Apr Smart Identity System

Krushna M. Patil[1], Dr. Bhushan V. Patil[2], Aishwarya R. Marathe[3], Payal R. Patil[4] and Shwetali D. Bhalkar[5]

[1,3,4,5] UG-Students, Department of Electronics and Telecommunication Engineering, R. C. Patel Institute of Technology, Shirpur, Maharashtra, 425420, India

[2] Assistant professor, Department of Electronics and Telecommunication Engineering, R. C. Patel Institute of Technology, Shirpur, Maharashtra, 425420, India

***Abstract*—Identity verification in India, when verifying identity, users frequently need multiple identity verification documents, such as Aadhaar Card, PAN Card, and Ration Card, and as a result, this process will take more time, and will likely lead to delays due to manual entries, or errors in entries and verification processes. The proposed system introduced is called The APR Smart Identity System, which is an In-One Solution that will consolidate the three identity verification documents into one Identity Verification Document using RFID Technology. The APR Smart Identity System includes the NodeMCU ESP8266 and the MFRC522 RFID Reader for authenticating users and displaying the results on a 16 x 2 LCD, while also allowing the automatic upload of verification logs and information to the cloud using Internet of Things (IoT) technologies. The system will allow users to verify their identity faster, reduce the amount of paperwork required to do so, and allow for a single place to maintain a record of their identity verification. Therefore, the APR Smart Identity System will be a viable solution for both government and public service organisations.**

***Index Terms*—RFID, IoT, APR Smart Identity System, Aadhaar Verification, PAN Verification, Ration CardIntegration, NodeMCUESP8266, MFRC522, Smart Card Authentication.**

I. INTRODUCTION

In India, identity verification is vital to all administrative and financial systems. Citizens need to present at least three different types of identification issued by the government: the Aadhaar card, the PAN card and the ration card. Each of these cards serves a different function and is managed by different institutions. Although these documents provide accurate identification for citizens, they do so in a fragmented manner leading to inefficiencies and delays in the verification process, as well as increased reliance on manual handling. Therefore, it is challenging to manage identity verification consistently in public sector locations, such as government offices, ration distribution centres, banks and any other entity where Id verification is regularly required for essential services. For example, having to review each of these documents multiple times increases the likelihood of losing physical documents, slows down the processing time because of manual validation processes and ultimately necessitates the development of an integrated, automated approach to identity management. India has made significant strides toward digital governance via projects such as Digital India, Aadhaar e KYC, Online PAN Verification, and Digital Ration Cards; however, verification of identity is still largely decentralised and fragmented across the nation. These services provide improved accuracy in the area they are intended to serve; however, they do not address the central issue, which is, that citizens must still hold multiple identity documents and provide service providers with separate authentication processes for each of those documents. As a result, this presents a major administrative burden on both citizens and service providers and, thus, not only induces human error but also reduces efficiency and slows down the pace of service delivery. This is particularly true in areas where there is a high volume of transactions taking place, such as banks and public distribution shops.

The suggested system provides an economical, expandable, and simple method of managing identity, which makes it extremely beneficial for many governmental authorities, ration stores, banks, and other publicly funded organisations. The combination of user-friendliness with automation and integration into the cloud under the APR Smart Identity System will help to increase operational efficiency, decrease verification time, decrease the likelihood of human error, and improve service to customers. Furthermore, this project supports India's overall digital transformation strategy by providing a tangible model for implementing integrated identity verification and 'Smart Governance.

II. LITERATURE SURVEY

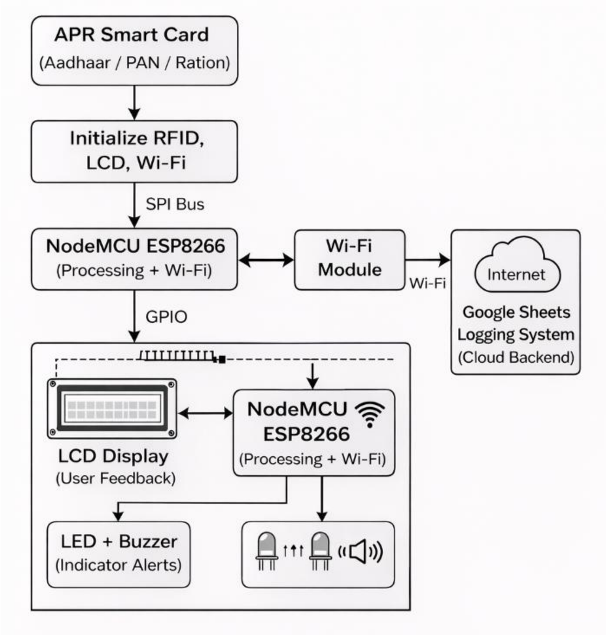
RFID has emerged as the solution of choice when it comes to automated identification since it is inexpensive, robust and is not line of sight based. Research indicates that it is extensively used in access control, attendance terminals and service authorisation with modules like the MFRC522 that provide fast UID based logins. However, the existing RFID systems are not capable of securely storing and authenticating a number of the identities issued by the government in addition to the single one that is verified. The use of IoT will enhance verification through cloud connection. It enables real time logging, central monitoring, and eliminates the use of manual record keeping. Low-power Wi-Fi microcontrollers (NodeMCU ESP8266 and ESP32) demonstrate that it is possible to upload authentication logs to such services as Google Sheets and Firebase. However, the majority of the existing systems are only compatible with event-based authentication and are not capable of integrating several sets of identities into a single verification card. Meanwhile, the ecosystem of India digital identity is advancing tremendously: Aadhaar, PAN and digitised public distribution. However, every system remains distinct, and each has its authentication policies that establish de-facto fragmented verification procedures of citizens. Research indicates that even smart-card solutions being implemented in universities and companies are specific to the institution and have no national identity data. The RFID security research identifies cloning as well as unauthorised access as risks. There are encrypted RFID and blockchain identity proposals, which are costly and inapplicable in rural regions. Altogether, no single system integrates RFID-based authentication, combining Aadhaar, PAN, and ration records with automatic registration of events to the cloud. In order to address this gap, the APR Smart Identity System is suggested. It is scalable, IoT-enabled, and affordable and it provides integrated identity verification of services to people.

III. METHODOLOGY

The approach taken on the APR Smart Identity System is developed such that it would guarantee the systematic manner of consolidating identity, RFID based authentication, and data transmission using IoT. The methodology proposed has 4 significant elements that include system architecture design, hardware integration system, software implementation and cloud-based communication workflow.

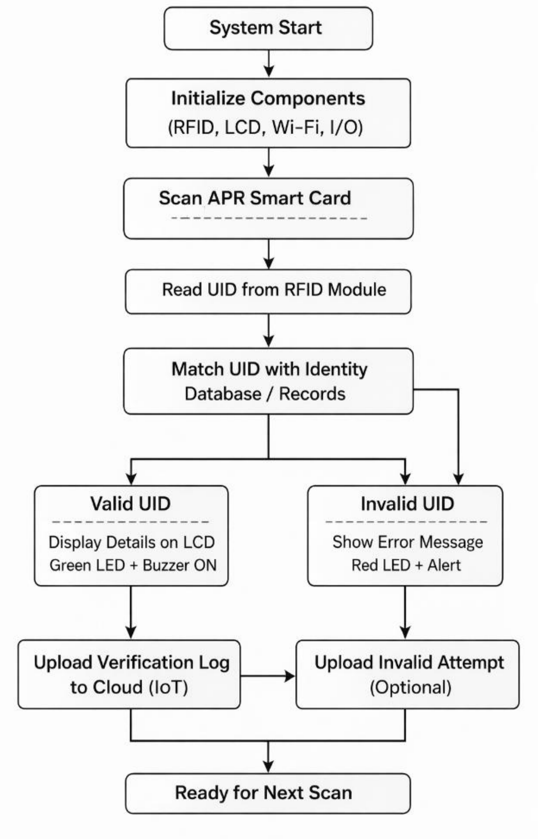
A. SYSTEM ARCHITECTURE

the architecture incorporates Aadhaar, PAN and ration card data in a single RFID identity token. It is powered by an MFRC522 RFID reader to derive the UID and a NodeMCU ESP8266 microcontroller to process and wifi and finally to a 162 LCD, LED displays, and buzzer. An API maintained in Google Sheets records data in real time. This design maintains hardware, software, and internet of things protocols abreast with less complexity and at low cost.



B. HARDWARE INTEGRATION

The MFRC522 RFID module is based on the 13.56 MHz frequency and communicates with the NodeMCU using SPI. Each time a card is scanned the module receives its UID and transmits it to the microcontroller. The NodeMCU compares the UID with stored data and generates feedback. User details or errors are displayed on LCD, visual and audio feedback are provided by LEDs and a buzzer. The control of power and grounding has also been included to ensure that the hardware remains constant across repeated scans.



C. SOFTWARE IMPLEMENTATION

The arduino IDE was used to write the firmware. The code begins with the loading of RFID and LCD libraries, UID reading, and comparison against stored identities with setting of a status flag. The card contains the UID only, all the personal data remain in the firmware, so the information is safe. The Wi-Fi of the NodeMCU links itself to a cloud script which auto-uploads logs. The UID, time, check result, and device ID is assigned to each log.

D. IOT-ENABLED CLOUD COMMUNICATION

We simply included an internet of things (IoT) layer that can make HTTP GET/POST requests to Google Apps Scripts. In both cases of successful and unsuccessful login, the information will be uploaded to a Google sheet that serves as a central log. This will permit real time surveillance, remote access, and impeccable records. The protocol was configured to reduce all latency and remain dependable with low bandwidth.

E. OPERATIONAL WORKFLOW

After a user swipes the card on the reader, the UID is read by the NodeMCU, which then verifies it, registers the event on LEDs and the buzzer and sends it to the cloud. In case the UID is valid, the LCD displays the user and a green LED goes on. Otherwise, an error message is showed, a red LED or a buzzer warns the user. The system then will restart and wait till the next scan. Not only does this flow provide fast, dependable, and automatic verification.

F. SYSTEM VALIDATION

Each part was run through unit test, and through the integration process, we ran the tests, checked UID accuracy and tested latency of the cloud-logs and tested the repeat scans to determine reliability. The system was rated to be highly accurate, responsive, and consistent communicating as evidence of its readiness to be used in real world.

IV. RESULTS AND DISCUSSION

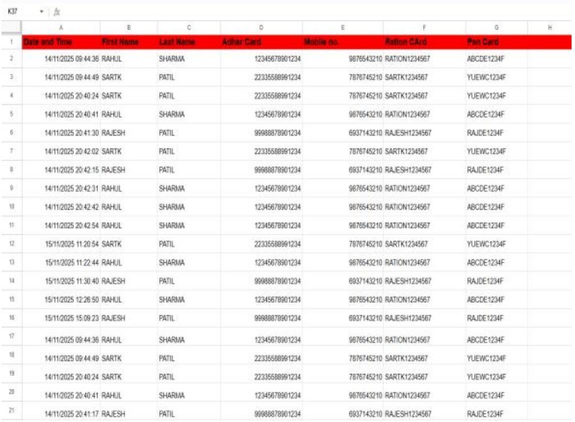
It was experimentally tested to check the accuracy, response time, reliability, and the overall performance of the proposed APR (Aadhaar-PAN-Ration) Smart Identity System in identity verification in the real-life situation. A prototype created was based on a NodeMCU ESP8266 microcontroller, a MFRC522 RFID reader, APR smart cards, 16 x 2 LCD display, LED indicators, and a buzzer, and Google sheets served as the cloud component behind the IoT based-logging. There were test cases of many cases with valid and invalid RFID cards in the stable network conditions.

When the cards were tested with authenticity, the system was always able to read RFID tags in the short scanning range of about 35 cm. The RFID reader was able to read the unique identifier (UID) and this was processed and compared to identity records stored locally. When this was successful it was able to show the relevant user information on the LCD display, this turns the green LED and produced one beep on a buzzer. At the same time, the verification data, UID and authentication status and timestamp were uploaded to cloud. On the contrary, the scanning of invalid or unauthorized cards resulted in a UID mismatch as immediately pointed out by the system. The LCD showed an error message, the red LED on was triggered, and a double buzzer warning was created, and it was clear a failure of authentication. Also validating invalid attempts was optional.

The analysis about performance showed that the overall time of verification (including card recognition until the display of the information to the user) was 1 to 2 seconds. These comprise acquisition of RFID UID, local verification, generation of output and asynchronous cloud logging. Since the matching of UID was done in the local area, the speed of authentication was not affected by the network latency, so the system was applicable in high-throughput settings like ration shops and government service centres. The system had 100 0 percent authentication accuracy across numerous trials of a number of valid and invalid cards and false acceptance and rejection were not observed.

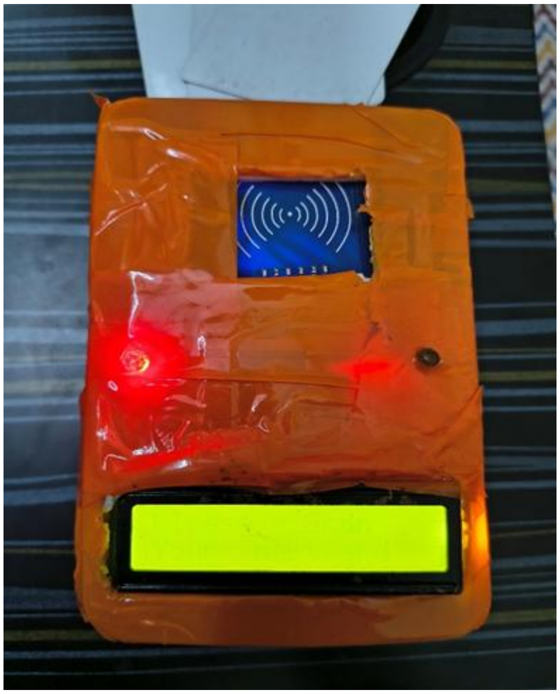
The IoT-based cloud logging system was very reliable and was tested to be so. All the verification records were always uploaded in Google sheets with proper timestamps and status of classification. The system also ensured data integrity when disconnected on momentary Wi -Fi by automatically rejoining the network without losing any data. Load testing which was done by passing through a series of cards did not reveal any observable delay, system failure or mismatch of display and cloud records. The entries in the cloud database were still in the appropriate chronological order which indicated the database to be working well under constant use.

Relative analysis with traditional manual validation systems points into the huge enhancement of efficiency, and transparency. The traditional way involves the use of various hard copies, use of a manual check and handwritten registers. The APR system allows the single card verification with automated digital record keeping, less paper work, no human errors, faster service delivery as well as auditability. All in all, the findings of the experiment validate the hypothesis that the APR Smart Identity System is a fast, accurate, and reliable unified identity verification system that has high prospects of scalable implementation in government and public service systems.



	A	B	C	D	E	F	G	H
1	Date and Time	First Name	Last Name	Adhar Card	Mobile no.	Ration CArd	Pan Card	
2	14/11/2025 09:44:36	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
3	14/11/2025 09:44:49	SARTK	PATIL	22335588991234	7876745210	SARTK1234567	YUEWC1234F	
4	14/11/2025 20:40:24	SARTK	PATIL	22335588991234	7876745210	SARTK1234567	YUEWC1234F	
5	14/11/2025 20:40:41	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
6	14/11/2025 20:41:30	RAJESH	PATIL	99988878901234	6937143210	RAJESH1234567	RAJDE1234F	
7	14/11/2025 20:42:02	SARTK	PATIL	22335588991234	7876745210	SARTK1234567	YUEWC1234F	
8	14/11/2025 20:42:15	RAJESH	PATIL	99988878901234	6937143210	RAJESH1234567	RAJDE1234F	
9	14/11/2025 20:42:31	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
10	14/11/2025 20:42:42	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
11	14/11/2025 20:42:54	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
12	15/11/2025 11:20:54	SARTK	PATIL	22335588991234	7876745210	SARTK1234567	YUEWC1234F	
13	15/11/2025 11:22:44	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
14	15/11/2025 11:30:40	RAJESH	PATIL	99988878901234	6937143210	RAJESH1234567	RAJDE1234F	
15	15/11/2025 12:26:50	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
16	15/11/2025 15:09:23	RAJESH	PATIL	99988878901234	6937143210	RAJESH1234567	RAJDE1234F	
17	14/11/2025 09:44:36	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
18	14/11/2025 09:44:49	SARTK	PATIL	22335588991234	7876745210	SARTK1234567	YUEWC1234F	
19	14/11/2025 20:40:24	SARTK	PATIL	22335588991234	7876745210	SARTK1234567	YUEWC1234F	
20	14/11/2025 20:40:41	RAHUL	SHARMA	12345678901234	9876543210	RATION1234567	ABCDE1234F	
21	14/11/2025 20:41:17	RAJESH	PATIL	99988878901234	6937143210	RAJESH1234567	RAJDE1234F	

GOOGLE SHEET DATA



FINAL PRODUCT

V. CONCLUSION

This study will examine the design, implementation and evaluation of the APR (Aadhaar PAN Ration), a single RFID and IoT-based system that can streamline identity checking in India. The suggested system eliminates the shortcomings of the traditional ways, which are based on a plurality of physical documents, manual verifications, and fragmented accountability. The APR system has been able to provide contactless, fast, and automated authentication of identities by combining Aadhaar, PAN, and ration-card credentials on a single RFID smart card. The APR provides an MFRC522 RFID reader together with a NodeMCU ESP8266 microcontroller, which offers an effective and cost-efficient embedded solution that is capable of processing real-time data and transmitting it wirelessly. A local UID-based validation is fast to authenticate in situations where the network connection is not available, whereas the use of cloud logging provided by Google sheets also introduces transparency and traceability to the process and an easy access to information. Experimental tests indicate that the system attains high system accuracy, low system response time and reliable system performance during sustained use making it appropriate to use in the real world.

We find that the APR Smart Identity System has a significant reduction of manual effort, eradication of human error and an increase in service efficiency over slow exhausting procedures. Its scalable nature is designed in different modules that can fit government offices, public distribution systems, banks, schools, and any other identity-related services. To conclude, the system will provide a viable, economical, and scalable identity authentication solution and contribute to larger objectives of digital governance and the Digital India program.

VI. REFERENCES

[1] Unique Identification Authority of India (UIDAI), Aadhaar Authentication API Specification, Government of India. [Online]. Available: https://uidai.gov.in

[2] Ministry of Finance, Government of India, PAN–Aadhaar Linking Guidelines, Income Tax Department, India.

[3] Patil, B.V. and Patil, P.S. (2025), IoT-Enhanced Meta-Heuristic Hybrid Deep Learning Model for Predicting Cotton Leaf Diseases. J Phytopathol, 173: e70058. https://doi.org/10.1111/jph.70058

[4] NXP Semiconductors, MFRC522 RFID Reader Datasheet, 2022.

[5] Espressif Systems, ESP8266EX Datasheet, Espressif Inc., 2021.

[6] S. Want, “An Introduction to RFID Technology,” IEEE Pervasive Computing, vol. 5, no. 1, pp. 25–33, 2006.

[7] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 3rd ed., Wiley, 2010.

[8] R. Want, “Near Field Communication,” IEEE Pervasive Computing, vol. 10, no. 3, pp. 4–7, 2011.

[9] M. A. Al Mamun et al., “Internet of Things (IoT) Based Smart Authentication Systems,” IEEE Access, vol. 8, pp. 129–145, 2020.

[10] Google Developers, Google Apps Script Web API Documentation. [Online]. Available: https://developers.google.com/apps-script

[11] A. Juels, “RFID Security and Privacy: A Research Survey,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 2006.

[12] Patil, B.V., Patil, P.S. (2021). Computational Method for Cotton Plant Disease Detection of Crop Management Using Deep Learning and Internet of Things Platforms. In: Suma, V., Bouhmala, N., Wang, H. (eds) Evolutionary Computing and Mobile Sustainable Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 53. Springer, Singapore. https://doi.org/10.1007/978-981-15-5258-8_81S. Singh and N. Singh, “Internet of Things (IoT): Security Challenges, Business Opportunities & Reference Architecture,” IEEE International Conference on Green Computing and Internet of Things, 2015.

[13] A. Kumar et al., “Smart Card Based Multi-Application Identity Systems,” International

Journal of Engineering Research and Technology (IJERT), vol. 9, no. 5, 2020.

[14] D. Johnson, A. Menezes, and S. Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA), IEEE Press, 2001.

[15] Government of India, Digital India Programmed, Ministry of Electronics and Information Technology (MeitY).

[16] B. V Patil and P. S. Patil, "A Composite Meta Model for the Identification of Cotton Pathologies Utilizing an IoT-Enabled Framework and Stacked Generalization Learning Methodology", Int. Res. J. multidiscip. Tec novation, vol. 6, no. 6, pp. 128–144, Nov. 2024.