

# KYC Smart Card

Andrew Neil<sup>1</sup>, Dselva Jagan<sup>2</sup>, Manas Manjerkar<sup>3</sup>, Aakash Nadar<sup>4</sup>, Nilambari Narkar<sup>5</sup>

*Xavier Institute of Engineering, Mahim*

**Abstract**—This project introduces KYC SmartCard, a modern identity verification platform integrating RFID smartcards and Bluetooth-based mobile authentication via an ESP32, Flutter app, and Django backend. Users can register, authenticate, and securely manage encrypted documents through dual-mode (smartcard tap or mobile pairing) interactions. Using JWT sessions and key encryption across devices and the backend, the system ensures secure, real-time, and efficient KYC processes for educational, corporate, and institutional use.

**Index Terms**— KYC, Smartcard Authentication, Bluetooth Low Energy (BLE), ESP32, Django Backend, Flutter, RFID, JWT, Key-Encryption, Encrypted Document Management.

## I. INTRODUCTION

1. Background: In today's digital landscape, robust identity verification is critical for securing access to sensitive services and safeguarding user data. Traditional KYC processes often rely on manual document checks, which can be time-consuming, error-prone, and vulnerable to forgery. The KYC SmartCard project addresses these limitations by delivering a unified platform that leverages both physical smartcards and Bluetooth-enabled mobile authentication through an ESP32 module, streamlining secure identity verification for educational, corporate, and institutional applications.

2. Motivation: Organizations and institutions face mounting regulatory requirements for accurate KYC (Know Your Customer) procedures, yet existing solutions often lack flexibility, scalability, and user convenience. Manual verification is labor-intensive, while RFID-only systems necessitate specialized hardware and offer limited mobility. This project is motivated by the need to create a cost-effective, scalable, and user-friendly verification system that empowers users to authenticate via either a smartcard tap or wireless mobile pairing, reducing operational bottlenecks and enhancing security.

3. Problem Statement: Current KYC workflows suffer from: a) Dependence on manual verification, leading to inefficiencies and increased costs. b) Fragmented authentication modes, forcing

users to switch between multiple systems for document verification. c) Security risks associated with document forgery, unauthorized access, and poor encryption management. There is a clear need for an integrated platform that consolidates physical and mobile authentication streams, ensures robust encryption, and delivers a seamless experience across web and mobile interfaces.

4. Objectives: a) Develop a dual-mode authentication mechanism supporting RFID smartcards and Bluetooth-enabled mobile devices. b) Implement JWT-based session management to maintain secure, stateless user sessions. c) Design a multi-key encryption protocol combining smartcard, database, and server keys for secure document storage and retrieval. d) Create intuitive web and mobile interfaces for registration, authentication, document upload, and secure access. e) Ensure scalability and extensibility for future enhancements, such as biometric integration or AI-driven risk assessment.

## II. LITERATURE SURVEY

1. Existing Systems Review: Existing identity verification and KYC platforms can be broadly classified into four categories:

- Manual KYC Workflows: Traditional banks and institutions rely on in-person document checks, manual data entry, and offline record-keeping. While familiar, these methods are time-consuming, error-prone, and difficult to scale.
- RFID-Based Smartcard Systems: Many organizations issue RFID-enabled ID cards or e-passports for rapid access control and verification. These systems improve speed over manual checks but require dedicated hardware readers and lack remote/mobile support.
- Mobile-Based Authentication: Solutions such as OTP/SMS verification, mobile ID apps, and biometric scanners (fingerprint or face) enable remote identity checks. Although convenient, they depend on network connectivity and often do not integrate physical card verification or secure document storage.

• **Hybrid Platforms:** A few emerging systems combine smartcards with web or mobile apps for two-factor authentication. However, they rarely support seamless Bluetooth connectivity, robust multi-key encryption, or unified document management across both web and mobile interfaces.

2. **Limitations and Gaps:** Despite advancements, current systems present several challenges:

- **Hardware Dependency:** RFID-only solutions necessitate specialized readers, increasing infrastructure costs and reducing portability.

- **Single-Mode Authentication:** Platforms typically support either card-based or mobile verification, forcing users to switch between disparate systems.

**Document Handling:** Limited support for secure document upload, real-time verification status, and automated receipt generation reduces transparency and trust.

Page 15 of 28

2.3 Mini Project Contribution

This KYC SmartCard project addresses these gaps by delivering:

- **Dual-Mode Authentication:** Users can verify identity via RFID smartcard taps or Bluetooth-enabled mobile pairing through an ESP32 bridge.

- **JWT-Based Session Management:** Stateless, token-based sessions enhance scalability and security across web and mobile clients.

- **Multi-Key Encryption Framework:** Documents are protected using keys stored on the smartcard, in the database, and on the server backend, requiring all three to decrypt.

- **Unified Web & Mobile Interfaces:** Consistent user experiences are provided through a Django web portal and a Flutter mobile app

3. Contributions:

USER	CONTRIBUTIONS
Andrew Neil	Developed the website backend, ensuring seamless communication between the server and the RFID system.
Dselva Jagan	Responsible for hardware development, including the selection and integration of RFID components.
Aakash Nadar	Worked on the frontend design, creating a user-friendly interface for accessing and managing identification data.
Manas Manjrekar	Developed the software for the RFID reader and controller, enabling

effective data processing and communication.

### III. PROPOSED SYSTEM

1. **Introduction:** Our system introduces Bluetooth-based authentication as an alternative to traditional RFID-based identity verification. The system includes:

- RFID smartcard authentication for users preferring physical verification.
- Mobile app-based authentication via Bluetooth, eliminating RFID reader dependency.
- A secure, centralized document repository to validate user identities.
- JWT-based session management for seamless and secure authentication.
- API-driven backend for handling user requests efficiently.
- Login, registration, and document upload available via both web and mobile app.
- Document sharing is facilitated via ESP32, which interacts with the smartcard and mobile app to retrieve necessary keys and send them to the website for decryption.

2. **Architecture/Framework:** The system consists of:

- RFID smartcards with encrypted user data, which communicate via ESP32 for authentication.
- Flutter-based mobile application for authentication and document management.
- Web server with API keys for login, registration, and document storage.
- ESP32 as a secure bridge between the smartcard, mobile app, and the web server.

• **Encryption Mechanism:**

- o Documents are encrypted using a combination of three keys:

- A key stored in the smartcard or generated by the app.
- A key stored in the database.
- A key stored in the server backend.

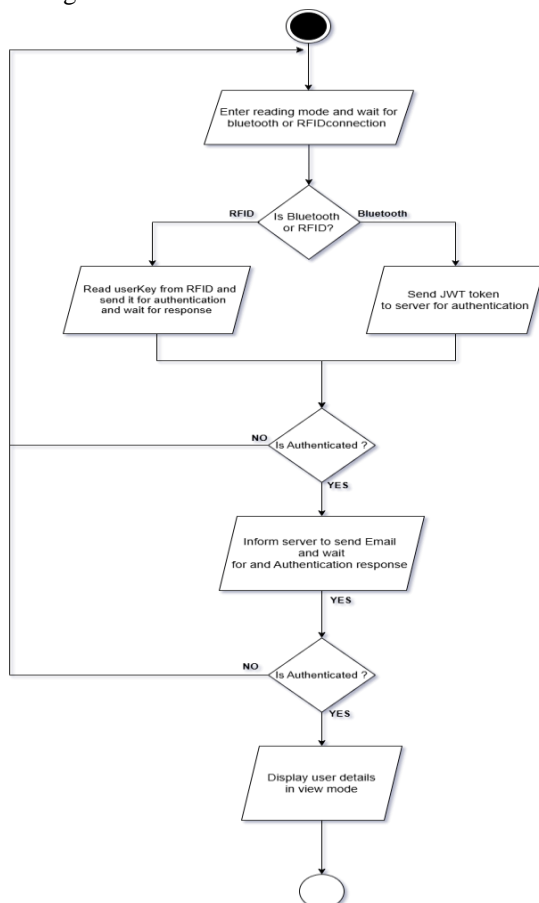
- o Only when all three keys are retrieved and combined can the document be decrypted and displayed.

3. **Algorithm and Process Design:**

1. **User Registration:**

- a. Users sign up via the Flutter mobile app or web platform.
- b. API calls authenticate users and store documents securely.

2. Authentication: a. If using RFID smartcard, tap the card on an RFID reader. b. If using mobile app, establish a Bluetooth connection and authenticate.
3. Document Upload: a. Users can upload documents via both the web platform and mobile app.
4. Document Sharing: a. The smartcard and mobile app retrieve the necessary key and send it to ESP32. b. ESP32 sends the key to the website, where it is combined with the database key and server backend key for decryption. c. Once decrypted, the document is securely displayed.
5. Access Granted/Denied: a. The app or system displays verification results.
  - The process starts with the initialization of the authentication system through the rfidcard or the Bluetooth device.
  - Next the esp32 sends the id to the backend for the backend to check if the user exists and this sends a response to esp32.
  - If the backend response is positive the email is sent to the users email else the system goes to back and waits for any initiation of authentication.
  - Then the email containing the authentication link is send to the user
  - If it is successful then the documents are displayed else the system goes back to its state where it is waiting for authentication initiation.



#### IV. DETAILS OF HARDWARE & SOFTWARE

##### 1. Hardware:

- RFID Smartcards with integrated Bluetooth modules.
- Mobile devices with Bluetooth connectivity.

##### 2. Software:

- Flutter-based Mobile App with JWT-based session management.
- Web Server Django with API endpoints.

##### 3. Database:

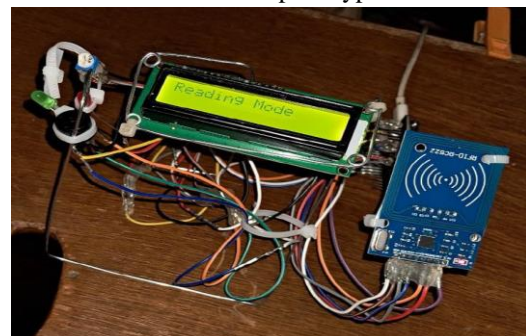
- SQLite for secure data storage.

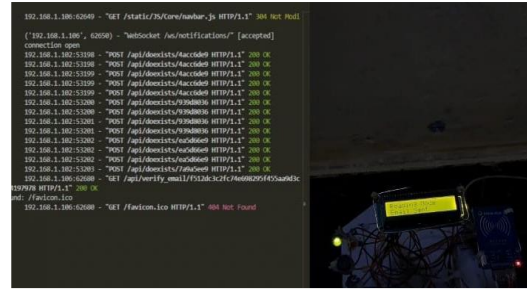
##### 1. Components Used:

- RFID Reader (RC522): The system employs an RC522 RFID module, which is responsible for reading the RFID tags presented by the user.
- 16x2 LCD Display: A liquid crystal display (LCD) is used to provide real-time information feedback, such as system status or document retrieval modes.
- ESP32 (Microcontroller): The system is driven by a microcontroller, which coordinates the communication between the RFID module and the server.
- Buzzer and LEDs: Visual and audio indicators are provided to signal successful or failed operations, improving user interaction.
- Wiring Setup: The various components are interconnected with a well-organized set of jumper wires to facilitate communication and power distribution.

#### V. EXPERIMENTS & RESULTS

- This is how the actual prototype looks like

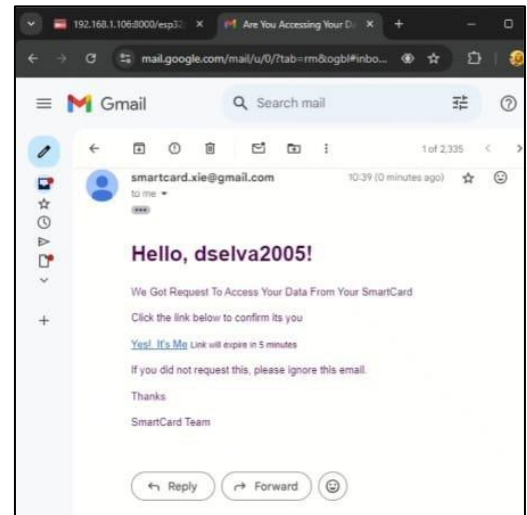





- 

- 

- This is the email sent to the user for 2-step verification.

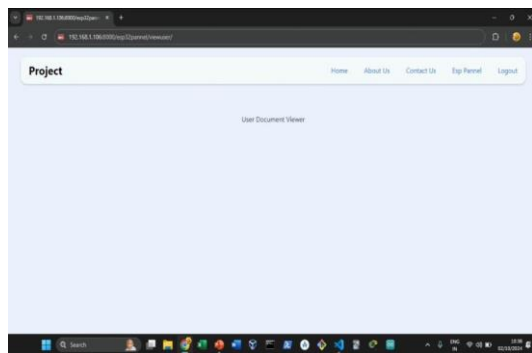


- 

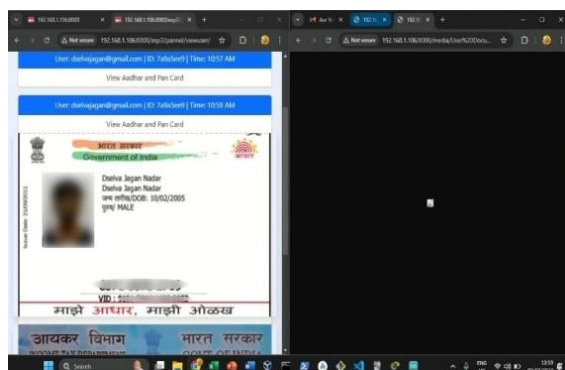
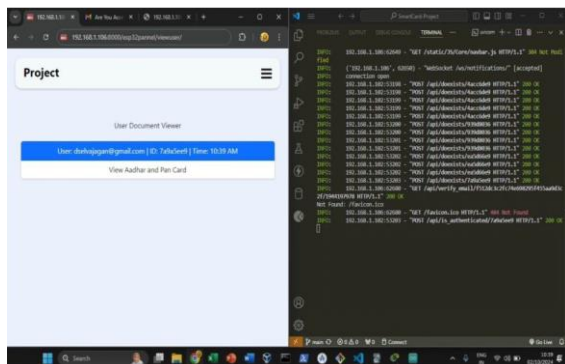
- 
- A screenshot of a web browser window. The address bar shows the URL '192.168.1.106:8000/api/verify\_email/f512d...' with a 'Not secure' warning. The main content area displays the text 'Access Granted' in a large, bold, black font.

- When the user is found in the database and is authenticated. The green light indicates successful verification. The terminal shows the endpoints hits at the server.

- This is the “VIEW ONLY” page where the documents are shown for KYC. These documents are displayed when the user clicks the verification link sent on to their email.



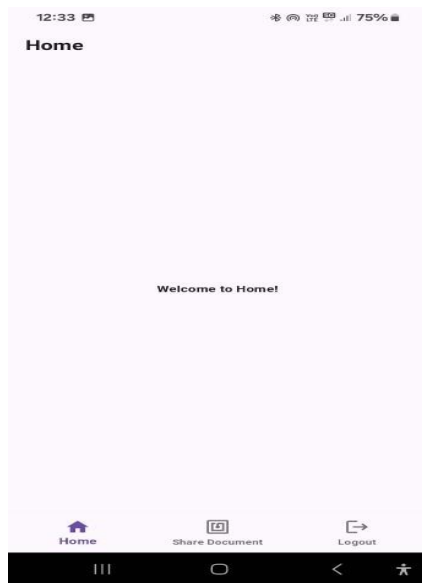
- The user documents are shown in “VIEW ONLY MODE”. But the documents are encrypted in the backend.



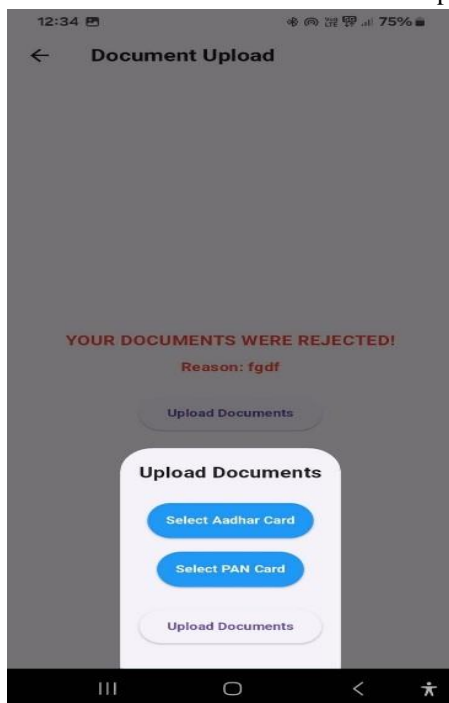
- App Register Page, this is the first page shown to a new user who opens the application here the user will register himself and the otp verification through email also takes place.

- This is app Login Page, this page is followed by the previous registration page here the user will login with the details that he/she has used during the registration process.

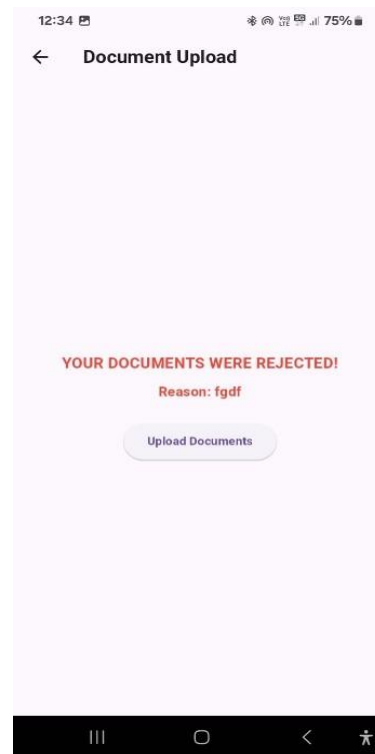
- This is App Home Page, when the login is successful this is the page where the user is directed to, similar to the home page of the website here the use will manage his account, and any message if exists will be shown to the user and here too a form for new user will be shown to enter his/her documents.



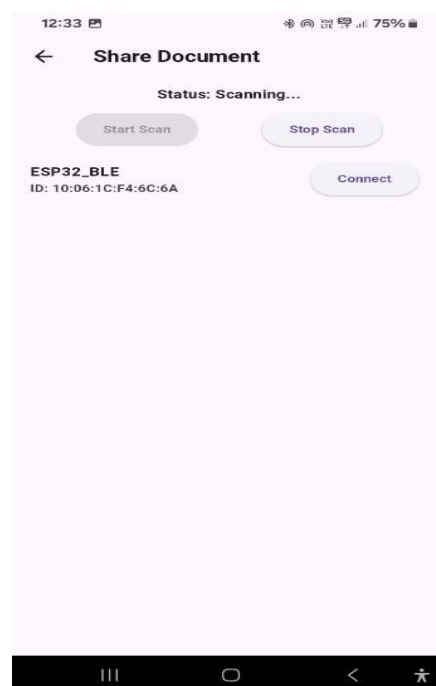
- This is App document upload page, this is the form that expects the user documents, as shown below the form will ask the user for the documents to upload.



- This page indicates the state of the documents, now it is in verification state. Once the admin verifies the documents and approves this message will disappear.
- This is the same page as above, but not the state of the document is rejected, if the admin rejects the application this page show that the document is rejected with the reason for rejection of the documents once the user rectifies the issue he can reupload the documents.



- This page detects our Bluetooth verification system, the application scans its vicinity for any Bluetooth device and filters out our verification system with its name, here the user can initiate the authentication process by clicking the connect button, this action is same as using the card and tapping it on the reader, after this the two-step verification kicks in and the documents are displayed.



## VI. CONCLUSION

The Bluetooth-enabled KYC SmartCard system successfully integrates dual authentication modes, combining RFID smartcard and mobile app-based verification to deliver a secure, efficient, and accessible identity verification solution. By leveraging Bluetooth connectivity through the ESP32 module and a Flutter-based mobile app, the system eliminates dependency on dedicated RFID hardware, enhancing user convenience and scalability. The implementation of JWT-based session management and a robust encryption mechanism, utilizing three-key document decryption, ensures secure data transmission and controlled document sharing, significantly reducing risks of unauthorized access. The system's architecture supports seamless integration across educational, corporate, and other sectors requiring reliable KYC processes.

## VII. FUTURE WORKS

1. Strengthen security with advanced encryption
2. Implement features of registering groups and permissions of file access
3. Expand scalability to diverse sectors like healthcare, banking, and government services.
4. Incorporate real-time analytics and machine learning for performance optimization and anomaly detection.

## ACKNOWLEDGMENT

We as a group, consisting of Andrew Neil (41), Dselva Jagan (37), Aakash Nadar (38), Manas Manjrekar (31) would like to express our heartfelt gratitude to the Principal, Dr. Y. D. Venkatesh, the Head of Department, Prof. Kavita Jain, Guide, Prof. Nilambari Narkar and the Xavier Institute of Engineering, Mahim for giving us the best guidance possible and making learning a fun experience.

## REFERENCES

- [1] "RFID in Document Management: Design and Implementation"  
Publisher: IEEE, 2018  
Electronic ISSN: 2169-3536
- [2] "Improved RFID Authentication for Secure Document Access"  
Publisher: IEEE, 2011  
Electronic ISSN: 1556-6013

- [3] "RFID-based Authentication for Digital Documents"  
Publisher: IEEE, 2021  
Electronic ISSN: 2469-7281
- [4] "An introduction to RFID technology"  
Publisher: IEEE, 2006  
Electronic ISSN: 1558-2590
- [5] "Design and Implementation of RFID Based E-Document Verification System"  
Publisher: IEEE, 2021  
Electronic ISSN: 6654-3877
- [6] "Django: Developing web using Python"  
Publisher: IEEE, 2023  
Electronic ISSN: 3503-9926
- [7] "Python & Django the Fastest Growing Web Development Technology"  
Publisher: IEEE, 2024  
Electronic ISSN: 3503-7304
- [8] "IoT based Circuit Breaker with Access Control"  
Publisher: IEEE, 2023  
Electronic ISSN: 3503-3360
- [9] "Design of a people access control system using the ESP32 module and Internet of Things for a sanitary facility in a shopping mall"  
Publisher: IEEE, 2022  
Electronic ISSN: 6654-5082