# ATM Bank Management System With Facial Recognition And Multilingual Voice Recognition

Abdul Aziz Kalsekar

3142831

Preetha V K

July 2024

Word count – 17,520

Dissertation submitted in partial fulfilment for the degree of

Bachelor of Science with Honours Software Engineering

Computing Science and Mathematics

University of Stirling

## Abstract

As for the ATM security, the classical form of user authentication through the PIN remains the primary object of interest for various threats, from the classic skimming and phishing to more complex cybercrimes. Thus, as these threats and their combinations develop and become more sophisticated, the need for more robust and sophisticated solutions to combat fraud, embezzlement, and other types of criminal activities related to ATMs increases. This project focuses on implementing facial recognition to ATM systems to improve the ATM security that was previously based on user's pin code entry. Also, it has Multilingual Voice Command Recognition to ease the operations of an ATM particularly to the disabled with no language barriers.

The objective of this project is to greatly decrease the chances of intrusion and fraud by means of biometric identification, which is much harder to mimic or steal than regular PINs. In addition, the incorporation of voice command recognition seeks to enhance the convenience of the ATMs especially to the disabled people through multiple language configuration.

This solution's facial recognition aspect is developed using OpenCV library which is a computer vision library that supports the development of strong facial recognition features. The Multilingual Voice Recognition module is implemented with the help of the voice recognition library and googletrans library which helps in accurate and efficient voice command processing in any language. The system architecture is built around the concept of the smooth incorporation of these new technologies into the existing architecture of ATM hardware and software. UI is built using React, backend is built using Python and the database used is MongoDB. In order to have a reliable and a sound system, the following testing procedures were used; unit testing, integration testing, performance testing and security testing [1] [3].

This new system integrates facial recognition with traditional PIN entry, significantly enhancing ATM security through two-factor authentication. This approach improves resistance to conventional security threats. It has been tested under various conditions and scenarios to ensure effectiveness. While natural factors can affect facial recognition accuracy, the system maintains enhanced security without impacting transaction speed or usability. Additionally, it incorporates multilingual voice recognition, further improving accessibility and user experience.

## Attestation

I Abdul Aziz Kalsekar, therefore, declare that “ATM Bank Management System with Facial Recognition and Multilingual Voice Recognition” is my own work that I have done as a final year project under the guidance of Miss Preetha V. K in adherence to the Code of Conduct of the University of Stirling. The work does not include any copyrighted materials or materials written by other persons except for the following:

The face_recognition library used in the project was developed by Adam Geitgey and is available for use on https://pypi.org/project/face-recognition.

The speech_recognition library used in the project was developed by Anthony Zhang and is available for use on https://pypi.org/project/SpeechRecognition.

It does not include any materials submitted for another degree or diploma, unless proper references have been made. I know what is plagiarism and the penalties related to it, and therefore, the submitted work in this dissertation is plagiarism free. In writing this dissertation I have ensured that I have observed the set ethical considerations in conducting research as per the guidelines provided by the university.

Signature: Abdul Aziz Kalsekar Date: 9/04/2024

## Acknowledgement

I would like to thank my parents and Miss Preetha V. K. for their encouragement and help during the preparation of my final year project dissertation.

I would like to extend my special thank to my parents who have always supported and encouraged me all the time. They have stood by me and never gave up on me and I can only say that they have been my backbone and source of encouragement. They have given up many things for me to be able to be where I am today and their advice and affection have been my compass in this academic process and in life.

I am also highly thankful to Miss Preetha V. K. my supervisor, who has been a source of knowledge and directions in the preparation of this dissertation. She was always ready to contribute her extensive experience and knowledge and was always there to encourage me academically and morally. Miss Preetha's critical suggestions and splendid words of encouragement have not only made me improve my work but have also developed a very scientific attitude in me.

Their joint support has been a backbone of not only my project but also my development as a student and as a personality. It is indeed a privilege to have such a wonderful family and friends, and I am very grateful for all the help and motivation that they have offered me during this significant period of my academic life.

I want to thank all of you for inspiring me and for all the efforts, the large and small ones, that have made this possible.

# Table of Content

# List of Figures

# 1. Introduction

ATM still remains one of the most important interfaces between the bank and its customers in the constantly developing technological environment and offers a wide range of services. The objective of this project is to enhance the security of the current ATMs and its usability by implementing the facial recognition system that uses OpenCV and a database for safe storage of the clients' information [2].

Facial recognition technology, a recent innovation in the security systems, employs biometric identification to guarantee that only the right people are allowed to make the most sensitive financial operations and that such operations are specific to the individual. This project uses OpenCV thus using the Cascade Classifier model trained to detect faces at high speed, accuracy and with high reliability [2]. This classifier that uses Haar cascades first breaks down an image into parts and then looks for patterns that are similar to facial components and thus is a good way of providing authentication to a user [3].

## 1.1 Background and Context

Application of facial recognition in ATM systems also enhances security and enhances the convenience of the customers through the elimination of having to use the cards or pins that are easily misplaced or forgotten. Furthermore, since MongoDB is applied in database management, the details of the users shall be safe and can be easily accessible. We store user data in the MongoDB databases and provide an unstructured approach to the data organization, including users' information and their history of transactions, which let the application work with a stable and efficient solution.

### 1.1.1 Technological Shifts in Banking

The banking system has evolved in the past few decades supported by technological improvements in the society. Technology has gradually shifted the nature of banking services from the conventional branch banking to ATM banking, online banking, and mobile banking. There has been a general shift towards increasing the convenience of the customers, security, and reach of banking services.

Such advanced technologies as artificial intelligence, machine learning, and blockchain are becoming a new path to a safer, faster, and more convenient system of banking services.

### 1.1.2 Biometric Technology

Among the recently developed and widely used technologies, there is biometric technology that has become indispensable in the sphere of security, including banking. Whereas, traditional methods of authentication include the use of PINs or passwords, biometric authentication uses biological factors including fingerprints, face recognition, voice recognition, and many more; therefore, it cannot be easily counterfeited or hacked. Biometric technology in banking is employed in a bid to overcome the weaknesses that are present with the conventional forms of authentication in a bid to minimize on fraud and unauthorized access.


Figure 1. Biometric Technology, source: (Self)

### 1.1.3 Integration of OpenCV in ATMs

OpenCV, an open-source computer vision library has the ability to implement facial recognition features effectively. It has been incorporated into ATMs as a sign of boosting up the security and the authentication procedures of the user. OpenCV can be integrated to ATMs to enhance the facial recognition, a real time process, besides the PIN entry [4].

Apart from confirming that the person using the ATM is indeed the holder of the particular account, this technology also enhances the usability of the ATM as the authentication process becomes smooth and fast.

### 1.1.4 Data Security with NoSQL Database

Therefore, data security cannot be overlooked in the modern banking systems. MongoDB a form of NoSQL database provides a flexible, efficient, and secure way to store and manage data especially large data. Unlike the old SQL databases, MongoDB uses JSON-like documents to store data and this makes it easier to design schemas and access data. The security features such as encryption, authentication, and access control help prevent unauthorized access and breaches to the user information stored in the database.

Figure 2. Database, source: (Self)

Protecting data in MongoDB databases is important, especially since the data they store can be very valuable. Here are essential strategies and best practices to safeguard data:

**Data Encryption:**

Encryption at Rest: It means encrypting the databases that are stored on a media or disk to prevent access of the data if the disk is stolen. MongoDB offers native encryption for data in rest for the purpose of enhancing the security of the information.

Encryption in Transit: To protect from eavesdropping and man-in-the-middle attacks, it is recommended to use SSL/TLS protocols for the data transmission. MongoDB provides built-in support for SSL/TLS which means that the data traveled between the clients and the servers is encrypted.

**Access Controls:**

Authentication: Use of proper authentication procedures to confirm that only the right people get to access the database. MongoDB offers many authentication mechanisms such as SCRAM and LDAP.

Authorization: Tightly control the authorization by implementing the user roles and permissions. RBAC (Role-Based Access Control) of MongoDB enable controlling the level of user access with the level of detail required.

**SQL Injection Prevention:**

Input Validation and Sanitization: To prevent injection attacks, it is imperative to always validate and sanitize all input data. MongoDB has its way of preventing injection through the use of query formats.

Parameterized Queries: To prevent injection attacks, it is recommended to use parameterized queries or prepared statements, this is because the input data will be treated as values and not as code.

**Regular Updates and Patching:**

Security Patches: It is crucial to keep the MongoDB server and its environment up to date with the latest security patches as this will prevent the exploitation of some of the available vulnerabilities. MongoDB frequently comes up with updates and patches to fix the loopholes that are considered as the security threat.

Database Software Updates: It helps in applying the latest features and security measures in the database software when the software is up to date.

**Auditing and Monitoring:**

Activity Auditing: Increase the verbosity of the database logs and audit activities to identify and prevent unauthorized actions as early as possible. MongoDB's auditing feature enables the monitoring of operations carried out on the database.

Continuous Monitoring: Utilize the continuous monitoring tools in order to monitor the database activity and look for security risks in real time.

**Backup and Recovery:**

Regular Backups: This makes the information secure, easily retrievable and above all, accurate through regular, secure and encrypted backups. MongoDB has commands that allow the creation of backups that are encrypted.

Recovery Plan: Put in place a sound recovery strategy in order to counter check for data loss from security threats. Conduct the recovery process on a frequent basis to determine its efficiency.

**Network Security:**

Firewalls and Network Segmentation: To prevent the database server from being attacked and infected while online, it is recommended to install firewalls and network segmentation to separate the server from the rest of the network. Firewalls can be set to let through only the needed traffic to and from the MongoDB server which is another level of security.

Secure Configuration: To make the database and the environment in which it is located more secure, remove the features that are not needed and adjust the settings. MongoDB has listed certain security checklist which should be followed for making the configuration secure.

**Security Training:**

Personnel Training: All personnel that are involved in the management of databases should undergo training on a regular basis. Teach the employees how to identify security risks like phishing and other cyber threats as a way of enhancing the human factor of security.

Adopting all these multiple level security measures greatly minimizes the likelihood of data leakages and unauthorized access to MongoDB databases. Thus, it can be stated that the concept of comprehensive security should be employed to guard crucial and sensitive information of organizations.

### 1.1.5 Multilingual Voice Recognition Module

To make the service even more convenient, in particular for people with disabilities, it is necessary to integrate a multilingual voice input module. This module uses the voice recognition and googletrans libraries to allow customers to engage with the ATM by using voice commands in different languages. The developed system has the ability to handle a multitude of languages; hence, it eliminates the possibility of language being a hindrance to accessing the banking services. The implementation of the multilingual voice recognition module has greatly improved the accessibility and use to users with disabilities. Thus, using the voice recognition and googletrans libraries, the module makes it possible to perform the control of the ATM using voice commands in different languages. This way, language constraints will not be a hindrance to the users in as far as banking services are concerned thus enhancing the user's experience across different segments. The module implements state of the art speech recognition technology to interpret voice commands spoken in different accents and dialects. A lot of testing has been done in various conditions, including public areas with loud background noise, and it has been proved to be very precise and efficient. This performance is rather stable and guarantees that everyone will have an equally comfortable experience [7].

The system has an interface that has buttons that help the user to enter the voice command and gives visual and audible feedback when it recognizes the command. Available options enable the selection of language and voice mode, which increases the level of comfort and trust of a user when communicating with the ATM.

Still, there is the issue of security and the voice recognition module includes strict features to protect the user data. Other forms of authentication include; Voice biometrics, which check the user's identity and ensure that the system does not grant access to unauthorized persons. This way, the security is improved and, at the same time, users can easily and conveniently authenticate their transactions without coming into contact with any surface [7].

For the users with color blindness, the system contains voice output functions; thus, the ATM will reads options and messages. This helps all users with or without visual impairments to access and use the ATM on their own and this is in accordance with the company's policy of providing equal banking opportunities to all customers.

The multilingual voice recognition module is also regularly refined and enhanced in accordance with the users' recommendations and the progress of technology. It is updated from time to time so that it can accommodate the new languages and dialects in order to meet the ever changing demands of the customers. Thus, adopting new technologies and focusing on the ease of use, we have improved the quality of banking service and made it available for everyone.

### 1.2 Scope and Objectives

The objective of this study is to design a new ATM system with better security and convenience by applying Biometric technology. This system will incorporate facial recognition as one of the main ways of identifying the users of the system which will in turn minimize on the cases of fraud and unauthorized access.

Together with the above stated biometric methods, it also plans to incorporate the use of other conventional methods such as PINs and passwords, which are easily forgotten and easily hacked, to come up with a more reliable authentication mechanism.

Scope:

Facial Recognition for Security: Using facial recognition to check the genuineness of the user, and hence, increasing the level of security and decreasing the probability of illegitimate use.

Multimodal Authentication: Improving the security measure to include the use of the conventional PIN entry as well as the new facial recognition to give a two-level security.

Multilingual Voice Recognition Module: Using voice command recognition that is able to recognize different languages for the purpose of meeting the needs of different users.

User Experience Enhancement: Enhancing the authentication process in a way that the process is less time-consuming and cumbersome than conventional methods, this is because the user will be in a position to access their account without having to enter several security keys.

Data Management: Applying MongoDB for the best way of storing and managing data with the focus on data confidentiality, data integrity, data availability.

Scalability and Flexibility: Ensuring that the system is scalable in order to accommodate future upgrades as well as the inclusion of other biometrics. This flexibility can be useful in expanding the size of the database to accommodate for a larger number of users as well as changes in the regulations [14].

Inclusive Design: To ensure that all the users are able to use the system, the system should be designed in a simple manner hence following the principles of inclusive design.

Objectives:

Increase Security: Introduce a facial recognition that will greatly minimize the chances of an individual accessing the account without authorization or commit fraud.

Improve User Convenience: Improve the usability by shortening the time spent on the authentication and making it easier for users to complete.

Ensure Data Privacy and Integrity: Apply MongoDB to handle user data, and ensure the data is well protected with strong privacy and data integrity.

Support Scalability: Create the system architecture that will be easily expandable and would be able to meet the future requirements and changing technology.

Promote Accessibility: Make sure that the system is easy to navigate and easy to use for people of all disabilities to make it one that is friendly user.

## 1.3 Achievements

It has used facial recognition and ATA PIN in the project to achieve better security of ATMs. The application of OpenCV for real-time facial recognition, MongoDB for effective data storage and management has shown a great enhancement in the security as well as usability of the system. The multilingual voice recognition module has thus made it easy for the user to communicate with the ATM in any language of their choice thus making it comprehensible to many people. The system has been tested on unit level, integration level, performance level and security level and proved to be efficient and reliable.

## 1.4 Overview of Dissertation

The dissertation is structured into six main chapters, each detailing various aspects of the project from conception through to conclusion:

Chapter 1: Introduction, providing the background, context, scope, objectives, and achievements of the project.

Chapter 2: Literature Review, discussing previous works and existing technologies related to biometric authentication, ATM security, and voice recognition.

Chapter 3: System Design, detailing the architecture of the proposed system, including the integration of facial recognition, voice recognition, and the backend infrastructure.

Chapter 4: Implementation, describing the development process, technologies used, and integration steps.

Chapter 5: Testing and Evaluation, presenting the testing methodologies, results, and performance evaluation of the system.

Chapter 6: Conclusion and Future Work, summarizing the findings, achievements, and potential future enhancements for the system.


Figure 3. Achievements, source: (Self)

# 2. State of The Art

Its application in banking and other industries has been on the rise due to its improved efficiency and low rate of errors especially in the identification process of users to boost the security system. In this chapter, the theoretical background of the facial recognition using OpenCV is discussed, the existing ATMs with similar technologies are analyzed, and the algorithms used to provide safe and fast transactions are described. The transition from PINs and swipe cards to biometric authentication solves the problems of traditional systems, which are the fight against fraud and user convenience – the trends that define the further evolution of ATMs. This chapter provides an overview of the project and locates the research within the framework of comparative studies and models, as well as identifying the innovations most pertinent to the field of this study [12].

## 2.1 Background of Facial Recognition Technology

### 2.1.1 Facial Recognition Technology (FRT)

FRT has progressed from an academic idea to a common technique utilized in security, commerce, and Smartphone management. The history of FRT started in the early 1960s, but there have been major improvements in the last two decades due to the improvement in machine learning and computational power. First created as a security tool, FRT makes use of a digital map of the subject's face and compares it with a database of faces to determine who could be similar. This process involves specific mapping of certain landmarks on the face like the distance between the eyes and shape of the jaws to come up with facial signature. The uses of FRT are not only restricted to security but also include photo tagging in social media, unlocking of mobile phones, and marketing to know the reaction of customers. Its use in consumer applications clearly shows that it is widely used and has a lot of applications.

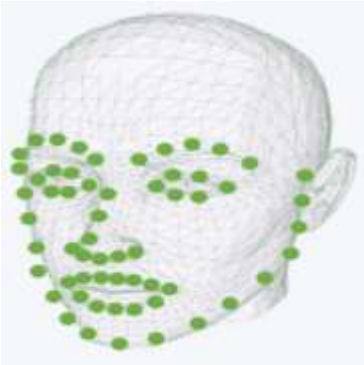

Figure 4. Facial Recognition Technology (FRT), source: (Self)

### 2.1.2 Ethical and Privacy Concerns

However, FRT has some ethical issues regarding privacy and surveillance. The two major concerns are privacy concerns and the possibility of governance. The applications of FRT in law enforcement and public security agencies are relatively risky when there are no specific rules and laws.

### 2.1.3 Accuracy and Bias

Besides privacy issues, FRT attracts controversy regarding its effectiveness and efficiency among various populations. According to the existing studies, the FRT systems seem to be prejudiced, which leads to the different levels of efficiency depending on the race and ethnicity of the individuals. These biases have to be countered for making FRT applications more fair and just to all concerned. New techniques like 3D modeling and skin texture analysis are enhancing the recognition rates and these issues. Thus, the ethical concerns of FRT remain topical and fuel debates on the need to regulate its application.

## 2.2 OpenCV

OpenCV that is short for Open Source Computer Vision Library is one of the most important tools for facial recognition technology as it provides a powerful and adaptable platform for the researchers and developers. It offers a range of face detection, tracking, and analysis tools that offer high accuracy and operate in real-time [12].

### 2.2.1 Application Development

OpenCV that is short for Open Source Computer Vision Library is one of the most important tools for facial recognition technology as it provides a powerful and adaptable platform for the researchers and developers. It offers a range of face detection, tracking, and analysis tools that offer high accuracy and operate in real-time.

### 2.2.2 Algorithmic Innovations

OpenCV is known to apply machine learning algorithms for detection of facial features and that is its core advantage. They are fed with a large amount of data and hence improve with time on their performance. The incorporation of deep learninig techniques especially the convolutional neural networks has boosted OpenCV face detection to recognize faces of people of different ethnicity and in different conditions. This is because the OpenCV library is compatible with the Processing

programming framework through which one can easily and quickly develop and host facial recognition applications since it is friendly to educators and non-specialist developers [12].

### 2.2.3 Challenges and Limitations

Nevertheless, OpenCV has its difficulties in preserving the precision during the changes in lighting conditions or partial occlusion of the face. Some more challenges that have been reported with the use of OpenCV-based applications include Ethical challenge of privacy and surveillance However, future developments of OpenCV should be expected to focus on enhancing the efficiency of algorithms, decreasing the level of bias, and improving the protection of users' privacy [10] [14].

## 2.3 Comparative Analysis of ATM Systems

The evolution of ATM systems has been driven by the need to enhance security and user experience, especially as instances of fraud continue to rise. Conventional PIN-based authentication, while widely used, has its limitations in terms of security and convenience. As a result, newer authentication methods have been developed to address these challenges. Below is a comparative analysis of some existing state-of-the-art ATM systems, highlighting their strengths and weaknesses. This analysis sets the stage for explaining the benefits of creating a new version of the ATM system.

Biometric ATMs have emerged as a prominent solution, offering enhanced security through the use of fingerprint, iris, or facial recognition. These systems provide a higher level of security compared to traditional PIN-based systems, as biometric data is unique to each individual, making it difficult for fraudsters to replicate. Additionally, biometric ATMs improve user convenience, as users do not need to remember PINs or passwords, reducing the risk of forgotten credentials. However, the use of biometric data raises significant privacy concerns, as users may worry about how their biometric information is stored and used. Implementing biometric systems can also be expensive due to the cost of the technology and the need for high-quality hardware.

Multi-Factor Authentication (MFA) ATMs offer increased security by combining multiple authentication factors such as PINs, biometrics, and mobile authentication codes. This significantly enhances security and makes it much harder for fraudsters to gain unauthorized access. However, MFA systems can be more complex and time-consuming for users, potentially leading to frustration

and slower transaction processes. Additionally, some users may resist adopting MFA due to the perceived complexity and additional steps required for authentication.

As a result, the need to increase the security of ATM as more cases of fraud continue to be reported has driven the development of ATM technology. The conventional PIN-based technologies have their limitations hence the advancement of new authentication methods to meet the balance between efficiency and user experience.

### 2.3.1 Enhanced Security through Biometrics and Multi-Factor Authentication

The commonly adopted ATM systems largely depend on the use of PINs for identification of the user and this has its weaknesses. PINs are easily hacked or stolen and this grants the hackers access to the user's account. As a result, current ATMs are also using biometrics and multi-factor authentication to enhance the security feature. For example, if a three-level verification system is used, then the password, biometric marker (fingerprint), and OTP shall be used. Nevertheless, in my project, I pay my attention to the integration of facial recognition with the conventional PIN entry, and OTPs are not to be used.

### 2.3.2 Comparative Efficiency and User Experience

Even though multi-factor systems are beneficial for security they are also known to prolong transactions and affect the experience of the users. Security on the other hand comes face to face with efficiency and this is a big issue for banks and other financial institutions. The expense of using sophisticated security measures is also a critical factor to look at. Despite the fact that the installation and management costs are higher compared to traditional systems, the long-term advantages like minimizing of the fraud and enhancing of the customer trust can compensate for these expenses. It is for this reason that future ATM systems can be expected to incorporate such features as facial recognition and behavioral biometrics to provide a more secure environment through an understanding of the user's actions and appearance [9] [14].

## 2.4 Multilingual Voice Recognition

### 2.4.1 Overview of Multilingual Voice Recognition Technology

Voice recognition system allows ATMs to accept voice commands in different languages and thereby improve the convenience of the users. It applies the natural language processing (NLP) and

machine learning concepts that enable the software to understand what the user is saying regardless of his/her language [7].

Figure 5. Voice Recognition Technology, source: (self)

### 2.4.2 Integration in ATM Systems

Integrating multilingual voice recognition in ATMs involves capturing voice input through a microphone, processing it using speech recognition software, and responding appropriately. This integration enhances user interaction by allowing users to perform transactions and access information through voice commands. Multilingual capabilities ensure that users can interact with the ATM in their preferred language, improving the overall user experience.

### 2.4.3 Challenges and Innovations

The process of implementing multilingual voice recognition in ATMs include; capturing the voice through a microphone, using of speech recognition software to process the voice input and responding to it. This integration improves the user experience because it enables the users to make transactions and gain information via voice. The multilingual functions allow users to communicate with the ATM in various languages they are comfortable with hence enhancing the user experience.

## 2.5 Algorithmic Implications for ATM Systems

The shift from the use of PIN to the current use of facial recognition, and multilingual voice recognition in ATMs to enhance security is quite exemplary.

### 2.5.1 Facial Recognition Algorithms

Facial recognition technology that is used in OpenCV entails image processing and feature extraction to prepare and analyze the image data for identification. Preprocessing of images

includes geometric and photometric image correction to eliminate the influence of the factors that depend on the environment. Feature extraction techniques like Haar Cascades compare the pixel intensity to detect the face features. These machine learning algorithms are efficient and fast working that help real time applications such as ATM systems in user authentication [10] [13].

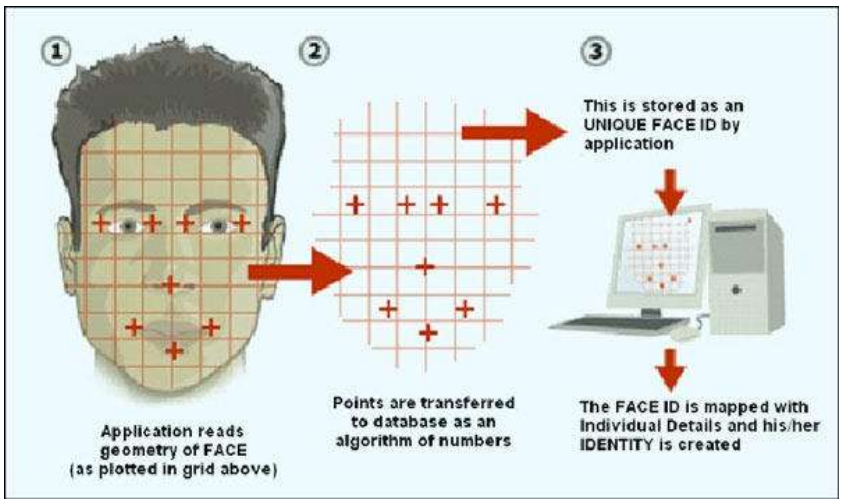


Figure 6. Facial Recognition Algorithm, source: (Self)

### 2.5.2 Voice Recognition Algorithms

Voice recognition in languages is implemented with the help of NLP and machine learning to convert user's voice commands into text. These algorithms analyse the actual speech, phonetics and context from the spoken language without difficulty. The system that is proposed in this paper applies continuous learning and adaptation, and the system's performance is fine-tuned over time hence it performs accurately regardless of the language used.

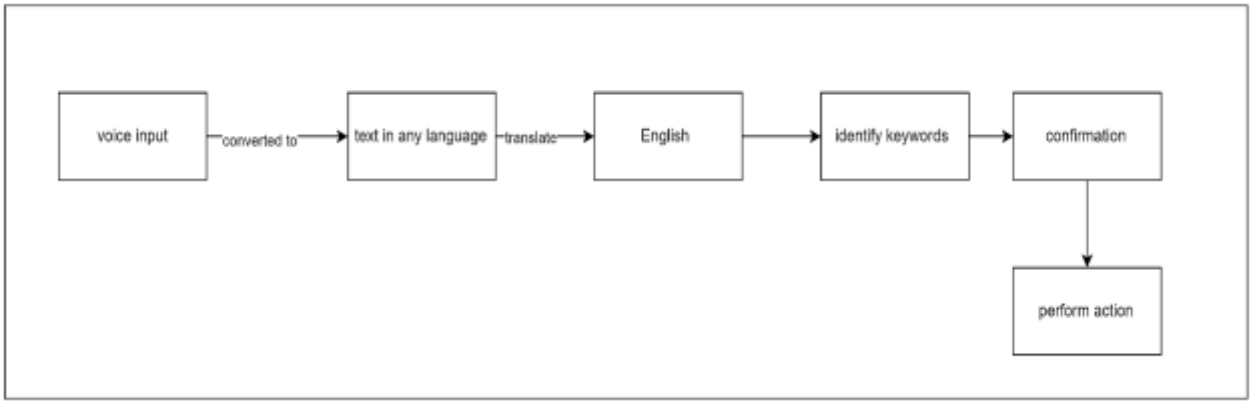


Figure 7. Voice Recognition Algorithm, source: (Self)

## 2.6 Implications

The use of facial recognition and multilingual voice recognition tools in ATMs is of great consequence to the security and usability axes. OpenCV has Haar Cascade models that help in facial recognition, and it is hard for the fraudsters to mimic the users' identity. Multilingual voice recognition simply enhances the convenience by enabling customers to communicate with the machines in their mother tongue [11].

Incorporating the use of MongoDB in data management is a clear emphasis of the project on data security and data quality. MongoDB as a database also has features of scalability and reliability in storing biometric data which are sensitive and meet the international standards on data protection. The implementation of these high-tech innovations into ATMs is a big step toward enhancing the level of security and convenience in the banking services. One of the vital features is facial recognition, which is based on OpenCV's Haar Cascade models that improve the overall security of the system with an extra biometric check. This makes it much harder for the fraudsters to bypass the security measures in place as facial recognition involves physical attributes that cannot easily be mimicked or obtained. This not only makes users safe from scams but also enhances the trust in the ATM system since the individuals' information is secure.

The multilingual voice recognition feature improves the usability of the ATMs and makes the interaction with them even more convenient. Thus, the ability to work with multiple languages allows users of different languages to use the banking services without the language limitation. This is especially helpful in multicultural areas and for tourists, thus increasing the accessibility of banking services and their comprehensiveness. The voice recognition system, in combination with the visual and the auditory feedback results in the user getting a positive indication that an operation has been completed; this drastically reduces the chances of the user making a mistake and in the process increasing the overall satisfaction of the user.

Data management is a crucial factor of this integrated system, and using MongoDB displays a clear focus on the protection of data. MongoDB offers a scalable and reliable architecture due to this it is well suited to store and manage biometric data such as facial recognition and voice recognition data. It has scalability to allow the system to scale up and accommodate more data without having to sacrifice on speed or on security. Also, the app has had to ensure that it meets all the global data

protection standards hence giving the users the assurance that their data is well protected within the MongoDB database.

Also, the flexibility of MongoDB enables data of any type and from different sources to be easily incorporated and managed within the database for intricate biometric data. This flexibility is important in ensuring that the system is able to adapt quickly to technological changes and/or regulatory changes that may be put in place. Scheduled updates and upgrades to the database management system guarantee that the most recent measures against potential threats are implemented to secure the users' information.

Thus, the facial recognition, multilingual voice identification, and secure data storage make the ATM experience more secure and convenient. This approach not only improves the performance of banking operations, but it also corresponds to the current need to increase the level of security and focus on customers' needs in the provision of financial services. Thus, the described integrated system takes a significant role in the further development and becoming the basis for future biometric technologies that will be used commonly in the banking sphere [14].

# 3. Analysis and Design

## 3.1 Problem Definition

The core challenge that facial and voice recognition technologies try to address is the improvement of security measures in ATMs. Facial recognition is one of the non-transferable authentication means which has very little margin of error in terms of granting access to unauthorized person. Whereas the PINs or the magnetic cards are not very difficult to duplicate or fake, facial features are very hard to duplicate, given that they are unique to each and every individual. Likewise, the voice recognition provides one more factor to apply for security as voice is unique to every person. However, there is a difficulty on the recognition of objects and voice in real time for the ATM system especially on the issue of light intensity, gradient changes, and noisy conditions [17].

There is also a problem of achieving high levels of security while at the same time ensuring that the transactions take less time to be completed. This is because customers expect efficient services from the ATMs and any other procedures that are put in place should not slow this down. Hence, the use of OpenCV's facial recognition, alongside reliable voice recognition, is poignant in the complex environments in which ATMs function. Thus, both technologies have to coexist in such a manner that they do not compromise on the security aspect of the transaction yet at the same time make the process quite fast.

## 3.2 System Analysis

### 3.2.1 Key Terminologies

This paper uses several important terms related to the ATM system project concerning facial recognition technology to explain the system design, implementation, and testing.

#### 3.2.1.1 Facial Recognition Technology (FRT)

Biometric software technology for the recognition or authentication of a person from a digital image or video frame. FRT employs biometric markers that are related to the facial geometry to identify people.

3.2.1.2 OpenCV (Open-Source Computer Vision Library)

It is a library of functions for real time computer vision mainly for real time programming. In this project, OpenCV captures and analyzes images from the ATM cameras to recognize the users using facial recognition algorithms [13].

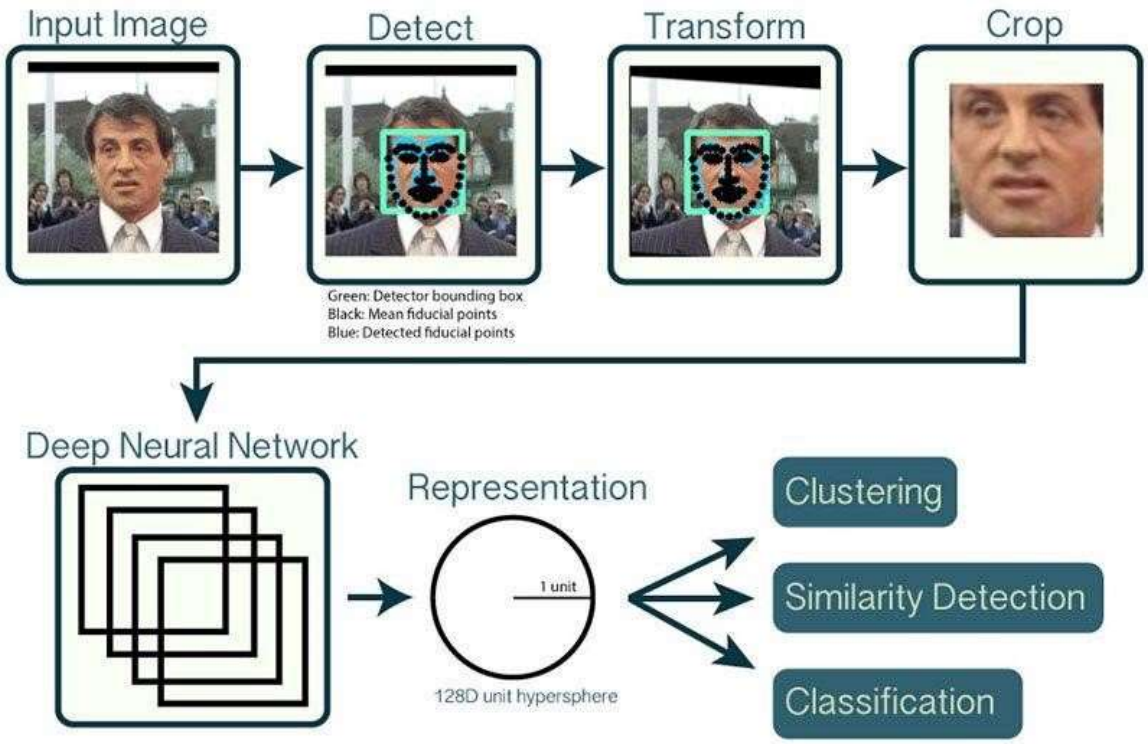


Figure 8. Working flow of OpenCV for face recognition, source: [12]

3.2.1.3 Haar Cascades

An object detection model that is used in machine learning to detect objects in an image or video stream. This is especially common in face recognition and is applied in this case to identify features on the face quickly.

Haar Cascades is one of the classical methods within the field of computer vision and more specifically in the context of facial recognition. This object detection method that uses positive and negative images to train the classifiers was developed by Paul Viola and Michael Jones. Positive images have the object of interest in them while negative images do not have the object of interest in them. it thereof assigns features that define the object to determine the rapid and efficient detection process in real time [13].

Haar Cascades are more efficient in the face recognition application because they are able to analyze images and video streams at a rapid rate. This speed is obtained from the application of integral images and a classifier which is in cascade. An integral image is efficient in calculating rectangular features and this speeds up the computation for every image. The cascaded classifier, however, ensures that only the most potentially informative areas of an image are submitted to the detailed analysis, which, naturally, also improves the algorithm's performance [13].

In the aspect of ATM security, Haar Cascades are quite useful to detect faces and identify people in real time since they have some facial recognition capabilities. The algorithm is able to rapidly identify and authenticate a user's face against the biometric data kept in the system, thus denying access to banking services to anybody but the rightful user. This real-time identification capability is very important in situations that require the identification process to be very fast and efficient in order to enhance the security of the environment as well as the convenience of the users. Thus, ATMs are capable of delivering a smooth and secure experience to the users through the implementation of Haar Cascades to avoid fraud and other forms of unauthorized access. Haar Cascades is not only limited to the recognition of facials but it has many applications. This makes it to be useful in detecting several objects and thus can be applied in many different fields. Some of the scenario that can be encompassed in the banking sector include identifying any fraudulent activities around the ATMs, for instance, tampering or vandalism. Thus, implementing Haar Cascades to surveillance systems, banks can improve the level of security, making the atmosphere more secure for the users.

Although, the use of Haar Cascades has its benefits, it has some setbacks in its application. The algorithm needs a large set of training images and suffers from such factors as illumination and partial occlusion. To overcome these issues, the current research and development is directed towards enhancing the stability of the technique as well as its dependability. This encompasses the integration of better approaches, including deep learning, in the identification of Haar Cascades in various conditions [11].

The combination of Haar Cascades with other state of the art techniques, for instance the multilingual voice recognition and the secure data storage systems are some of the ways that have been put in place in order to improve the overall working of the ATM. When integrating such

technologies, the banks are in a position to provide more secure, efficient and convenient services to the clients. This approach is beneficial as it guarantees the consumers' ability to make use of these financial services while at the same time having their data protected by the highest level of security.

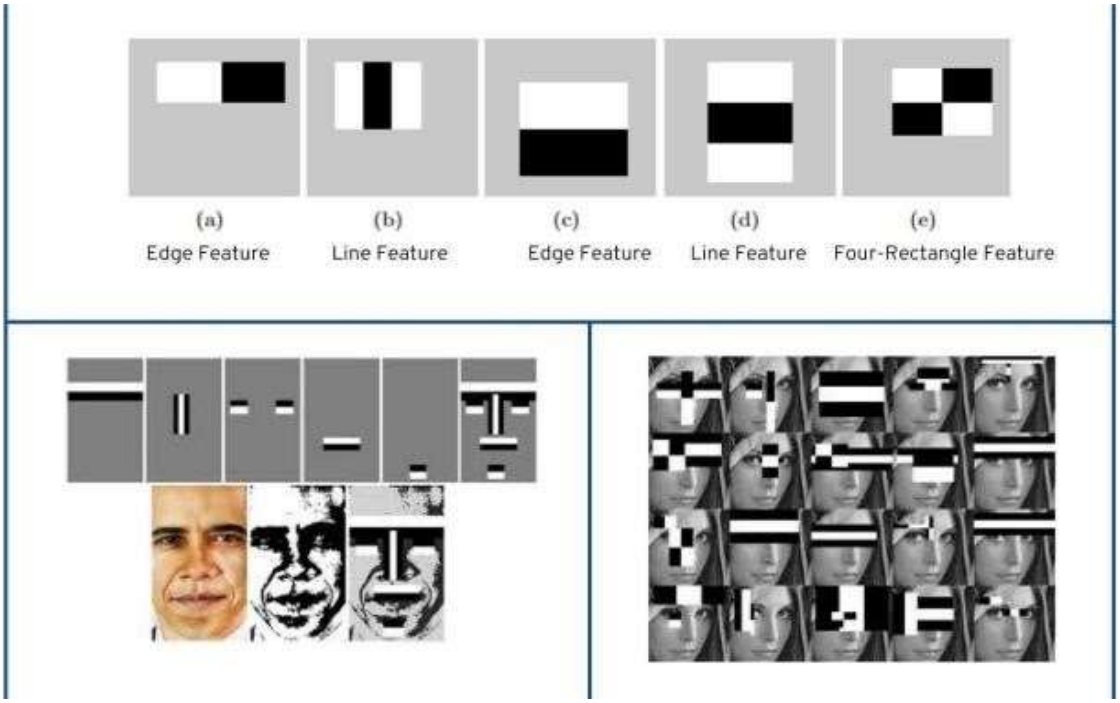


Figure 9. Haar Cascades feature detection through greyscale images, Source: [2] [11]

#### 3.2.1.4 MongoDB

A non-relational database that stores the data in the form of JSON like documents with or without schema. The data of the users is collected, stored, retrieved, managed and protected in this project with the help of MongoDB.

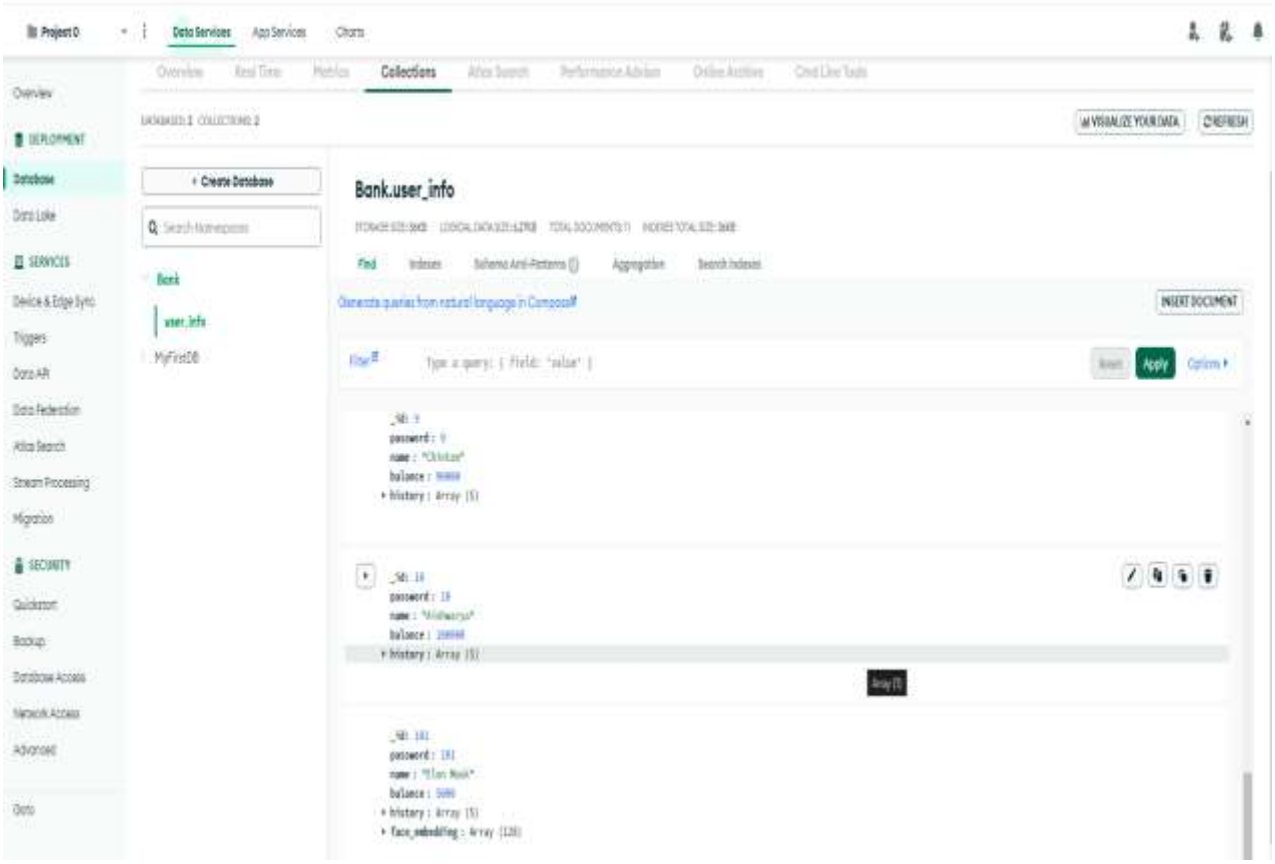


Figure 10. MongoDB Atlas Database and collection, Source: [18]

#### 3.2.1.5 Biometric Data

Data that is visible or qualitative and pertains to a particular person's body or bodily features. In this system, facial images are the biometric data used for identification that is, for authorization of the user.

#### 3.2.1.6 User Interface (UI)

The manner in which a user engages with a system especially in terms of placing input and receiving output. For ATMs, the UI covers such elements as screens, input panels, and voice prompts that help the user perform operations [8].

#### 3.2.1.7 Real-Time Processing

Meaning the ability of the system to operate a data feedback loop where information is put in and results are given out almost simultaneously. The facial recognition in an ATM has to be real time since the users want fast and efficient services when making the transactions.

#### 3.2.1.8 Multilingual Voice Recognition

Vocal recognition feature of the ATM system that makes it possible to respond to voice commands given in any language. This feature improves navigation and thus the usability of the website or application that is being developed [8].

### 3.2.2 Target Users

The target customers of the ATM system are the public who perform basic banking operations like with draw, deposit, account information, and transfer of funds. This user group includes people of all ages, with and without technical knowledge, and with or without disabilities in accessing information. The system must be user friendly, self-explanatory, and fast in conducting a transaction for the use of the tech savvy and the non-tech savvy.

Bank officials, security personnel and maintenance personnel also are in a position to interface with the ATM system. They demand interfaces for configuration, maintenance, and repair in such a way that does not lead to long outages. It should also contain features for diagnostics, for checking the performance of the system and security logs.

### 3.2.3 User Goals

#### 3.2.3.1 General Public

Security: The consumers need high security measures for their financial transactions. The incorporation of facial recognition should provide a better level of security than using a PIN number to log in [10].

Efficiency: The users want to get the service without waiting for a long time and with a short time of the transaction, thus speed is the vital attribute.

Usability: The design of the ATM interface should be simple and easy to understand and should be easily navigable by all users including those who are technically less aware. Clarity of the instructions and layout of the website should not be complicated.

Accessibility: The ATM should be easily reachable to all the users including the disabled ones. Elements such as audio command, height knob, and input keys should meet standards such as the one put in place for the disabled.

#### 3.2.3.2 Bank Staff

Monitoring and Control: It is also necessary for the employees to have some means of monitoring, and managing the operations of the ATMs including the software and system updates, diagnostics, and transactions.

Technical Support: Efficient and very basic technical support measures to limit the amount of time lost. Tools for predictive maintenance for the application of high reliability.

Reporting: The creation of detailed reports of transactions, security check processes, and system failures to meet legal requirements and for auditors' review.

Training: Low training needs because of the well-designed interface, with ongoing help and readily available instructions for addressing any issues or changes.

### 3.2.4 System Usage Patterns

#### 3.2.4.1 General Public

The majority of the users access the ATMs with the purpose of conducting basic banking tasks including the withdrawal of cash, depositing of money, checking the balance, and transferring of funds. Such transactions should be easy and without much complications. It is used at certain times of the day for example after working hours or on pay days and the ATM has to deal with a heightened number of transactions in a given time without any form of delay.

Other less frequent operations include changing PIN codes, modifying personal data, or addressing the bank services via the integrated communication means. These functions should be easy to use through the main interface and should not be easily susceptible to hacking.

#### 3.2.4.2 Bank Staff

Such procedures should be carried out at frequent intervals and at times when business is not being conducted. The staff should also be able to supervise several ATMs at a given time from a central position. Reactive maintenance takes place when there is a problem of hardware or software while preventive maintenance takes place when transaction logs and operational metrics are analyzed. It should be easy to train people for new features or security updates, and the employees should be able to have administrative privileges to change the look and feel of the user interface and other marketing options.

### 3.2.5 Use Case

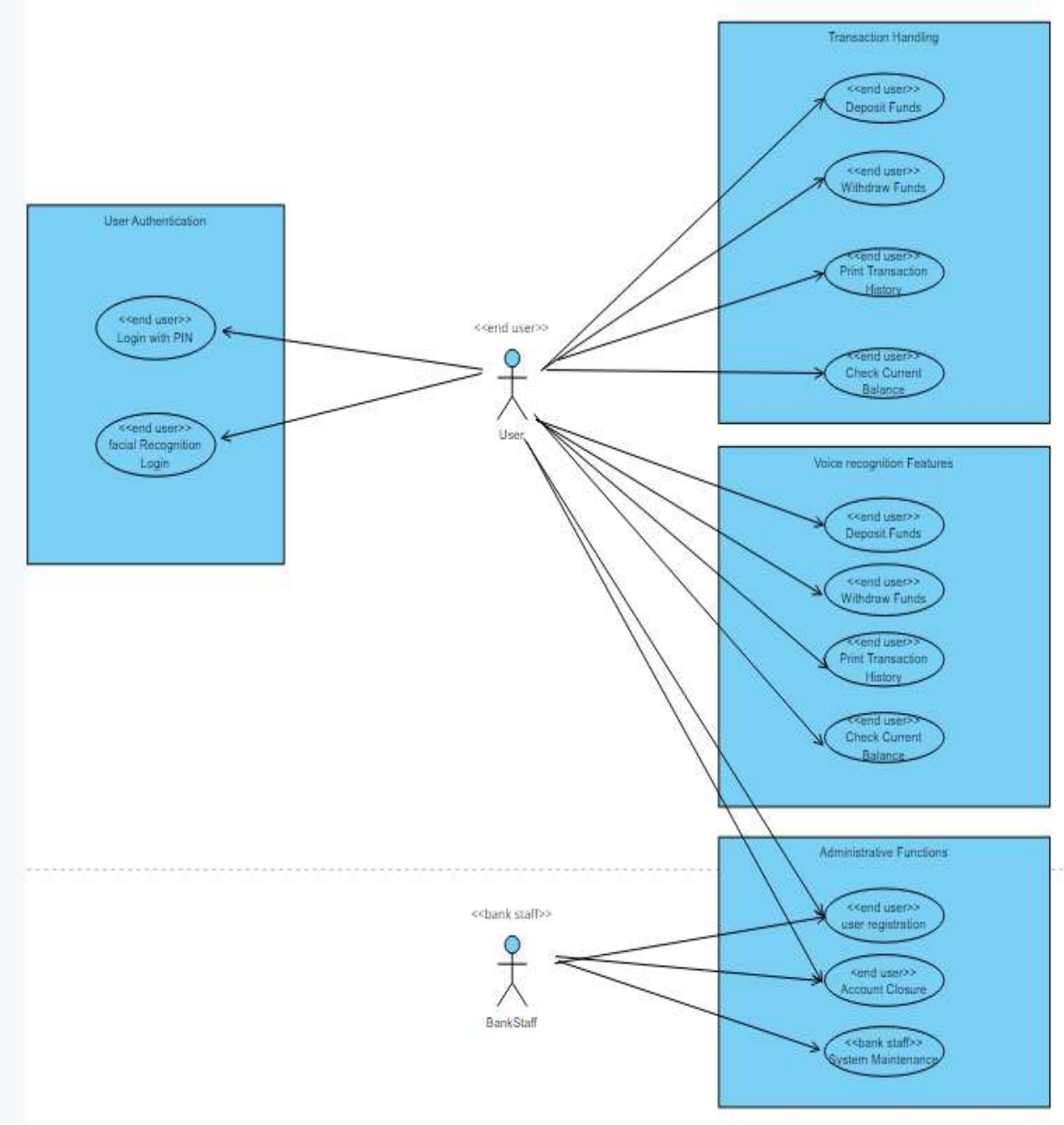


Figure 11. Use case diagram for the application ATM system. (Source: self)

The following is the Use Case Diagram that depicts the different activities that the bank's customers and employees perform with the banking system: It is organized into several areas with each area showing different aspects and activities of the system usage.

The first activity presented in the first section, User Authentication has two options that users can use to log into the system. The users are able to log in using the personal identification number (PIN) or they can use facial recognition to log in which is more secure.

The second section, Transaction Handling describes the general financial activities that the end users are able to conduct. These operations include deposit, withdrawal, making a print of all the transactions that have been made, and the check on the current balance of their account. These are basic aspects that help users in the management of their financial matters in the best way possible [9].

Also, Voice Recognition Features are presented in the diagram, which perform the transaction handling operations but through voice commands. This implies that users are able to place money into their accounts, withdraw, obtain a record of their transactions and check their current balance by voice interaction, which is advantageous as it is a contact free method of operating their accounts [6].

The Administrative Functions section is aimed at the end users of the system as well as the personnel of the bank. End users can create new accounts and delete old accounts which give the consumers the power over their banking services. The employees of the bank are in charge of the general maintenance of the system which makes sure that the banking system is in full working order.

Thus, this Use Case Diagram demonstrates the overall view of the banking system and identifies the possible interactions between end users and bank staff. It explains the methods for user authentication, ways to handle financial transactions, voice recognition features, and management, thus creating a productive user experience.

### 3.2.6 System Overview

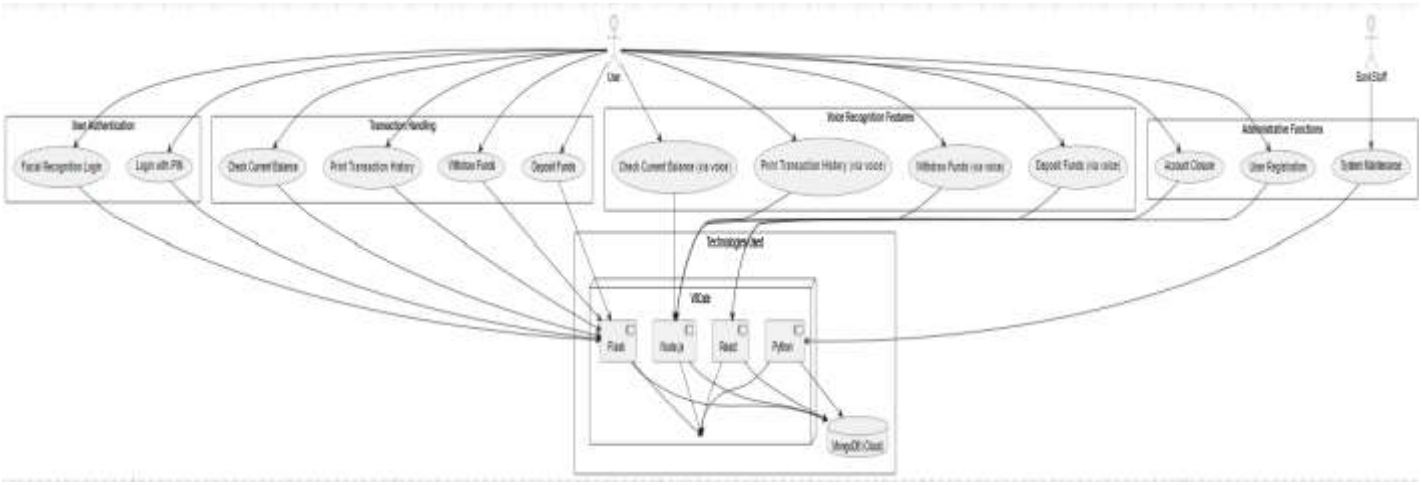


Figure 12. System overview diagram for the application ATM system. (Source: self)

This diagram provides a holistic view of the banking application system and maps out the various stakeholders' relationships with the application and the system as a whole, including the technologies and the environment for development.

The process kicks off with User Authentication as the initial section of the diagram. It includes two methods for users to access the system: There are two ways of authentication that are used which include; logging in with a PIN and logging in via the use of facial recognition. The above methods assure that the users are first able to prove their identity before being allowed to access their accounts [17].

Transaction Handling is the next one, which elaborates on the main functions of the application that are related to financial activities. Some of the functions include; deposits, withdrawals, print out of the transaction slip, and checking of balance. For the purpose of carrying out business on a daily basis, these functionalities are very vital.

Another section of the application is Voice Recognition Features where the same transactions are presented, but this time they can be started by voice commands. This is through making deposits, withdrawals, getting a print-out of transactions, and confirming the balance through voice. These features give the users an opportunity to operate the accounts without having to use their hands, thus improving ease and convenience.

The Administrative Functions section contains activities that any user of the system, as well as the bank employees, can execute. Some of the functions include user registration where they can create new accounts and also close the existing ones to control their banking services. Bank staff are however in charge of system support, this involves making sure that the system is up and running effectively.

The Technologies Used section is placed in the center of the diagram, which explains the development environment and tools that are applied in the development of the system. This diagram reveals that the system is developed in VSCode with technology components such as Python, Flask, React and Node [1]. js. Also, MongoDB is applied as the cloud database for the storage and management of the system data [9].

Lines and arrows in the diagram show relationship of one part to the other and their relationship within the system. For instance, the functionalities under User Authentication and Transaction Handling are integrated with Flask while those of voice recognition are integrated with Node. js. Management tasks encompassing User Interfaces use React while rest of the processing is done in Python [1]. All these technologies interact with MongoDB that is hosted in the cloud for the purpose of data storage [17].

In conclusion, this diagram gives a clear picture of the structure of the banking system to show how various parts and technologies are interconnected to give the users a smooth experience [3].

## 3.3 User Interface Design

### 3.3.1 Login Page

The Login Page is the Default Landing Page where the user is supposed to input the Account Number and Account Pin. Once the user enters all the Credentials, he/she is redirected to the Face Authentication Page where the user's face is compared.

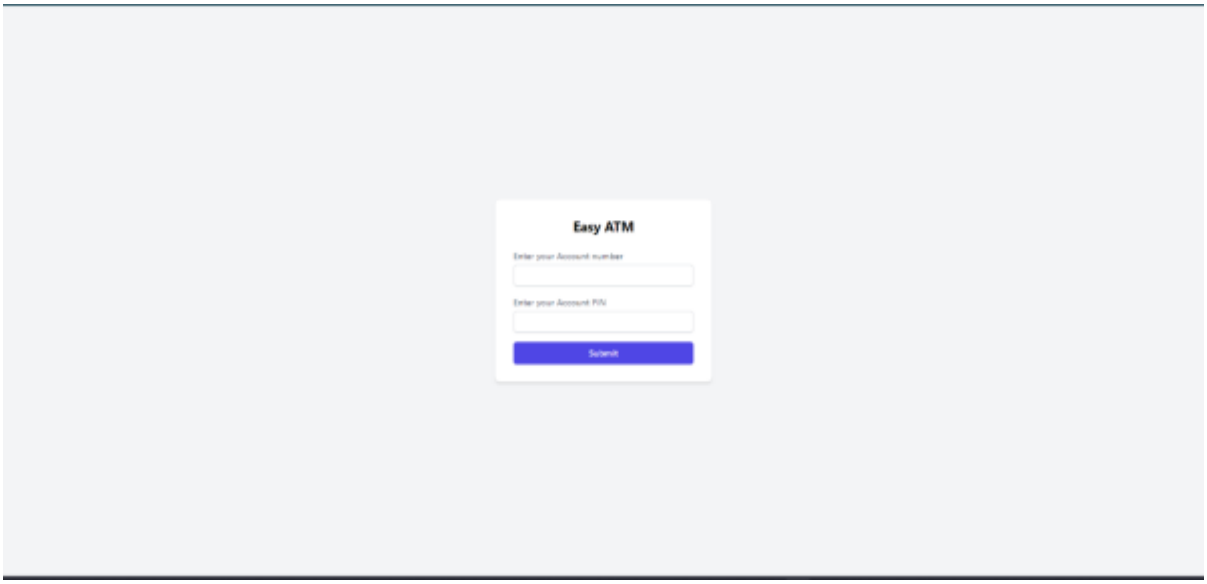


Figure 13. Login Page of the ATM system application

### 3.3.2 Face Authentication Page

The Face Authentication page is the page where the user is asked to open the camera and the face recognition module starts looking for face, upon successful facial authentication of the user, the user is directed towards the Home page of the ATM application where he can perform all the operation.

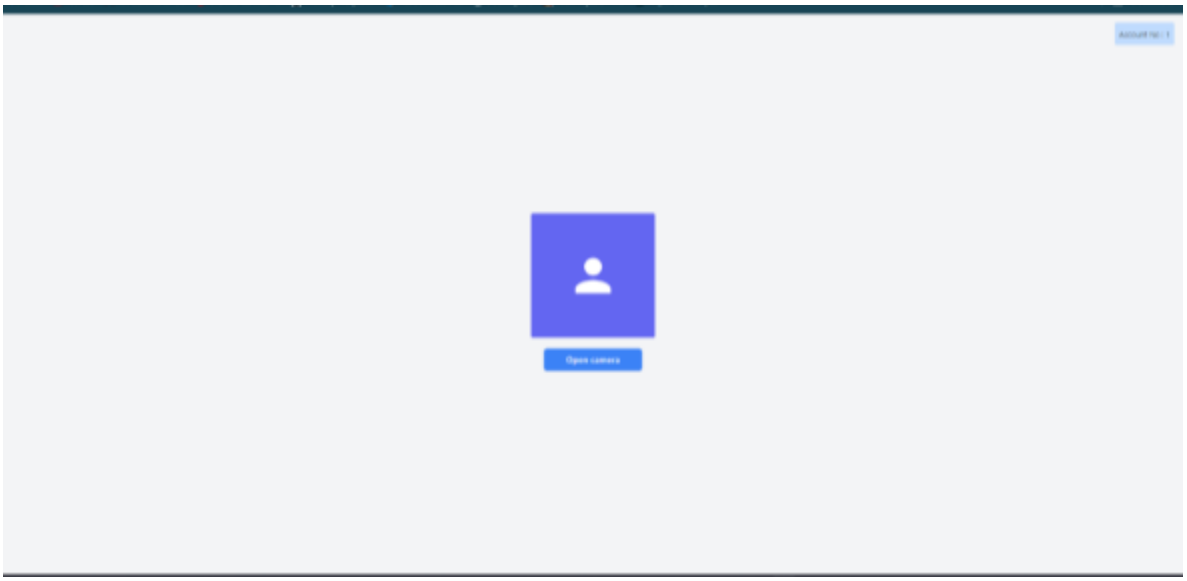

Figure 14. Snapshot of the Face Authentication Page from the ATM system application

### 3.3.3 Home Page

The Home Page as the primary window for a user after they have entered their user name, password and facial recognition. This Page offers the users a menu from which they can conduct all the ATM transactions such as deposit, withdrawal, balance check and transaction history check. The Home Page is constructed in such a way that it meets the needs of all the customers and at the same time is easy to use. The interface has understandable and concise choices for every activity related to banking and thus makes the process easier for users. Also, there is a voice button which is easily seen, and this is for the multilingual voice recognition where operations can be done through voice.

**Key features of the Home Page include:**

**Deposit and Withdrawal:** This way, users are able to transfer money into or out of their accounts with ease through easy to understand prompts and confirmation messages.

**Balance Inquiry:** A special part of the application helps the user to determine the current balance and shows the current state of the account.

**Transaction History:** The same also provides a detailed record of the user's transaction history in the form of date, amount, and type of the transaction allowing the user to track his or her financial activities.

**Voice Recognition:** The voice button allows the users to carry out the transactions using the voice commands in any language of their choice thus making it easier to use especially to the disabled persons or those who have the preference of speaking to a machine.


Figure 15. Snapshot of the Home Page from the ATM system application

### 3.4 Database Design

The ATM system uses MongoDB Atlas, a NoSQL based cloud database service to manage and store a large amount of data and perform complex as well as transactional operations. Considering that the data to be stored can be of various formats pertinent to ATMs, such as user authentication and transaction processing, MongoDB's schema-free structure is beneficial.

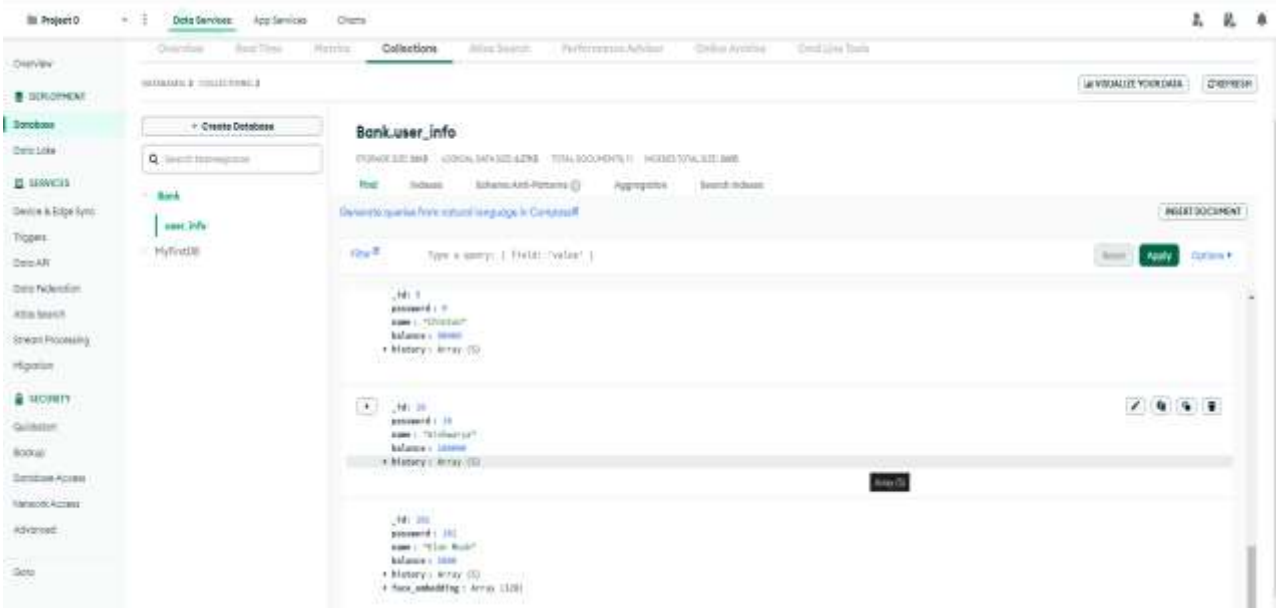


Figure 16. Snapshot of the MongoDB Atlas Database [18]

### 3.4.1 Design Overview

The database of the ATM system is well design to meet the basic function of the system including account management, transactions, and security. The design's main component is a set of collections in MongoDB where user data, account information, transactions and authentication records are stored. Each collection is organized in a way that makes it easy to search for and access the needed data, which allows the system to handle a large amount of transactions safely [9] [17].

Key Collection and Its Structure:

The user_info collection, here, holds the documents that are related to user profiles. Fields include:

_id: A string which is a way of identifying each user individually.

account_no: Easiest identification number to remember.

account_pin: Encrypted PIN for user login, for instance, by the use of Passwords.

name: User's complete name is as follows.

balance: The present statement of the account.

history: List of all the transactions made in the form of records showing each transaction made.

face_encoding: Facial recognition information that have to be encrypted. data.

## 3.5 Development Languages

The ATM system uses various programming languages and technologies to implement all its components, based on the best language/technology for each part of the system; the UI, business logic, and data storage.

### 3.5.1 React for Frontend Development

The graphic user interface of the proposed ATM system is implemented using the React framework. React is a JavaScript library used for creating reusable web components that are specifically efficient in creating user interfaces. The component based design of the application permits to create and implement individual and reusable code that is necessary to keep the interface of ATM

uniform across the various screens. The use of the Virtual DOM by React helps to make changes promptly only on the segments that are required, for instance, to display the balance, history of transactions or the authentication process [15] [17].

Therefore, due to the vast library of React and the large community that supports it, there is a high rate of development and sustainability of the ATM frontend. This framework is well suited for the management of the state and the integration with other libraries that are written in JavaScript which makes it a suitable choice for creating applications with fluid and interactive user interfaces.

### 3.5.2 Python for Backend Services

The programming language that is mostly used for the backend of the ATM system is Python. Python is easy to learn and flexible to use and thus can be used to implement fundamental functions like user authentication, handling of transactions and interaction with database [17]. The Flask framework on Python is used to design APIs that manage requests from the frontend so that there is proper interaction between the user interface and the backend services [1].

Due to the abundance of libraries and modules in Python and readily available third-party packages, it is possible to incorporate specific functionalities such as facial recognition and multilingual voice recognition [3]. These functionalities increase the security aspect of the system as well as the usability which is suitable for the ATM system as it requires a strong authentication process as well as efficient transaction processing.

### 3.5.3 MongoDB Atlas for Database Management

For the management of the database of the ATM system, MongoDB Atlas a cloud based NoSQL database is used. The nature of MongoDB's document store model allows it to store data of different types and structures, for instance, user information, transactions, and credentials. This schema less design of the model is also considered as advantageous since it facilitates easy expansion and modification of the model in the banking environment [9].

The SQL (Structured Query Language) operations are also eliminated by the query language of MongoDB which provides the simple CRUD (Create, Read, Update, and Delete) operations on collections including users, transactions, and logs. This capability assures the proper handling of data and information, which is vital in transactions as well as user information.

# 4. Implementation

## 4.1 Front End Design

### 4.1.1 Technology Framework

The web technologies used in the development of the ATM project enable the application to have a good, intuitive interface that adjusts to the size of the screen being used. The primary frameworks and tools used include:

React. js: Chosen because of the component based approach, the framework selected is React. The use of js is beneficial in the creation of the UIs especially the interactive ones. It plays a role in controlling the state of the application and makes the UI update properly when the data changes.

Tailwind CSS: This utility first CSS framework is used for the styling of the application. Tailwind CSS has a collection of pre-defined classes which makes the job easier in creating responsive and good looking ui without the need of writing a lot of custom css.

React Router: Used for business application navigation. To make the applications easily understandable and more user friendly, React Router helps to navigate from one page to another in a very declarative manner.

State Management: Even though this example is quite simple and uses the React's built-in hook called useState, there are more advanced libraries for state management like Redux or using Context API [9].

### 4.1.2 Interface Layout

The interface of the ATM application is developed in a way that it is easily understandable and easily navigable. Key components of the layout include:

Login Screen: The first interface in which the user has to input the card number and the PIN to get into the account.

Dashboard: After logging in, users are then directed to a page which contains different services that one can make including balance check, withdrawing, and depositing.

Transaction Screens: A different screen for balance check, withdrawal, and deposit with spaces for inputs and labels for buttons.

Responsive Design: The layout is well thought out so that the application will function properly on any device, including desktop, tablet, or mobile devices. It is made possible by the use of Tailwind CSS's responsive utility classes.

#### 4.1.3 Interactive Components

The application includes several interactive components to enhance user engagement and functionality:

Buttons: To submit forms and make actions which lead to certain operations. These buttons are colored and they alter their color when the mouse pointer is over them or when they are clicked to yield a feedback.

Input Fields: Input data (e. g. , withdrawal amount, deposit amount) are introduced in these fields by the users. The fields are arranged in a way that they can easily be seen and also get to be selected.

Icons and SVGs: Some of them are used for indicating certain operations or states, for instance, the face recognition icon on the face scan screen.

Modals: Modal dialogs are used for voice command input and confirmation message. When the microphone button is clicked, a modal pops up informing the user that the system is now in a voice recognition mode.

#### 4.1.4 User Experience Enhancements

To improve user experience, several enhancements are implemented:

Feedback Messages: This is notified to the user through error messages when they provide wrong input such as entering a string for the withdrawal amount. Success messages indicate that the transaction has been done.

Loading Indicators: Feedback elements are displayed as the application considers a request, thus, notifying the user the action is being worked on.

Animations: Worse still, there are no transitions like when buttons change color when you hover over them to give the interface a more alive feel.

Voice Commands: They also can make the transactions using the voice commands, which increases the convenience of using the application.

#### 4.1.5 Accessibility Features

The application is designed with accessibility in mind, ensuring it is usable by people with various disabilities:

Keyboard Navigation: All interactive elements can be triggered and manipulated with the keyboard which make the application compatible with motor disabled people.

Aria Labels: ARIA (Accessible Rich Internet Applications) roles are used to give more semantic information to the screen reader, which increases the possibilities of using the web page for the visually impaired.

High Contrast Mode: The application has a feature where it has a high contrast option that enhances the visibility to the users with low vision.

Voice Feedback: Important actions and errors are accompanied by the voice feedback thus enhancing the application's usability to users with visual impairments.

#### 4.1.6 Integration with Backend Systems

Although this project currently uses mock data, it is designed to integrate seamlessly with backend systems in a real-world scenario:

Mock Data: It stands for the fake data that is used to make the frontend work and be tested without a real backend.

API Endpoints: The application is designed to interact with RESTful API to handle the transactions, balance check and other functionalities with the help of Flask.

Data Flow: There is proper communication between the front-end and the back-end and state updates are instant. This guarantees that the client will not experience any inconvenience as they use the application.

## 4.2 Database Utilization

### 4.2.1 Database Configuration

In the ATM project, the database is optimized for storing users' information and their transactions as well as account balances. Key aspects include:

Database Type: To save data of different structures and for its versatility, a NoSQL database such as MongoDB Atlas is used.

Configuration Files: Some of the important DBMS parameters such as connection details, username and password and connection pooling options are stored in environment variables and configuration files to make them easily configurable and secure.

### 4.2.2 Setting Up the Development Environment

Setting up the development environment involves configuring the local machine to run the database and connect it to the application:

Installation: Ensure that you have MongoDB Client Installations or you can use MongoDB Atlas for database management if the database is hosted on the cloud [9].

Environment Variables: Define some environment variables where you will be storing information that may be considered as confidential like the MongoDB connection details.

Migration Tools: For managing the schema changes of the database and maintaining the same schema in all environments, one can use some migration tools like Mongoose or tools provided by MongoDB.

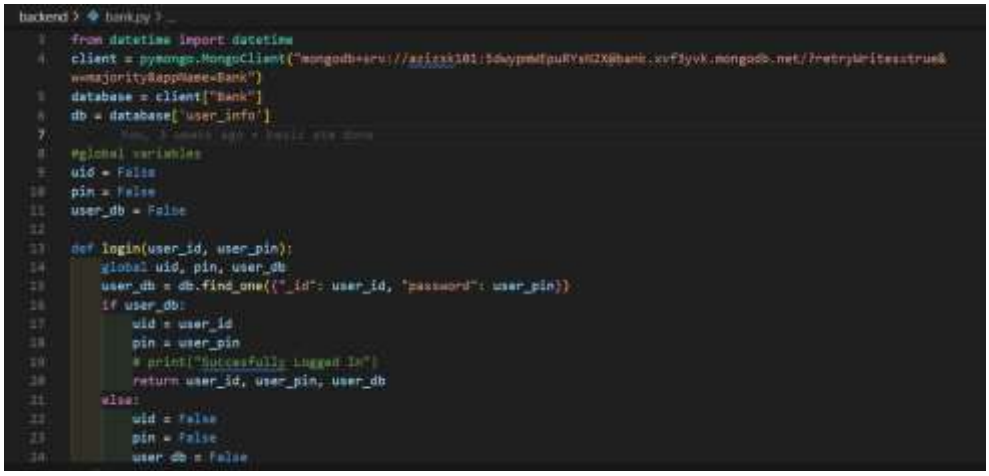


Figure 17. Code snippet of the MongoDB atlas connectivity to the Application

### 4.2.3 Database Creation and Schema Design

The database schema is designed to ensure data is organized efficiently and relationships between entities are clearly defined:

Collections: Develop a collection that is to be called user_info.

Schema Design: Develop the schema to help in storing and retrieving of data in the best way possible. The user_info collection includes the following fields:

_id: This contains a unique identifier for every user which is automatically assigned by MongoDB.

account_no: User's identification number.

account_pin: User's account PIN – This is a numerical password the user sets for their account and is the only information that is store in the system database of the application.

balance: The amount that the user has currently in his/her account.

name: User's name.

history: This paper presents a list of transactions of the user in chronological order.

face_encoding: Facial features used in the storage of information in a database.

### 4.2.4 Data Integrity and Relationships

Ensuring data integrity and properly defining relationships between entities is crucial:

Primary Keys: Make sure that _id field is used to create a unique index for records in the user_info collection.

Constraints: Although MongoDB is schemaless, it is possible to use Mongoose or other such libraries to specify validation on fields such as: field is required, field can only be of this data type, etc.

Referential Integrity: MongoDB does not support foreign keys as in the case of SQL, but the application has to do some workarounds to enforce referential integrity where required.

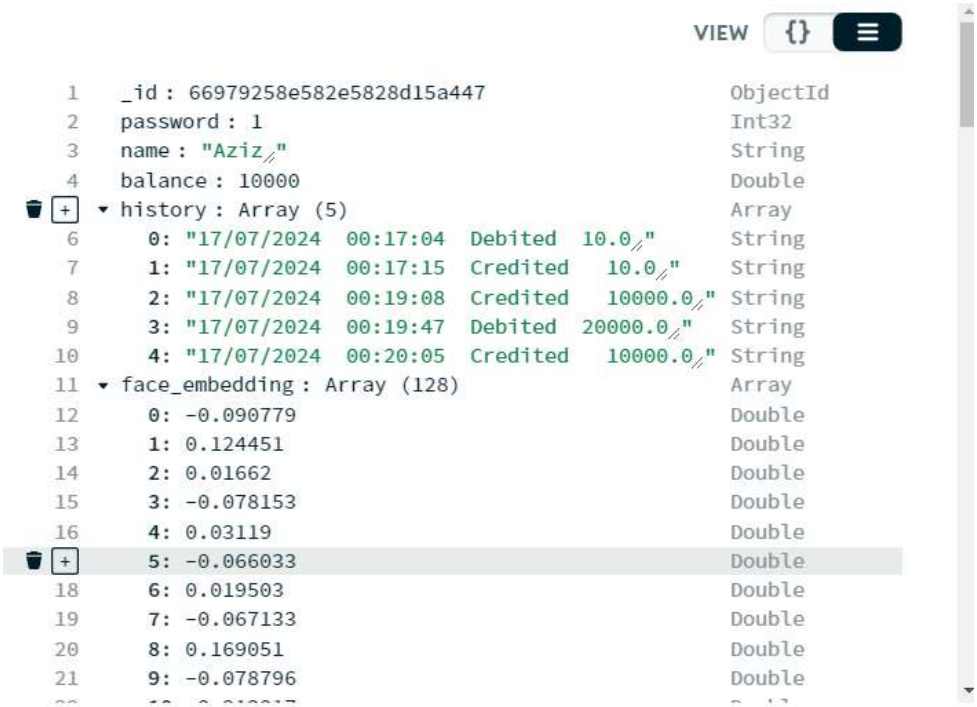


Figure 18. Snapshot of the fields in a record in the Database [18]

### 4.2.5 Data Integrity and Security

Encryption: Secure all the information that is considered as sensitive (for instance, account PINs, transactions) while at rest and in transit.

Access Control: It is recommended to apply RBAC to set up access control on the basis of certain roles and positions to prevent unauthorized users from accessing the information.

Backup and Recovery: Some of the recommendations are backup of data and recovery of data. MongoDB Atlas has the feature of backup and restore.

### 4.2.6 Connection Handling

Efficient handling of database connections ensures optimal performance and reliability:

Connection Pooling: To optimize the database connection and minimize the overhead, the connection pooling should be used.

Timeouts and Retries: Add timeout and retry logic to gracefully handle transient failures and for better availability.

Monitoring: Keep an eye on the database performance and the connections and find and solve the problems before they occur. MongoDB Atlas offers some features for the management and tuning of the database performance [9].

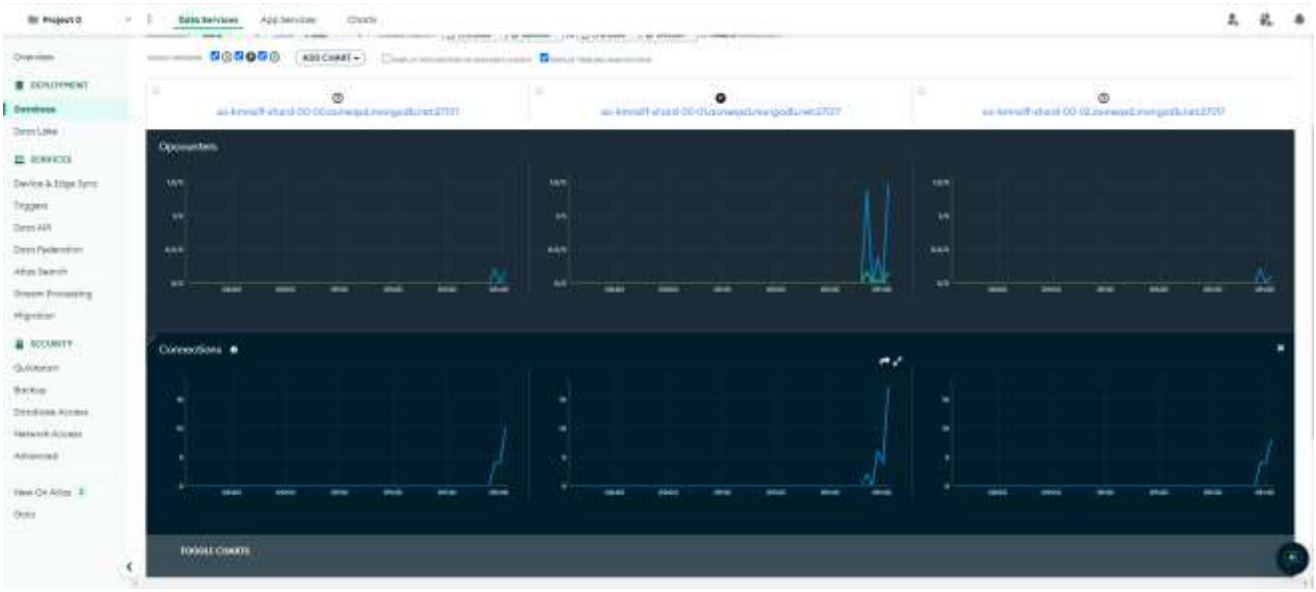


Figure 19. Data Monitoring in MongoDB Atlas [18]

# 5. Testing and Evaluation

The testing and evaluation are crucial in the development of the ATM system particularly due to the fact that the ATM system will be very complicated and will involve the facial and voice recognition besides the advanced data management systems [6]. To this end, this section looks into the various methods and strategies that have been employed in the ATM system to enable it to operate optimally and securely as it meets the various technical specifications and the customer.

## 5.1 Unit Testing

The unit testing is used for checking the functionality of the particular units or the modules of the face recognition system and the handling of the backend data. To verify the functionality of each unit the system is tested in isolation.

Scope: Verify the proper working of individual functions, methods, and classes used in face detection, feature extraction, and database.

Tools: Use testing frameworks like JUnit, pytest, or NUnit to make tests and run them. Process: Test each unit, create test cases, and check that the actually obtained results are the same as the expected ones.

Examples: Verification of the reliability of facial recognition techniques, effectiveness of the used features for face recognition, and confirmation of the proper reading and writing operations of the database.

## 5.2 Integration Testing

Integration This stage of testing checks how two or more integrated modules function and produces the expected output.

Scope: Check the correct functionality of the interactions of physical components like cameras with the software components like OpenCV, TensorFlow and the back end systems.

Tools: For integration testing, it is advisable to use the Selenium, TestNG or Postman for API testing. Process: Design the test scenarios that include all the end to end functions, run tests and verify the data and its working condition.

Examples: We will test entire process from capturing the face image, preprocessing face image, feature extraction and comparing with the data stored in the database.

### 5.3 System Testing

System testing is the process of testing the complete and integrated face recognition and backend data handling system to check whether the system is able to meet the stated requirements as intended.

Scope: Carry out tests on the whole complex of apparatus and programmes incorporated into the system.

Tools: System Testing tools like HP ALM, TestRail or Manual Testing techniques can also be used.

Process: Run full test cases based on actual use cases, check whether the system satisfies the functional and non-functional requirements, and discover the issues.

Examples: Checking the system's behavior concerning lighting conditions, confirming the user's identification across various situations, and stress testing the system.

### 5.4 Security Testing

It verifies the feature and its attendant database for possible security threat and attacks that may be inherent in the system.

Scope: Evaluate the system security features such as the use of encryption, access control and measures against common security threats.

Tools: Some of the security testing tools that you should use include the OWASP ZAP, Burp Suite, and penetration testing frameworks.

Process: Carry out vulnerability assessments, penetration testing and security audit. Discuss possible problems related to the security.

Examples: The three types of CSC are cross-site scripting (XSS), the strength of data encryption, and the security of data transfer.

### 5.5 Usability Testing

Usability testing is a crucial phase in the development of the ATM system, aimed at assessing the user-friendliness and ease of use of the face recognition system and the overall user interface. The scope of this testing includes evaluating the usability, aesthetics, and learnability of the interface to ensure a seamless user experience. Various tools, such as User Testing, Morae, and simple manual testing with direct user feedback, were employed to gather comprehensive insights.

The testing process involved developing realistic use-cases that simulated typical user interactions with the ATM system. Participants were observed to understand their behaviour, thoughts, and actions while using the system. This data collection was instrumental in identifying areas for improvement and making necessary design modifications. Key aspects under scrutiny included the ease of capturing the user's face image, the clarity of on-screen text, and the overall satisfaction with the authentication procedure.

The usability testing involved 50 diverse users, representing a broad spectrum of demographics to ensure comprehensive feedback. These users were asked to perform a series of tasks, including face recognition for authentication and navigating through the various features of the ATM interface. Their feedback was meticulously recorded, focusing on their experiences, difficulties encountered, and suggestions for improvement.

The feedback from users was overwhelmingly positive, particularly regarding the intuitive design and ease of use of the interface. Many users appreciated the straightforward instructions and the quick response of the face recognition system. However, some users highlighted areas for improvement, such as the need for better guidance during the initial setup of facial recognition and slight adjustments to the on-screen text for improved readability.

Based on the feedback, several iterations were made to enhance the user experience. These included refining the face capture process to be more intuitive, enhancing the clarity of on-screen instructions, and making aesthetic adjustments to improve the overall visual appeal of the interface. This iterative process ensured that the final design was not only user-friendly but also met the high standards of usability and accessibility required for an ATM system.

## 5.6 Testing Outcome

The proposed ATM system with facial and voice recognition testing approach has been very useful and efficient as per the results obtained and played a positive role in all the test categories. It has to be noted that all the above results have been the basic validation of the system as regards its functionality, security and end user's acceptance. In this section we shall discuss the outcomes of the testing phases and what can be learned from them in the light of the final system performance and reliability [6].

### 5.6.1 Unit and Integration Testing Results

Record unit and integration test results and any problems and solutions that were identified. Summarize the Test Cases executed, the number of Tests, the number of Tests passed/failed and Critical Bugs identified.

Details: Number of unit tests conducted and number of integration tests conducted along with their pass rates. Document any and all major flaws and their fixes.

### 5.6.2 Security Testing Results

Describe the findings from the security testing and any open issues and how they were addressed. Convey the totality of the security state of the system.

Details: Enumerate and explain some of the most critical findings of penetration testing, measures taken to mitigate the risks and any remaining threats.

### 5.6.3 Usability Testing Results

Summarize the results of the usability test; users' quotes, identified problems, and changes made to design to address the issues.

Details: Incorporate the user satisfaction rating, Usability metrics that can be identified and the improvement made on the usability.

### 5.6.4 Compliance and Regulatory Testing Results

Ensure that the system complies with the set legal and/or industry standards and regulations. Describe the tests done and results and any changes made to make the system meet the set compliance.

Details: Ensure that the document complies with the industry standards and data protection laws and any certification done.

## 5.7 Implications Based on Test Results

### 5.7.1 Enhancing Facial Recognition Accuracy and Robustness

Thus, based on given test results, it is possible to identify the ways that can help to enhance the facial recognition system's effectiveness and reliability.

Actions: Develop better algorithms, improve the data preprocessing, and improve feature extraction process. Ensure that there is a constant update of the training set with various images of faces.

### 5.7.2 Scalability and System Architecture Optimization

Evaluate the system under high stress and provide recommendations to improve the system's capacity and effectiveness.

Actions: Minimise the use of database queries, use load balancing and opt for cloud computing options for future expansion. Apply the performance monitoring tools to determine and eliminate the performance problems.

### 5.7.3 Advanced Security Protocols and Data Protection

Thus, it is necessary to implement a multi-level approach towards the security of the banking system to protect it from the new and increasing threats as well as to maintain data protection. MFA should be put in place as one of the ways of enhancing the security of the users' credentials. This is because it involves the use of two or more independent factors for example passwords, tokens and or biometric for instance fingerprint or iris scan to increase the authentication process. Other dynamic tokens such as time-based one time passwords (TOTP) that are sent via SMS or authenticator applications can also be used to enhance security. The use of biometric identification

mechanisms like using the face or fingerprints to identify the user adds more security on the user authentication process.

Higher level of encryption is necessary to secure information both within storage and in transmission. Such algorithms like AES-256 make it very hard to decrypt the data even if it has been intercepted to something that can be understood. End to end encryption makes sure that the data in transmission is encrypted from the sender to the receiver. Thus, the usage of PKI for the purpose of secure communication, digital signatures, and authentication processes along with the usage of SSL/TLS for web communications offers a reliable method for protection of data integrity and confidentiality.

To enhance the safety of the system, it is advised to conduct the security audits on regular basis. Scheduled audits and penetration testing can be used to detect and eliminate the possible risks before they become glaring issues. It is equally important to conform with the norms and policies concerning security, including GDPR and PCI-DSS norms. This is advantageous since the security assessments are done by independent third-party security professionals who offer a thorough assessment of the system's security and its compliance with the best practices in the industry as well as the legal framework.

Another key measure is that of strict access control measures as well. RBAC restricts access to the data and systems to only the extent that is required for the user's job function, which is the principle of least privilege. Regular audits of access permissions ensure that access is as it should be, and can be adapted when someone's position changes or they leave the organization. This way prevents insider threats and accidental data leaks because access to the sensitive data is granted only to the persons who are allowed to have it.

Surveillance of activities is a vital component of any sound security plan as it helps detect any irregularities. Use of IDPS in network traffic analysis in real-time can assist in identification of intrusions and prevent occurrences. Sophisticated behavioral analysis can recognize an unusual activity and possible risks by their behavior's patterns. Implementing a strong incident response plan will help security incidents to be addressed and contained fast and thus reduce the impact and risk of data loss.

Therefore to Ensure the effectiveness of the banking system and its safety against the increasing risks, there is the necessity to embrace these advanced measures of security. Security measures include multi-factor authentication, encryption, security assessments, access controls, and surveillance are some of the measures that should be employed in any organization. Thus, adopting these measures, the system can provide strong data protection, preserve the users' confidence, and avoid potential threats.

Actions: USE several forms of Authentication, ENCRYPT data using strongest possible encryption, and do security checks frequently. Enforce the access control measures and watch out for unusual behaviors.

## 6. Conclusion

The ATM system that has features of face recognition technology is one of the most modern trends of the banking sector automation [16]. The major goals included increasing the security standards, increasing the users' convenience, and speeding up the transactions. For facial recognition, we used OpenCV; for voice recognition, googletrans [6]; MongoDB Atlas for storing data; Python and Flask for the backend; and React for the frontend design. Thus, the use of these technologies secured, simplicity, and effectiveness of the system [3].

My security upgrade mainly relies on OpenCV that is enriched with facial recognition features. Thus, by using the Haar Cascade classifiers [11], we were able to detect facial features in a fast and accurate manner to enable the user verification. This technology also enhances the security by denying access to unauthorized persons while on the same note, it makes the process of logging in easier since one does not have to input a PIN or a password. The efficiency of OpenCV algorithms is a guarantee of the product's high performance and comfort for the user [5].

Googletrans was incorporated for voice recognition and this made the system more convenient and friendly to use. Through this, users can be able to transact business with the ATM in the language of their choice thus eliminating linguistic barriers in the delivery of banking services. The voice recognition component is to enable the handling of multiple languages and give audible prompts to the user throughout the transaction. This feature is very useful for users who may have challenges in using the touch interface of the device.

This is where MongoDB Atlas was used in order to handle the substantial volumes of biometric data containing information that is rather sensitive. These two features make it germane to dealing with the data structures that are characteristics of facial recognition and voice command. MongoDB Atlas provides that the data is safe by using strong encryption and meeting the legal requirements on protection of data across the globe. This makes the database to easily work hand in hand with other parts of the system to make sure that data can be easily transferred from the front end to the back end.

Python and Flask have been selected for the backend part owing to their flexibility and simplicity. Flexibility of Flask helped in the development of the backend part of the application that was

designed to be interactive and fast, providing user authentication, data handling, and interaction with the frontend. Python offered quick and effective development and deployment with the abundance of libraries and tools which could be used for the purpose [1].

The frontend part of the application was implemented using React which offers a sleek and easy to use interface to the users. Due to the utilization of the React library, we were able to design an interface that is easily adjustable to the user's actions in real-time due to the use of components. The design follows the principle of minimalism and simplicity, so the user can easily understand the interface and quickly perform the desired actions.

During the development of the system, a number of tests, as well as repeated steps, were carried out in order to increase the stability of the system and its protection. Feedback from the users was used in the fine-tuning of the interface and enhancement of user satisfaction. Thus, constant analysis of the system and its regular adjustments prevent it from becoming vulnerable and help meet the ever-changing requirements of users and new technologies.

Thus, the implementation of facial recognition and voice recognition technologies into the ATM system can be considered as a great advancement in banking automation [16]. With the use of OpenCV [5], googletrans, MongoDB Atlas, Python, Flask, and React, we came up with a secure and efficient system that improves the banking experience of all the users [3]. This new concept of ATM opens new possibilities of advanced security and friendly design for the customers of today's banking services.

### 6.1 Summary

The establishment of the ATM machine that has face recognition feature is a proof of the enhanced banking automation [16]. The goals set were to increase on security, ease of use by the user, and accelerate the process of transaction. For the implementation of the facial recognition we have used OpenCV [4], for voice recognition we have used googletrans, for data management and storage we have used MongoDB Atlas, for backend we have used Python and Flask and for the Front end we have used React. Thus, the mentioned features made it possible to create a secure, convenient, and efficient system based on these technologies [3].

My project objectives were to increase the security of ATMs through face recognition, increase users' convenience through voice recognition, increase the effectiveness and efficiency of transactions through optimization, and maintain data consistency and security using MongoDB Atlas. To achieve these goals, we employed a variety of technologies: In order to develop the backend API, I have used Python with Flask, for the user interface, I used React, for storing the user data, transaction history and account balances I used MongoDB Atlas, for implementing the face recognition feature I used OpenCV and for voice command I used googletrans [5].

The development process included first designing and implementing the backend API using Flask, and the frontend with the help of React; this was followed by the integration of MongoDB Atlas for data storage and management [9]; the integration of facial recognition using OpenCV and voice recognition using googletrans. To guarantee the system stability and to meet the needs of the users, constant testing and updating were done [4] [5].

Some of the major achievements of the project include the efficient implementation of face recognition, thus boosting the security of the system, increasing the rate of transactions and the satisfaction of the users and the proper storage and retrieval of data through the use of MongoDB Atlas. Also, the simple user interface based on React was well received by the users, confirming that the system was efficient and useful.

## 6.2 Critical Evaluation of Achievements

### 6.2.1 Data Management and Integrity

Effectiveness: The implementation of MongoDB Atlas in the data management process was very efficient. It offered a scalable and efficient way of managing users, transactions and accounts balances respectively.

Data Integrity: To ensure the data integrity, schemas and validation rules were used. The system made sure that all the details of the transactions are properly documented and the information created and/or updated by the users are credible.

Security: Structurally, there was data encryption of account PINs and facial encodings both when the data was in use and when it was in transit. Security was improved by limiting the access of data according to the role of the person using it and other measures.

Efficient Retrieval: The indexing of the most often queried fields, as well as the usage of effective query structures, made it possible to retrieve data quickly, which also positively affected the system's functioning.

### 6.2.2 User Interface and Accessibility

Design: The frontend had been developed on the React framework, which gave the interface a clean, simple, and efficient look. The design aspect of the system had taken into consideration the usability and accessibility to ensure that everyone including the disabled could be able to use the ATM system.

Usability Testing: To understand the users' perception of the system, usability test was carried out to gather user inputs. The findings suggested that the interface was easy to use and well received by the users. Some changes have been done according to the feedback to enhance the accessibility to users with disabilities.

User Feedback: People liked it when they could use voice commands and facial recognition to make the identification process faster and simpler, and make the application more user-friendly.

### 6.2.3 Operational Efficiency and User Experience

Performance: The system proved to be very efficient in terms of operation with fast transaction times and very little downtime. Python and Flask for the backend together with the React for the frontend ensured the creation of a sound and stable platform [1].

Facial Recognition Accuracy: The application of OpenCV for recognition of the face was highly efficient and effective in the obtaining of high precision outcomes. Such testing together with constant tweaking of the algorithms made it possible to achieve high precision in different lighting conditions and angles [4].

Transaction Speed: Due to the enhanced back end and improved database query, transactions were processed at a reasonable speed to meet the users' desire and confidence.

User Experience: In conclusion, it was established that the users' feedback was quite encouraging, especially on the face recognition feature as being convenient and secure. The voice recognition feature which was also integrated in the system also improved the usability of the system.

## 6.3 Limitations

### 6.3.1 Environmental Sensitivity of Facial Recognition

One of the major issues that is being encountered when developing the ATM system is related to the issue of environmental influence on the facial recognition. Some of the challenges that affect the facial recognition include illumination changes, the pose in which the face is presented, and occlusion which could be a hat or glasses among others [4]. These environmental factors can produce false negatives or positive, meaning that the system's outcome is not accurate. In order to address these challenges several recommendations have been made. Such techniques include preprocessing that can be used to fix lighting and pose of the face. Also, more than one camera to take pictures of the user's face from different perspectives may increase the recognition rate. Also, the use of adaptive algorithms that can change their parameters and rules as they work can also help in the improvement of the facial recognition system as it can learn from the changing environment.

### 6.3.2 Dependence on High-Quality Hardware

There is also a concern on the hardware components of the system, particularly the high-resolution cameras used. However, such tools require high-quality hardware for their correct functionality, which is often expensive, as well as the problems with its maintenance and updates. There are also the cost factors, which can be significant especially for the large scale adoption of the technology. In view of these, it is important to enhance the quality of the hardware solutions that are more efficient but still affordable so that they can meet the middle ground between the two. To implement effective maintenance of the hardware components and timely upgrades that is required to maintain the durability of the system, the following should be considered.

### 6.3.3 Data Privacy Concerns

The biometric data, for example facial information, needs to be handled and stored which is a major concern of privacy. The protection of this type of data is crucial in order to avoid the intrusion of the users and thus safeguard their trust. The following measures must be put in place to enhance security of data: Strong encryption to be used in the data during transit as well as at the time of storage. Adherence to regulation that pertain to data protection especially the GDPR is crucial in the protection of user data. Implementing proper measures in storage of data and access to data

helps to minimize the risk of invasion of privacy since only the right people will have access to the information.

### 6.3.4 Scalability Challenges

This means that as the number of users increases and as more users simultaneously request to be authenticated, the performance of the facial recognition system will be affected. A large number of users and a high number of transactions may put a significant amount of stress on the system which may cause delays in response time and even crashes. The following measures can be taken to increase scalability. Some of the load balancing methods and mechanisms that can be used in handling the load balancing include; Cloud-based services provide adaptability and scalability whereby the system can easily accommodate different loads. Optimizing the queries in the database and enhancing the efficiency of the algorithms can also be very effective in high traffic situations.

### 6.3.5 Integration and Compatibility Issues

Incorporating the new facial recognition system into the current ATM software and hardware also poses a problem on how the two will co-exist with other operating systems and network configurations. Some of the causes include differences in the software versions, hardware, and network configuration. Thus, it is possible to detect and eliminate possible conflicts in the development stage by performing a comprehensive compatibility test. Defining the integration protocols and procedures helps to avoid problems with the integration with other systems and improves the functionality of the entire system.

### 6.3.6 Regulatory and Ethical Implications

Facial recognition technology has legal and ethical issues and that is why it should be well understood before applying it. It is imperative to adhere to the set legal requirements including those on data protection and privacy. This is because issues of ethics that include the act of revealing to the public how data will be used and seeking their permission to do so, are equally crucial in order to ensure confidence. One has to liaise with the legal bodies to know the laws and make sure the system complied with the legal use of the system. The principles that should be adhered to include; informing the users on the use of their data and seeking permission to collect and use their data.

## 6.4 Future Work

### 6.4.1 Enhancing Facial Recognition Accuracy

For the enhancement and reliability of the facial recognition system, further studies should be conducted on the enhancement of the algorithms and methods in use. Expanding the training set to include various faces and facial conditions will improve the system's learning capacity. Such models of continuous learning that can be updated and optimized over time with new data will also increase system performance. These shall help in increasing the reliability and efficiency of the facial recognition systems [14].

### 6.4.2 Upgrading Hardware Components

This paper presents various ways through which the system is likely to meet the increasing demands, which include acquiring high resolution and adaptive cameras, fast processors, and efficient storage solutions. Technological improvement in the hardware can help improve the efficacy and efficiency of the facial recognition system and its functionality regardless of conditions. This way, the system will always be up to date with the latest hardware technologies because of routine assessments and upgrade [4].

### 6.4.3 Expanding Biometric Options

Biometric factors such as fingerprints, iris, voice, will be added on to the system to enhance the multi-factor authentication. This linear approach greatly improves the security measures since there are different levels of authentication that need to be completed in order to access the intended resource. This will ensure that since the different biometric options will be provided, it will be suitable for any user and any situation, thus increasing the flexibility and satisfaction of the users [17].

### 6.4.4 Improving Data Security and Privacy

Continuous work on the improvement of the data protection is still important. Applying the stronger methods of encryption, performing the regular security check and being in the know of the latest rules on data protection will help in safeguarding information. Differential privacy can be used to protect the user data even when used for analysis by aggregation. These measures will help in sustaining the user confidence and meeting the legal standards.

#### 6.4.5 Cloud Integration

This is because cloud solutions for data storage, computation, and machine learning model hosting will improve system extendibility and adaptability. Cloud-based solutions are quite good in handling fluctuations in the traffic load as they are always reliable and available. This follow the fact that through the use of cloud services, it becomes easier to add or modify components, and thus contribute to the sustainability of the system in the long-term basis and its performance.

#### 6.4.6 UI and Accessibility Improvement

Some of the recommendations include carrying out frequent usability testing and integrating the user's feedback so as to enhance on the User Interface and the accessibility features. Therefore, following the best practices of accessible design makes it possible for the system to be accessible to persons with disabilities. Future improvements to the UI will ensure that it is easy to use and intuitive for the end user across the board.

#### 6.4.7 Information and Training

A detailed user manual, training modules, and support materials will also be of great assistance to the users and managers in the use of the system. Thus, holding training sessions and workshops will help to elaborate the system's usage and maintenance for all the parties involved. Thus, the continual education and assistance will improve the use of the system and the satisfaction of the users.

#### 6.4.8 Addressing Regulatory Challenges

It is crucial to know about new changes in the regulation and make the system correspond to the new rules. To maintain compliance in the future, the organisation should maintain communication with the regulatory authorities and incorporate the review of the documentation on a regular basis. Prevention of the existing regulatory risks will ensure the legal and ethical performance of the system.

### 6.5 Critical Review of the Project

#### 6.5.1 Highlighted Achievements

According to the information given the ATM system project has the following accomplishments. This paper also highlighted some of the major achievements that were made in the present model;

these include the integration of advanced technologies such as face recognition for user identification, handling of secure transactions, and a simple and easily understandable interface. The utilization of OpenCV for facial recognition and googletrans for voice recognition ensured that the user was well protected as it incorporated a biometric method of identification and a PIN entry method [5]. The graphical user interface of the system was built using React and was made very cascading and easy to use in order to enhance the user interface experience. Most of the users complained of high levels of satisfaction due to the implementation of a simple and fast interface [8]. The performance metrics showed that the system was able to process the transctions with high speed and low latency time, hence it means that the response time and the rate of transacting was fast. A complete set of measures was taken to secure user information with the help of data encryption and safe data storage to provide safe shopping.

### 6.5.2 Areas for Improvement

Although the project was rather successful, it has found several opportunities for the improvement. The first key area is to enhance the security functions. Despite the fact that current protocols are quite effective, it is possible to extend the use of multi-factor authentication to increase the protection [17]. This could include integrating the facial recognition with other biometrics such as fingerprints or tokenization such as SMS codes. Also, integrating more and more user feedback into the product development process can result in the constant enhancement of the interface and functionality. Improving the current error handling systems to display better messages to the users when they encounter a problem will improve their experience and hence boost their morale. Feature enhancement is also one of the main areas for improvement. Some enhanced features like, Transactions history, Balance notifications, and Financial advice can help the users to enhance their banking experience.

### 6.5.3 Scalability and Future Readiness

The matters of scalability and future-proofing are of utter importance when it comes to the system's design. The ATM system has been designed so that as the user base and the number of transactions grow, there is little or no degradation in the system's performance. Some of the key strategies that can be used to scale up include the use of load balancing, efficient query to the database and utilization of cloud base services in handling large load. It should also be related to future developments of the system including voice recognition, AI in customer support, and data

mining of relevant data. This will mean that at every given time, the system will be up to date with the latest technology and this will mean that the system will be performing to its best and also will be secure. This way proactive approach will ensure that the system is always up to date with the changing needs of the users and the ever-changing technological environment.

### 6.5.4 User Acceptance and Interface Usability

Ease of use and user acceptability were very important factors that governed the project from the beginning to the end. To collect the data and make sure the interface effectively met the needs of the users extensive testing was performed. Feedback was used to make the interface more simple and understandable to the user and to minimize the time it would take to familiarize new users with the interface. Another critical goal was to make the interface easily available to the users. The design adhered to the standard guidelines to enable users with disabilities to use the system without any challenges. Some of the positives that users provided feedback on included the effectiveness of the measures in improving the user interface and making it more user-friendly.

### 6.5.5 Regulatory and Ethical Considerations

The project adhered to the recommended guidelines regarding the legal and moral issues in order to be on the safe side and maintain the trust of the users. Approximation of all the relevant legislation, for instance, the General Data Protection Regulation (GDPR), was strictly observed in order to safeguard the privacy of the users. The use of facial recognition technology was done in a proper manner to prevent any form of prejudice and to achieve equality in the operation of the system. Accountability to the users with regard to the data gathering and utilization practices was observed at all times during the project. The participants were told on how their information would be utilized, managed and safeguarded in the system thus making them have confidence in the system. This way, the system not only adheres to the legal norms but also works in a proper and moral way to protect the users' privacy.

## References


[1] gyiernahfufieland, "ATM machine with Python," Medium, Mar. 19, 2021. https://medium.com/analytics-vidhya/atm-machine-with-python-d90b9ee300e

[2] Askar Boranbayev, Seilkhan Boranbayev, and Askar Nurbekov, "Java Based Application Development for Facial Identification Using OpenCV Library," Advances in intelligent systems and computing, pp. 77–85, Aug. 2020, doi: https://doi.org/10.1007/978-3-030-55187-2_8.

[3] "Building an ATM Machine Project using Python," Programming Boss: Programming for Beginners, Jun. 12, 2023. https://www.programmingboss.com/2023/06/building-atm-machine-project-using.html#google_vignette. [Accessed May. 21, 2024].

[4] A. Jaiswal, "Build Your Face Recognition System Using Python," Analytics Vidhya, Apr. 04, 2022. https://www.analyticsvidhya.com/blog/2022/04/face-recognition-system-using-python [Accessed May. 26, 2024].

[5] P. Nayak, "Building an Application for Facial Recognition Using Python, OpenCV, Transformers and Qdrant," Medium, Dec. 15, 2023. https://nayakpplaban.medium.com/building-an-application-for-facial-recognition-using-python-opencv-transformers-and-qdrant-a144871f40d9 [Accessed May. 28, 2024].

[6] "Create a real time voice translator using Python," GeeksforGeeks, Nov. 03, 2021. https://www.geeksforgeeks.org/create-a-real-time-voice-translator-using-python/ [Accessed 28 June 2024].

[7] GeeksforGeeks, "Voice Assistant using python," GeeksforGeeks, Feb. 14, 2020. https://www.geeksforgeeks.org/voice-assistant-using-python [Accessed June. 01, 2024].

[8] A. C. Codex, "How to Create a Voice User Interface with Python | Reintech media," reintech.io, Jul. 27, 2023. https://reintech.io/blog/create-voice-user-interface-python#google_vignette (Accessed Jun. 05, 2024).

[9] Mohit Codes, "Bank Management System - Python Database Project Complete," YouTube, Jan. 26, 2024. https://www.youtube.com/watch?v=KDIt2YO6euw. [Accessed Jun. 06, 2024].

[10] (PDF) the struggle for recognition in the age of Facial Recognition Technology, https://www.researchgate.net/publication/359103835_The_struggle_for_recognition_in_the_age_of_facial_recognition_technology [Accessed Jun. 6, 2024].

[11] R. Ranu, "Terminologies used In Face Detection with Haar Cascade Classifier: Open CV," Medium, Sep. 22, 2020. https://ai.plainenglish.io/terminologies-used-in-face-detection-with-haar-cascade-classifier-open-cv-6346c5c926c

[12] A. Rosebrock, "OpenCV Face Recognition," PyImageSearch, Sep. 24, 2018. https://pyimagesearch.com/2018/09/24/opencv-face-recognition [Accessed Jun. 10, 2024].

[13] Learning image processing with opencv | request PDF, https://www.researchgate.net/publication/280234357_Learning_Image_Processing_with_OpenCV [Accessed Jun. 12, 2024].

[14] PCE, "Facial Recognition Technology: Where Will It Take Us?," Prosecutors' Center for Excellence, May 30, 2019. https://pceinc.org/facial-recognition-technology-where-will-it-take-us/

[15] "ATM SOFTWARE USING JAVA SWINGS AND OOPS CONCEPTS," International Journal of Progressive Research in Engineering Management and Science, Oct. 2023, doi: https://doi.org/10.58257/ijprems32089.

[16] M. Mann and M. Smith, "Automated facial recognition technology: Recent developments and approaches to oversight," University of New South Wales Law Journal, vol. 40, no. 1, Apr. 2017. doi:10.53637/kavv4291

[17] M. O. Onyesolu and A. C. Okpala, "Improving security using a three-tier authentication for Automated Teller Machine (ATM)," International Journal of Computer Network and Information Security, vol. 9, no. 10, pp. 50–56, Oct. 2017. doi:10.5815/ijcnis.2017.10.06

[18] K. P. Ryan, "MongoDB," MongoDB, 25 August 2009. [Online]. Available: https://cloud.mongodb.com/v2/6683ca01c955685dc6df06e7#/overview. [Accessed 25 June 2024].