Improvising ATM Security via Face Recognisation

Nisarga K, Poornika J, Supriya M, Vaishnavi Desai, A T Sathynarayana Reddy
Department of Information Science And Engineering
Rao Bahadur Y Mahabaleswarappa Engineering College Ballari, Karnataka, India

Abstract*: Automated Teller Machines also known as ATM's are widely used nowadays by each and everyone. The ATM machine (Automated Teller Machine) is an electronic device that is usedby the banks to perform banking tasks like withdrawal of money, transferring of money, and many to get many information about a user's bank account without the need to visit a bank.Weare implementing a system where money will be withdraw using face recognition and pin authentication .If incase it fails it will shows display all the invalid pin details to police offices.*

Keywords: Automated Teller Machines

I. INTRODUCTION

Motivation:

The motivation behind implementing face recognition and PIN authentication in ATM transactions stems from the need to enhance security and user experience. Traditional PIN- based authentication methods are susceptible to fraud and theft, leading to financial losses for users and banks. By integrating face recognition technology, we aim to significantly reduce the risk of unauthorized access and fraudulent transactions. This advanced security measure not only provides users with peace of mind but also improves the overall ATM experience by eliminating the need to remember and input PINs for every transaction, making it more convenient and user-friendly.

Problem Statement:

Our project aims to develop a secure ATM system that utilizes both face recognition and PIN authentication for money withdrawal. The system will allow users to authenticate themselves using either their face or PIN. In case of authentication failure, the system will capture the invalid PIN details and notify the police authorities. This integration of advanced security measures not only enhances the user experience but also significantly reduces the risk of unauthorized transactions and fraudulent activities.

Objective of the project:

The objective of our project is to develop a highly secure ATM system that incorporates advanced biometric technology, specifically face recognition, along with traditional PIN authentication for money withdrawal. This system aims to provide users with a convenient and secure method of accessing their funds. In case of authentication failure, the system will capture the invalid PIN details and automatically notify the police authorities for further investigation. By integrating these advanced security measures, we aim to significantly reduce the risk of unauthorized transactions and fraudulent activities, thereby enhancing the overall security and reliability of the ATM system for both banks and customers.

Scope:

The scope of our project encompasses the development of a secure ATM system integrating face recognition and PIN authentication for money withdrawal. In case of authentication failure, the system will notify police authorities with the invalid PIN details for further action.

Project Introduction:

Automated Teller Machines (ATMs) have become an indispensable part of modern banking, providing convenient access to financial services. However, traditional ATM authentication methods, primarily reliant on Personal

Identification Numbers (PINs), are vulnerable to theft and fraud. To address these security concerns, our project proposes the integration of face recognition technology with PIN authentication for ATM transactions.

This advanced security measure aims to enhance the security and user experience by providing a more robust and convenient method for accessing ATM services. By combining face recognition with PIN authentication, our system will offer users a multi-factor authentication process, significantly reducing the risk of unauthorized access and fraudulent transactions. In case of authentication failure, the system will capture invalid PIN details and automatically notify the police authorities for further investigation. Our project will focus on developing and implementing this innovative system to provide users with a more secure and convenient way to access their funds, ultimately making ATM transactions safer and more reliable.

II. LITERATURE SURVEY

[1]" S. Chaudhary, S. Singh, and A. Sharma Enhancing ATM Security Using Biometric Technology"-2017 explored the integration of biometric technology, including face recognition, to enhance ATM security. The study emphasized the effectiveness of biometric authentication in preventing unauthorized access and reducing the risk of fraudulent transactions.

[1] " R. Jain, S. Upadhyay, and S. Shukla Biometric Authentication Systems for ATM Security: A Review" 2019: conducted a comprehensive review of biometric authentication systems for ATM security. The study discussed various biometric modalities, including face recognition, and their potential to improve security and user experience in ATM transactions.

[2] " V. Patel, R. Prajapati, and D. Patel Face Recognition Technology for ATM Security: A Review" 2020 reviewed the application of face recognition technology in ATM security. The study highlighted the advantages of face recognition, such as accuracy and convenience, and its potential to mitigate security threats in ATM transactions.

[3] " S. K. Singh, A. K. Singh, and N. K. Roy Biometric Authentication in ATM Banking: A Survey" 2018: conducted a survey on biometric authentication in ATM banking. The study discussed various biometric modalities, including face recognition, and their implementation challenges and security implications in ATM systems.

[4] " A. Yadav, S. Bhadauria, and A. Srivastava (2017) A Comprehensive Review on ATM Security Using Biometrics" 2017: provided a comprehensive review of ATM security using biometric technology. The study discussed the advantages of biometric authentication, including face recognition, in enhancing security and preventing ATM-related frauds.

III. SYSTEM ANALYSIS

The existing method for ATM transactions primarily relies on traditional PIN authentication. Users are required to input their PIN to access their accounts and perform transactions such as cash withdrawals and balance inquiries. However, this method solely depends on something the user knows, making it susceptible to fraud through stolen or guessed PINs. While some ATMs may also feature cardless transactions using mobile banking apps, the security level is still dependent on PINs or other authentication methods linked to the user's mobile device.

Disadvantages:

- Vulnerability to PIN theft: Traditional PIN-based authentication is susceptible to theft through methods such as shoulder surfing, card skimming, or phishing attacks.
- Limited security: Relying solely on PINs for authentication lacks robust security, as PINs can be easily forgotten, stolen, or guessed.
- Risk of unauthorized access: Stolen or lost cards can be misused for unauthorized transactions, leading to financial losses for users.
- Inconvenience: Users may face inconvenience due to the need to remember and input PINs, which may be forgotten or mistyped.

Proposed System:

The proposed method for ATM transactions involves integrating face recognition technology with PIN authentication to enhance security and user convenience. Users will register their faces with the ATM system, which will authenticate their identity by comparing it with the registered data. Additionally, users will enter their PINs for an added layer of security. In case of authentication failure, the system will capture the invalid PIN details and notify the police authorities for further investigation. This integration of face recognition and PIN authentication will significantly reduce the risk of unauthorized transactions, ensuring a higher level of security for ATM users..

Advantages:

- Enhanced security: Integrating face recognition with PIN authentication provides a higher level of security compared to traditional PIN-based methods, reducing the risk of unauthorized access and fraudulent transactions.
- Improved user convenience: Users no longer need to remember or input their PINs for every transaction, making the process more convenient and user-friendly.
- Reduced risk of PIN theft: Face recognition adds an extra layer of security, reducing the risk of PIN theft through methods such as shoulder surfing, card skimming, or phishing attacks work Flow of Proposed system
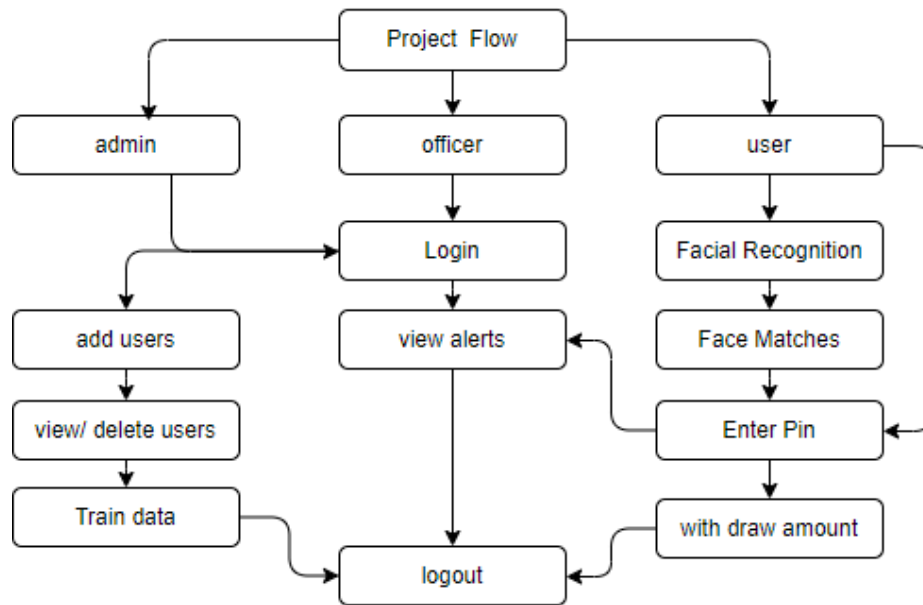
IV. REQUIREMENT ANALYSIS

Functional and non-functional requirements

Requirement's analysis is very critical process that enables the success of a system or software project to be assessed. Requirements are generally split into two types: Functional and non-functional requirements.

Functional Requirements: These are the requirements that the end user specifically demands as basic facilities that the system should offer. All these functionalities need to be necessarily incorporated into the system as a part of the contract. These are represented or stated in the form of input to be given to the system, the operation performed and the output expected. They are basically the requirements stated by the user which one can see directly in the final product, unlike the non-functional requirements.

Examples of functional requirements:

1) Authentication of user whenever he/she logs into the system

2) System shutdown in case of a cyber-attack

3) A verification email is sent to user whenever he/she register for the first time on some software system.

Non-functional requirements: These are basically the quality constraints that the system must satisfy according to the project contract. The priority or extent to which these factors are implemented varies from one project to other. They are also called non-behavioral requirements.

They basically deal with issues like:

• Portability

• Security

• Maintainability

• Reliability

• Scalability

• Performance

• Reusability

• Flexibility

Examples of non-functional requirements:

1) Emails should be sent with a latency of no greater than 12 hours from such an activity.

2) The processing of each request should be done within 10 seconds

3) The site should load in 3 seconds whenever of simultaneous users are > 10000

Hardware Requirements

- Processor - I3/Intel Processor
- Hard Disk - 160GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA
- RAM - 8GB

Software Requirements:

- Operating System : Windows 7/8/10
- Server side Script : HTML, CSS, Bootstrap & JS
- Programming Language : Python
- Libraries : Django, Pandas, Os
- IDE/Workbench : PyCharm,VSCode
- Technology : Python 3.6+

V. SYSTEM DESIGN

Introduction of Input Design:

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the input devices such as PC, MICR, OMR, etc.

Therefore, the quality of system input determines the quality of system output. Well-designed input forms and screens have following properties −

• It should serve specific purpose effectively such as storing, recording, and retrieving the information.

• It ensures proper completion with accuracy.

• It should be easy to fill and straightforward.

• It should focus on user's attention, consistency, and simplicity.

• All these objectives are obtained using the knowledge of basic design principles regarding −

o What are the inputs needed for the system?

o How end users respond to different elements of forms and screens.

Objectives for Input Design:

The objectives of input design are −

• To design data entry and input procedures

• To reduce input volume

• To design source documents for data capture or devise other data capture methods

• To design input data records, data entry screens, user interface screens, etc.

• To use validation checks and develop effective input controls.

Output Design:

The design of output is the most important task of any system. During output design, developers identify the type of outputs needed, and consider the necessary output controls and prototype report layouts.

Objectives of Output Design:

The objectives of input design are:

• To develop output design that serves the intended purpose and eliminates the production of unwanted output.

• To develop the output design that meets the end user's requirements.

• To deliver the appropriate quantity of output.

• To form the output in appropriate format and direct it to the right person.

• To make the output available on time for making good decisions.

UML Diagrams:

Use Case Diagram:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.
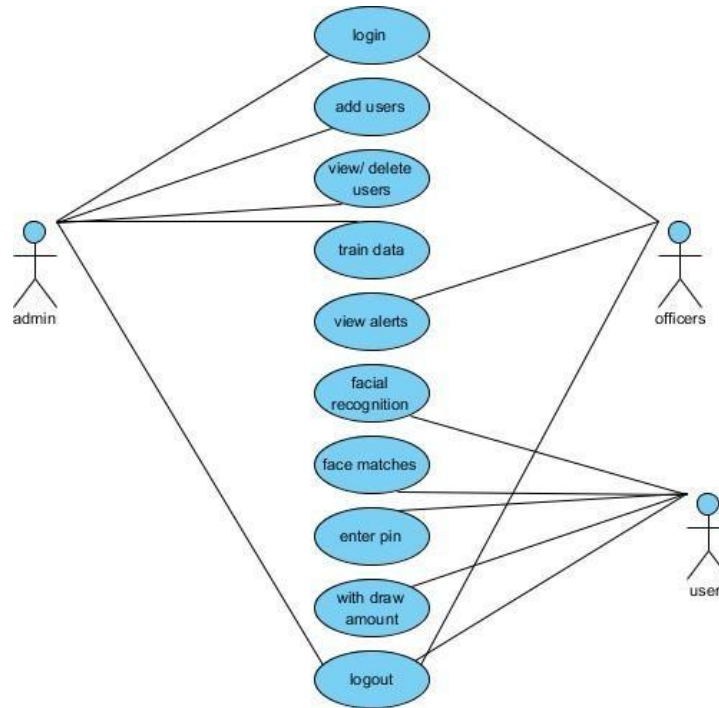
Class Diagram:

In software engineering, a class diagram in the Unified Modelling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information
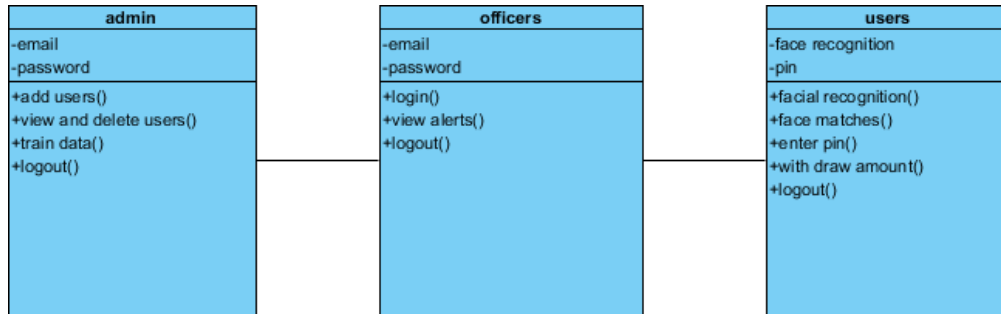

Sequence Diagram:

A sequence diagram in Unified Modelling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, eventscenarios, and timing diagrams.
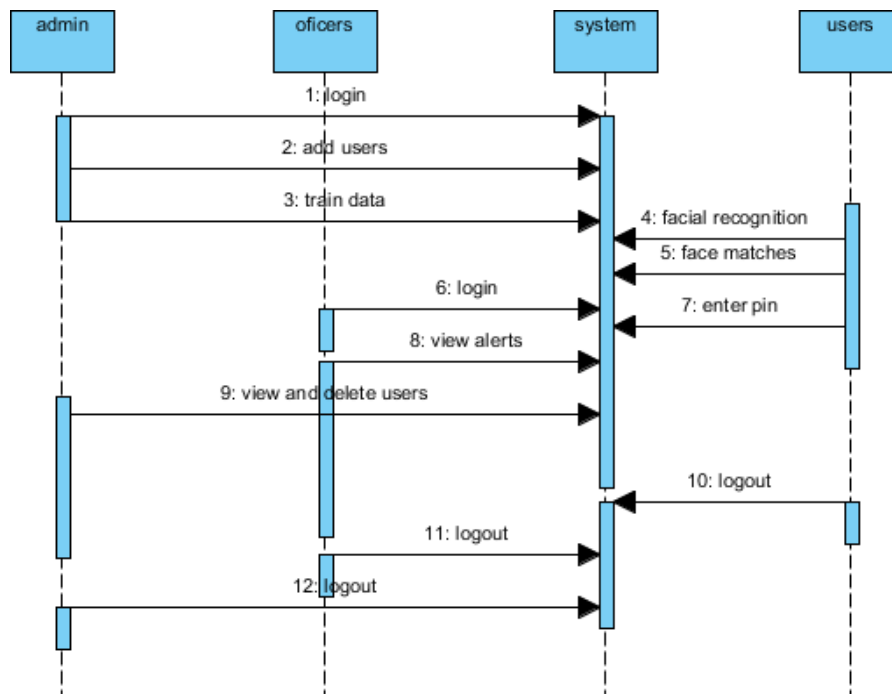
Collaboration Diagram:

In collaboration diagram the method call sequence is indicated by some numbering technique as shown below. The number indicates how the methods are called one after another. We have taken the same order management system to describe the collaboration diagram. The method calls are similar to that of a sequence diagram. But the difference is that the sequence diagramdoes not describe the object organization whereas the collaboration diagram shows the object organization.
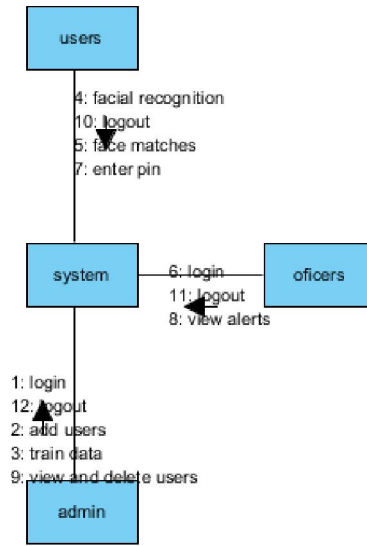
Deployment Diagram

Deployment diagram represents the deployment view of a system. It is related to the component diagram. Because the components are deployed using the deployment diagrams. A deployment diagram consists of nodes. Nodes are nothing but physical hardware's used to deploy the application


Activity Diagram:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.
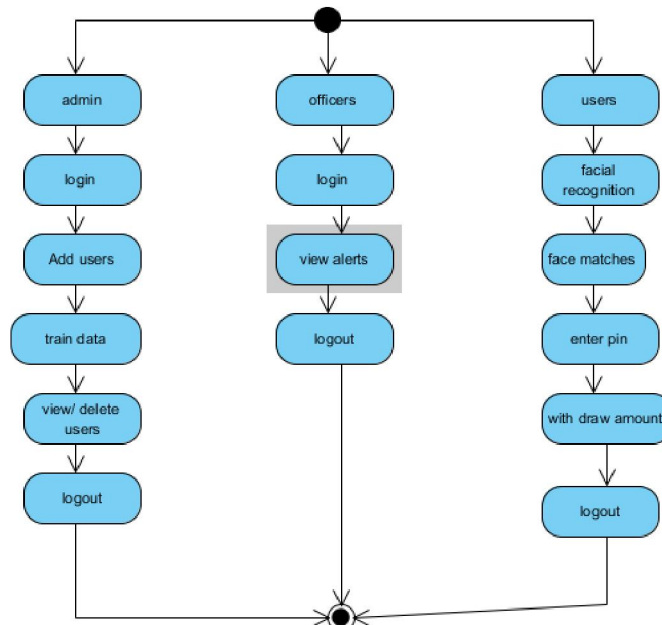
Component Diagram:

A component diagram, also known as a UML component diagram, describes the organization and wiring of the physical components in a system. Component diagrams are often drawn to help model implementation details and double-check that every aspect of the system's required functions is covered by planned development.
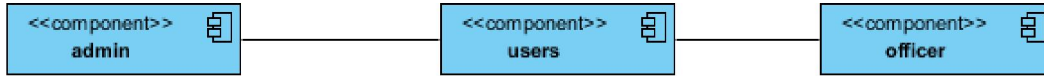
ER Diagram:

An Entity–relationship model (ER model) describes the structure of a database with the help of a diagram, which is known as Entity Relationship Diagram (ER Diagram). An ER model is a design or blueprint of a database that can later be implemented as a database. The main components of E-R model are: entity set and relationship set.

An ER diagram shows the relationship among entity sets. An entity set is a group of similar entities and these entities can have attributes. In terms of DBMS, an entity is a table or attribute of a table in database, so by showing relationship among tables and their attributes, ER diagram shows the complete logical structure of a database. Let's have a look at a simple ER diagram to understand this concept
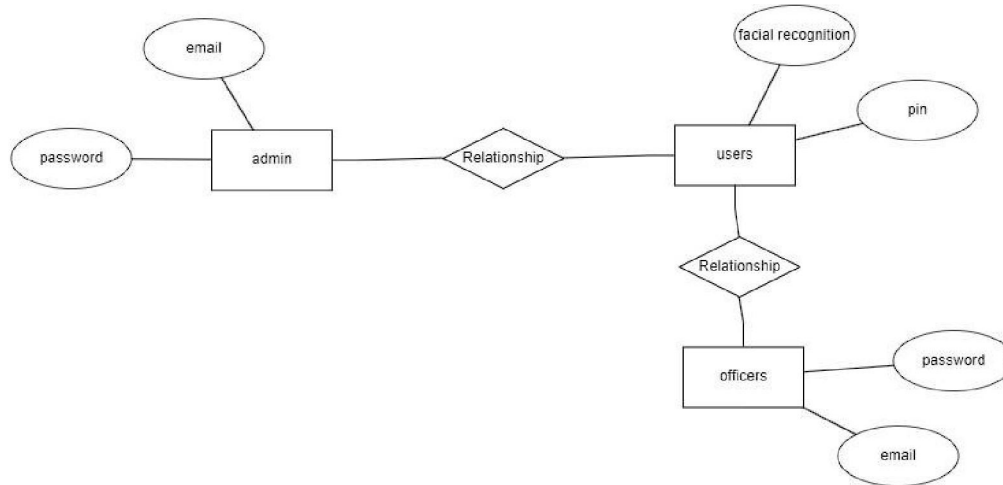

DFD Diagram:

A Data Flow Diagram (DFD) is a traditional way to visualize the information flows within a system. A neat and clear DFD can depict a good amount of the system requirements graphically. It can be manual, automated, or a combination of both. It shows how information enters and leaves the system, what changes the information and where information is stored. The purpose of a DFD is to show the scope and boundaries of a system as a whole. It may be used as a communications tool between a systems analyst and any person who plays a part in the system that acts as the starting point for redesigning a system.

Level 0 Diagram:
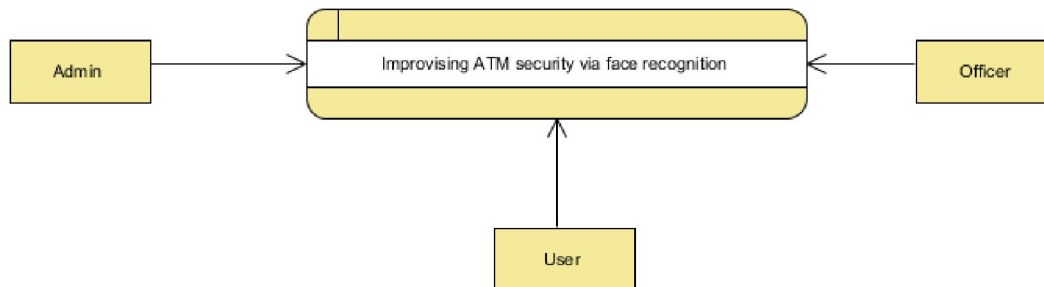
Level 1 Diagram:
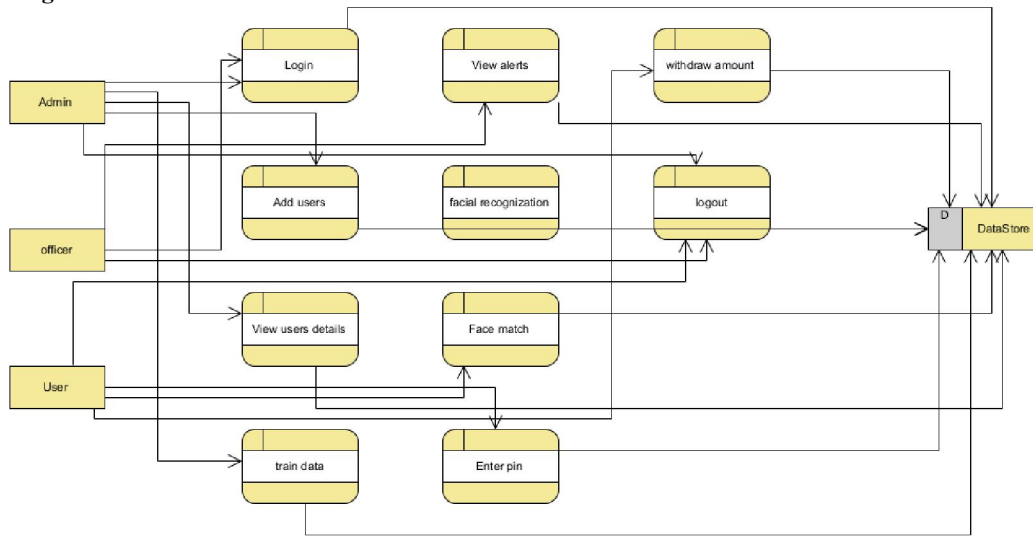
Level 2 Diagram:
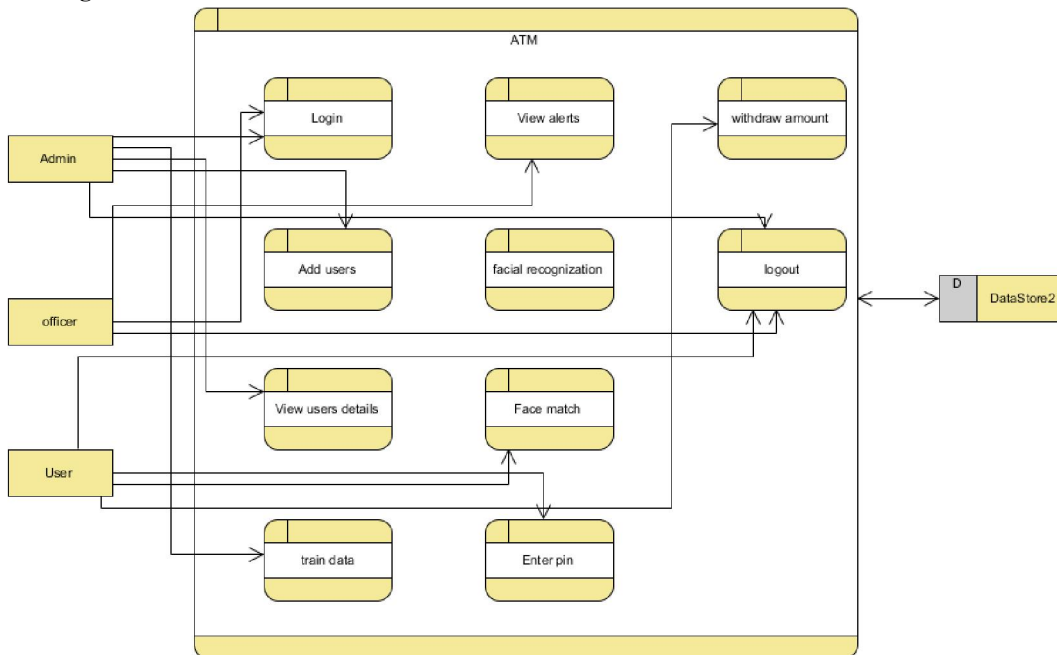
VI. IMPLEMENTATION AND RESULTS

6.1 Modules:

Admin Module:

- Login: Admin can login using default email and password.
- Add User: Admin will add the user and face images will collected here.
- Add Users: Admin can view all the users .
- Delete User: Admin can delete the user.
- Train Data: Admin will train the image which are collected in Add users .
- Logout: The admin will logout.

USER MODULE:

- Facial Recognition : user will be recognized through face recognition
- Pin Authentication : user will be authenticated by the bin also
- View Account: use can view account details.
- Withdraw Amount: user will withdraw amount from his account
- Logout: The user should be logout.

Police Office:

- Login : Officer will login with default username and password
- View Alerts : Officer will view all the alerts which are generated when user using invalid passwords.
- Logout: finally officer will logout

VII. SYSTEM STUDY AND TESTING

Feasibility Study

The feasibility of the project is analysed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

• Economical feasibility
• Technical feasibility
• Social feasibility

Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

System Testing

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Types of Tests
Unit testing
Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing
Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.
Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.
The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.
Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Acceptance Testing
User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.
Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Functional testing
Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.
Functional testing is centered on the following items:
Valid Input : identified classes of valid input must be accepted. Invalid Input : identified classes of invalid input must be rejected. Functions : identified functions must be exercised.
Output : identified classes of application outputs must be exercised. Systems/Procedures: interfacing systems or procedures must be invoked.
Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

White Box Testing
White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing
Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests,

ISSN
2581-9429
IJARSCT

must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

Test objectives
• All field entries must work properly.
• Pages must be activated from the identified link.
• The entry screen, messages and responses must not be delayed.

Features to be tested
• Verify that the entries are of the correct format
• No duplicate entries should be allowed
• All links should take the user to the correct page.

• TEST CASES:

Input	Output	Result
Face Recognition	Success or Fail	Success

Test cases Model building:

S.NO	Test cases	I/O	Expected O/T	Actual O/T	P/F
1	Admin Login	Enter Email, password	Admin login success	Admin login success	P
2	Train user Faces	Train Images	Face Images	Trained successfully	P
4	Recognise Face	Face Recognition	Faces Recognition	Recognition successfully	P

VIII. CONCLUSION

In conclusion, our project aims to enhance ATM security and user convenience by integrating face recognition technology with PIN authentication for money withdrawal. This advanced system provides a multi-factor authentication approach, significantly reducing the risk of unauthorized transactions and fraudulent activities. In case of authentication failure, the system automatically notifies the police authorities with the invalid PIN details for further investigation. By implementing this innovative solution, we aim to provide users with a more secure and convenient way to access their funds, ultimately making ATM transactions safer and more reliable.

IX. FUTURE ENHANCEMENT

For future enhancement, our system could be further improved by integrating additional biometric modalities such as fingerprint or iris recognition for enhanced security. Additionally, implementing machine learning algorithms could improve the accuracy and efficiency of face recognition. Moreover, incorporating real-time monitoring and alert systems to detect suspicious activities could provide an added layer of security. Furthermore, expanding the system to support more advanced banking tasks such as account opening and bill payments would enhance its functionality. These enhancements would not only strengthen ATM security but also offer users a more comprehensive and convenient banking experience.

REFERANCES

[1]. Chaudhary, S., Singh, S., & Sharma, A. (2017). Enhancing ATM Security Using Biometric Technology. International Journal of Computer Applications, 171(2), 18-21.

[2]. Jain, R., Upadhyay, S., & Shukla, S. (2019). Biometric Authentication Systems for ATM Security: A Review. International Journal of Advanced Research in Computer Science, 10(1), 339-344.

[3]. Patel, V., Prajapati, R., & Patel, D. (2020). Face Recognition Technology for ATM Security: A Review. International Journal of Innovative Technology and Exploring Engineering, 9(2), 1715-1718.

[4]. Singh, S. K., Singh, A. K., & Roy, N. K. (2018). Biometric Authentication in ATM Banking: A Survey. International Journal of Computer Applications, 179(11), 14-19.

[5]. Yadav, A., Bhadauria, S., & Srivastava, A. (2017). A Comprehensive Review on ATM Security Using Biometrics. International Journal of Computer Sciences and Engineering, 5(11), 199-204.

[6]. Jain, A., & Ross, A. (2012). Handbook of Biometrics. Springer Science & Business Media.

[7]. Gupta, S., Vishwakarma, S. K., & Singh, A. K. (2016). Biometric Based ATM Cash Withdrawal System: A Review. International Journal of Computer Applications, 139(6), 24-27.

[8]. Khedkar, A., Agrawal, D., & Khandelwal, K. (2018). Security Issues in ATM Transaction Using Biometric Authentication. International Journal of Computer Applications, 182(10), 20-23.

[9]. Afolabi, I. T., & Osunmakinde, I. O. (2020). Biometric Authentication in Enhancing ATM Security: A Review. Journal of Computer Science and Its Application, 27(1), 1- 14.

[10]. Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer Science & Business Media.