Secure Cardless Withdrawal In ATM

Mrs. Sindhu Biravi S[1], Abinaya S[2], Dharani D[3], Malini S[4], Keerthana L[5]
[1]Assist prof, Dept of Computer Science and Engineering
[2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Vivekanandha College of Technology for Women, Namakkal, Tamil Nadu, India

Abstract- *Card-based ATM authentication has been a primary target for skimming, cloning, and PIN theft attacks, resulting in billions of dollars in losses for account holders and financial institutions every year. This paper presents a Secure Cardless Withdrawal System that eliminates the physical card and routes every transaction through a two-step authentication process based on user type. Local citizens authenticate using their face, captured live by the ATM webcam, along with a six-digit one-time password sent to their registered mobile number via the Twilio SMS gateway. Foreign visitors undergo the same face capture and mobile OTP steps, along with an additional verification of their passport number. This matches the submitted document identifier against the credentials stored in the bank database at the time of registration, providing foreign users with a stronger three-factor authentication path that meets their higher identity assurance needs. Both branches merge at a decision engine that allows a transaction only when all required checks are completed. A Gemini-powered conversational assistant included in the interface supports Tamil, Hindi, Telugu, Kannada, Malayalam, and English, making the platform easier to use for individuals who struggle with English-only terminals. The system uses a Python-Flask backend, an SQLite database, and an HTML/CSS frontend, demonstrating that it is possible to develop a secure, user-friendly, and fully cardless ATM authentication platform using common web technologies.*

Keywords: cardless ATM, face recognition, mobile OTP, passport verification, Twilio SMS, two-factor authentication, three-factor authentication, Gemini API, multilingual chatbot, Python Flask, SQLite, digital banking security.

I. INTRODUCTION

Automated Teller Machines have been essential to retail banking since the late 1960s. They allow customers to access cash anytime without needing to visit a branch. One thing that hasn't changed is the way transactions are authenticated: a plastic card in a reader and a PIN typed on a keypad. Although this method is familiar, it was never designed to handle modern digital fraud threats. Card-skimming devices, which can fit over a legitimate card slot without attracting notice, quietly record magnetic-stripe data from cards used afterward. Nearby pinhole cameras capture the corresponding PIN. Within hours, attackers can clone the card and start draining money from the account. Stolen cards with a compromised PIN are also very risky. The account remains vulnerable from the moment of theft until the card is blocked. Even everyday wear can create issues. A demagnetized or cracked card might be rejected at the terminal, leaving the cardholder without access to their funds for days while waiting for a replacement.This problem is complicated by the fact that ATM users are not all the same. A domestic account holder has a registered mobile number and a locally issued credential. A foreign visitor has neither; they arrive with a passport and possibly a roaming SIM. Most cardless ATM solutions in the literature assume a domestic user base and overlook foreign travelers. The system outlined in this paper addresses that gap by providing separate authentication methods for both domestic and foreign users that align with their actual credentials while ensuring the same level of fraud protection for both.Local citizens confirm their identity using webcam-based facial capture and a mobile OTP sent through Twilio. Foreign visitors undergo the same face capture and mobile OTP process, then provide their passport number as a third factor, which is verified against a record from registration. A single decision engine manages both paths, and a Gemini-powered multilingual assistant guides users through the process in six regional languages.

II. OBJECTIVE

The project proposes to construct and showcase a working cardless ATM withdrawal system that is more secure, more inclusive, and easier to use than traditional card-and-PIN terminals. The specific objectives are as follows: Substitute the physical ATM card with face capture using webcams as the primary biometric credential for all users. Authenticate local citizens using face recognition, followed by a six-digit OTP sent to their registered mobile number via Twilio SMS, forming a two-factor authentication process. Authenticate foreign visitors by combining the same face capture and mobile OTP, along with an additional passport number verification against the credential database.

Ensure that the passport number check is applied only to foreign users, while local citizens are exempt from this

additional step. Implement a decision engine that verifies all required checks for the respective user type before allowing a transaction to proceed.Integrate a multilingual assistant based on the Gemini API to support Tamil, Hindi, Telugu, Kannada, Malayalam, and English, reducing language barriers for non-English-speaking users.

III. PROBLEM STATEMENT

The traditional card-and-PIN authentication model used in global ATM systems was developed during a time when card forgery required specialized equipment and electronic fraud was relatively rare. However, this assumption is no longer valid in today's environment. With advancements in technology, skimming devices have become inexpensive, compact, and easy to install or remove within seconds. As a result, unattended ATMs are increasingly vulnerable and can be exploited as tools for silently capturing users' sensitive data.

Skimmers can extract magnetic-stripe information from cards, while PINs can be obtained through hidden cameras or shoulder surfing. When combined, this information is sufficient to create cloned cards that function like legitimate ones. This enables attackers to withdraw money from victims' accounts before they even become aware of the breach.

Another major concern is physical card theft. If a stolen card is accompanied by knowledge of the PIN, unauthorized access to the account becomes immediate. In such cases, significant financial loss can occur within a very short period, sometimes within hours. Even when the PIN is not compromised, users who lose their cards often face delays in obtaining replacements, temporarily losing access to their own funds.

An additional issue, often overlooked, involves foreign travelers. Many ATM authentication systems proposed in academic research assume that users possess a local bank account, a registered local mobile number, and familiarity with the local language. These assumptions do not hold true for international visitors who rely on foreign passports and roaming SIM cards. Such users may be unable to register local mobile numbers, may face language barriers, and often lack locally recognized credentials for identity verification.

To address these limitations, the proposed system introduces a flexible and inclusive authentication approach. For international users, a secure three-factor authentication process is implemented, combining facial recognition, mobile-based One-Time Password (OTP) verification, and passport-based identity validation. For local users, a simplified two-factor authentication mechanism is provided, ensuring both convenience and security while aligning with their available credentials.

IV. METHODOLOGY

A. System Architecture:

The architecture is based on the client-server architecture where the ATM terminal has a client-side interface consisting of a browser-based interface and a Python-Flask server that does all the authentication logic, credential storage, OTP generation, and transaction management. The Flask backend has routes dedicated to uploading faces to the webcam, registering a user, launching withdrawal by a user-type, OTP verification, and the Gemini chatbot. All user data, including name,mobile number, face-folder path, optional passport number, hashed PIN and account balance is stored in an SQLite database. The distinctive architectural characteristic is the type of split at the withdrawal stage which is user-type.The system identifies a local or global citizen and switches to the appropriate branch. The two branches culminate at a decision engine that evaluates the extent to which all the required steps to that branch are already taken before the transaction can be approved.

B. Face Capture and Storage:

During registration, the browser activates on the device webcam and streams a live feed to the registration page. The user clicks a capture button. he frontend then encodes each frame as a Base64 PNG string and sends it to the/upload face endpoint.

The server decodes the image bytes and saves each file in a per-user folder at static/captures/faces/<mobile number>/, naming them sequentially as face_1.png, face_2.png, and so on. Registration is blocked until the system collects at least twenty face images. This ensures that there is a reliable reference set for the user.

User Registration:

The registration form gathers the user's name, mobile number, and the opening account balance. It includes an optional passport number field: local citizens can leave it blank, whereas foreign visitors can fill it in. The passport number is normalized to uppercase and then stored in the system. A default six-character PIN is generated based on the last four digits of the mobile number along with the first two characters of the passport number, if a passport is provided; otherwise, it is based on the last six digits of the mobile

number. Before being written to the database, it is hashed using the generate_password_hash function from Werkzeug. A unique constraint is applied to the mobile number column to prevent duplicate registrations.

C. Local User Flow – Face and Mobile OTP:

When a local citizen initiates a withdrawal, they enter their registered mobile number and the amount they wish to withdraw. The system queries the database to find a matching record and verifies that the account balance can cover the requested amount. After passing both checks, the webcam captures the user's face at the terminal. A six-digit OTP is generated using random.randint(100000, 999999) in Python and is sent to the customer via the Twilio SMS API. The OTP and transaction parameters are stored in the Flask session, and the system redirects to the OTP entry page.

Upon successful OTP verification, an atomic SQL UPDATE operation subtracts the withdrawn amount and records the transaction with a generated receipt ID, completing the two-factor authentication cycle.

D. Foreign User Flow – Face, Mobile OTP and Passport:

Foreign visitors follow the same steps as local users for face capture and mobile OTP, with an additional passport number verification step. After the mobile number and balance checks are passed and the OTP is verified, the system prompts the user to enter their passport number. This value is compared with the passport number provided during registration.When all three checks - face capture, OTP, and passport verificationare successfully satisfied, the decision engine authorizes the transaction. This three-factor authentication path provides a higher level of identity assurance, which is appropriate for users whose credentials cannot be verified solely through a domestic banking record.

E. Decision Engine:

The convergence point is the decision engine, where both authentication branches meet. For local users, it requires face capture confirmation and a valid OTP. For foreign users, it also requires a successful match of the passport number. If any of the required checks are missing or fail, the engine blocks the transaction and redirects the user to the appropriate step. It authorizes balance deduction and receipt generation only after all checks are successfully completed.

F. Multilingual Chatbot Assistant:

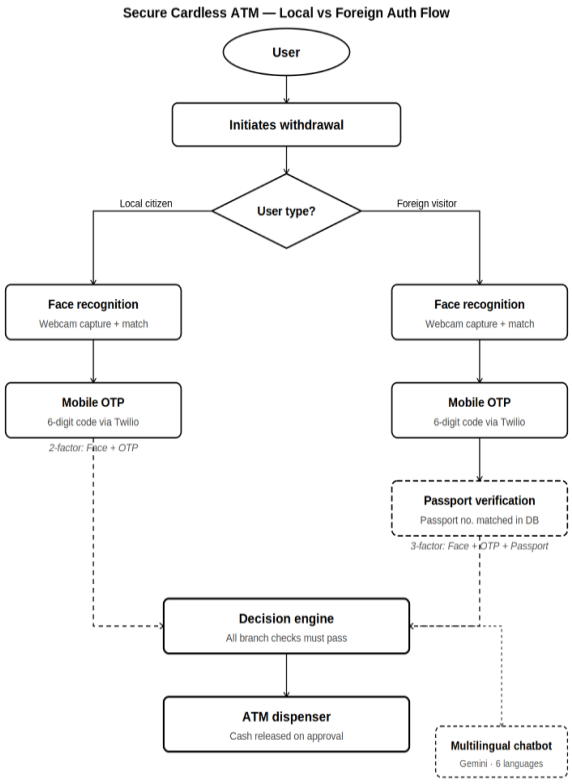
The Gemini-powered chatbot is accessed through a floating button on the withdrawal page. The language picker includes Tamil, Hindi, Telugu, Kannada, Malayalam, English, and an auto-detect mode. Each message is sent to the Flask /chat endpoint along with the selected language. The endpoint constructs a prompt that instructs the Gemini model (defaulting to gemini-2.5-flash-lite, with fallback options) to respond only in the chosen language and to keep answers brief and relevant to ATM users. The assistant handles navigation queries, explains the verification process, and delivers error messages in the user's preferred language.

G. Hardware and Software Setup:

The prototype operates on a system with an Intel Core i9-14900K processor, 16 GB RAM, and 1 TB storage. The webcam is a standard HD model operating at 30 frames per second. The software stack includes Python 3.x, Flask, SQLite3, the Twilio Python client library, the Requests library for making Gemini API calls, and Werkzeug for password hashing.

V. SYSTEM FLOW DIAGRAM

Figure 1 shows the authentication flow of the proposedsystem.After starting a withdrawal, the system identifies the user type.Local citizens follow a two-factor process: face recognitionat the terminal, followed by a Twilio OTP sent to their registeredmobile number.Foreign visitors follow a three-factor process:the same face recognition and mobile OTP, along with a passportnumber check against the database. Both processes feed into thedecision engine, which approves the transaction only when allchecks for the relevant branch have been successfully completed.The multilingual chatbot is available throughout the entire session.



VI. RESULT AND DISCUSSION

The proposed Secure Cardless Withdrawal System was successfully implemented and evaluated through a web-based simulation environment. The system integrates face recognition technology with OTP-based two-factor authentication to facilitate card-free ATM transactions. The following subsections describe each functional module along with the corresponding output screens observed during testing.

A. Home Page:

Figure 2 presents the home page of the SecureATM system, which serves as the primary entry point for all users. The landing page displays the system name, the tagline "Next-Generation Authentication using Face ID and Twilio OTP," and three feature badges: AI Powered, End-to-End Encrypted, and Instant OTP. The options for Login and New User Registration are clearly separated. This screen does not show any account data or session tokens. The homepage provides two navigational paths: a **Login** option for returning users and a **New User Registration** button for first-time enrolments.

Figure2:Homepage(newregistration)

B. Use rRegistration:

Figure 3 captures the New User Registration screen, which collects the essential credentials required to enroll a customer into the Secure ATM system. The registration screen asks for the user's name, mobile number, opening balance, and an optional passport number. A live webcam panel on the right side of the form captures at least twenty face images. Each image is saved as a numbered PNG file in a server-side folder. After capturing the images, the backend creates a hashed PIN, adds the record to the database, and redirects to the withdrawal page.Local users can leave the passport field blank. Foreign users must fill it in at this stage so their credential is ready for the three-factor check during withdrawal.

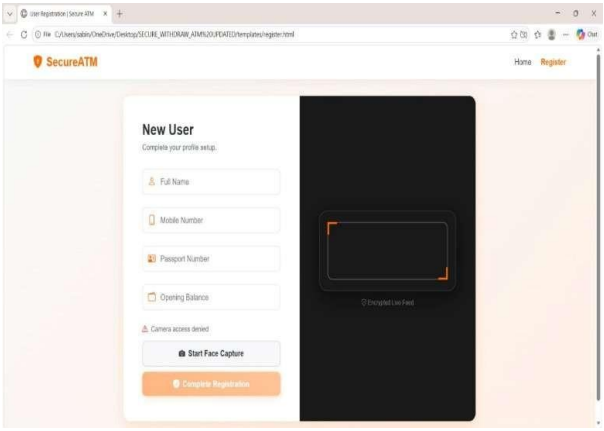


Figure3:UserRegistrationprocess

C. Withdrawal Interface:

Figure 4 illustrates theWithdraw Funds page, which is the core transactional screen of the application. The withdrawal page has a form on the left and a live webcam feed on the right. Local users enter their mobile number and the withdrawal amount. Foreign users also enter their passport number. The Verify Identity button stays disabled until face capture is complete, ensuring the steps are followed in the correct order. Once all inputs are filled in and face capture is

confirmed, submitting the form activates the appropriate authentication process for the user type.

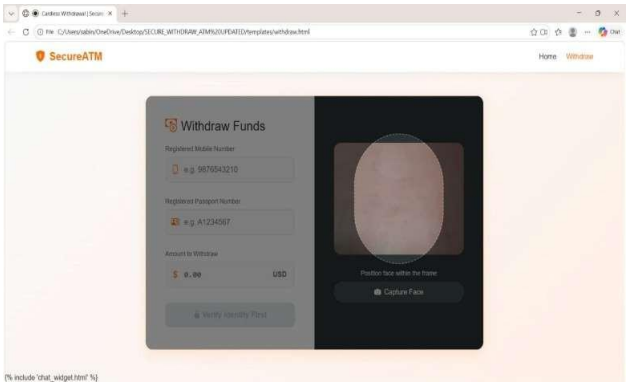


Figure4:Withdrawal Interface

D. MultilingualAssistant:

Figure 5 demonstrates an additional accessibility feature embedded within the withdrawal page — a multilingual chatbot assistant accessible via the floating orange button at the bottom-right of the screen. A floating button opens the Gemini chatbot panel, which includes a language selector offering Tamil, Hindi, Telugu, Kannada, Malayalam, English, and auto-detect. The assistant responds in the selected language, helping users understand the verification steps, troubleshoot errors, and navigatethe interface without relying on English literacy.

Figure5:MultilingualAssistant

E. OTP Verification:

Figure 6 shows the OTP Verification page, which is the second layer of the dual authentication system. After the credential checks pass, the user receives a six-digit OTP on their registered mobile number and enters it on the OTP screen. The code is session-bound and cleared after each use, so it is valid for only one transaction. There is a resend option with a countdown timer for situations where the initial SMS is delayed.

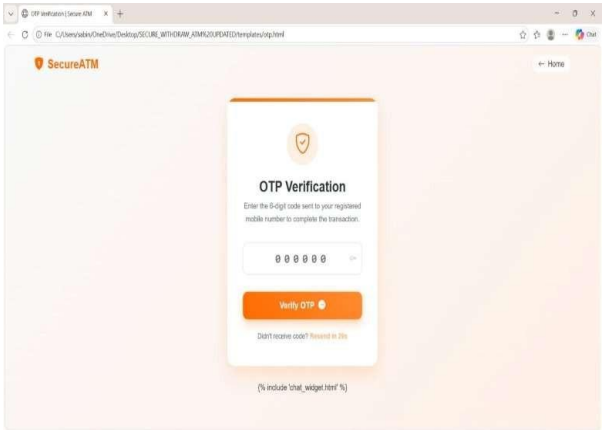


Figure6: OTPVerification

F. TransactionSuccess:

Figure 7 depicts the final confirmation screen displayed upon the successful completion of a withdrawal transaction. The screen presents a clear Cash Dispensed Successfully! message along with a detailed transaction summary.The receipt section includes the following information: Transaction ID, Date and Time, Account, AmountDispensed, MobileNumber, Remaining Balance.

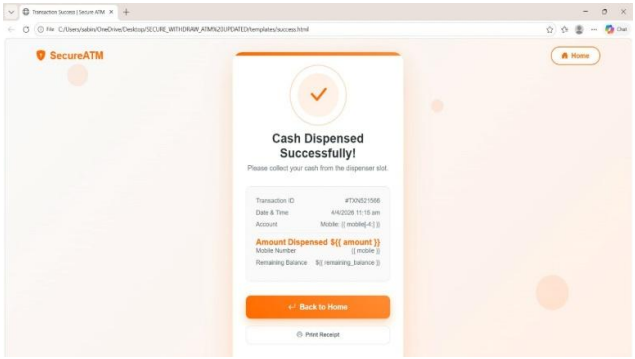


Figure7:CashTransactionprocess

G. Summary of Output Screens:

The following table provides a consolidated view of each system module, its corresponding screen, and thesecurity function it fulfils.

Fig.	Module	Local user	Foreign user
1	Home page	Entry + navigation	Entry + navigation
2	Registration	Face + mobile + balance	Face + mobile + passport + balance
3	Withdrawal form	Mobile + amount + face capture	Mobile + passport + amount + face capture
4	Multilingual chatbot	6 languages, Gemini API	6 languages, Gemini API
5	OTP verification	Twilio 6-digit OTP	Twilio 6-digit OTP
6	Success screen	Receipt + balance	Receipt + balance

Across all six screens, the system consistently enforces the principle of least privilege — each interface reveals only the information strictly necessary for that step.

The combination of face recognitionand OTP authentication,validatedthrough this working prototype, demonstrates that cardless ATM access is not only technically feasible but also practical for deployment in real-world banking environments.

VII. FUTURE SCOPE

There are a few guidelines that can be used to develop and enhance the existing prototype.

Cryptographically Secure OTP: Replaces Python's random module with a CSPRNG for truly unpredictable, banking-grade OTP generation.

Face Recognition Library: Adds real biometric matching with a similarity score and configurable acceptance threshold, beyond just detecting face presence.

OTP Expiry & Rate Limiting: Enforces server-side expiry and resend limits to block brute-force attacks, with depth detection to prevent photo spoofing.

Alternative 2FA for ForeignUsers: Provides email OTP or authenticator app as a fallback for international users with unreliable roaming SMS.

Voice Biometric Layer: Adds voice recognition as a second biometric factor, improving both security and accessibility for visually impaired users.

Blockchain Audit Trail: Logs every transaction hash to an immutable ledger, ensuring tamper-proof records for compliance and forensic review.

VIII. CONCLUSION

Decades of relying on card-and-PIN authentication have made ATM users vulnerable to threats that have become much more complex than the system was ever meant to handle. Instead of adding more fixes to a weak foundation, this work takes a straightforward approach by removing the card entirely and redesigning the authentication process around credentials that are much harder to steal or duplicate.The outcome is a system that does something no other cardless ATM proposal seems to have achieved: it sees user diversity as a key part of the design rather than an afterthought. A local customer and a visitor from abroad are not the same at a terminal, and the authentication framework acknowledges that. Domestic users go through a two-step process—a live face capture followed by a one-time code sent to their phone. This approach is quick, familiar enough to require little instruction, and protects against the skimming and cloning attacks that often affect card-based systems. International visitors have one extra step; they provide their passport number as a third credential to connect the transaction to a document they already have. A decision engine behind both paths ensures that no withdrawal goes through until all checks relevant to that user type have been met.The Gemini-powered assistant built into the interface addresses a challenge that is often overlooked in security discussions,yet is crucial in practice. Language should not prevent someone from accessing their own funds, and supporting six languages directly at the terminal is an easy way to make the system truly accessible, not just functional.Constructed entirely on open, widely available technologies - Flask, SQLite, and a standard webcam - the platform makes an important point: we do not need to wait for new hardware or large budgets to improve ATM security and inclusivity. The technical challenges are less daunting than many believe. What this work shows, above all, is that fixing the gaps left by traditional ATM design is both possible and overdue.

Traditional ATM card infrastructure carries persistent costs that are often overlooked: card manufacturing, chip personalization, bulk mailing, and reissuance when cards are lost or compromised. A cardless system eliminates all of these. The addition of a webcam module and a Twilio API subscription represents a far lower recurring expense, making the transition economically attractive, especially for smaller cooperative banks and regional institutions operating on tight margins.

User acceptance will determine whether systems like this move beyond the prototype stage. The registration flow here is low-effort — requiring under a minute for face capture and a standard form — with no hardware token, smart card reader, or app installation required. The shift from inserting a card to standing before a camera is behaviorally familiar to anyone who unlocks a smartphone with face recognition, and that familiarity significantly reduces the friction that typically slows the adoption of new banking security mechanisms.

the architecture aligns with the direction financial regulators have been taking globally. Many jurisdictions now mandate multi-factor authentication for high-value transactions and formally recognize biometrics as a valid factor. The three-factor path for foreign users — combining face recognition (inherence), OTP (possession), and passport number verification (knowledge) — satisfies standard regulatory combinations. Additionally, each transaction generates a timestamped audit trail of face data, OTP logs, and session outcomes, which is considerably harder to dispute or forge than a PIN entry record, this approach is quick and also familiar to

More broadly, this work reflects the shift in financial security from artifact-centric to identity-centric authentication. When there is no card to clone and no PIN to shoulder-surf, the most common ATM fraud vectors lose their target entirely. The threats that remain — deepfake spoofing and SIM swapping — are more sophisticated, and addressing them is the natural next step. The fact that the conversation has moved to these higher-order concerns is itself a sign of progress, and this prototype demonstrates that the foundation for secure, cardless, and inclusive cash access can be built today using standard, accessible technology.

REFERENCES

[1] S. Tilloo and S. Bhingarkar, “Cardless cash withdrawal using palm vein technology,” in Proc. Int. Conf. Futuristic Technologies (INCOFT), Belgaum, India,2022,pp.1–5,doi:10.1109/INCOFT55651.2022.10094450.

[2] M. M. G. B. Ahmed,A.A.Aman,A. Rafeeque, and M. S. Baig, “Facial recognition & eye blink secured cardless ATM using CNN,” in Proc. IEEE Int. Conf. Block chain Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1–8, doi:10.1109/ICBDS61829.2024.10837137.

[3] R. Pote and S. Kulkarni, “Securing cash withdrawal from ATM with the help of smart mobile banking application,” In Proc. Interdisciplinary Research in Technology and Management (IRTM), Kolkata, India, 2022, pp. 1–4, doi:10.1109/IRTM54583.2022.9791786.

[4] J.Tang, S.Wang,T. Bai, S. Lu, and J. Xiong, “Intelligent ATM replenishment optimization based on hybrid genetic algorithm,” in Proc. Int. Conf.Advanced Communication Technology (ICACT), PyeongChang, South Korea, 2022, pp.469–475,doi:10.23919/ICACT53585.2022.9728791.

[5] S.D.V.,A. R.,E.R.K.,andA. S.,“Enhancedsecurity feature ofATMs through facial recognition,” in Proc. Int. Conf. Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 1252–1256, doi:10.1109/ICICCS51141.2021.9432327.

[6] A. K. Jain, K. Nandakumar, andA. Nagar, “Biometric template security,” IEEE Signal Processing Magazine, vol. 38, no. 5, pp. 75–88,2021.

[7] N. Damer, A. B. J. Teixeira, and A. Kuijper, “Face recognition: Past, present and future,”ACM Computing Surveys, vol. 54, no. 10, pp. 1–36, 2022.

[8] R. Raghavendra and C. Busch, “Presentation attack detection for face recognition systems: A review,” IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1– 15, 2023.

[9] V. Pateland H.Shah,“ATMfrauddetectionusing machine learning techniques,” Procedia ComputerScience,vol.218,pp.1120–1129, 2024.