secure Identity Verification: Ensures accurate identification of travelers using fingerprint biometrics and RFID technology.
2. Airport Immigration Systems: Used at airports for fast and automated passport verification during international travel.
3. Border Control Security: Helps authorities monitor and control entry and exit at national borders.
4. Counterfeit Passport Detection: Reduces the use of fake or duplicate passports through biometric authentication.
5. Law Enforcement Support: Allows police departments to access and update criminal records linked to passport holders.
6. Travel Management Systems: Enables users to store and manage their travel and journey details securely.
7. Lost or Stolen Passport Prevention: RFID technology helps track and prevent misuse of lost or stolen passports.
8. Government Identity Systems: Can be integrated with national identity and security systems for better citizen verification.

VI. CONCLUSION

The proposed RFID and fingerprint-based digital passport system provides a secure and efficient solution for identity verification. By integrating RFID technology with biometric authentication, the system improves the accuracy and reliability of passport verification compared to traditional methods[4][6].

The RFID tag stores a unique identification number that is linked to the user's personal and biometric data in the database. During verification, the RFID reader retrieves the information and the fingerprint scanner confirms the identity of the passport holder.

The integration of machine learning for crime classification adds an intelligent feature to the system. It helps in analyzing crime data and identifying potential risk levels, which can assist authorities in improving security and monitoring suspicious activities.

Overall, the system enhances security, reduces identity fraud, and speeds up verification processes. This approach demonstrates how combining RFID, biometrics, and machine learning can support modern identity management and strengthen national security.

ACKNOWLEDGMENT

With a deep sense of gratitude, we would like to thank all those who have illuminated our path with their valuable guidance during the Project Selection, Design, and Development phases. We are sincerely grateful to the intellectuals and experts who supported us and contributed to the successful completion of our project work.

It is our proud privilege to express our deep sense of gratitude to **Prof. P. T. Kadave**, Principal, K. K. Wagh Polytechnic, Nashik, for his encouragement, insightful comments, and kind permission to carry out and complete this project.

We are highly indebted to **Prof. Mrs. R. Y. Thombare**, Head of the Artificial Intelligence & Machine Learning Department, for her timely suggestions, motivation, and valuable guidance throughout the project.

We extend our sincere thanks to **Prof. H. M. Gaikwad**, Project Coordinator, for his constant support and coordination during every stage of the project work.

We also thank our classmates for their encouragement and helpful suggestions.

Lastly, we are deeply grateful to our parents and friends for their continuous support, motivation, and encouragement throughout the completion of this project.

REFERENCES

[1]Vignesh, T. et al., "An Improved E-Passport System with Secured IoT and Wireless Communication Technology," AIP Conference Proceedings, 2022.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026
DOI: 10.17148/IJARCCE.2026.15386

[2]Honade, S., Sarwar, A., Kanawade, S., Hawle, A., "Electronic Passport using RFID," International Journal of Innovative Science and Research Technology, 2022.
Al-Ajeely, Y., "Passport Verification System Development via IoT Equipment," Yanka Kupala State University of Grodno, 2022.

[3]Kumar, V. K. N., Srinivasan, B., "Biometric Passport Validation using RFID," International Journal of Computer Network and Information Security, 2021.

[4]Nirmala, M. et al., "E-Passport Verification System," International Journal of Innovative Technology and Exploring Engineering, 2020.

[5]Deepthi, M., Eranna, U., "RFID and IoT Electronic Passport Verification System," International Journal of Innovative Research in Technology, 2020.

BIOGRAPHY

Name: Mr. H.M. Gaikwad
Qualification: **B.E. Computer Engineering**
Name: Saili Ravindra Borse
Qualification: Diploma, Artificial Intelligence and Machine Learning
Name: Krutika Ravindra Bhamare
Qualification: Diploma, Artificial Intelligence and Machine Learning
Name: Vidhi Anil Daryani
Qualification: Diploma, Artificial Intelligence and Machine Learning
Name: Darshana Chetan Kothari
Qualification: Diploma, Artificial Intelligence and Machine Learning