IoT-Enabled Smart ATM Security System Using Face Recognition, RFID, and OTP Verification

V.Shravya [1], Dr.Md.Asim iqbal [2] , Dr.K.Devarajan [3]

[1]M.Tech Scholar, Dept of ECE, Kakatiya University Campus, Warangal, Telangana, India.

[2]Assistant Professor, Kakatiya University Campus, Warangal, Telangana, India

[3]Assistant Professor, Annamalai University, Tamilnadu, India

shravyavodapelly@gmail.com[1] , mdasimiqbal605@gmail.com[2] ,devarajan_lecturer@yahoo.com[3]

ABSTRACT

The growing incidents of cyberattacks and ATM-related crimes have created a pressing need for smarter and more secure banking systems. This project introduces an IoT-enabled ATM Security System that combines facial recognition, RFID authentication, and OTP verification to establish a strong, multi-layer security framework before any cash withdrawal is permitted. In this system, the verification process begins with face detection and recognition, implemented using Python and OpenCV. The user's image is captured through a camera and compared with the existing records in a secure database to confirm identity. Once facial verification is successful, the system requests the user to scan an RFID card, which is validated against the stored information. If the RFID data matches, an OTP (One-Time Password) is automatically generated and sent to the registered mobile number to provide an additional layer of security. After entering the correct OTP through a mobile application, the user can specify the amount to withdraw. The mobile app communicates with a NodeMCU ESP8266 microcontroller through Firebase or MQTT, which manages the interaction between the software and hardware components. The NodeMCU then activates a motor mechanism that simulates the cash dispensing function, and an LCD with an I2C interface shows real-time transaction updates and status messages. This integrated system enhances ATM security by uniting biometric verification, RFID authentication, and OTP validation within a single IoT framework. It allows real-time monitoring, remote access, and data management, ensuring a reliable and intelligent solution for preventing unauthorized access and improving user safety in modern banking environments.

Keywords: IoT, ATM Security, Face Recognition, RFID Authentication, OTP Verification, NodeMCU, Image Processing.

1.INTRODUCTION

In today's digital era, banking systems play a vital role in ensuring financial convenience and accessibility to customers worldwide. Among various financial services, the Automated Teller Machine (ATM) is one of the most widely used facilities that enables users to perform banking operations anytime and anywhere. However, as ATM usage continues to grow, so does the risk of fraudulent activities such as card skimming, unauthorized withdrawals, and identity theft. These threats have raised serious concerns about the reliability and safety of traditional ATM systems, which often depend solely on card and PIN-based authentication methods.

The increasing sophistication of cybercriminals and the rise in physical ATM attacks have highlighted the need for a more secure, intelligent, and multi-layered security mechanism. Traditional methods like PIN entry are no longer sufficient because personal identification numbers can be easily stolen or guessed. To overcome these limitations, integrating modern technologies such as biometrics, IoT, and real-time data communication can significantly enhance security and reliability.

This project focuses on developing a Smart IoT-Based ATM Security System that combines facial recognition, RFID verification, and OTP authentication to ensure multiple levels of user validation before allowing any transaction. The system leverages image processing techniques using Python and OpenCV for accurate face detection and recognition, which acts as the primary security layer. Once facial identity is verified, RFID technology is used to authenticate the user's ATM card, and a final One-Time Password (OTP) is sent to the registered mobile number for additional verification.The integration of NodeMCU ESP8266, Firebase or MQTT communication, and a mobile application provides seamless connectivity between the user interface and hardware components. The NodeMCU controls the motor mechanism that simulates cash dispensing and displays transaction updates on an LCD screen. This interconnected IoT system allows remote monitoring, real-time alerts, and secure data exchange, ensuring improved reliability and accountability in every transaction.

Overall, this project aims to provide a secure, efficient, and intelligent ATM model

capable of preventing unauthorized access and financial fraud. By incorporating IoT and biometric technologies, the proposed system offers a modern approach to ATM security, ensuring enhanced user safety, transparency, and trust in the banking environment.

OBJECTIVES

The main objective of this project is to develop a secure and intelligent ATM system that combines biometric face recognition, RFID-based card verification, and OTP authentication to ensure multi-level user authentication. The system aims to prevent unauthorized access and reduce the risk of ATM fraud by providing real-time monitoring and transaction verification through an IoT-enabled framework. Additionally, the project seeks to enhance user convenience by automating the authentication process, enabling remote monitoring, and integrating a mobile application for seamless interaction with the ATM system. The ultimate goal is to create a reliable, efficient, and modern banking security solution that addresses the limitations of traditional ATMs.

2. LITERATURE SURVEY

1. Ramesh Kumar et al. (2018) In their study on "IoT-Based Smart ATM Security System," the authors proposed an IoT-integrated model for enhancing ATM security. The system used sensors, GSM modules, and microcontrollers to detect unauthorized access and send alerts to authorities. Their approach demonstrated that integrating IoT devices could significantly improve real-time monitoring and prevent ATM vandalism.

2. Priya Sharma and Ankit Verma (2019) These researchers introduced a model focusing on biometric authentication using fingerprint recognition for ATM users. Their system replaced traditional PIN-based access with fingerprint scanning, improving accuracy and user convenience. The paper emphasized the importance of biometric verification for preventing card misuse.

3. Sanjay Gupta et al. (2020) This research proposed an intelligent ATM system that uses facial recognition through image processing techniques. Using OpenCV and Python, they achieved accurate facial detection and identification of users. The authors concluded that face recognition provides a reliable and user-friendly security

layer compared to conventional password systems.

4. Neha Patel and Suresh Babu (2020) Their work focused on combining RFID-based authentication with IoT communication for banking security. The RFID card stored encrypted user credentials, which were verified through a microcontroller. The study highlighted that RFID offers a fast, contactless, and secure method for identity verification in ATM systems.

5. Deepak Reddy et al. (2021) The authors developed an ATM protection system using GSM and RFID modules. Their system sent SMS alerts in case of unauthorized card usage or mechanical tampering. The research proved that GSM-based alert systems enhance response time and reduce damage during fraudulent attempts.

6. Sneha Joshi and Rahul Mehta (2021) They proposed a three-step ATM authentication system combining face recognition, OTP verification, and RFID authentication. Their implementation using NodeMCU and Firebase enabled cloud-based monitoring. The study showed that multi-layer authentication drastically reduces the chances of unauthorized transactions.

7. Aishwarya Nair et al. (2022) In their research, the authors presented an IoT-based banking model emphasizing secure communication using MQTT protocol. They demonstrated how IoT cloud platforms can integrate ATM hardware components and ensure secure data transmission between user devices and ATM units.

8. Harish Kumar and Preeti Singh (2022) This paper explored the integration of machine learning with biometric-based ATM systems. The authors used facial recognition and emotion detection to monitor user behavior. Their results suggested that adding behavioral analysis can help identify suspicious activities during transactions.

9. K. Venkatesh and Pooja Rani (2023) The researchers designed an intelligent ATM with a multi-factor authentication mechanism combining facial recognition, RFID tags, and password validation. Their prototype achieved higher security accuracy and reduced processing delays, showing the potential for real-time banking security applications.

10. Anjali Deshmukh et al. (2023) In their study, the authors proposed an IoT-driven ATM monitoring system that uses NodeMCU and sensors to detect both user verification and environmental conditions around the ATM. The model included alert notifications via mobile apps and cloud storage for transaction logs, ensuring both user safety and system transparency.

EXISTING SYSTEM

In traditional ATM systems, the primary method of user authentication is the combination of a debit/credit card and a Personal Identification Number (PIN). The user inserts the card into the machine, enters the PIN, and if the credentials match the bank records, the system allows cash withdrawal or other transactions. While this method is simple and widely used, it has significant security limitations. Card cloning, PIN theft, shoulder surfing, and skimming attacks are common ways fraudsters exploit these systems, putting both users and banks at risk. Some existing systems have attempted to integrate basic biometric verification, such as fingerprint scanning, but these are not widely implemented due to hardware costs and maintenance challenges. Additionally, conventional systems lack remote monitoring, real-time alerts, and multi-factor authentication, which makes them vulnerable to both physical attacks and cyber threats. The absence of real-time IoT integration also means administrators cannot instantly detect unauthorized access or monitor multiple ATM locations efficiently. Overall, the existing systems rely heavily on single-factor authentication, making them less secure in the modern threat landscape.

PROPOSED SYSTEM

The proposed system introduces a multi-layered ATM security model integrating facial recognition, RFID card verification, and OTP authentication. It uses IoT-based communication through NodeMCU and a mobile application for real-time monitoring and control. The system also displays transaction status on an LCD with I2C interface and simulates cash dispensing via a motor mechanism. This approach enhances security, prevents unauthorized access, and provides a smart, efficient, and user-friendly banking experience.

3 .METHODOLOGY

The proposed system is designed to implement a multi-level authentication process for ATM transactions using image processing, RFID, and OTP verification

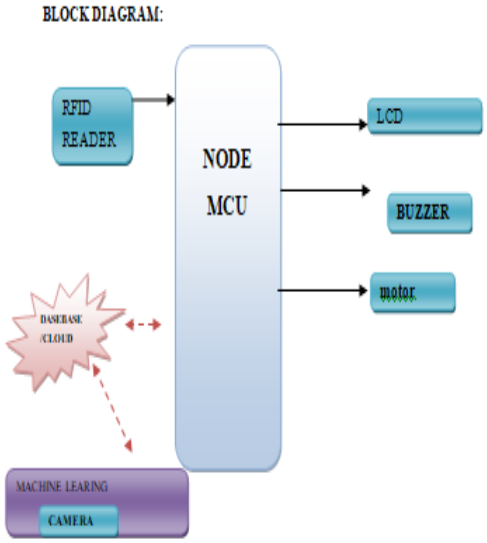
integrated through an IoT-based platform. The overall methodology consists of both hardware and software integration, ensuring secure user identification, real-time data transfer, and intelligent decision-making before authorizing cash withdrawal.The process begins with the facial recognition module, which serves as the primary level of authentication. A camera connected to the system captures the user's face image, which is then processed using Python and OpenCV. The system extracts key facial features such as eyes, nose, and jawline, and compares them with pre-stored images in the database. Only if the captured face matches the registered one does the system proceed to the next step. This ensures that only genuine users are granted access to the ATM interface.Once facial authentication is completed, the system activates the RFID verification stage. The user scans their RFID-enabled ATM card, which contains a unique identification number stored in the card's chip. The NodeMCU ESP8266 reads this information and verifies it with the registered credentials stored in the Firebase database. If the RFID data matches the authorized user record, the system continues to the final verification phase.

The third level of verification involves OTP authentication. Upon successful RFID validation, an OTP (One-Time Password) is automatically generated and sent to the user's registered mobile number through the integrated mobile application. The user must enter this OTP correctly within a limited time frame to confirm their identity. This step prevents unauthorized access even if the RFID card is stolen or cloned.

After completing all three authentication layers, the system allows the user to enter the desired withdrawal amount through the mobile application. The app communicates with the NodeMCU module via Firebase or MQTT protocol, ensuring secure and real-time data transmission. If the transaction is valid, the NodeMCU activates a DC motor mechanism that simulates the cash dispensing process. An LCD (I2C interface) displays the transaction status, including messages such as "User Verified," "OTP Accepted," and "Cash Dispensing."

The use of IoT technology enables remote monitoring and control of the entire ATM process. Administrators can track transaction data, authentication logs, and system status from any location. This interconnected structure enhances the reliability and

security of ATM operations while reducing the chances of fraud or unauthorized access.



4.TECHNOLOGIES IOT

All things that can exchange data across a network without requiring human or pc interaction are part of the Internet of Things (IoT), which includes mechanical and virtual machines, things, animals, and people that may have unique identifiers (UIDs).

FIREBASE:

The most prominent characteristic of Firebase developed into the Firebase Real-time Database, an API that synchronizes programming metrics across iOS, Android, and web platforms, storing data in Firebase's cloud infrastructure. The tool aids software developers in producing uniform, cooperative applications.

NODEMCU:

One open-source Internet of Things platform that is affordable is NodeMCU. Software running on the Espressif Systems ESP8266 Wi-Fi System on Chip (SoC) and devices primarily using the ESP-12 module were initially part of it. Support for the 32-cycle ESP32 microcontroller was subsequently added.

RFID DESCRIPTION AND WORKING

Radio Frequency Identification (RFID) is a contactless identification technology that uses electromagnetic waves to transfer data between a tag and a reader. In this project, RFID is used to verify the authenticity of the user's ATM card as the second layer of security. Each RFID card contains a unique identification number (UID) stored in a microchip, which is read by the RFID reader

when the card is brought into its range. The reader communicates this information to the NodeMCU ESP8266 through the SPI interface, allowing the system to check the user's identity against the registered credentials stored in the database.

When the user scans the RFID card, the reader captures the tag's UID and sends it to the NodeMCU for validation. If the card's ID matches the authorized data in Firebase**,** the system confirms the user's legitimacy and moves to the next stage — OTP verification. If the card is unregistered or invalid, the system denies access and displays an alert message on the LCD. This RFID-based authentication method ensures quick, secure, and contactless identity verification, reducing the risks associated with card theft and skimming in ATM transactions.

FACE DETECTION USING IMAGE PROCESSING

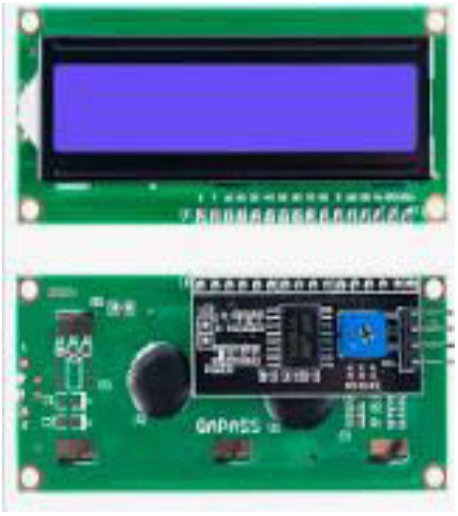
Face detection is the first and most crucial stage of the proposed ATM security system, serving as the primary layer of user authentication. It involves identifying and locating a human face in an image or video frame captured by a camera. In this project, Python along with OpenCV (Open Source Computer Vision Library) is used to process real-time video input and detect facial features such as eyes, nose, and mouth. The system utilizes algorithms like the Haar Cascade Classifier **or** LBPH (Local Binary Pattern Histogram**)** to extract and compare these features with pre-stored facial data in the database. If the detected face matches a registered user, the system grants access to the next level of verification; otherwise, access is denied.

The process of face detection ensures that only legitimate users can initiate a transaction. Since facial features are unique to every individual, this biometric verification method offers a higher level of accuracy and security compared to traditional PIN-based systems. The integration of image processing with IoT enables real-time recognition and monitoring through connected devices. This not only prevents unauthorized ATM access but also provides an intelligent, automated, and user-friendly security solution that strengthens overall transaction safety.

LCD WITH I2C INTERFACE

The LCD (Liquid Crystal Display) with I2C interface is used in the proposed ATM security system to display important

information such as authentication status, user verification results, and transaction updates. The I2C (Inter-Integrated Circuit) interface allows communication between the **LCD and NodeMCU** using only two wires — **SDA (Serial Data)** and **SCL (Serial Clock)** — which simplifies circuit connections and reduces the number of GPIO pins required. This interface makes the system more compact and efficient compared to traditional parallel LCD connections. During operation, messages such as "Face Verified," "RFID Matched," "OTP Accepted," and "Transaction Successful" are shown on the LCD screen in real time, providing clear feedback to the user. The use of I2C communication ensures fast data transmission, easy wiring, and reliable performance, making it an ideal choice for IoT-based embedded applications like smart ATM systems.



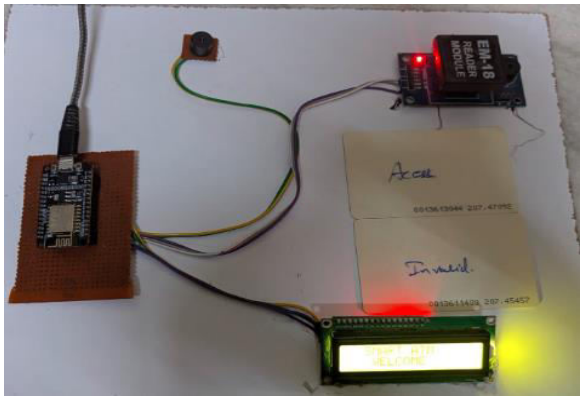
WORKING OF THE SYSTEM

The system begins with facial recognition as the first level of authentication. When a user approaches the ATM, a camera captures their face, and image processing algorithms in Python and OpenCV detect and extract facial features. These features are then compared with a pre-registered database of authorized users. If the face matches, the system proceeds to the second level of authentication, which involves scanning the user's RFID-enabled ATM card. The RFID reader captures the card's unique identification number (UID) and sends it to the NodeMCU ESP8266. The NodeMCU cross-verifies the UID with credentials stored in Firebase. If the UID is valid, the system triggers the OTP verification stage.

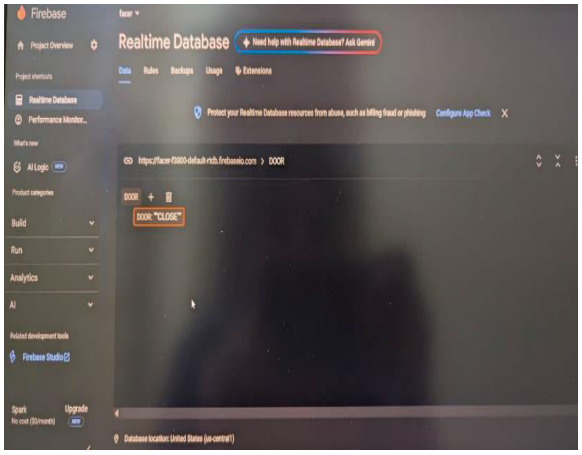
In the final stage, a One-Time Password (OTP) is sent to the user's registered mobile number via the mobile application. The user enters the OTP in the app, and the system verifies it through the NodeMCU. Upon successful verification, the user is allowed to enter the withdrawal amount. The NodeMCU controls a motor mechanism that simulates cash dispensing and updates the LCD display (I2C interface) with real-time status messages, such as "Transaction Successful." All hardware components

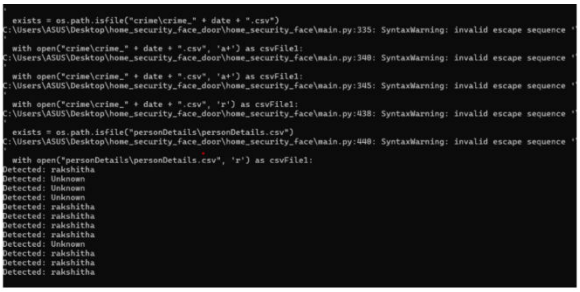
communicate via IoT protocols like Firebase or MQTT, enabling remote monitoring, data logging, and secure transaction processing. This multi-layered approach ensures a highly secure, efficient, and intelligent ATM operation, minimizing risks of unauthorized access or fraud.

RESULTES:



Design of the Smart IoT-Based ATM Security System KITthis is fire base storage cloud





5.CONCLUSION

The proposed Smart IoT-Based ATM Security System successfully integrates facial recognition, RFID authentication, and OTP verification to provide a multi-layered security mechanism for ATM transactions. By combining biometric verification, contactless card scanning, and mobile-based authentication within an IoT framework, the system ensures enhanced accuracy, reliability, and user safety. Real-time monitoring through NodeMCU and cloud communication allows for efficient transaction tracking and quick response to unauthorized access attempts. Overall, this intelligent and secure approach addresses the vulnerabilities of traditional ATMs, reduces

the risk of fraud, and demonstrates how IoT and image processing technologies can be effectively applied to modern banking systems.

FUTURESCOPE

The Smart IoT-based ATM Security System can be further enhanced with several advanced features to improve reliability, scalability, and user experience. In the future, deep learning models can be integrated to improve the accuracy of face recognition under various lighting and environmental conditions. Voice recognition and fingerprint scanning can be added as additional biometric layers for even higher security. The system can also be connected to a centralized bank server for real-time fraud detection and alert generation. Integration with GPS modules could enable location-based verification, and AI-powered anomaly detection could prevent suspicious transactions. Overall, this system has great potential for expansion and real-world implementation in modern banking infrastructures.

REFERENCES

1.Alsheakh, H.; Bhattacharjee, S. Towards a Unified Trust Framework for Detecting IoT Device Attacks in Smart Homes. In Proceedings of the 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Delhi, India, 10–13 December 2020; pp. 613–621.

2.Talal, M.; Zaidan, A.A.; Zaidan, B.B.; Albahri, A.S.; Alamoodi, A.H.; Albahri, O.S.; Alsalem, M.A.; Lim, C.K.; Tan, K.L.; Shir, W.L.; et al. Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors. Multi-driven systematic review. J. Med. Syst. 2019, 43, 42.

3.TAlrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. Sok. Security evaluation of home-based iot deployments. In Proceedings of the MIn2019 IEEE symposium on security and privacy (sp), San Francisco, CA, USA, 19–23 May 19; pp. 1362–1380.

4.Ghayvat, H.; Mukhopadhyay, S.; Gui, X.; Suryadevara, N. WSN-and IOT-based smart homes and their extension to smart buildings. Sensors 2015, 15, 10350–10379

5.Yang, J.; Sun, L. A Comprehensive Survey of Security Issues of Smart Home System: “Spear” and “Shields”, Theory and Practice. IEEE Access 2022, 10, 124167–124192.

6.Paudel, R.; Muncy, T.; Eberle, W. Detecting dos attack in smart home iot devices using a graph-based approach. In Proceedings of the 2019 IEEE international conference on big data (big data), Los Angeles, CA, USA, 9–12 December 2019; pp. 5249–5258

7.Kumar, S.; Benedict, S.; Ajith, S. Application of natural language processing and IoTCloud in smart Homes. In Proceedings of the 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), Jaipur, India, 28–29 September 2019; p. 2025.