Journal of Interdisciplinary Science & Technology
Volume: 01 Issue: 01 | Jun-2024

CNN-Enhanced Cardless ATM Security with Facial and Eye Blink Detection

Shaikh Fahad Naushad
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik, India
sf9527057516@gmail.com

Shubham Krushna Sirsat
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik, India
shubhsirsat12@gmail.com

Tushar Chandrabhan Dange
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik, India
tushardange1@gmail.com

Kiran Sanjay Hyalij
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik, India
hyalijkiran4@gmail.com

Prof. (Dr)Amol Potgantwar
(co-guide: Prof. Rais Shaikh)
Department of Computer Engineering
Sandip Institute of Technology and Research Centre Nashik,
rais.shaikh@sitrc.org

Abstract

Cardless Cash Withdrawal offers a modern solution for secure ATM transactions without the need for a debit card. Leveraging ubiquitous mobile phone use, this method integrates advanced Convolutional Neural Networks (CNN) for dual-layer biometric authentication: facial recognition and eye blink detection. The system employs sophisticated CNN models to verify users through unique facial features, ensuring authorized access. Additionally, analyzing eye blink patterns provides a secondary authentication layer, enhancing security and minimizing unauthorized access risks. To further validate the transaction, a one-time password (OTP) is generated and sent to the user's mobile phone, serving as an extra verification step. This innovative approach combines the robustness of CNN-powered facial and eye blink recognition with OTP verification, offering a secure, convenient, and efficient cardless ATM experience.

I. Introduction

The traditional banking system requires customers to visit the bank branch in person to perform transactions, which can be time-consuming and heavily reliant on paper documentation. This manual process often leads to delays and frustration for customers. To address these issues, Automated Teller Machines (ATMs) were introduced, providing a more efficient and accessible way for customers to manage their financial transactions. ATMs offer various services, including cash withdrawals, balance inquiries, and fund transfers, all without the need for a bank teller.

In conventional card-based ATM systems, users utilize debit or credit cards and enter a Personal Identification Number (PIN) to verify their identity. These systems provide the convenience of self-service and eliminate the need for paper-based transactions. However, they come with certain drawbacks. For instance, ATM cards can be lost or forgotten, and if someone knows the correct PIN, they can access the account and withdraw funds without being the legitimate account holder. This poses significant security risks.

To enhance security, there is a shift towards cardless ATM systems that replace ATM cards and PINs with biometric authentication methods such as facial recognition and eye blink detection. These advanced technologies ensure that only authorized users can access the ATM. Facial recognition relies on the unique facial features of each user, making it nearly impossible for unauthorized individuals to gain access. Additionally, eye blink detection adds an extra layer of security by verifying the user's identity through specific blink patterns, further reducing the likelihood of fraud.

The traditional banking system requires customers to visit the bank branch in person to perform transactions, which can be time-consuming and heavily reliant on paper documentation. This manual process often leads to delays and frustration for customers. To address these issues, Automated Teller Machines (ATMs) were introduced, providing a more efficient and accessible way for customers to manage their financial transactions. ATMs offer various services, including cash withdrawals, balance inquiries, and fund transfers, all without the need for a bank teller. In conventional card-based ATM systems, users utilize debit or credit cards and enter a Personal Identification Number (PIN) to verify their identity. These systems provide the convenience of self-service and eliminate the need for paper-based transactions. However, they come with certain drawbacks. For instance, ATM cards can be lost or forgotten, and if someone knows the correct PIN.

II. EXISTING SYSTEM

The mobile app consists of a special code which flashes on the screen for a period of 1 minute. This code provides strong authentication by dynamically generating a one-time security code. This code can be generated even if there is no network or internet connection. Here the user will first login to the mobile app using the details such as user-id and password. After this the user generates a reference number as per his choice and also specifies the amount to be withdrawn. This reference number would remain valid for a certain period of time and can be used only once. Having generated the reference number, the user visits the nearest ATM and enters the user-id and password along with the code in the app to sign in. If the authorized user is present, he/she would be logged in and would be required to enter the reference number to withdraw the specified amount. If the reference number is correct, the amount is withdrawn else transaction fails. This idea is an amalgamation of current ATM system and online transactions involving OTP. By eliminating the use of OTP the problems related to sharing of OTP are successfully overcome.

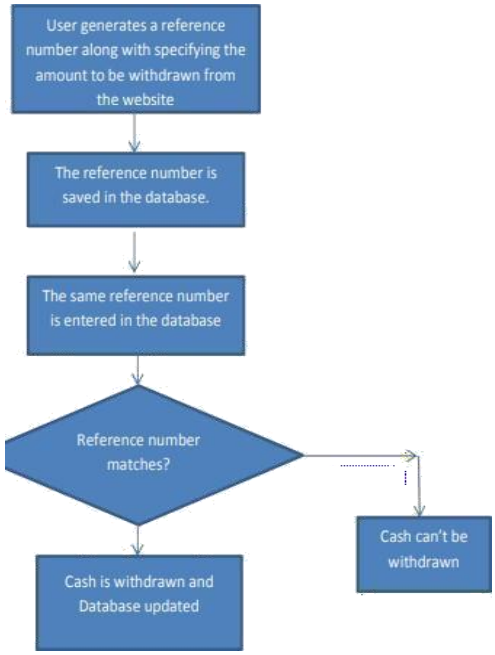

Fig-1.1 Existing System

III. PROPOSED SYSTEM

Camera is used for authentication of user. We are using Keypad and camera of PC/laptop. Whenever a person enters in ATM camera captures image and display information about him. GUI (Graphical User Interface) is developed for user and system interactions. An OTP, which along with face recognition comprises two levels of security. When face and OTP are matched then customer's account will open in ATM machine. GUI will display user name, debited money, authentication status etc.

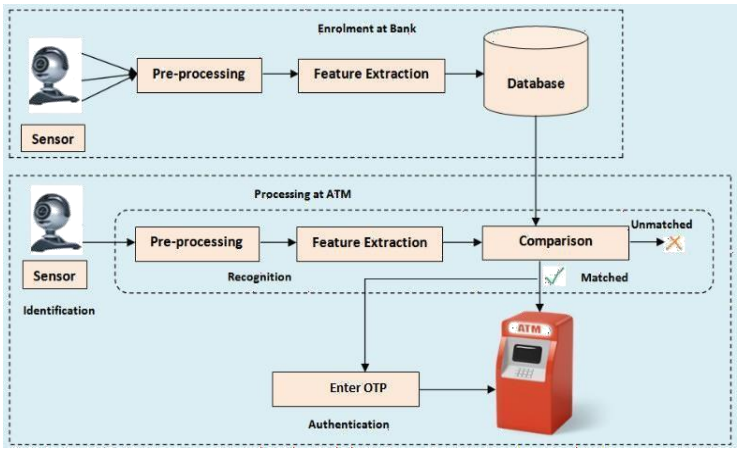

Fig-1.2 System Architecture

A. Enrollment At Bank:

1) Input from Camera

The user's facial image is captured and stored in the database which is implemented by the python face recognition API. It implements the built-in detect method to complete the enrolment process. The user enrolls their facial and eye blink data at the bank. This data is stored in a database.

2) Preprocessing

User facial images are undergoes to pre-processing to standardize and enhance quality and it is an essential step of detection in order to remove noise such as hair clothing and other artifacts and enhance the quality of original image. The main purpose of this step is to improve the quality of skin image by removing unrelated and surplus parts in the back ground of image for further processing. Good selection of preprocessing techniques can greatly improve the accuracy of the system.

3) Feature Extraction

A feature is a piece of information which is relevant for solving the computational task related to a certain application. Feature extraction is the process of extracting this information from an image. At the enrolment phase, we use GoogleLeNet architecture to extract the features from an image. The CNN extracts features from the facial and eye blink data. These features are used to represent the user's unique identity. The CNN does this by learning a set of filters that are applied to the input images. The filters are designed to extract different types of features from the images, such as edges, corners, and textures. The CNN learns the filters by being trained on a dataset of labeled facial and eye blink images. The dataset contains images of different people with different facial expressions and eye blink patterns.

4) Database

These extracted images are stored in the database for further

use at the time of authentication. he database stores the CNN features extracted from the facial and eye blink data of enrolled users. The database also stores the user's demographic information, such as their name, Mobile number, and date of birth.

B. Authentication:

At the time of login at ATM user will go through the series of authentication like facial recognition and Eye blinking and OTP to access the system.

1) Input from Camera

The python face recognition API implements the built-in verify method to turn on the camera and captures the image of the user. A sensor captures the user's face and eye blink data at the ATM. The sensor may be a camera or a combination of a camera and an infrared sensor. The camera captures a series of images of the user's face from different angles. The infrared sensor captures a series of images of the user's eye blinks.

2) Pre-Processing

User facial images are undergoes to pre-processing to standardize and enhance quality and it is an essential step of detection in order to remove noise such as hair clothing and other artifacts and enhance the quality of original image. The main purpose of this step is to improve the quality of skin image by removing unrelated and surplus parts in the back ground of image for further processing. Good selection of preprocessing techniques can greatly improve the accuracy of the system. The user's face and eye blink data is preprocessed to normalize it and make it suitable for input to the CNN.

3) Feature Extraction

After pre-processing images are goes to feature extraction which is CNN's core function here convolutional layers scan images to capture meaningful features like edges, textures, and patterns. These extracted features are stored in the database for further use. The CNN extracts features from the user's face and eye blink data again. This is done to ensure that the user is the same person as the person who was identified at the beginning of the transaction.

4) Comparison

At this stage the user's captured image is compared to the one of the existing image of the user stored in the database if matched means the user is authorized or genuine user. The CNN compares the two feature vectors extracted from the user's face and eye blink data to ensure that they match. If the two feature vectors match, then the user is authenticated and can proceed with the transaction.

5) Enter OTP

The user enters a one-time password (OTP) to authenticate the transaction. The OTP is generated by the bank and sent to the user's mobile phone. OTP is sent only to the user which is confirmed as genuine and allowed to choose one of the particular bank from the list that the user has registered at enrolment and gain access Lastly user can perform various operations at the ATM, such as withdrawal, deposit, balance check, etc.

IV. System Protocol

The interactions and messages exchanged between the user, the ATM, and the server are explained in the following steps:
Step 1: Registration Phase for new users, means same step as if we got a new atm card we go the atm machine for the register its same process, where we have to enter our name, Adhaar number, mobile number and Our Face Capture process will start. After Capturing the face it stores to Data base and the registration phase is completed.
Step 2: Login Phase for Existing users, the camera will open captures the face and further process of entering data related to Withdraw.
Step 3: Authentication Phase Where it will authenticate with the face verified and second authentication that is it will send the OTP to the registered Number.
Step 4: After Entering the proper details mentioned in authentication method, It successfully Withdraw the money without Card.

V. Conclusion

The system is purposefully engineered to be highly resilient against various types of attacks, including card-skimming, observation attacks, replay attacks, and relay attacks. By utilizing a combination of technologies and security measures, this system offers a level of efficiency and security that surpasses traditional ATM systems. In this system, malpractices and fraudulent activities are significantly mitigated, making it a robust and secure solution for ATM transactions.

VI. Future Scope

Better pre-processing techniques are essential to remove noise from data, ensuring that noise doesn't interfere with subsequent processes like classification and prediction. These techniques involve cleaning, normalization, outlier handling, and feature selection, ultimately enhancing data quality and the reliability of analytical results. Noise-free data forms a solid foundation for accurate and meaningful classification and prediction.

Acknowledgment

- First and foremost, we wish to record our sincere gratitude to the Management of this college and our Respected Principal **Prof. (Dr) M. M. Patil.**
- Our sincere thanks to **Prof.** (**Dr) Ankita V. Karale**, Head, Department of Computer, Sandip Institute of Technology and Research Centre, Nashik.

➢ We express our sincere gratitude to our Guide, **Prof. Rais Shaikh** for guiding us in the investigations of this project and in carrying out experimental work.

REFERENCES

[1] KhushbooYadav; SuhaniMattas; LipikaSaini; Poonam Jindal, "Secure Card-less ATM Transactions", 2020 First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA)

[2] OTP Based CardlessTransction using ATM Md. Al Imran, M.F. Mridha, Md. KamruddinNur 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), doi:10.1109/ICREST.2019.8644248

[3] Hassan, Ahsana; George, Aleena; Varghese, Liya; Antony, Mintu; K.K, Sherly (2020). [IEEE 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) - Coimbatore, India (2020.7.15-2020.7.17)] 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) - The Biometric Cardless Transaction with Shuffling Keypad Using Proximity Sensor. , (), 505–508. doi:10.1109/ICIRCA48905.2020.9183314

[4] Banerjee, Indranil; Mookherjee, Sjivangam; Saha, Sayantan; Ganguli, Souradeep; Kundu, Subham; Chakravarti, Debduhita (2019). [IEEE 2019 International Conference on OptoElectronics and Applied Optics (Optronix) - Kolkata, India (2019.3.18-2019.3.20)] 2019 International Conference on Opto-Electronics and Applied Optics (Optronix) - Advanced ATM System Using Iris Scanner. , (), 1–3. doi:10.1109/OPTRONIX.2019.8862388

[5] Tyagi, Abhishek; Ipsita, ; Simon, Rajbala; khatri, Sunil Kumar (2019). [IEEE 2019 4th International Conference on Information Systems and Computer Networks (ISCON) - Mathura, India (2019.11.21-2019.11.22)] 2019 4th International Conference on Information Systems and Computer Networks (ISCON) - Security Enhancement through IRIS and Biometric Recognition in ATM. , (), 51– 54. doi:10.1109/ISCON47742.2019.9036156

[6] Mahansaria, Divyans; Roy, Uttam Kumar (2019). [IEEE 2019 International Carnahan Conference on Security Technology (ICCST) - CHENNAI, India (2019.10.1-2019.10.3)] 2019 International Carnahan Conference on Security Technology (ICCST) - Secure Authentication for ATM transactions using NFC technology. , (), 1– 5. doi:10.1109/CCST.2019.8888427

[7] Kale, PriyankaHemant; Jajulwar, K. K. (2019). [IEEE 2019 9th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing 51 (ICETET-SIP-19) - Nagpur, India (2019.11.1-2019.11.2)] 2019 9th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-19) - Design of Embedded Based Dual Identification ATM Card Security System. , (), 1–5. doi:10.1109/ICETET-SIP-1946815.2019.9092027

[8] Fingershield ATM – ATM Security System using Fingerprint Authentication Christiawan1 , BayuAji Sahar2 , Azel Fayyad Rahardian3 , ElvayandriMuchtar doi:10.1109/ISESD.2018.8605473

[9] Swathi, H; Joshi, Suraj; Kiran Kumar, M.K. (2018). [IEEE 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC) - Bangalore, India (2018.2.9-2018.2.10)] 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC) - A Novel ATM Security System using a User Defined Personal Identification Number With the Aid of GSM Technology. , (), 1–5. doi:10.1109/ICAECC.2018.8479533.

[10] Embarak, Ossama H. (2018). [IEEE 2018 Fifth HCT Information Technology Trends (ITT) - Dubai, United Arab Emirates (2018.11.28-2018.11.29)] 2018 Fifth HCT Information Technology Trends (ITT) - A two-steps prevention model of ATM frauds communications. , (), 306–311. doi:10.1109/CTIT.2018.8649551