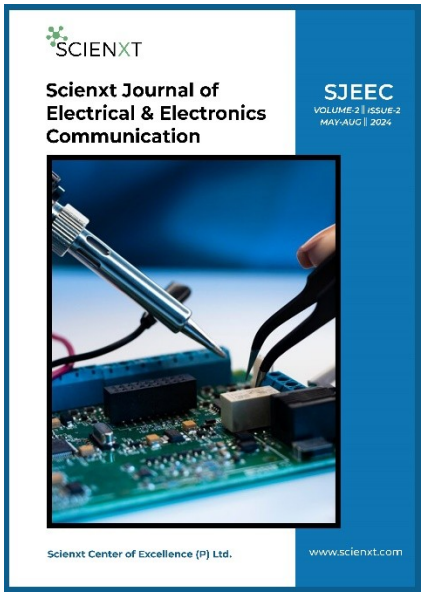


Scienxt Journal of Electrical & Electronics Communication
Volume-2 || Issue-2 || May-Aug || Year-2024 || pp. 1-9

Next-gen biometric ATM protection and monitoring system

[*1]Dr. Kavitha Jayaram, [2]Namitha B.M, [3]Rajath Prabhu, [4]Shree Raksha R

Associate Professor, Department of Computer Science and Engineering BNM Institute of Technology Bengaluru, India
Department of Computer Science and Engineeering, BNM Institute of Technology Bengaluru, India

**Corresponding Author: Dr. Kavitha Jayaram*
Email: kavithajayaram@bnmit.in

Abstract:

Rapid and precise user identification and verification are becoming more and more necessary as the number of electronic transactions rises. There are various benefits of using biometric authentication in ATMs. Facial recognition and fingerprints are used in biometric authentication. The existing ATM authentication technique has the drawback of using password-based PINs, which can be readily traced and abused. To increase security and put an end to these illegal actions, our suggested method is made to secure ATMs more. In this instance, OTP is created at random and communicated via IoT in addition to PINs. The project's objective is to do away with ATM card usage entirely. The customer can proceed with the transaction after completing the biometric and OTP pin authentication processes. The account will be blocked after three unsuccessful tries in a row. The prevention of ATM fraud is another focus of this program. The ATM doors close, the fainting gas is released, and the surrounding area is informed if the vibration sensor picks up any suspicious behavior. This will stop the scam from happening and catch the offender in the act.

Keywords:

Internet of Things, ATM, face recognition, fingerprint sensor, microcontroller, biometric authentication, and OTP (one-time password).

1. Introduction:

London saw the introduction of the first Automated Teller Machine (ATM) in 1966. Around the world, a large number of theoretical and applied ATM research have been carried out. This is because more ATMs are available, which helps people become more frugal and cashless. Similar to cash recessions, cash deposits, money transfers, and mileage payments, ATMs are a sort of electronic telecommunications equipment. ATM fraud has become a major worldwide issue in recent years. Bank drivers and visitors are both impacted by ATM fraud.

They're dealing with criminals and security threats in the existing card system. In order to authenticate, the existing ATM system relies on PINs and ATM cards that have certain disadvantages. Criminals are using methods like ATM skimming, cash traps, shoulder surfing and card trap for stealing bank cards and their data. Some customers use their phone number or date of birth as a PIN, making it easy for scammers to guess or for cybercriminals to attack. ATM card and PIN problems can be solved with biometric authentication. This is because biological details are unique and cannot be copied by others.

ATMs have become high-value targets for hackers and thieves. ATMs are susceptible to hacks, fraud, theft, and security breaches. To detect similar anomalous behavior, a stable system is needed. The maturity of vending machines has now included the installation of surveillance cameras.

Therefore, there is a need for an effective system that can detect suspicious attempts and prevent theft by stopping miscreants before they get away. Thanks to that, public safety is guaranteed, crime is reduced and serious tragedies are avoided. The disadvantage of the current ATM authentication model is using a PIN code as a password.

The model proposed in this paper uses biometric authentication, including fingerprint and facial recognition authentication as well as OTP generation and verification. Along with the PIN, a randomly generated OTP will be sent via IoT services. In case of theft, the sensor will detect vibrations of the ATM, the surrounding area will be alerted with a buzzer and the door to the ATM room will immediately close. A fainting gas was also pumped inside the ATM to render the thief unconscious.

2. Related works:

The significant increase in ATM usage motivated researchers to study the development, security, and improvement of ATM facilities.

Samina Anjum, Achal Sontakke, Aditya Tapase and Asfiya Saba Sheikh, Huzaif Sheikh, replaced ATM cards with fingerprints and IDs of all users that were stored in a database. One machine Fingerprint scanning was used to capture an individual's fingerprints [1].

C. Karthik, V Praveen Kumar, P. Bhargavi, P Nagendra Babu used facial recognition technique to authorize users. The system compares the face entered by the individual with the user's facial details in the database and determines whether a match is found. By comparing the data of the specified individual with the data of all other individuals in the database, the system generates a ranked list of matches. After verification, an OTP will be generated to proceed with the transaction [2].

Gyanprakash Singh and Pragati Goel used fingerprint recognition, which speeds up transactions while enhancing security. The proposed system uses biometric fingerprints to replace the existing ATM transaction card system. Testing false rejection rate (FRR), false acceptance rate (FAR), and average match time (AMT) on the app illustrates the completeness and applicability of user verification and authentication ATM [3].

Dr. Y.V. Ram Kumar, Kotikalapudi Satya Syamala Kameswari, Pattabhi Keerthana, Koppanati Sri Harshavardhan, Boosa Pavan Vinay, Kusampudi Sri Venkata Abhishikth, used face recognition technology that analyzed the unique shape, pattern, and positioning of the facial features. The facial image of the user was stored in the database at the time of registration. So, if any user wanted to withdraw an amount from their account, then that user had to scan their face at the camera present in the ATM. This system used HOG-SVM algorithm for face recognition [4].

If the provided information does not match, the system won't let the process to continue. After entering the OTP, the software compares it to the corresponding data. After three failed attempts, the user's account is going to be blocked. If all three authentication methods match, the customer will be asked to select a Bank from the provided option. Following this selection, the ATM allows the customer to complete the transaction in their respective bank account.

Chandana P, Kushi Sangani and A. Rengarajan, proposed a system that allows the user was asked for the account number and ATM PIN, after which the user receives an OTP on his/her

registered mobile number. After logging into the OTP, the user was asked to withdraw or deposit. A GSM Modem was used to send the OTP to the user [5].

Pratiksha Shetiya, Meryl Mascarenhas and Mrunal Deshmukh offered a new solution for security by analyzing the random pattern of the iris. The iris recognition system automatically recognized the identity of a person from a new eye image by comparing it to the human iris patterns stored in an iris template database[6].

Sumanth C M, developed a secure unintelligible PIN authentication protocol for ATM terminals using personal mobile devices (SPAQ). SPAQ was a mobile application that allowed users to scan a QR code from a device's screen of a point-of-service terminal and connected to the bank's SPAQ server to get secure one-time-use PIN templates [7].

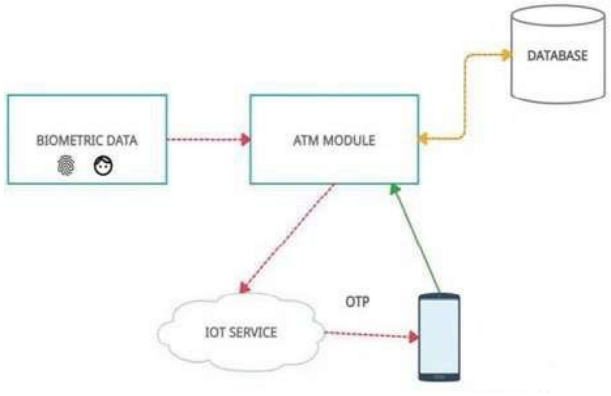
3. Proposed solution:

We proposed a new concept which improves the entire experience, usability, protection, and easy access of ATM transactions. First, the customer's face and fingerprints should be received and uploaded into the database. To establish connection with the customer, an interface for users is created using the Python GUI. The entire transaction will be displayed via the user interface. The image of the customer's face and fingerprint is encoded in digital data and then it gets stored in a database. While registering biometric information, the customer will be given a bank account and balance. They are additionally required to provide a four-digit PIN while registering their account with the administrator of the relevant bank.

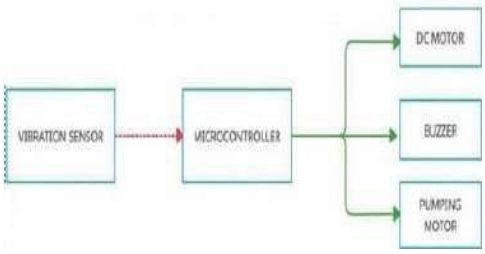
When someone wants to use an ATM, he or she must choose if the user is authorized or unauthorized user. If authorized, user inserts the RFID card and enters the PIN. Then the user must put their finger on the fingerprint module. Following approval, they should face the camera in front of them. The biometric information is converted into digital code. This digital info is now compared to a database of registered customers' biometric information. If the data matches, the user must select the bank for the transaction process. If unauthorized, user inserts the RFID card and enters the PIN. The software is going to send a confirmation message to the account holder's mobile device via IoT, as illustrated in Fig. 1(a). If the account holder's confirms the transaction, then an OTP is generated and delivered to the

account holder, the account holder forwards it to the user, which is then verified by the system.

If the provided information does not match, the system won't let the process to continue. After entering the OTP, the software compares it to the corresponding data. After three failed attempts, the user's account is going to be blocked. If all three authentication methods match, the customer will be asked to select a Bank from the provided option. Following this selection, the ATM allows the customer to complete the transaction in their respective bank account.



(a)



(b)

Figure. 1: (a) Block diagram for ATM software and (b) Hardware are for security system

Users can access any bank account, but it must be linked to their ID. Customers can use the ATM to get account information, withdraw money, make deposits, and transfer money. They can also view previous transactions from that account. After a successful transaction, the user is able to continue or exit. This system will be created using Python and hardware peripherals to provide a low-cost ATM system. This system also provides access to various bank accounts.

The ATM security system keeps the system safe from robbery. It also allows the cops to apprehend the robber without incident. When someone attempts to damage or break into an ATM, the vibration sensor identifies the vibration. The vibration sensor sends an input to the microcontroller. The microcontroller then activates a buzzer and a red LED to warn the ones surrounding it. The ATM door will be controlled by a servo motor, as illustrated in Figure 1(b).

4. Biometric authentication:

4.1. Face recognition:

Face detection typically serves as the initial stage for various facial-related applications, such as facial recognition or authentication. Face recognition involves the automated identification of individuals by analyzing facial features and patterns. The process typically begins with face detection, where algorithms locate and extract facial regions from an image or video. Feature extraction follows, capturing key facial attributes like the arrangement of eyes, nose, and mouth. Following this, the characteristics are converted into a distinct template that depicts the person's facial attributes. During recognition, a live face is compared to stored templates in a database using matching algorithms. The degree of similarity determines the likelihood of a match, allowing the system to identify the person. The level of resemblance dictates the probability of a match, enabling the system to recognize the individual. Facial recognition finds extensive application across various domains.

Face Detection: Identifying faces within the image marks the initial step in our process. Next, we'll extract the exact coordinates of the detected face for further analysis.

Feature Extraction: The technique involves selecting and transforming raw data into a reduced and informative representation, facilitating efficient analysis and pattern recognition.

Comparing faces: With facial patterns extracted for each face in our database, we proceed to compare them. Recognition occurs when the generated pattern closely resembles any other patterns within the dataset.

4.2. Fingerprint recognition:

Fingerprint verification operates by capturing and analyzing unique patterns present in an individual's fingerprints for secure identification. The process begins with the acquisition of a fingerprint image, typically through optical or capacitive sensors. Ridge and valley patterns,

minutiae points (ridge endings, bifurcations), and other distinctive features are extracted from the fingerprint. The features are converted into template as a digital representation. During verification, a live fingerprint is similarly processed, and its template is compared with a stored template in the database. Matching algorithms assess the similarities between the live and stored templates, determining the degree of correlation. If the match surpasses a predefined threshold, the verification is successful, confirming the individual's identity. Fingerprint verification is renowned for its accuracy and reliability in personal authentication.

4.3. One-time password (OTP) authentication:

OTP generation is a process which is based on a secure algorithm within the ATM system that generates a unique code based on various factors such as transaction details, timestamp, and user identity. This code is delivered to the card owner's phone number through SMS or other secure communication channels, ensuring its confidentiality and integrity.

To complete the transaction, the user must enter the received OTP into the ATM interface, thereby validating their ownership of the registered mobile device and confirming the authenticity. The OTP acts as a one-time code that is only valid for a short period of time, typically a few minutes, enhancing the transaction's security by ensuring its time-bound validity

5. Result & discussion:

Therefore, the hardware and software configurations are integrated and processed for user authentication and security protocols. Stringent security measures will be upheld during the transaction process, with additional provisions for physical security in the ATM environment. tkinter, the python GUI is used to develop the user interfaces.

The integration capabilities of tkinter allows it to interact harmoniously with other ATM Surveillance System modules, such as the backend handling biometric authentication, OTP generation, and database management, ensuring a cohesive and efficient user experience. Overall, the role of tkinter in this project is to build a user-friendly interface that simplifies user interactions while seamlessly integrating with the system's core functionalities for optimal performance and usability.

6. Conclusion:

Due to the rise in fraudulent activities within traditional card-based systems, this proposed ATM system utilizes RFID cards, biometrics, and OTP for authorization. The biometric authorizations include both fingerprint and face recognition, where fingerprint and face patterns of every individual is uniquely identified. The OTP is transmitted to the account holder's mobile phone via IoT services. This integrated system ensures secure ATM cash transactions. The vibration detection system, equipped with sensors, identifies any suspicious behavior by individuals. This system aids law enforcement in apprehending robbers seamlessly.

In addition to this, the release of fainting gas will also be shown by a prototype model. By this means of features, we provide safety and security to both bank's money and customers.

7. References:

(1) Samina Anjum, Achal Sontakke, Aditya Tapase, Asfiya Saba Sheikh, Huzaif Sheikh, "Fingerprint Based ATM Systems". International Research Journal of Modernization in Engineering Technology and Science, Vol.5, Issue.4, April 2023.

(2) C.Karthik, V Praveen Kumar, P.Bhargavi, P Nagendra Babu. "A Protected and Improved ATM Security System exploitation Image Capture and SMTP Protocol". Industrial Engineering Journal, Vol.50, Issue.7, July 2021.

(3) Gyanprakash Singh and Pragati Goel, "ATM Using Fingerprint", International Journal of Research Publication and Reviews, Vol.3, no.7, July 2022.

(4) Dr. Ram Kumar, Kotikalapudi Satya Syamala Kameswari, Pattabhi Keerthana, Koppanati Sri Harshavardhan, Boosa Pavan Vinay, Kusampudi Sri Venkata Abhishikth, "An Efficient Application to Provide Security to The Banks Using Face Recognition Using Open CV", Journal of Science and Technology, Vol.8, Issue.4, April 2023.

(5) Chandana P, Kushi Sangani and A. Rengarajan, "Study on ATM with OTP for a safe and smart future", International Journal for Research in Applied Science and Engineering Technology, Vol.10, Issue.2, Feb 2022.

(6) Pratiksha Shetiya, Meryl Mascarenhas and Mrunal Deshmukh, "ATM Security System using Iris Recognition by Image processing", International Journal of Engineering Research and technology, Vol.9, Issue.7, July 2020.

(7) Sumanth C M, "Securing ATM Transactions Using QR Code based Secure PIN Authentication", International Journal of Scientific Research in Computer Science Engineering and Information Technology, Vol.5, Issue.3, June 2019