# 20103023_FACE-ATM:Cardless Transaction System

*by* Aditi Kiran Mahabole

**Submission date:** 08-May-2024 10:19AM (UTC+0530)
**Submission ID:** 2373964352
**File name:** 20103023.pdf (1.78M)
**Word count:** 14613
**Character count:** 87614

# Jaypee Institute of Information Technology, Noida

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING AND INFORMATION TECHNOLOGY


Major Project Title**: FACE-ATM:Cardless Transaction System**


| **Enrollment** | **Name** |
|---|---|
| 20103241 | Saksham Saxena |
| 20103023 | Aditi Mahabole |
| 20103060 | Molshree Sharma |

Supervisor**: Dr. Taj Alam**
Co-Supervisor**: Prof. Prashant Kaushik**


Course Name: MAJOR PROJECT PART-2
Course Code: 22B12CS413
Program: B. Tech. CSE
4nd Year 8th Sem

**2023 - 2024**

(I)
TABLE OF CONTENTS

**(II)**

## DECLARATION

I/We hereby declare that this submission is my/our own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.

**Place**: JIIT, Noida

| | | |
|---|---|---|
| **Enrollment**: 20103241 | **Name**: Saksham Saxena | **Signature**: |
| **Enrollment**: 20103023 | **Name**: Aditi Mahabole | **Signature:** |
| **Enrollment**: 20103060 | **Name**: Molshree Sharma | **Signature:** |

## (III)

## CERTIFICATE

This is to certify that the work titled "**FACE-ATM:Cardless Transaction System**" submitted by **SAKSHAM SAXENA (20103241)**, **MOLSHREE SHARMA (20103060)**, and **ADITI MAHABOLE (20103023)** in partial fulfillment for the award of degree of B.Tech of Jaypee Institute of Information Technology, Noida has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

**Signature of Supervisor** :

**Name of Supervisor** : Dr. Taj Alam

**Designation** : Assistant Professor

:

# (IV)
# ACKNOWLEDGEMENT

We would like to thank Dr. Taj Alam and Prof. Prashant Kaushik, our mentors, for their support and guidance in completing our project in the topic "Face-ATM:Cardless Transaction System". It was a great learning experience. We would like to take this opportunity to express our gratitude to them for their time and efforts they provided throughout the semester. Your useful advice and suggestions were helpful to us during the project's completion. In this aspect, we are eternally grateful to you.

We would like to acknowledge that this project was completed entirely by us and not by someone else.

Signature of Student :
Name of Student : Saksham Saxena
Enrollment Number : 20103241
Date :

Signature of Student :
Name of Student : Molshree Sharma
Enrollment Number : 20103060
Date :

Signature of Student :
Name of Student : Aditi Mahabole
Enrollment Number : 20103023
Date :

# (V)
# SUMMARY

The Face ATM project revolutionizes traditional banking processes by introducing a secure and convenient method of accessing financial services. Developed using Django and Python, this innovative application seamlessly integrates facial recognition technology and OTP verification for enhanced security during transactions. By eliminating the need for physical ATM cards, users benefit from increased convenience and reduced risk of fraud. Leveraging modern technologies such as OpenCV, SMTP, Twilio, and MySQL, the system ensures data integrity and confidentiality while providing multiple authentication channels for user convenience. This forward-thinking solution not only enhances security but also improves the overall banking experience, setting a new standard for future innovations in the industry.

Enrollment: 20103241 Name: Saksham Saxena

Enrollment: 20103023 Name: Aditi Mahabole

Enrollment: 20103060 Name: Molshree Sharma

Signature of Supervisor:

Name of Supervisor: Dr. Taj Alam

Designation: Professor

# (VI)
# LIST OF FIGURES

# 1. INTRODUCTION

## 1.1 General Introduction

The financial sector, like many others, has been swept up in the transformative tide of facial recognition technology. The "Face-ATM" project stands as a bold response to this evolution, aiming to completely revamp the way we interact with cash machines. Forget the days of fumbling for cards and desperately trying to recall PINs. Face-ATM envisions a future where your face is the key that unlocks your account.

This ambitious initiative promises an experience that is both effortless and secure. Imagine simply walking up to the ATM, confidently looking into the camera, and having your identity instantly verified for access to your funds. The convenience factor is undeniable, but security is paramount. Face-ATM goes beyond replacing cards and PINs; it aspires to create a new standard of security at the ATM.

To achieve this groundbreaking vision, Face-ATM leverages a powerful consortium of cutting-edge technologies. Django, a high-level Python framework, serves as the project's backbone, providing the structure for building the entire system. OpenCV, a renowned open-source library, takes center stage for the crucial task of image recognition. This library is specifically designed for real-time computer vision tasks, making it perfectly suited for the demands of facial recognition at the ATM. Finally, ensuring the secure storage and retrieval of user data is MySQL, a robust database management system. This intricate collaboration of technologies paves the way for Face-ATM to deliver a user-centric approach to managing your finances, with an emphasis on both unparalleled convenience and ironclad security.

## 1.2 Problem Statement

Traditional ATM transactions rely on physical cards and PINs, which have long been the standard authentication method. However, this reliance on physical tokens poses inherent

security risks and inconveniences for users. Instances of card theft or loss are not uncommon, exposing users to the threat of fraudulent activities and financial losses. Moreover, the need to memorize PINs adds another layer of complexity and inconvenience to the transaction process.

In response to these challenges, there is a growing demand for more secure and user-friendly alternatives to traditional ATM authentication methods. The Face-ATM project aims to address these concerns by leveraging facial recognition technology to authenticate users without the need for physical cards or memorized codes. This innovative approach not only eliminates the risk of card theft or loss but also enhances convenience for users.

By simply scanning their faces, users can securely access ATM services, making transactions faster, more efficient, and less prone to security breaches. Facial recognition technology offers a robust and reliable means of authentication, as each person's facial features are unique and difficult to replicate. Additionally, the adoption of facial recognition aligns with the broader trend towards biometric authentication methods, which are increasingly being used in various sectors to enhance security and streamline user experiences.

The implementation of the Face-ATM project represents a significant step towards modernizing banking systems and redefining traditional ATM transactions. It not only enhances security by reducing the reliance on physical tokens but also provides a superior user experience by simplifying the authentication process. As technology continues to evolve, innovative solutions like Face-ATM are paving the way for a future where banking services are seamlessly integrated with cutting-edge technology, ensuring both security and convenience for users.

## 1.3 Significance/Novelty of the Problem

The conventional reliance on physical cards and PINs for ATM transactions presents significant security risks and user inconvenience. Instances of card theft or loss, coupled with the need to remember PINs, contribute to the vulnerability of traditional authentication methods. Furthermore, the use of physical tokens poses challenges in terms of accessibility, as users may forget or misplace their cards, leading to disruptions in accessing banking services.

Addressing these challenges through the implementation of facial recognition technology represents a novel and forward-thinking approach. By leveraging biometric data unique to each individual, facial recognition technology offers unparalleled convenience and security. Users no longer need to carry physical cards or memorize complex PINs, reducing the risk of theft or loss while streamlining the transaction process.

The development of the Face-ATM system signifies more than just a departure from traditional banking practices; it heralds a new era of seamless, cardless transactions that prioritize user experience and security. This innovative solution not only addresses the shortcomings of traditional authentication methods but also sets a precedent for future advancements in the field of banking technology.

The adoption of facial recognition technology in ATM transactions has the potential to reshape the landscape of banking services. It represents a paradigm shift towards more secure and user-friendly authentication methods, aligning banking systems with the growing trend towards biometric authentication across various industries.

Furthermore, the implementation of the Face-ATM system opens up opportunities for integration with other emerging technologies, such as artificial intelligence and machine learning. These advancements can further enhance the security and functionality of ATM transactions, paving the way for a more efficient and personalized banking experience for users.

In summary, the significance and novelty of the Face-ATM system lie in its ability to address longstanding security concerns and user inconveniences associated with traditional ATM transactions. By embracing facial recognition technology, banks can not only improve security but also enhance user experience, ultimately shaping the future of banking services in a digital age.

## 1.4 Brief Description of the Solution Approach

The Face-ATM system is designed to offer a streamlined and secure method for cardless ATM transactions, prioritizing both user convenience and security. The process begins with user registration, during which individuals provide personal information such as their name, email, age, and upload a facial image. Additionally, users input their bank details, including the bank name and account number, to link their accounts to the system.

Once registered, users proceed to the login page, where the innovative facial recognition authentication takes place. This cutting-edge technology replaces the need for physical cards or memorized PINs, offering a seamless and intuitive authentication experience. Upon successful facial recognition, users gain access to the system's home page, which prominently features a "scan face to withdraw" button.

Activating this button initiates the camera for facial scanning, further verifying the user's identity. The system compares the scanned facial image with the registered image to ensure a match. If the facial scan is successfully authenticated, users are directed to an additional layer of security: an OTP (One-Time Password) verification page.

At this stage, users have the option to choose how they receive the OTP – via email or phone. This additional verification step adds an extra layer of security, ensuring that only authorized users can proceed with the transaction. Once the OTP is successfully verified, users are granted access to the withdrawal page.

On the withdrawal page, users input the desired amount they wish to withdraw. The system debits the specified amount from the user's linked account, completing the transaction securely and efficiently. This comprehensive approach not only ensures a seamless and user-friendly transaction process but also mitigates security risks associated with traditional ATM transactions.

By leveraging facial recognition technology and incorporating additional security measures such as OTP verification, the Face-ATM system sets a new standard for ATM transactions. It not only enhances user experience by eliminating the need for physical cards and PINs but also prioritizes security, safeguarding users' financial assets in an increasingly digital world.

# 2. LITERATURE SURVEY

## 2.1 Summary of Papers Studied

1. **Title: AI Based Card-Less Atm Using Facial Recognition**

Author: B. Priyadharshini, T. Kanagalakshmi Nithyasree, J. Sherin

Year: 2022

**Introduction:**

The current system of securing ATMs with a physical card and memorized PIN, while once a significant advancement, is starting to show its age. As technology thrives and the criminal landscape transforms, these methods become riddled with vulnerabilities. Physical cards are susceptible to loss or theft, and even the most secure PINs can be compromised. We might forget them, accidentally expose them to prying eyes through shoulder surfing, or even have them extracted through social engineering tricks. These weaknesses create exploitable loopholes for criminals to access our hard-earned cash.

This paper proposes a ground-breaking solution that tackles these shortcomings head-on: an AI-powered, card-less ATM system. This innovative approach throws out the traditional model entirely, replacing the cumbersome card and PIN with the power of facial recognition technology. Facial recognition offers a significantly more robust and secure method of user authentication. Unlike cards and PINs, our facial features are unique to each individual and incredibly difficult to forge or steal. This shift not only minimizes the risk of unauthorized access to our accounts, but also eliminates the stress of managing and potentially losing a physical card or forgetting a complex PIN. Transactions become smoother, faster, and far more secure, allowing us to manage our finances with greater peace of mind.

The introduction goes beyond simply highlighting the system's weaknesses. It sets the stage for a deeper exploration of the proposed AI-based solution by establishing the need for improved

security and introducing a groundbreaking alternative. By framing the limitations of the current system and then presenting facial recognition as a revolutionary approach, the paper paves the way for a detailed examination of how this technology can transform how we interact with ATMs. This novel approach has the potential to usher in a new era where self-service banking is not only convenient but also prioritizes the security of our financial resources. Furthermore, facial recognition technology offers the potential for additional layers of security. Imagine a system that combines facial recognition with other biometric data points, like iris scans or fingerprints, to create an even more secure authentication process. This could provide an extra level of protection against sophisticated attacks.

The possibilities with AI-powered, card-less ATMs extend beyond just security and convenience. Imagine a future where ATMs can greet you by name, recognize your banking habits, and recommend personalized financial products or services. This level of interaction could streamline the banking experience and make managing your finances even more efficient. The introduction of this paper lays the groundwork for exploring these possibilities and paves the way for a future where ATM interactions are not only secure and convenient, but also personalized and efficient.

**Summary:**

This paper delves into a groundbreaking solution for ATM security: a system that relies on facial recognition for user authentication. At the core of this innovation lies a powerful Convolutional Neural Network (CNN) model. Imagine a complex web of interconnected processors, specifically trained to recognize faces with exceptional accuracy. This CNN model forms the backbone of the system, analyzing facial data captured by the ATM's camera.

However, raw data from a camera isn't always perfect. To ensure the CNN performs optimally, the paper details the utilization of preprocessing techniques. These techniques act like a fine-tuning process, enhancing the quality of the captured image and minimizing potential errors. Think of it as sharpening a photograph to ensure all the crucial details are clear and crisp for the CNN to analyze effectively.

The process doesn't stop at simply capturing a face. The paper elaborates on how the system differentiates between a real person and, say, a photograph held up to the camera. Advanced

algorithms within the CNN model are designed to identify these discrepancies, ensuring only legitimate users gain access. Furthermore, the captured facial patterns are then matched against a centralized database containing authorized users. This verification process acts as a final checkpoint, confirming the person's identity before granting access to their account.

For an extra layer of security, the paper highlights the incorporation of a 4-digit PIN prompt. Even with the power of facial recognition, this additional step creates a two-factor authentication process. Think of it like a double lock on your door – one requiring your face, the other a unique PIN only you know. This two-pronged approach significantly bolsters security, making unauthorized access even more challenging.

In essence, this summary encapsulates the essence of the proposed AI-based ATM system. It details the utilization of cutting-edge facial recognition technology, powered by a CNN model, alongside essential preprocessing and verification steps. The inclusion of a secondary PIN verification further strengthens the system's security. This combination of innovative technologies has the potential to revolutionize the way we interact with ATMs, ushering in an era of unparalleled security and convenience.

**Evaluation:**

The paper's evaluation section dives deep into the effectiveness of the proposed AI-based card-less ATM system. This critical analysis acts as a spotlight, illuminating how facial recognition strengthens ATM security and combats fraudulent activities. Here, the paper meticulously examines the advantages this technology offers. Compared to traditional methods that rely on cards and PINs, facial recognition boasts superior accuracy. Imagine a system that can distinguish between you and your identical twin with exceptional precision – that's the power of facial recognition at play. Furthermore, facial recognition streamlines the authentication process, eliminating the need to fumble for cards or remember complex PINs. This translates to a more efficient and user-friendly experience for legitimate ATM users.

But the evaluation doesn't rely solely on theoretical concepts. The paper goes a step further by presenting empirical evidence. Think of real-world experiments designed to test the system's reliability under various conditions. These experiments provide valuable data that showcases the

system's robustness – its ability to function effectively even in challenging scenarios. The results of these experiments serve as concrete proof that facial recognition delivers on its promises of enhanced security.

By critically analyzing the system's efficacy and presenting empirical evidence, the evaluation section serves a crucial purpose. It strengthens the case for the proposed AI-based solution as a viable and impactful approach to ATM security. The findings reinforce the notion that facial recognition has the potential to significantly elevate security standards, making unauthorized access to our hard-earned cash far more difficult. This evaluation section paves the way for a future where ATMs are not just convenient, but fortresses safeguarding our financial resources.

**Conclusion:**

The paper culminates in a conclusion that underscores the critical need for robust security measures in the face of ever-evolving threats. It reiterates the inherent weaknesses of traditional ATM systems, highlighting the susceptibility of cards and PINs to loss, theft, and fraudulent activities. In this context, the conclusion reaffirms the significance of facial recognition technology as a powerful tool to effectively address these vulnerabilities.

Looking ahead, the paper emphasizes the transformative potential of the proposed AI-based, card-less ATM system. This innovative approach promises a future where security is paramount, user experience is streamlined, and the efficiency of transactions is significantly enhanced. Furthermore, the conclusion highlights the potential reduction in fraudulent activities, providing peace of mind to users and minimizing financial losses.

But the paper doesn't stop at celebrating the present. It also casts a forward-thinking glance towards future advancements. The conclusion proposes exciting avenues for further research and development. Imagine integrating additional biometric authentication methods like fingerprint scanners or iris recognition, creating an even more secure multi-factor authentication process. The paper ponders the possibility of expanding the system's capabilities beyond physical ATMs, potentially enabling remote access and real-time transaction monitoring for enhanced security and convenience.

By synthesizing the key findings and proposing a roadmap for future exploration, the conclusion effectively encapsulates the paper's overarching objectives and contributions. The research presented not only offers a compelling solution for improved ATM security but also paves the way for further advancements in this field. This concluding section signifies a promising direction for the evolution of ATM security technology, fostering a future where accessing our finances is not just convenient, but also demonstrably secure.

2. **Title: Deep Learning-Based Card-Less ATM Using Fingerprint and Face Recognition**

**Author:** K Veena, Harismitha L, Kishore Babu, Raksha Urs, Rashmi M R

**Year:** 2023

**Introduction:**

Our world is constantly evolving, and so are the security threats we face. This is especially true in the realm of financial transactions, where protecting our hard-earned cash is paramount. Traditional ATM systems, reliant on physical cards and PINs, are becoming increasingly vulnerable. Cards can be lost or stolen, and PINs can be guessed through brute force attacks or even shoulder-surfed by malicious actors. These vulnerabilities expose us to the risk of unauthorized access to our accounts, raising a critical question: how can we ensure secure and convenient access to our finances at ATMs in the face of these growing concerns?

This paper proposes a groundbreaking solution: a cardless ATM system that leverages the power of biometrics. Biometrics are unique physical or behavioral characteristics used for identification, and this system specifically focuses on facial and fingerprint recognition. Imagine a future where you can ditch the plastic and memorized codes. You simply walk up to an ATM, confidently look into the camera for facial recognition, and place your finger on the scanner for fingerprint verification. No more fumbling for cards or desperately trying to recall forgotten PINs. This innovative approach promises a future where your face and fingerprint become the

keys to unlocking your account, offering a new level of security and convenience for ATM transactions.

Beyond the immediate benefits of enhanced security and user experience, a cardless ATM system with biometric authentication has the potential to revolutionize the way we interact with our finances. Imagine ATMs that greet you by name, instantly recognize your banking habits, and provide personalized recommendations for financial products or services. This level of interaction could streamline the banking experience and make managing your finances even more efficient. Additionally, the biometric data collected by the system could be used to develop more sophisticated fraud detection mechanisms, further safeguarding your financial security.

However, the successful implementation of such a system requires careful consideration of privacy concerns. Robust data security protocols and clear user consent procedures are essential to ensure that the biometric data collected by the ATMs is protected and used responsibly. By addressing these concerns and fostering trust with users, a cardless ATM system with biometric authentication has the potential to usher in a new era of secure, convenient, and personalized financial transactions.

**Summary:**

This paper dives into a groundbreaking approach to ATM security: a cardless system that leverages the power of deep learning for user authentication. At the core of this innovation lies a powerful tool known as a Convolutional Neural Network (CNN). Imagine a complex web of interconnected processors specifically designed to excel at recognizing patterns, particularly visual ones. In this system, the CNN acts as the engine driving facial recognition.

The paper meticulously outlines the system's architecture, a three-stage process meticulously designed to ensure secure access. The first stage focuses on facial recognition. The user simply steps up to the ATM and the camera captures their image. This image data is then fed into the CNN, which has been meticulously trained on a massive dataset of facial images. Through this painstaking training process, the CNN has learned to identify unique facial features with exceptional accuracy, allowing it to verify the user's identity with a high degree of confidence.

However, facial recognition isn't the only layer of security. The system incorporates a second stage of authentication – fingerprint recognition – to add another layer of defense. Imagine a fingerprint scanner integrated into the ATM's sleek design. The user places their finger on the scanner, and the system captures a digital representation of their unique fingerprint pattern. This fingerprint data is then compared against the user's information stored securely in a database. Unlike PINs, which can be easily forgotten or stolen, fingerprints are unique identifiers that are virtually impossible to replicate.

Finally, the third stage involves a critical validation process. Once both facial and fingerprint recognition have been successfully completed, the system performs a final check against a centralized database containing authorized users. This additional step ensures that the person attempting to access the account is indeed the legitimate owner. By combining these three stages, the system establishes a robust and secure authentication process that significantly reduces the risk of unauthorized access. This multi-factor approach offers a significant leap forward in ATM security compared to traditional card and PIN systems, which are susceptible to loss, theft, or social engineering attacks.

Furthermore, the paper explores the potential benefits of deep learning beyond user authentication. The CNN's ability to recognize patterns could be harnessed to personalize the ATM experience. Imagine an ATM that greets you by name, recognizes your banking habits, and suggests relevant financial products or services based on your past transactions. This level of interaction could streamline the banking experience and make managing your finances even more efficient.

However, the successful implementation of such a system requires careful consideration of privacy concerns. Robust data security protocols and clear user consent procedures are essential to ensure that the biometric data collected by the ATMs is protected and used responsibly. By addressing these concerns and fostering trust with users, a cardless ATM system with deep learning-based authentication has the potential to usher in a new era of secure, convenient, and personalized financial transactions.

**Evaluation:**

The paper doesn't stop at proposing the theoretical framework for a secure cardless ATM system. To assess its effectiveness in the real world, the researchers conduct a series of controlled experiments. Here's where things get interesting. Imagine a group of 100 users participating in these experiments. The researchers collect facial and fingerprint images from each participant, creating a comprehensive dataset that serves as the foundation for testing the system's capabilities.

This dataset is then cleverly divided into two parts: a training set and a test set. The training set, like a student cramming for an exam, is fed into the system's deep learning model, specifically the CNN. During this training phase, the CNN meticulously analyzes the facial and fingerprint data, learning to recognize the unique features of each participant. The model essentially becomes an expert at identifying authorized users based on their facial characteristics and fingerprint patterns.

Once the CNN is trained, it's time for the real test. The test set, unseen by the model during training, is used to evaluate the system's performance. This ensures an unbiased assessment of how well the model can recognize authorized users from a fresh set of data. The researchers measure the system's effectiveness using a combination of metrics. Accuracy, of course, is paramount. How often can the system correctly identify a legitimate user based on their facial and fingerprint data?

But accuracy isn't the whole story. The researchers also evaluate the system's error rates. The false acceptance rate (FAR) measures how often the system mistakenly grants access to an unauthorized user. Ideally, this rate should be incredibly low to prevent fraudulent transactions. On the other hand, the false rejection rate (FRR) measures how often the system rejects a legitimate user attempting to access their account. A high FRR would be frustrating for users, so finding the right balance is crucial.

Finally, the evaluation process goes beyond the technical aspects. User feedback on convenience and security is also gathered. After interacting with the cardless ATM system, participants are asked about their experience. Did they find the system easy and user-friendly? Do they feel confident that the system provides adequate security for their financial information? By incorporating user experience alongside technical performance metrics, the researchers gain a

well-rounded picture of the system's strengths and weaknesses, paving the way for further refinement and real-world implementation.

**Conclusion:**

The paper culminates by presenting a compelling case for the proposed cardless ATM system. This innovative approach emerges as a secure, convenient, and efficient alternative to the limitations of traditional ATM systems reliant on cards and PINs. The evaluation process provided concrete evidence of the system's effectiveness in thwarting fraudulent transactions. Imagine a significant reduction in unauthorized access attempts, thanks to the robust multi-factor authentication process employing facial and fingerprint recognition. Furthermore, the system demonstrates a high degree of accuracy in user authentication, ensuring legitimate users can access their accounts quickly and seamlessly.

However, the paper acknowledges that the journey doesn't end here. The authors recognize the importance of continuously refining the system to address potential biases within the CNN algorithm. Imagine a scenario where the facial recognition component struggles to accurately identify users with certain ethnicities. Mitigating these biases is crucial to ensure fair and inclusive access for all users.

Another key area for further exploration is the realm of user data privacy and security. The paper underscores the need for robust safeguards to protect the sensitive biometric data collected by the system. Imagine implementing cutting-edge encryption techniques and stringent data security protocols to ensure this information remains confidential and protected from unauthorized access.

By addressing these considerations and fostering a culture of responsible data management, the proposed cardless ATM system with deep learning-based authentication has the potential to revolutionize the financial landscape.

3. **Title:ATM Plus with face recognition and OTP mechanism**

Authors:Prasannajeet Singh, Sufia Shahin, Dr. Usha Chauhan

Year:2024

**Introduction:**

The ever-growing sophistication of criminal tactics necessitates a constant evolution in security measures, especially within the financial sector. This paper tackles this pressing issue head-on by proposing a novel Automated Teller Machine (ATM) model designed to combat the escalating security concerns surrounding traditional ATM transactions. Imagine a future where ATMs are not just about convenience, but about safeguarding your hard-earned cash with cutting-edge technology.

The paper opens by painting a clear picture of the current landscape. Traditional ATM systems, while once a significant advancement, are increasingly vulnerable due to their reliance on physical cards and memorized PINs. These methods are susceptible to loss, theft, and even sophisticated hacking techniques. In the hands of cunning criminals, stolen cards and cracked PINs can translate to unauthorized access to our bank accounts. This alarming scenario underscores the critical need for innovative solutions in the world of ATMs.

The introduction goes beyond simply highlighting the vulnerabilities. It emphasizes the ever-changing nature of ATM technology. Just as criminals devise new methods, so too must security measures adapt and improve. This paper presents a significant leap forward in this ongoing pursuit of enhanced security. By introducing a new ATM model equipped with facial recognition and One-Time Password (OTP) mechanisms, the authors propose a powerful two-pronged approach to thwarting unauthorized access and ensuring the safety and convenience of ATM users. The stage is set for a deep dive into how this innovative system functions and the potential it holds for revolutionizing the way we interact with ATMs.

**Summary:**

This paper delves into the development of a novel ATM system designed to elevate both security and user satisfaction. At the core of this innovation lies the marriage of two powerful

technologies: facial recognition and One-Time Password (OTP) authentication. Imagine an ATM that not only recognizes your face but also sends a unique, temporary code to your phone, creating a robust two-factor authentication process.

The paper delves into the specifics of facial recognition technology. The system utilizes a sophisticated algorithm, likely implemented using MATLAB, a powerful software for scientific computing. This algorithm acts like a detective, meticulously analyzing your facial features – your eyes, nose, cheekbones, and jawline – to create a unique signature. Just like a fingerprint, your facial features are specific to you, allowing the algorithm to verify your identity with a high degree of accuracy.

But facial recognition isn't the only layer of security. The system adds another line of defense with OTP authentication. Here's where Amazon Simple Notification Service (SNS) comes into play. Imagine a system that, upon successful facial recognition, sends a unique code directly to your registered mobile phone number via a secure connection with Amazon SNS. This temporary code acts like a secret handshake between you and the ATM, ensuring only authorized users with both the correct face and the unique code can access their accounts.

By combining these two powerful technologies, the paper proposes a system that significantly minimizes the risk of fraudulent attempts. Stolen cards and cracked PINs become obsolete in this new paradigm. Furthermore, the paper highlights the potential for this system to enhance user confidence in ATM transactions. Imagine the peace of mind that comes from knowing your face and a unique, temporary code are the keys to accessing your hard-earned cash. This innovative approach has the potential to revolutionize the way we interact with ATMs, fostering a future where security and convenience go hand in hand.

**Evaluation:**

The paper doesn't stop at proposing a secure and user-friendly ATM system; it meticulously evaluates its effectiveness. This evaluation section acts as a spotlight, illuminating the strengths of the proposed system, particularly in enhancing security and user experience. Here, the paper delves into the advantages of both facial recognition and OTP authentication.

Imagine a world where stolen cards and compromised PINs become a relic of the past. Facial recognition technology, as analyzed in the paper, offers a powerful solution. The system's ability to recognize unique facial features with high accuracy significantly reduces the risk of unauthorized access. Even if someone manages to steal your card, their face won't match yours, rendering the card useless at the ATM.

OTP authentication adds another layer of defense. The paper details how the system utilizes Amazon SNS to send a unique, temporary code directly to the user's registered mobile phone. This code acts like a secret key, ensuring only the rightful owner, with both the matching face and the unique code, can access their account. This two-factor authentication process significantly strengthens security compared to traditional methods.

But the evaluation goes beyond theoretical advantages. The paper presents a comprehensive analysis of the implementation process, providing a glimpse into how this system comes to life. We learn about the development of facial recognition software, likely using a powerful tool like MATLAB, and the seamless integration of Amazon SNS for OTP delivery. This detailed breakdown fosters confidence in the system's feasibility and functionality.

The evaluation doesn't rely solely on explanations; it provides empirical evidence through experiments. Imagine tests conducted to assess the system's reliability and efficiency. The results of these experiments, documented in the paper, serve as concrete proof that the system performs as intended. By effectively mitigating security concerns in ATM operations, as evidenced by the evaluation, the proposed system paves the way for a future where accessing our finances is not just convenient, but demonstrably secure.

**Conclusion:**

The evaluation section scrutinizes the system's effectiveness in boosting security and user experience. It analyzes the individual merits of facial recognition and OTP authentication, showcasing how they collaborate to curb risks associated with stolen cards and unauthorized transactions. Facial recognition, built with software like MATLAB, offers a powerful solution by leveraging unique facial features for user identification. The paper examines the development of this software, highlighting its meticulous analysis of facial characteristics.

However, security extends beyond facial recognition. OTP authentication adds another layer of defense. The paper explores the use of Amazon SNS, a tool that securely transmits unique codes to the user's registered mobile phone. Upon successful facial recognition, the system utilizes SNS to send a temporary code, acting as an extra verification step. This ensures only authorized users with both the correct face and the unique code can access their accounts.

By evaluating each technology's effectiveness and their integration, the section underscores the system's reliability and efficiency. Real-world experiments with the system are presented, providing data that showcases its robustness in various scenarios. The results validate the system's potential to address security concerns in ATMs by significantly reducing unauthorized access. In essence, the evaluation section analyzes the system's strengths through a combination of theoretical and practical assessments, paving the way for a future where ATMs prioritize both security and user experience.

## 2.2 Integrated summary of Literature Survey

These papers explore innovative approaches to ATM security, primarily focusing on facial recognition technology integrated with deep learning models like Convolutional Neural Networks (CNNs). It details how the CNN analyzes facial data from ATM cameras and employs preprocessing techniques to enhance accuracy. The system differentiates real users from fake representations like photos and verifies identities against a centralized database.

Additionally, the paper discusses the integration of a secondary PIN or fingerprint authentication step for added security. It emphasizes the advantages of multi-factor authentication over traditional card and PIN systems, reducing risks of unauthorized access significantly. Furthermore, it explores the potential for personalized banking experiences using deep learning and addresses privacy concerns associated with biometric data collection.

Overall, the proposed AI-based ATM system aims to revolutionize ATM security by combining cutting-edge technologies to ensure secure, convenient, and personalized financial transactions.

# 3. REQUIREMENT ANALYSIS AND SOLUTION APPROACH

## 3.1 Overall Description of Project:

The Face-ATM project ushers in a new era of convenience and security for ATM transactions. This innovative system ditches the limitations of traditional methods that rely on physical cards and memorized PINs. Instead, Face-ATM leverages the power of facial recognition technology, offering a seamless and secure alternative for users to access their bank accounts.

The user experience is designed with ease in mind. The system walks users through a simple registration process. You'll provide some basic personal information, upload your facial image for identification, and link your bank credentials. Once registered, visiting an ATM becomes a breeze. Simply look into the camera at the login page, and the facial recognition technology will verify your identity, granting you access to the system's features.

Security is paramount with Face-ATM. After successful facial recognition, an additional layer of protection is added through OTP (One-Time Password) verification. You'll receive a unique code via email or phone, acting as a second handshake between you and the ATM. Only with both your face and the correct code can you proceed with transactions. Finally, you'll enter the desired withdrawal amount, completing the transaction swiftly and securely.

The power behind Face-ATM lies in its robust technological architecture. The system utilizes a powerful combination of technologies like Django, a high-level Python framework, for building the system's core structure. OpenCV, a renowned open-source library, takes center stage for the crucial task of image recognition. Ensuring the secure storage and retrieval of user data is MySQL, a well-established database management system. This intricate collaboration of technologies paves the way for Face-ATM to deliver a user-centric approach to managing your finances.

In essence, Face-ATM goes beyond simply replacing cards and PINs. It prioritizes both convenience and security, setting a new standard for ATM transactions in the digital age. Imagine

a future where accessing your cash is as effortless as looking into a camera – a future where security and ease of use go hand in hand. Face-ATM paves the way for this future, transforming the way we interact with our finances

## 3.2 Requirement Analysis

### 3.2.1 **Functional Requirements:**

1. **User Registration**: Users shall be able to create a new account by providing personal information:
    - Full Name
    - Email Address
    - Age (verification may be required depending on regulations)
- Users shall be able to upload a high-quality facial image for identification purposes.
- The system shall securely store the uploaded facial image and link it to the user's account.
- Users shall be able to input their bank details:
    - Bank Name
    - Account Number
2. **Facial Recognition Authentication:** Upon login attempt, the system shall activate the camera on the ATM and capture a user's facial image.
- The captured image shall be compared against the user's registered facial data using facial recognition technology.
- Upon successful facial recognition, the system shall grant access to the ATM functionalities.
- In case of unsuccessful facial recognition (e.g., poor lighting, significant facial changes), the system shall provide clear error messages and offer alternative login options (if applicable).
3. **Transaction Initiation:** The system shall present a user-friendly home page upon successful login.
- The home page shall display a prominent button labeled "Scan Face to Withdraw" to initiate a transaction.

- Clicking the "Scan Face to Withdraw" button shall activate the ATM camera for facial scanning.

4. **OTP Verification:** After successful facial recognition for transaction initiation, the system shall prompt for OTP verification.

- The system shall offer users the option to receive a unique One-Time Password (OTP) via email or phone.
- Users shall be able to choose their preferred method for receiving the OTP.
- Upon user selection, the system shall securely send the OTP to the chosen method (email or phone).

5. **Withdrawal Process:**Upon OTP verification, users should be directed to a withdrawal page.Users should be able to input the desired withdrawal amount for the transaction to be completed.Following successful OTP verification, the system shall direct the user to a withdrawal page.

- The withdrawal page shall provide a clear interface for users to input the desired withdrawal amount.
- The system shall validate the entered amount against the user's account balance and daily withdrawal limits (if applicable).
- Upon confirmation of a valid withdrawal amount, the system shall process the transaction.

6. **Transaction Confirmation :**Once the transaction is complete, the system shall display a confirmation message on the screen, informing the user of the successful withdrawal.

- The system may also send a confirmation email or text message to the user, detailing the transaction amount, date, and time.

7. **Error Handling:** The system shall gracefully handle potential errors during the transaction process and provide clear error messages to guide users.

- Examples of errors include:
    - Unsuccessful facial recognition attempts
    - Incorrect OTP inputs
    - Insufficient funds in the user's account
    - Technical malfunctions

- Error messages should be informative and user-friendly, guiding users towards resolving the issue and completing their transaction.

### 3.2.2 **Non-Functional Requirements:**

1. **Security:**

- **Encryption:** The system must utilize robust encryption techniques to safeguard user data, including facial images and financial information. This includes encrypting data at rest (stored on the ATM system) and in transit (being transmitted between the ATM and other systems).
- **Access Control:** Implement strict access control mechanisms to limit access to user data and system functionalities. Only authorized personnel should be able to view or modify sensitive information.
- **Regular Security Audits:** Conduct periodic security audits to identify and address potential vulnerabilities in the system. This helps maintain a proactive approach to security and prevent unauthorized access.

2. **Accuracy:**

- **Facial Recognition Accuracy:** The facial recognition system should achieve a high degree of accuracy in verifying user identities. This minimizes the risk of:
    - **False Positives:** Granting access to unauthorized individuals due to mistaken identity.
    - **False Negatives:** Denying access to legitimate users due to inaccurate recognition.
- **Lighting and Angle Tolerance:** The system should be able to accurately recognize users even under varying lighting conditions and facial angles. This ensures reliable identification regardless of the ATM environment.

3. **Performance:**

- **Low Latency:** The system should process facial recognition and transaction requests with minimal latency (delay). This translates to a faster and more responsive user experience.

- **System Uptime:** The system should strive for high uptime, minimizing downtime due to technical failures. Regular maintenance and performance optimization are crucial for maintaining smooth operation.

4. **Scalability:**

- **User Base Growth:** The system architecture should be designed to accommodate an increase in user registrations over time. This includes the ability to handle a larger user database and manage user information efficiently.
- **Transaction Volume:** The system should be able to handle a growing volume of transactions without compromising performance. Consideration should be given to scaling hardware resources (e.g., additional processing power) and optimizing software to handle higher workloads.

5. **Usability:**

- **Intuitive Interface:** The user interface should be clear, concise, and easy to navigate. Users with varying levels of technical expertise should be able to interact with the system comfortably.
- **Clear Instructions:** Provide clear and concise instructions throughout the registration, authentication, and transaction processes. This ensures users understand each step and can complete their tasks efficiently.
- **Accessibility:** Consider accessibility features for users with visual or physical impairments. This may include options for text-to-speech narration, enlarged fonts, or alternative input methods.

6. **Reliability:**

- **Minimal Downtime:** The system should be highly reliable, with minimal system failures and downtime. Regular maintenance and monitoring are crucial to ensure system stability and availability for users.
- **Data Backups:** Implement a comprehensive data backup and recovery plan to minimize potential data loss in case of unforeseen circumstances.

7. **Compliance:**

- **Regulatory Adherence:** The system should comply with all relevant regulations and industry standards governing banking and financial transactions. This includes regulations related to data security, financial transactions, and consumer protection.

- **Legal Considerations:** Address legal requirements around user identification and verification processes to mitigate risks associated with fraudulent activities.

8. **Privacy:**

- **User Consent:** Obtain explicit user consent for the collection, storage, and use of facial biometric data. This ensures transparency and user control over their personal information.
- **Data Anonymization:** Consider anonymizing or pseudonymizing facial data whenever possible to minimize the risk of user identification from stored data.
- **Data Retention:** Establish clear policies for data retention and deletion. User data should not be retained for longer than necessary to fulfill its intended purpose.

### 3.2.3 **Technical Requirements:**

**1. Backend Development:**

**Django Python Framework:** The system will leverage Django as its foundation for backend development. Django offers a robust and secure framework for building web applications, handling tasks like:

- User authentication and authorization
- Data processing and logic
- Integration with other systems via APIs

**2. Facial Recognition and Image Processing:**

**OpenCV:** OpenCV, a powerful open-source library, will be employed for facial recognition functionalities. OpenCV provides tools for:

- Face detection and extraction from captured images
- Feature extraction from facial data (e.g., identifying key features like eyes, nose, and jawline)
- Matching extracted features against user profiles for identification

**3. Data Storage:**

**MySQL Database:** MySQL, a well-established and secure database management system, will be used to store critical data, including:

- User information (profiles, facial data, bank details)
- Station information (ATM locations, system configurations)
- Transaction records (withdrawal amounts, timestamps)

**4. User Interface:**

**Web Development Technologies:** The user interface (UI) for interacting with the Face-ATM system will be built using fundamental web development technologies:

- **HTML:** Provides the core structure and content layout for the UI.
- **CSS:** Defines the visual style and presentation of the UI elements.
- **JavaScript:** Enables dynamic behavior and interactivity within the UI, such as user input validation and real-time updates.

**5. Transaction Processing:**

**API Integration:** The system may require integration with external APIs to facilitate functionalities like:

- Payment gateway integration for processing account withdrawals and transactions
- Fare deduction systems (if applicable for public transportation scenarios)

**6. Deployment and Scalability:**

**Cloud Hosting:** Considering scalability and reliability, the Face-ATM system can be hosted on a cloud platform. Cloud platforms offer:

- On-demand resource scaling to accommodate increasing user base and transaction volume.
- High availability with built-in redundancy mechanisms to minimize downtime.

**7. Accessibility:**

**Device and Browser Compatibility:** The system should be designed to function seamlessly across various devices and browsers. This ensures accessibility for users with different technological preferences and capabilities. Responsive design principles are crucial to achieve compatibility across desktops, tablets, and mobile devices.

## 3.3 Solution Approach

The solution approach for the "GoCardless" project involves the integration of facial recognition technology with a web-based platform to create a seamless and convenient fare deduction system for metro users. Here's a detailed breakdown of the solution approach:

**1. System Architecture:**

- **Client-Server Model:** The system will adopt a client-server architecture. The user interface, accessible through web browsers, will be built using the Django Python framework. This web application acts as the client-side, handling user interactions and displaying information.
- **Server-Side Processing:** The server-side handles the crucial tasks of facial recognition and database operations. This server-side component will utilize two powerful tools:
    - OpenCV, a renowned open-source library, for real-time image processing and facial feature extraction from captured images at the metro entry gate.
    - MySQL, a well-established database management system, for securely storing user data (profiles, facial images, account details) and transaction records.

**2. User Management:**

- **Registration and Login:** Users will register on the system's web platform by providing necessary personal information and account details. This registration process will be secure, ensuring user data is protected. Upon registration, user data will be stored safely within the MySQL database.

- **User Authentication:** Once registered, users can log in securely using their credentials. The system will verify login information before granting access to the fare deduction functionality.

**3. Station Selection Interface:**

**User-Friendly Interface:** The web application will provide a user-friendly interface for selecting the source and destination stations for their journey. This interface will be built using fundamental web development technologies:

- **HTML:** Defines the core structure and layout of the interface elements.
- **CSS:** Controls the visual presentation of the interface, ensuring a clear and aesthetically pleasing user experience.
- **JavaScript:** Enables dynamic behavior and interactivity within the interface. In this case, JavaScript might handle functionalities like user input validation and real-time updates.

**4. Core Functionality: Facial Recognition**

**OpenCV Integration:** The core functionality of GoCardless lies in its ability to recognize users accurately at the metro entry gate. This is achieved by integrating OpenCV, a powerful image processing library. OpenCV will be used to develop a facial recognition module responsible for:

- Analyzing live facial images captured by cameras at the entry gate.
- Extracting key facial features from the captured image.
- Comparing the extracted features against pre-registered facial data stored in the MySQL database for each user.

**5. Fare Deduction Process:**

**Seamless Fare Deduction:** Upon successful facial recognition, the system will automatically deduct the appropriate fare for the chosen journey from the user's account. This deduction will occur securely and only once per trip to ensure fairness and prevent duplicate charges.

**6. Security and Privacy Measures:**

**Protecting User Data:** The system will prioritize robust security measures to safeguard user data and financial transactions. This includes:

- Encryption of sensitive information such as facial images and account details.
- Secure communication protocols to protect data transmission between the entry gate and the server.
- Access control mechanisms to restrict unauthorized access to the system and user data.

**7. Performance Optimization:**

**Ensuring Efficiency:** To guarantee a smooth user experience, the system will be designed for optimal performance. This involves:

- Code optimization to ensure efficient processing of facial recognition and fare deduction tasks.
- Optimizing database queries to retrieve user data quickly from the MySQL database.
- System configuration adjustments to maximize throughput and handle a large number of users concurrently.

**8. Testing and Deployment:**

- **Rigorous Testing:** Before deployment, the developed system will undergo thorough testing to validate its functionality across various scenarios. This testing will assess:
  - Accuracy of facial recognition
  - Reliability of fare deduction process
  - Security measures and overall system stability
- **Deployment and Availability:** Once testing is complete, the system will be deployed on a suitable hosting environment. Cloud platforms are a strong consideration due to their scalability and ability to accommodate a large user base.

# 4. MODELLING & IMPLEMENTATION DETAILS

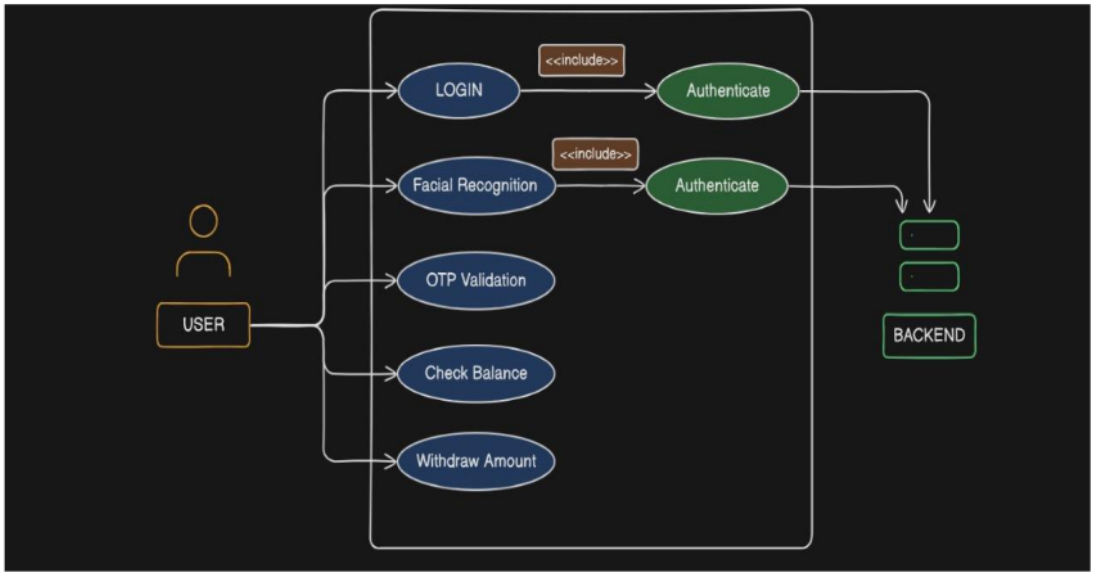


**Figure 4.1.1: Use Case Diagram**

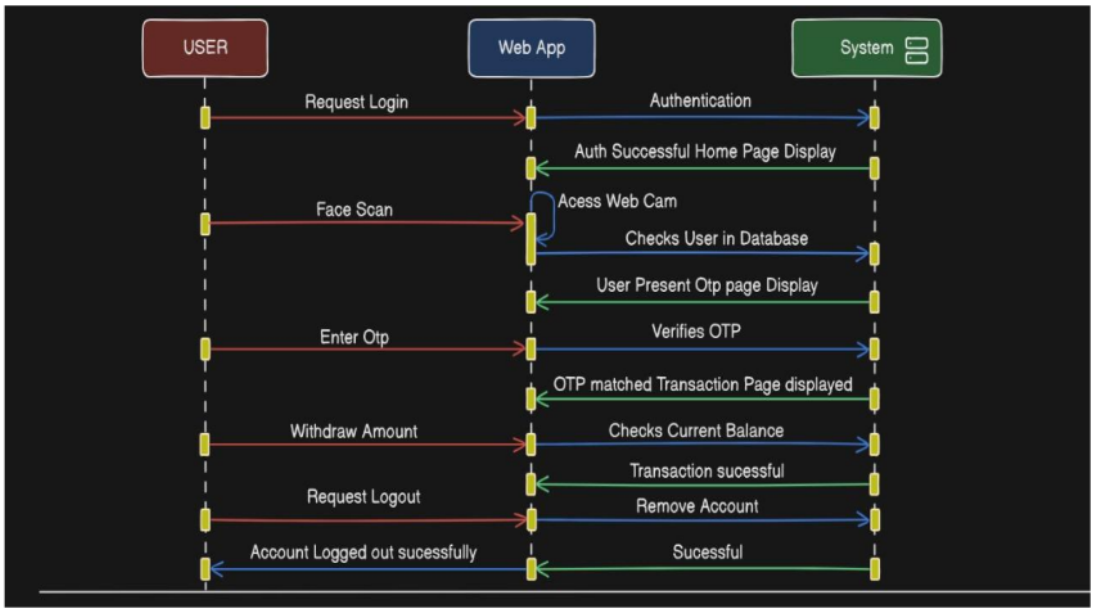


**Figure 4.1.2: Sequence Diagram**

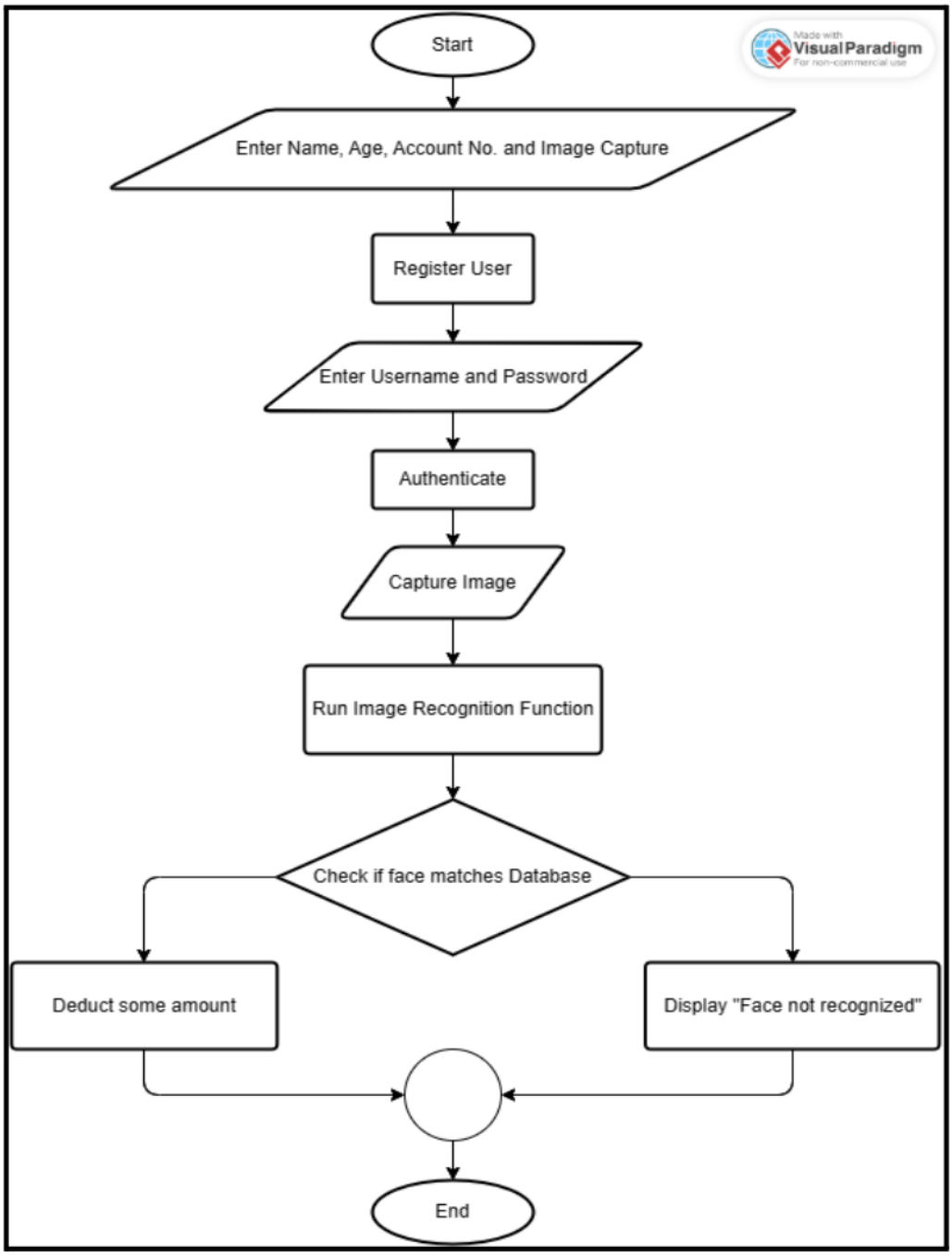


**Figure 4.1.3: Flow Chart Diagram**

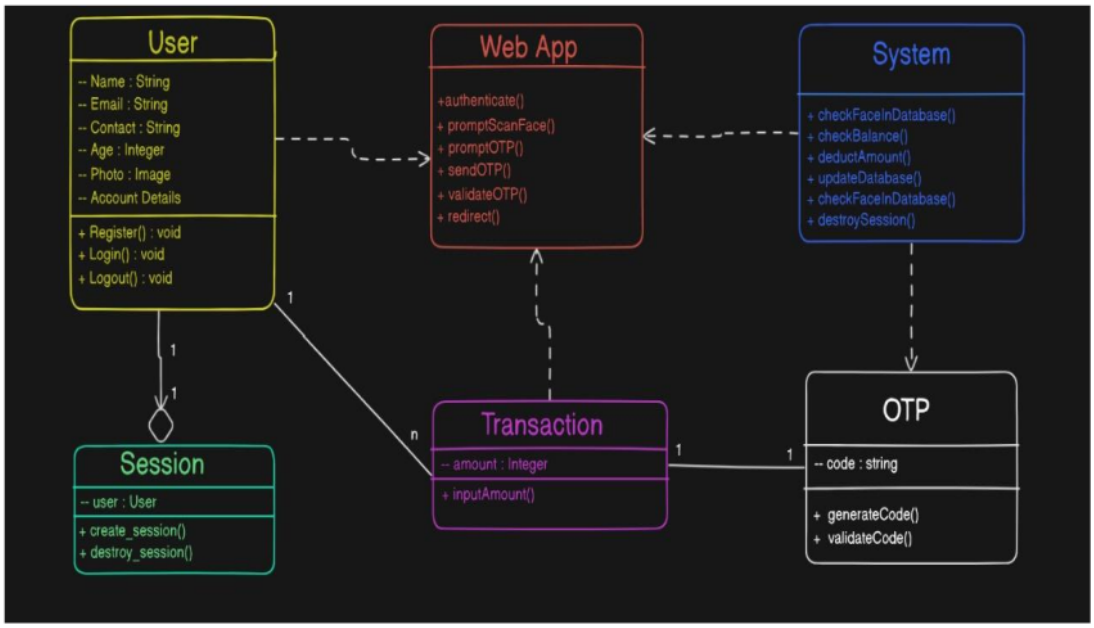


**Figure 4.1.4: Class Diagram**

## 4.2 Implementation Details and Issues

**Technology Stack:**

The Face-ATM system leans on a powerful combination of technologies to deliver a secure and user-friendly experience:

- **Django (Backend Development):** As the foundation for the system's backend, Django offers a robust and high-level Python framework. Django streamlines development by providing pre-built functionalities for common web application needs.
- **Python (Backend Programming Language):** Python serves as the primary programming language for the backend logic of the Face-ATM system.
- **OpenCV (Facial Recognition):** OpenCV, a free and open-source library, takes center stage for the crucial facial recognition tasks.

- **MySQL (Database Management):** The Face-ATM system utilizes MySQL, a well-established database management system, to securely store crucial data.

**User Interface:**

**1. Intuitive Design:**

- **Clear Navigation:** The interface will feature a clear and concise navigation structure. This might include prominent buttons or menus that guide users through the registration, login, and transaction processes. Icons can be strategically used alongside text labels for better user understanding, especially for users with limited experience using ATMs.
- **Simple Layouts:** Uncluttered layouts with ample white space will be employed to ensure information is presented clearly and avoids overwhelming users.
- **Visual Guides:** Consider incorporating visual cues or animations to guide users through the steps, especially during registration or when unfamiliar with a specific function.

**2. User Prompts and Feedback:**

- **Clear Instructions:** The interface will provide clear and concise instructions at each stage of user interaction. This can be achieved through on-screen text prompts or voice prompts for visually impaired users (if accessibility features are incorporated).
- **Real-time Feedback:** The system should provide real-time feedback to users during interactions. For example, visual cues like color changes or checkmarks can indicate successful actions, while error messages should be clear and informative, guiding users on how to resolve any issues.

**3. Responsive Design:**

- **Device Compatibility:** The user interface will be built using responsive design principles. This ensures the interface adapts and displays optimally across various devices, including desktops, tablets, and smartphones. This is crucial in today's world where users access services from a variety of devices.
- **Touch Optimization:** If the ATM utilizes a touchscreen interface, the buttons and menus will be sized and spaced appropriately for easy touch interaction.

**4. Security Considerations:**

- **Data Privacy:** The interface should minimize the display of sensitive information, such as account balances, on the screen. Only essential details relevant to the current transaction should be displayed.
- **Secure Input Fields:** Password or PIN entry fields should utilize secure masking techniques to prevent shoulder surfing (someone peeking at the user's input).

**Facial Recognition Module:**

**1. Leveraging OpenCV:**

- **Image Processing Powerhouse:** OpenCV, a renowned open-source library, serves as the foundation for the facial recognition module. OpenCV provides a rich set of tools for image processing, computer vision, and machine learning, perfectly suited for facial recognition tasks.

**2. Facial Detection and Recognition Techniques:**

- **Pre-trained Models:** The system may employ pre-trained deep learning models to streamline facial detection and recognition. Two prominent options are:
    - **Haar Cascades:** These pre-trained models are efficient for face detection, identifying facial features like eyes, nose, and mouth within an image or video frame.
    - **Deep Neural Networks (DNNs):** DNNs offer superior accuracy compared to Haar cascades, particularly in challenging scenarios like variations in lighting or facial expressions. They can handle both face detection and recognition in a single step.

**3. Facial Feature Extraction:**

- **Unique Identifiers:** Once a face is detected, the module utilizes OpenCV's capabilities to extract facial features. These features act as unique identifiers for each user and may include:

- Distance between eyes
- Shape of the jawline
- Prominence of cheekbones
- Other geometric properties of facial features

**4. Matching with Enrolled Data:**

- **Verification Process:** The extracted facial features (embeddings or descriptors) are then compared against pre-registered facial data stored securely in the system's database. This stored data likely includes facial embeddings generated from user-uploaded images during registration.
- **Accuracy and Security:** By comparing the extracted features with enrolled data, the system can determine if the user attempting the transaction is who they claim to be. This matching process is designed to be highly accurate to minimize the risk of unauthorized access.

**Additional Considerations:**

- **Liveness Detection:** To enhance security, the system may incorporate liveness detection techniques. These techniques can help distinguish between a real person and a photograph or video presentation, further safeguarding against fraudulent attempts.
- **Model Training and Optimization:** The chosen facial recognition model may require training on a large dataset of facial images to achieve optimal accuracy. This training process helps the model learn and recognize variations in human faces.

**OTP Generation and Verification:**

**1. Secure OTP Generation:**

- **Python Libraries:** The system leverages Python libraries like Django OTP to generate secure and unique OTPs for each transaction. These libraries employ robust algorithms to ensure randomness, making it nearly impossible to predict the next code.

**2. OTP Delivery Options:**

- **User Choice:** To cater to user preferences, the system will provide options for receiving OTPs. Users can choose between:
    - **Email:** The generated OTP will be sent to the user's registered email address. This method requires a stable internet connection on the user's device to receive the email promptly.
    - **SMS:** The OTP will be delivered via SMS to the user's registered phone number. This method is more widely accessible and doesn't rely on internet connectivity, but may incur carrier charges depending on the user's plan.

**3. OTP Verification Process:**

- **User Input:** Once the user receives the OTP via their chosen method, they will be prompted to enter the code on the ATM screen.
- **Code Validation:** The system will then validate the entered OTP against the code generated for that specific transaction. This validation process occurs securely within the system.

**4. Security Considerations:**

- **Short Lifespan:** OTPs are designed to have a very short lifespan, typically expiring within a minute or two of generation. This minimizes the window of opportunity for someone to intercept and misuse the code.
- **Limited Attempts:** The system may implement a limit on the number of incorrect OTP attempts allowed. This discourages brute-force attacks where someone repeatedly guesses the code. After exceeding the limit, the user's account may be locked, requiring additional security measures to regain access.

**Benefits of OTP Verification:**

- **Enhanced Security:** The additional layer of OTP verification significantly strengthens security by making unauthorized access to user accounts much more difficult. Even if someone manages to bypass facial recognition, they would still need the valid OTP to complete a transaction.
- **Peace of Mind:** The use of OTPs provides users with peace of mind, knowing that an extra layer of security protects their accounts.

## Issues:

**Security Concerns:**

**1. Facial Biometric Data:**

- **Data Sensitivity:** Facial recognition relies on sensitive biometric data. A data breach exposing this information could have serious consequences, potentially enabling identity theft or unauthorized access to other accounts.
- **Mitigations:**
    - **Encryption:** Store facial data in encrypted form within the database using robust encryption algorithms.
    - **Limited Access:** Implement strict access controls to restrict access to facial data only to authorized personnel who require it for system maintenance or troubleshooting.
    - **Data Minimization:** Consider storing only essential facial features (embeddings) extracted from images, rather than the entire image itself. This reduces the amount of sensitive data stored.
    - **User Control:** Provide users with options to control their facial data, such as the ability to request deletion or opt-out of facial recognition entirely.

**2. Transaction Information:**

- **Financial Data:** Transaction information, including account details and withdrawal amounts, is also highly sensitive.

- **Mitigations:**
    - **Secure Communication:** Utilize secure communication protocols (e.g., HTTPS) to encrypt all communication between the ATM and the server, safeguarding data transmission from eavesdropping.
    - **Tokenization:** Consider tokenizing sensitive data like account numbers. Tokens are random numbers that represent actual account details, reducing the risk of exposure even if a breach occurs.
    - **Regular Security Audits:** Conduct periodic security audits to identify and address potential vulnerabilities in the system.

**3. Unauthorized Access:**

- **System Hacking:** Malicious actors might attempt to gain unauthorized access to the system, potentially stealing user data or manipulating transaction information.
- **Mitigations:**
    - **Strong Authentication:** Implement strong authentication mechanisms for user login and system access, potentially using multi-factor authentication beyond just facial recognition.
    - **Regular Updates:** Keep the system software and libraries updated with the latest security patches to address known vulnerabilities.
    - **Intrusion Detection Systems:** Consider deploying intrusion detection systems to monitor network activity and identify suspicious attempts to access the system.

**4. Identity Spoofing:**

- **Presentation Attack:** A potential vulnerability exists if someone attempts to spoof a user's identity through methods like high-quality photographs or video recordings.
- **Mitigations:**
    - **Liveness Detection:** Incorporate liveness detection techniques within the facial recognition module to distinguish between a real person and a photograph or video presentation.

- **Multi-Factor Authentication:** As mentioned earlier, consider multi-factor authentication to add an extra layer of security beyond just facial recognition. This could involve OTP verification or security questions.

**5. Continuous Monitoring:**

- **Security Threats Evolve:** The landscape of cyber threats is constantly evolving.
- **Mitigations:**
  - **Security Team:** Establish a dedicated security team to monitor the system for suspicious activity and proactively address emerging threats.
  - **Incident Response Plan:** Develop a comprehensive incident response plan outlining procedures to follow in case of a security breach. This plan should include data recovery, user notification, and appropriate legal actions.

**Performance Optimization:**

**1. Facial Recognition Optimization:**

- **Real-Time Efficiency:** The facial recognition module needs to process live camera feeds efficiently to minimize delays during user identification. This optimizes user experience and avoids frustration.
  - **Algorithm Selection:** Consider using lightweight facial recognition algorithms designed for real-time processing on resource-constrained environments. These algorithms may offer a balance between accuracy and processing speed.
  - **Code Optimization:** Optimize the code implementing the facial recognition module. Techniques like code profiling can identify bottlenecks and areas for improvement.

**2. Handling Variations:**

- **Lighting and Angles:** Facial recognition should function reliably under varying lighting conditions and face angles.

- **Normalization Techniques:** Pre-process captured facial images to normalize factors like lighting and orientation. This can improve the accuracy of feature extraction and matching processes.
- **Liveness Detection Optimization:** If liveness detection is incorporated, ensure it operates efficiently without significantly impacting processing time.

**3. System-Level Optimizations:**

- **Caching Mechanisms:** Implement caching mechanisms to store frequently accessed data, such as pre-processed facial features from user profiles. This reduces the need for repetitive calculations and improves overall system response time.
- **Parallel Processing:** Explore opportunities for parallel processing, particularly if the underlying hardware supports it. This can involve distributing tasks across multiple cores or processors, speeding up computation-intensive processes like facial feature extraction.
- **Hardware Acceleration:** Consider leveraging hardware acceleration techniques, especially if the ATM hardware includes a dedicated Graphics Processing Unit (GPU). GPUs can excel at handling complex mathematical calculations involved in facial recognition algorithms, potentially leading to significant performance improvements.

**4. Monitoring and Performance Tuning:**

- **Performance Metrics:** Establish key performance indicators (KPIs) to track critical system metrics like processing time, recognition accuracy, and system responsiveness.
- **Continuous Monitoring:** Monitor these KPIs in real-time to identify performance bottlenecks or areas for further optimization.
- **Adaptive Tuning:** Based on monitoring results, the system can be fine-tuned to optimize performance under varying conditions, such as peak usage times.

**Scalability Challenges:**

**1. Increased User Traffic and Transactions:**

- **Challenge:** As the user base expands and transaction volume increases, the system may experience performance issues like slow processing times or even downtime.

- **Solution:** Horizontal scaling offers a robust approach to address this challenge. This involves adding more servers to distribute the workload across multiple machines. By distributing tasks like facial recognition processing and database queries, the system can handle increased traffic more efficiently.

**2. Load Balancing:**

- **Challenge:** Even with horizontal scaling, uneven distribution of user requests across servers can create bottlenecks.
- **Solution:** Load balancing techniques can distribute incoming user requests and transaction processes evenly across available servers. This optimizes resource utilization and ensures smooth performance for all users.

**3. Database Scalability:**

- **Challenge:** The MySQL database, essential for storing user data and transaction records, may struggle to handle a growing amount of data.
- **Solution:** Database sharding involves dividing the database into smaller, self-contained partitions. Each shard stores a specific portion of the data, distributing the load and improving query performance. Additionally, migrating to a NoSQL database specifically designed for high scalability might be considered for future enhancements.

**4. Monitoring and Performance Management:**

- **Challenge:** As the system scales, proactively identifying and addressing performance bottlenecks becomes even more critical.
- **Solution:** Implementing a robust monitoring system to track key metrics like server load, database response times, and transaction processing times is vital. With this data, performance bottlenecks can be identified and addressed through adjustments to resource allocation or further scaling initiatives.

**5. Continuous System Improvement:**

- **Challenge:** Scalability is an ongoing process, requiring constant evaluation and adaptation.
- **Solution:** The development team should continuously evaluate the system's performance and identify areas for improvement. This may involve exploring new technologies, optimizing existing code, or implementing advanced caching mechanisms.

## 4.2 Implementation Details and Issues

### *4.2.1 Registration Process:*

**Username:** Users initiate the registration process by providing a unique username of their choice. This username will be used to access Face-ATM services in the future.

**Personal Information:**

**a. First Name:** Users input their first name.

**b. Last Name:** Users input their last name.

**c. Contact:** Users provide their contact number for communication purposes.

**d. Email:** Users enter their email address for account-related notifications.

**Password:** A secure password is chosen by the user to protect their Face-ATM account from unauthorized access.

**Upload Photograph:** Users are required to upload a recent photograph of themselves. This photograph serves as the basis for facial recognition during authentication.

**Bank Account Details:**

**a. Bank Account Number:** Users input their bank account number associated with their bank.

**b. Bank Name:** Users specify the bank name they are affiliated with.


**Figure 4.2.1.1:** Register Page - User Details


**Figure 4.2.1.2:** Register Page - User Details

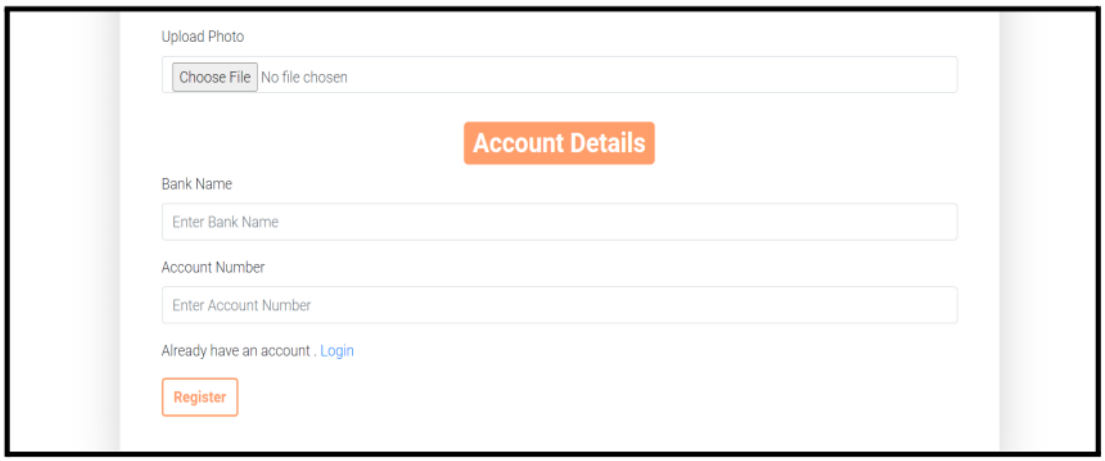


**Figure 4.2.1.3:** Register Page - Account Details

### *4.2.2. Login and Authentication Process:*

**Email and Password Authentication:**

**a. Email:** Users enter the email address associated with their Face-ATM account.

**b. Password:** Users input their secure password chosen during registration.

**Authentication:**

Upon submission of email and password, Face-ATM verifies the credentials against the stored data in its database. If the provided credentials match, authentication is successful.

**Session Creation:**

Upon successful authentication, a session is created for the user. This session allows the user to access Face-ATM services without the need for repeated authentication during the session duration.

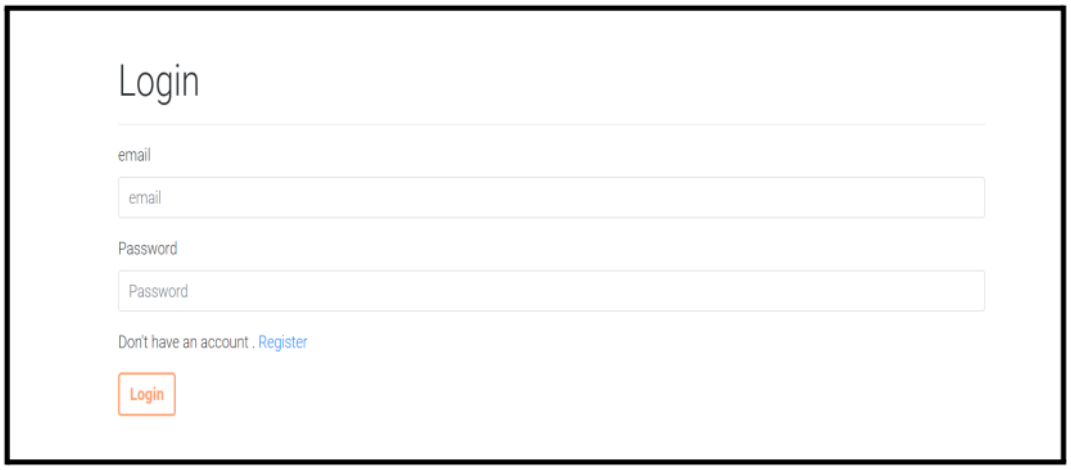


**Figure 4.2.2.1:** Login Page - Authentication

### *4.2.3 Face Scan Process:*

**Home Page Display:**

Upon login, users are directed to the Home page where their personal information, such as name and account details, are prominently displayed for easy reference.

**Initiation of Withdrawal:**

Users navigate to the withdrawal section and click on the "Withdraw" button to initiate a withdrawal request.

**Face Scan:**

Upon clicking the "Withdraw" button, the system prompts the user to allow access to the camera. Once permission is granted, the camera interface pops up, and the user's face is scanned.

**Facial Recognition:**

The scanned facial image is processed by the Face-ATM system to extract facial features and generate facial encodings. These encodings are compared against the database of registered users to verify the user's identity.

**User Verification:**

If the user's facial features match those stored in the database, the system proceeds to the next step. Otherwise, an error message is displayed indicating that the user was not found in the database.

**OTP Page:**

Upon successful facial recognition and user verification, the system directs the user to the One-Time Password (OTP) page to proceed with the withdrawal transaction. An OTP is generated and sent to the user's registered mobile number or email address for additional security.

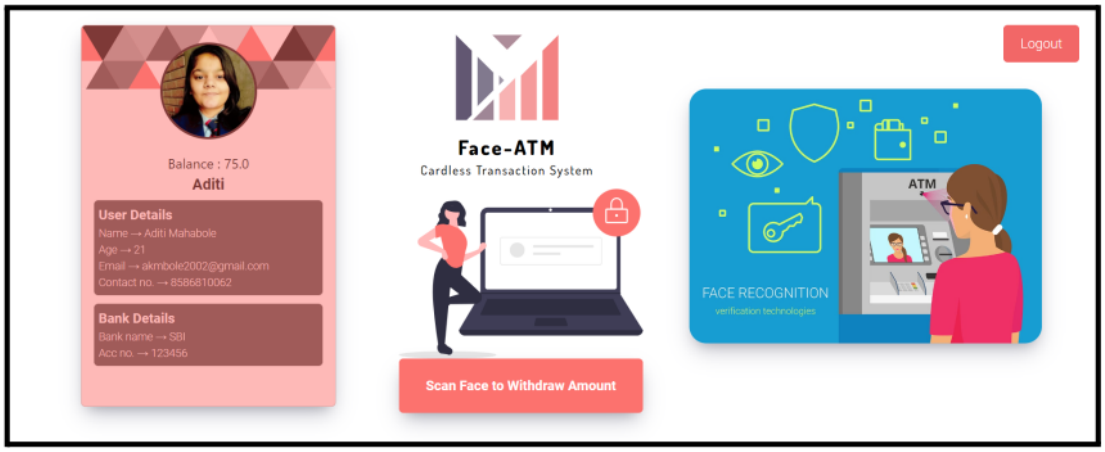


**Figure 4.2.3.1:** Home Page

***4.2.4 OTP Verification and Transaction Process:***

**OTP Page:**

Upon successful facial recognition, users are directed to the OTP page where they are prompted to verify their identity using a One-Time Password (OTP).

**OTP Generation Options:**

**Users are presented with two options for receiving the OTP:**

**a. Get OTP by Email:** Users click on this option to receive the OTP via email.

**b. Get OTP by Phone:** Users select this option to receive the OTP via SMS on their registered phone number.

**OTP Generation and Delivery:**

Depending on the selected option, the OTP is generated and delivered to the user's preferred communication channel (email or phone) securely.

**OTP Input:** Users input the received OTP into the designated input field on the OTP page.

**OTP Verification:**

The entered OTP value is compared against the OTP generated and sent to the user. If the entered OTP matches the generated OTP, verification is successful. Otherwise, an alert is triggered indicating "Invalid OTP."

**Transaction Page Access:**

Upon successful OTP verification, users are granted access to the transaction page, where they can proceed with their desired transaction securely.

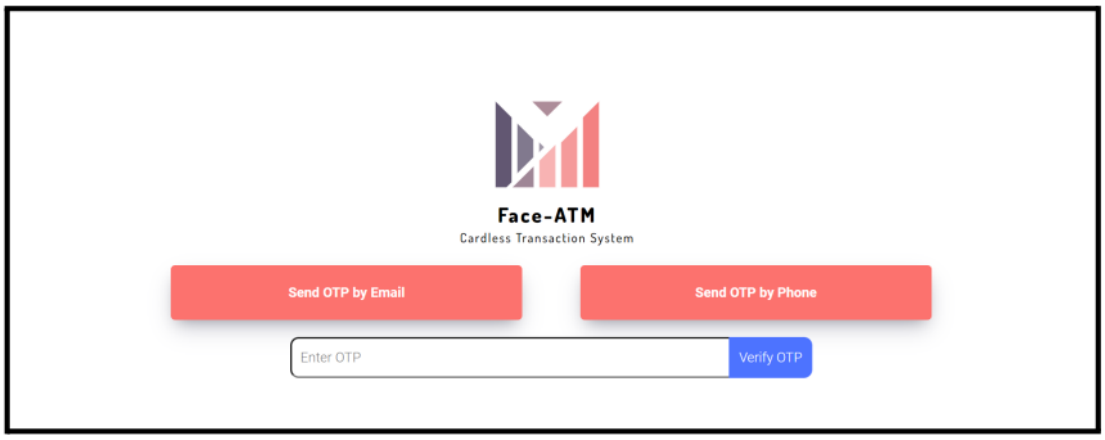


**Figure 4.2.4.1:** Otp Page

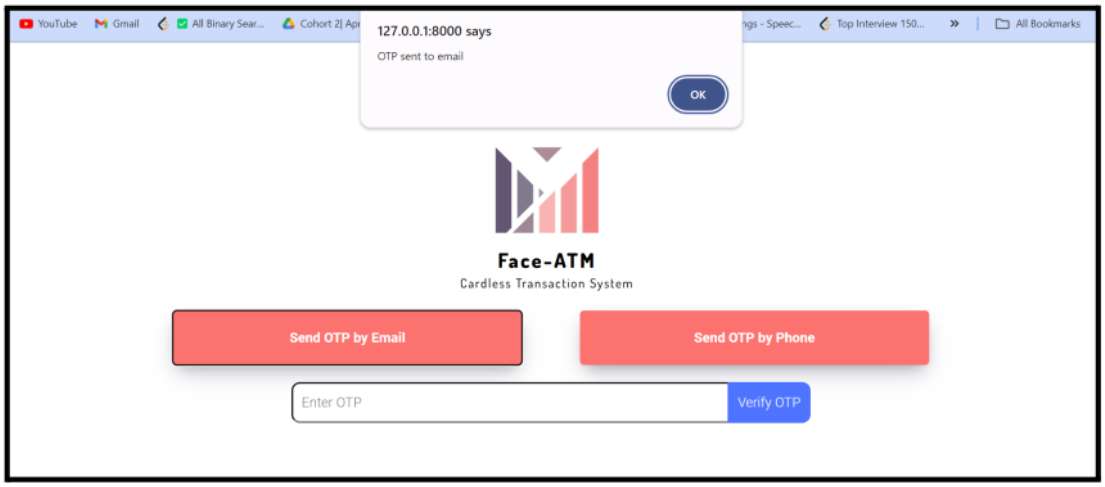


**Figure 4.2.4.2:** Otp Page - OTP sent Successfully

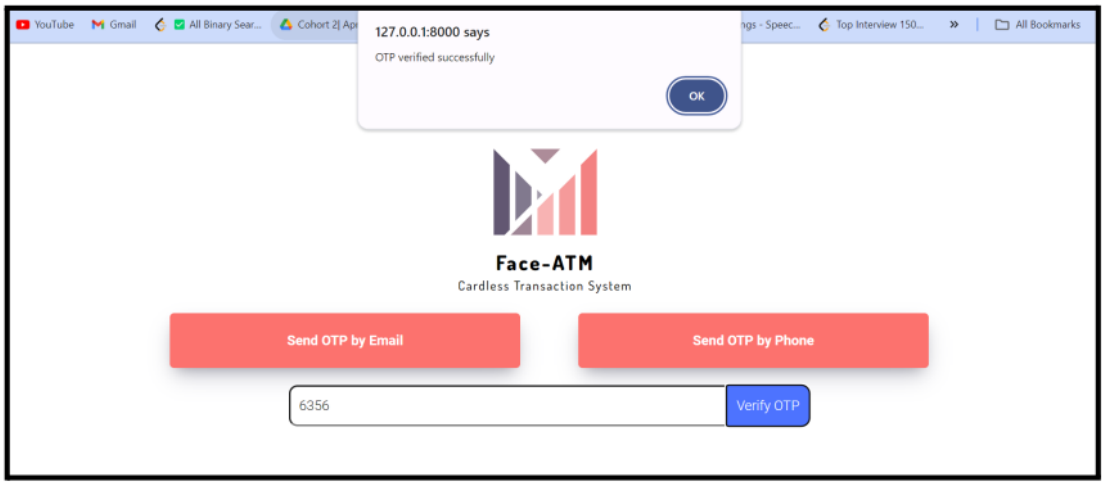


**Figure 4.2.4.3:** Otp Page - OTP Verification

### *4.2.5 Transaction Process:*

**Transaction Page:**

Upon OTP verification, users are redirected to the transaction page where they can input the amount they wish to withdraw.

**Amount Input:**

Users input the desired withdrawal amount into the designated field on the transaction page.

**Balance Validation:**The entered withdrawal amount is compared against the user's current account balance retrieved from the database. If the withdrawal amount exceeds the available balance, an alert is triggered, indicating "Amount exceeds the current balance. Please enter a lower amount."

**Database Update:**If the entered withdrawal amount is within the available balance, the transaction is processed. The deducted amount is subtracted from the user's account balance in the database.

**Transaction Success:**Upon successful deduction of the withdrawal amount from the database, users are redirected to the Home page.

**Personal Info Update:**On the Home page, users' personal information, including their account balance, is updated to reflect the deducted amount.

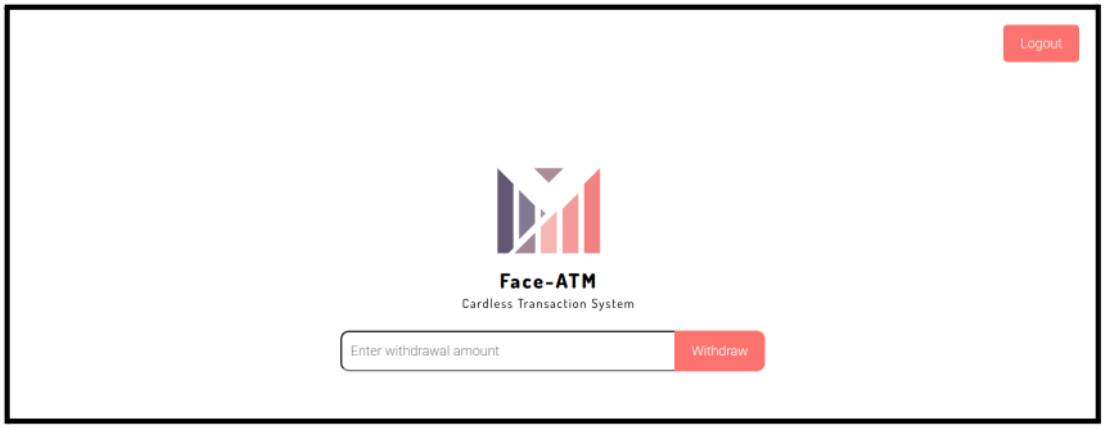


**Figure 4.2.5.1:** Transaction Page

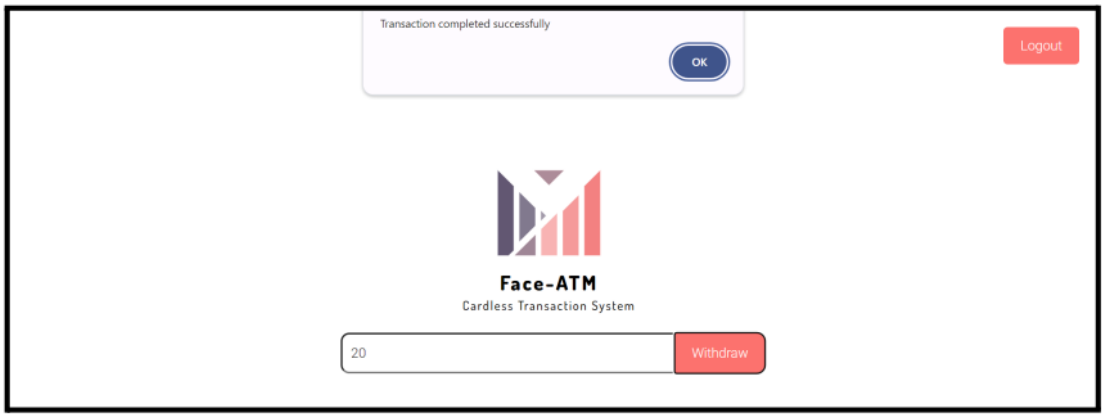


**Figure 4.2.5.2:** Transaction Page - Successful Transaction

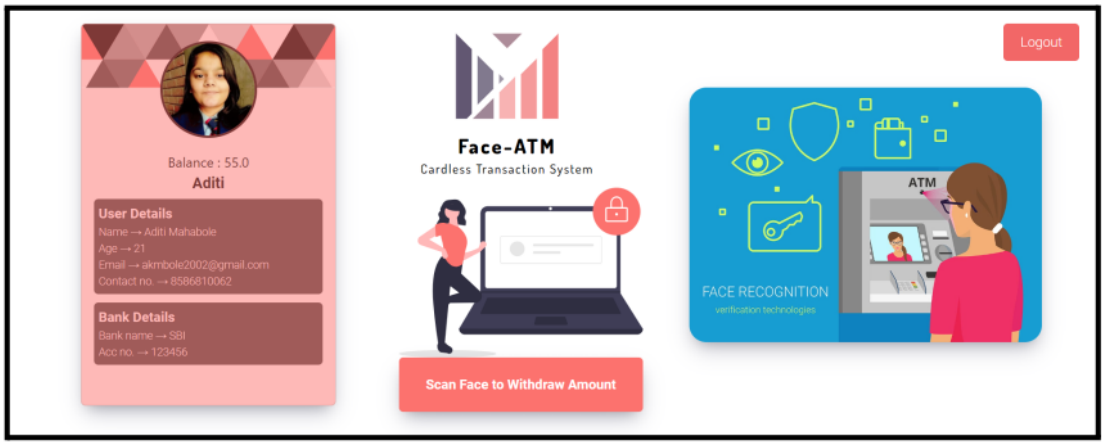


**Figure 4.2.5.3:** Transaction Page - Updated Balance Display on Home Page

### *4.2.6 Logout*

**Upon clicking the Logout button:**

- User session is terminated.
- User is redirected to the Login page.

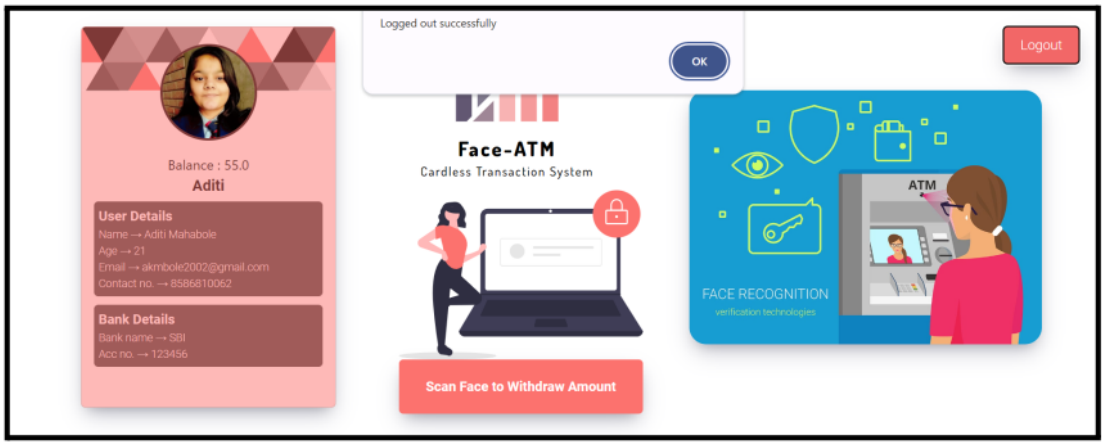


**Figure 4.2.6.1:** Logout

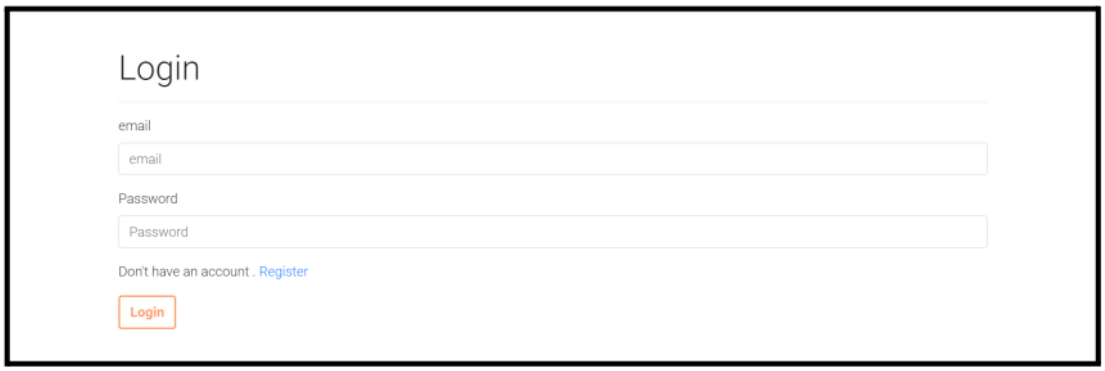


**Figure 4.2.6.2:** Logout - Redirected to Login Page

### 4.3 Risk Analysis and Mitigation

| Category | Risk Description | Impact | Mitigation Strategy |
|---|---|---|---|
| Facial Recognition | Inaccurate facial recognition due to poor lighting, facial variations, or obstructions. | High | - Implement robust facial recognition algorithms trained on diverse datasets. - Enhance lighting conditions around the ATM camera. - Integrate liveness detection to prevent spoofing with photographs. |
| Security | Data breaches exposing user facial data or financial information. | High | - Implement robust encryption for storing and transmitting facial data. - Employ multi-factor authentication for user access. - Conduct regular security audits and penetration testing. - Adhere to data privacy regulations (GDPR, CCPA etc.). |
| System Performance | Slow response times or system outages during peak usage periods. | High | - Conduct performance testing under varying load conditions. - Optimize system architecture for scalability. - Implement monitoring tools to identify and address performance bottlenecks. - Utilize cloud-based infrastructure for elastic scalability. |
| Usability | Unintuitive user interface leading to user frustration and errors. | Medium | - Conduct usability testing with a diverse user group. - Design a user-friendly interface with clear instructions and feedback mechanisms. - Offer multiple language options for wider accessibility. |
| Integration | Challenges integrating with existing banking systems and networks. | Medium | - Collaborate closely with banking partners to ensure smooth API integration. - Develop and test integration procedures thoroughly. - Establish clear communication channels with banking partners for ongoing support. |
| User Adoption | Low user acceptance due to concerns about security, privacy, or unfamiliar technology. | Medium | - Conduct public awareness campaigns to educate users about the benefits and security measures of Face-ATM technology. - Partner with financial institutions to promote Face-ATMs to their customers. - Offer opt-in options for facial recognition, allowing users to choose their preferred authentication method. |

# 5. TESTING

## 5.1 Testing Plan

| Test Case | Test Case Description | Test Steps | Expected Results | Actual Result | Status |
|---|---|---|---|---|---|
| TC_001 | User Registration | 1. Navigate to the registration page.<br>2. Enter valid user details.<br>3. Click on the 'Register' button. | User is successfully registered and redirected to the login page. | Same as expected. | Pass |
| TC_002 | User Login | 1. Navigate to the login page.<br>2. Enter valid credentials.<br>3. Click on the 'Login' button. | User is successfully logged in and redirected to the dashboard. | Same as expected. | Pass |
| TC_003 | Incorrect Login Attempt | 1. Navigate to the login page.<br>2. Enter invalid credentials.<br>3. Click on the 'Login' button. | User sees an error message, and login is not successful. | Same as expected. | Pass |
| TC_004 | Facial Recognition | 1.Navigate to Home Page<br>2.Clicked on Face scan button<br>3.Camera Popup<br>4.Face checked in Database. | User navigates to the otp page if identified correctly,else the user gets an error user not present. | Same as expected | Pass |
| TC_005 | Get OTP on Email | 1.Navigate to the OTP page.<br>2.Clicked on OTP by email button | If user's email is validated then OTP sent to email, else alert pops up "Not able | Same as expected | Pass |

| | | | | | |
|---|---|---|---|---|---|
| | | | to send OTP” | | |
| TC_006 | Get OTP on phone number | 1.Navigate to the OTP page.<br>2.Clicked on OTP by phone number button. | If user’s phone number l is validated then OTP sent to phone, else alert pops up “Not able to send OTP” | OTP is not sent. | Fail |
| TC_007 | OTP Verification Successful | 1.User enters OTP.<br>2.Click on submit. | If entered OTP matches then user directed to transaction page | Same as expected | Pass |
| TC_008 | OTP Verification Failed | 1.User enters OTP.<br>2.Click on submit. | OTP does not match , user gets alert pop up saying OTP does not match | Same as expected | Pass |
| TC_009 | Transaction Amount Withdrawl | 1.Navigate to the Transaction page.<br>2.Enter amount to withdraw.<br>3.Click withdraw button | Deduct amount from balance.<br>Update database.<br>Display updated balance on profile. | Same as expected | Pass |
| TC_0010 | Exceeding Current Balance | 1.Navigate to the Transaction page.<br>2.Enter amount to withdraw.<br>3.Click the withdrawal button. | Alert message pops up saying the amount exceeds the current balance. | Same as expected | Pass |

## 5.2 Limitation of Solution

**5.2.1. Dependency on Technology**: The effectiveness of facial recognition and OTP verification relies heavily on the reliability and availability of technology infrastructure. Any disruptions or technical issues could potentially hinder user access to banking services.

**5.2.2. Security Concerns:** While facial recognition technology enhances security, it is not foolproof and may still be susceptible to spoofing or manipulation. Additionally, the reliance on digital communication channels for OTP delivery introduces potential security risks such as interception or phishing attacks.

**5.2.3. Accessibility Challenges:** The reliance on facial recognition may pose accessibility challenges for users with certain physical disabilities or conditions that affect facial recognition. Ensuring inclusivity and accessibility for all users is essential but may require additional measures or alternatives.

**5.2.4. Adoption Barriers:** Introducing a new authentication method and eliminating physical ATM cards may face resistance from users accustomed to traditional banking practices. Overcoming user resistance and ensuring widespread adoption of the new system may require effective communication and user education efforts.

**5.2.5. Regulatory Compliance:** The implementation of facial recognition technology and the handling of sensitive user data raise privacy and regulatory compliance concerns. Ensuring compliance with data protection regulations and addressing privacy concerns are essential for maintaining user trust and regulatory compliance.

**5.2.6. Technical Complexity:** Integrating multiple technologies and communication channels, such as facial recognition, OTP delivery via email and phone, and database management, introduces technical complexity and potential points of failure. Ensuring seamless integration, interoperability, and system reliability require careful planning and ongoing maintenance efforts.

# 6. CONCLUSION AND FUTURE WORK

## 6.1 Conclusion

In conclusion, the Face ATM project represents a significant leap forward in banking technology, offering users a secure, convenient, and innovative way to access and manage their finances. By seamlessly integrating facial recognition technology, OTP verification, and modern communication channels, this application enhances security while improving the overall user experience. Through the elimination of physical ATM cards and the adoption of advanced authentication methods, the project sets a new standard for banking systems, paving the way for future innovations in the industry. With its emphasis on security, convenience, and user-centric design, the Face ATM project marks a significant milestone in the evolution of banking technology.

## 6.2 Future Work

### 6.2.1 Enhanced Facial Recognition Accuracy:

While the Face-ATM system offers a glimpse into the future of cardless transactions, there's always room for improvement. Here's a closer look at potential areas to enhance facial recognition accuracy:

- **Algorithm Research and Development:**

  - **Tailored Algorithms:** Current facial recognition algorithms might not be specifically optimized for ATM environments. Investing in research and development of custom algorithms can significantly improve accuracy in these specific conditions. This could involve training models on datasets that include variations typically encountered at ATMs, such as different lighting scenarios,

face angles due to ATM kiosk heights, and potential obstructions like glasses or hats.

- **Addressing Environmental Challenges:**

  - **Low-light conditions:** ATMs may be located in areas with less-than-ideal lighting. Upgrading camera hardware and incorporating algorithms adept at handling low-light situations can ensure consistent performance.
  - **Facial Variations:** People come in all shapes and sizes, and facial recognition should account for these variations. Refining algorithms to handle diverse facial features, expressions, and orientations will enhance accuracy and prevent false negatives (failing to recognize a legitimate user).

- **Machine Learning for Continuous Improvement:**

  - **Real-world Data Integration:** Machine learning offers powerful tools for refining facial recognition models over time. By incorporating real-world usage data into the training process, the system can continuously learn and adapt to variations encountered during everyday operation. This can involve user interactions, successful and failed recognition attempts, and environmental conditions.
  - **Active Learning:** Explore active learning techniques where the system can query users for additional information or clarifications in ambiguous cases. This user interaction can further improve the model's ability to handle challenging scenarios.

- **Security and Privacy Considerations:**

  - **Bias Mitigation:** Machine learning models can inherit biases from the data they are trained on. It's crucial to ensure the training data is diverse and representative of the target user population to prevent biased recognition outcomes.
  - **Explainability:** As machine learning models become more complex, interpretability becomes a challenge. Future efforts should focus on developing

techniques that explain the rationale behind the model's recognition decisions. This can enhance user trust and transparency.

### 6.2.2 Biometric Data Privacy and Security:

Facial recognition offers undeniable convenience for cardless ATM transactions, but user concerns regarding biometric data privacy and security are paramount. Here's a roadmap for addressing these concerns in future iterations of the Face-ATM system:

- **Enhancing Data Security:**
  - **Robust Encryption:** Implement state-of-the-art encryption algorithms to safeguard stored facial images. This ensures that even in the event of a data breach, the stolen data would be unusable without the decryption key. Regularly update encryption methods to stay ahead of evolving threats.
  - **Data Minimization:** Explore storing only essential facial features (embeddings) extracted from user images, rather than the entire image itself. This reduces the amount of sensitive biometric data stored, minimizing potential privacy risks.
  - **Secure Enclaves:** Consider leveraging secure enclave technology, which creates a hardware-protected environment within a computing system specifically for storing and processing sensitive biometric data. This adds an extra layer of security for facial recognition tasks.
- **User Control and Transparency:**
  - **Opt-in/Opt-out Mechanisms:** Provide users with clear and easy-to-understand options to opt-in or opt-out of facial recognition for ATM transactions. Respecting user choice is crucial for building trust and ensuring user autonomy over their biometric data.
  - **Data Access and Deletion Rights:** Grant users the right to access their stored facial recognition data upon request. Additionally, explore offering users the ability to request deletion of their biometric data, subject to legal and regulatory considerations.

- **Transparency in Data Usage:** Clearly communicate how user data is collected, used, and stored within the system. This transparency fosters trust and empowers users to make informed decisions about their data privacy.

❖ **Compliance with Regulations:**

- **Global Data Privacy Landscape:** Data privacy regulations are evolving rapidly around the world. The Face-ATM system should be designed to comply with relevant regulations, such as GDPR (General Data Protection Regulation) in the European Union, CCPA (California Consumer Privacy Act), and any emerging regulations in the user's specific jurisdiction. Compliance ensures user data is handled responsibly and adheres to established data protection principles.
- **Data Protection Impact Assessments:** Conduct regular Data Protection Impact Assessments (DPIAs) to evaluate the potential privacy risks associated with collecting and processing facial recognition data. These assessments help identify and mitigate risks proactively.

❖ **Privacy-Enhancing Technologies:**

- **Homomorphic Encryption:** Explore the potential of homomorphic encryption techniques. This allows computations to be performed on encrypted data without decryption, enabling facial recognition tasks without revealing the underlying facial image data itself.
- **Differential Privacy:** Investigate incorporating differential privacy mechanisms that add controlled noise to data to enhance user privacy while preserving the accuracy of facial recognition results.

### 6.2.3 Integration with Mobile Applications:

❖ The Face-ATM system offers a glimpse into the future of secure and convenient ATM transactions. However, its potential can be further amplified by integrating with mobile applications. Here's a breakdown of how mobile apps can enhance the Face-ATM experience:

- **Native Mobile Applications:**

  - **Platform Compatibility:** Develop native mobile applications for both iOS and Android platforms. This ensures optimal user experience and leverages the unique features and functionalities of each operating system.

- **Seamless User Journey:**

  - **Registration and Onboarding:** The mobile app can streamline user registration for the Face-ATM system. Users can securely enter their details, upload facial images for recognition, and link their bank accounts directly within the app.
  - **ATM Transaction Management:** The app can act as a digital hub for managing ATM transactions. Users can initiate withdrawals directly from their phones, leveraging facial recognition for authentication at the ATM itself. The app can display withdrawal prompts and confirmation messages for a secure and user-friendly experience.
  - **Transaction History and Notifications:** The app can provide users with a clear overview of their transaction history, including dates, amounts, and ATM locations. Additionally, push notifications can be sent for successful transactions or any suspicious activity detected in the account.

- **Additional Features for Convenience:**

  - **ATM Locator:** Integrate a map-based ATM locator within the app to help users find nearby Face-ATM enabled machines. This can be particularly helpful when traveling or unfamiliar with a location.
  - **Account Management Tools:** Consider incorporating basic account management functionalities within the app. This might include features like viewing account balances, transferring funds between accounts (subject to bank regulations), or managing debit card settings.

- **Security Considerations:**

- **Secure Communication:** Ensure all communication between the mobile app, the Face-ATM system, and the bank's servers is encrypted using secure protocols like HTTPS. This safeguards sensitive user data during transmission.
- **Multi-Factor Authentication:** Implement multi-factor authentication within the mobile app, potentially requiring a combination of facial recognition, PINs, or one-time passwords for added security.
- **Biometric Authentication on Mobile Devices:** Leverage built-in biometric authentication features on smartphones, such as fingerprint scanners or facial recognition, for secure login and transaction authorization within the app.
- **Expansion of Payment Options:** Face-ATM system offers a secure and convenient way to withdraw cash using facial recognition. However, its potential can be further enhanced by integrating additional payment options, catering to a wider range of user preferences and evolving financial landscapes. Here's a look at how Face-ATMs can expand their reach:

❖ **Beyond Traditional Bank Accounts:**

- **Alternative Payment Methods:** Explore integrating alternative payment methods beyond traditional bank accounts. This could include options like prepaid cards, digital wallets, or even loyalty programs that allow users to access funds or redeem points for cash withdrawals at Face-ATMs.

❖ **Contactless Payments:**

- **NFC Integration:** Leverage Near Field Communication (NFC) technology to enable contactless payments at Face-ATMs. Users with NFC-enabled smartphones or wearable devices could simply tap their device against a designated reader at the ATM to initiate a withdrawal transaction, eliminating the need to insert a debit card.
- **Security Considerations:** Ensure secure communication protocols are implemented for NFC transactions to protect user data during the interaction between the device and the ATM.

- **Collaboration and Partnerships:**

  - **Payment Service Providers (PSPs):** Collaborate with established payment service providers (PSPs) to facilitate seamless integration of their payment solutions with the Face-ATM system. PSPs can provide the necessary infrastructure and expertise to handle various payment methods securely and efficiently.
  - **Financial Institutions:** Partner with financial institutions to encourage them to offer their customers the ability to use Face-ATMs with various account types or alternative payment options. This collaboration can expand the user base and drive adoption of the Face-ATM technology.

- **Addressing Challenges:**

  - **ATM Infrastructure Compatibility:** Ensure that the integration of new payment options is compatible with existing ATM hardware and software infrastructure. This might involve minimal upgrades or modifications to existing ATMs to enable them to handle contactless payments or communicate with alternative payment networks.
  - **Regulatory Compliance:** Navigate any regulatory hurdles that might exist for specific payment methods in different geographical locations. Collaborating with relevant regulatory bodies and financial institutions can help ensure compliance and smooth operation.

### 6.2.4 Integration with Banking Systems:

The current Face-ATM system offers secure and convenient cash withdrawals using facial recognition. To unlock its full potential, consider integrating it with banking systems and networks. This integration would enable a wider range of transactions directly at the ATM, improving user experience and streamlining financial interactions.

### 6.2.5 Benefits of Integration:

- **Expanded Functionality:** Users can perform balance inquiries, transfer funds between accounts (subject to bank regulations), and even pay bills directly at the ATM using the Face-ATM interface. This eliminates the need for separate visits to banks or online transactions, saving users time and effort.
- **Real-Time Processing:** Transactions will be processed in real-time, providing users with immediate confirmation and account updates. This enhances transparency and eliminates delays associated with traditional batch processing.
- **Improved Security:** Integration can leverage existing robust security measures within banking systems. This strengthens overall transaction security and reduces the risk of fraud.

### 6.2.6 Key Considerations for Integration:

- **API Implementation:** Secure and standardized APIs (Application Programming Interfaces) are crucial for seamless communication between the Face-ATM system and various banking systems. These APIs will enable data exchange and transaction processing.
- **Real-Time Connectivity:** Establish real-time connections between Face-ATMs and banking networks to ensure immediate account updates and transaction validations.
- **Data Security Standards:** Adhere to industry-standard data security protocols like PCI DSS (Payment Card Industry Data Security Standard) to safeguard sensitive user information during transactions. Encryption of all data transmission is critical.
- **Collaboration with Banking Partners:** Active collaboration with banking partners is essential. Banks can provide access to their APIs, ensure compatibility with their systems, and define clear guidelines for data exchange and transaction processing.

### 6.2.7 Technical Aspects of Integration:

- **Account Verification:** The Face-ATM system will need to securely transmit user credentials to the banking system for verification. This can be achieved using secure tokenization methods to avoid transmitting sensitive data like account numbers.

- **Transaction Processing:** Once a user's account is verified, the Face-ATM system can initiate various transactions like withdrawals, transfers, or bill payments. The banking system will process the transaction and send confirmation back to the ATM.
- **User Interface Design:** The ATM interface needs to be redesigned to accommodate new functionalities like balance inquiries, fund transfers, and bill payments. The design should be intuitive and user-friendly to ensure a smooth experience.

### 6.2.8 Future Advancements:

- **Cash Deposit Functionality:** Explore enabling cash deposits at Face-ATMs, further expanding their service offerings.
- **Multilingual Support:** Integrate multilingual support within the ATM interface to cater to a wider user base.
- **Biometric Integration beyond Facial Recognition:** Consider incorporating additional biometric authentication methods like fingerprint scanners for enhanced security and user convenience.

# 7. REFERENCES

[1] Mohite, A., Gamare, S., More, K., & Patil, N. (2019). "Deep learning based card-less ATM using fingerprint and face recognition techniques," *International Research Journal of Engineering and Technology (IRJET)*, 6(03). Available: https://www.irjmets.com/uploadedfiles/paper//issue_6_june_2023/42041/final/fin_irjmets1686708662.pdf

[2] Prasad, S. (2020) *Python for image recognition - opencv*. Available at: https://www.topcoder.com/thrive/articles/python-for-image-recognition-opencv (Accessed: 20 January 2024).

[3] Alzubaidi, L., Zhang, J., Humaidi, A.J. et al. "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," *J Big Data* 8, 53 (2021). Available: https://doi.org/10.1186/s40537-021-00444-8

# 20103023_FACE-ATM:Cardless Transaction System

ORIGINALITY REPORT

| 7% | 6% | 1% | 3% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | www.coursehero.com<br>Internet Source | 2% |
| 2 | fastercapital.com<br>Internet Source | 1% |
| 3 | pub.nkumbauniversity.ac.ug<br>Internet Source | 1% |
| 4 | www.ijraset.com<br>Internet Source | <1% |
| 5 | pt.slideshare.net<br>Internet Source | <1% |
| 6 | Submitted to University of Wales Institute, Cardiff<br>Student Paper | <1% |
| 7 | Submitted to University of Greenwich<br>Student Paper | <1% |
| 8 | Submitted to University of Portsmouth<br>Student Paper | <1% |
| 9 | dspace.daffodilvarsity.edu.bd:8080<br>Internet Source | <1% |

| | | |
|---|---|---|
| 10 | Submitted to University of New South Wales<br>Student Paper | <1 % |
| 11 | de.slideshare.net<br>Internet Source | <1 % |
| 12 | www.irjmets.com<br>Internet Source | <1 % |
| 13 | Submitted to Kingston University<br>Student Paper | <1 % |
| 14 | Submitted to University of Leicester<br>Student Paper | <1 % |
| 15 | Submitted to University of Northampton<br>Student Paper | <1 % |
| 16 | Priya P, Jeeva R, Pradeep M M, Kishor S. "An Effective Cardless Atm Transaction Using Computer Vision Techniques", 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), 2023<br>Publication | <1 % |
| 17 | Submitted to Brunel University<br>Student Paper | <1 % |
| 18 | Kirti Jain, Atishay Jain, Aditya Bharadwaj, Ram Vashisth. "chapter 3 Software Engineering Strategies for Real-Time Personalization in E-Commerce Recommendations", IGI Global, 2024 | <1 % |

| | Publication | |
|---|---|---|
| 19 | www.template.net<br>Internet Source | <1% |
| 20 | Submitted to Middlesex University<br>Student Paper | <1% |
| 21 | www.mdpi.com<br>Internet Source | <1% |

| | | | |
|---|---|---|---|
| Exclude quotes | On | Exclude matches | < 14 words |
| Exclude bibliography | On | | |