International Journal of Gender, Science and Technology
ISSN: 2040-0748

UGC Care Group I Journal
Vol-12 Issue-01 2023

FINGER PRINT BASED ATM SYSTEM

Dr. A. Nagaraju[1]., K. Pruthvi Raj[2]., V. Sai Sri[3]., A. Akshitha[4].

[1] Head of the Department, [2,3,4]Students B. Tech -IT, (20S11A1227, 20S11A1231, 20S11A1205).

Malla Reddy Institute of Technology and Science., Maisammaguda., Medchal., Telangana, India

[1]dranraju.mrits@gmail.com , [2]pruthviraz.k@gmail.com ,[3]saisrireddy.v@gmail.com , [4]akshithareddy453@gmail.com

ABSTRACT

The increase in electronic transactions has contributed to a higher demand for fast and precise identification and authentication of users. In ATMs, biometric-based authentication offers different benefits. Fingerprints and facial identification are used in biometrical authentication. The drawback of the current ATM authentication method is the use of password PINs. Since PINs can be tracked and misused quickly. Our planned system is intended to provide greater protection for ATMs to achieve security and to resolve these criminal activities. Here, the PINs are replaced by randomly created OTP that are sent through the IoT. The goal of the work is to fully eradicate the use of ATM cards. The customer will be allowed to continue with the transaction after biometric and OTP pin authentication. The account will be blocked in the event of three consecutive incorrect attempts. This initiative also deals with ATM fraud prevention. In case of any suspicious activity is detected through the vibration sensor results in the closing of ATM doors followed by releasing of the fainting gas and alerting the surroundings. This will catch the perpetrator engaged in the crime and prevent the fraud from taking place.

1.INTRODUCTON

An Automated Teller Machine (ATM) was first used in London in 1966. Many theoretical and practical pieces of research about ATM have been made throughout the world. This is because of the increase in the range of ATMs to achieve a cashless economy. The ATM is an electronic telecommunication device that provides financial transactions such as cash withdrawal, cash deposits, funds transfer, and payments of utility. ATM fraud has become a global issue that has dramatically increased in recent years. ATM fraud has an impact on both customers and bank operators. They are facing the issues of crimes and security threats to the existing card system. The existing ATM system uses PIN and ATM cards for authentication, which have several drawbacks. To steal ATM card and their information, criminals use some techniques such as ATM skimming, Cash trapping, Shoulder surfing, and Card trapping. Some customers use their phone numbers, birthdates as their PIN which can be easily guessed by Fraudsters or hacked by cybercriminals. Biometric authentication has solutions to these problems of ATM card and PIN. This is because the biological details are unique and cannot be duplicated by others. ATMs have become a high priority target to hackers and stealers. ATMs are susceptible to hacker attacks, fraud, robberies, and security breaches. A stable system is needed to detect such anomalous behavior. Now a day's surveillance camera has been installed in most of the ATMs. But this can't prevent ATM robberies. Some ATM crime occurs due to the absence of security guards. Thus, there is a serious need for an efficient system that can detect suspicious activities and prevents robbery by catching the crime offender before they slip away. Thus, ensures public safety, reduce crime and prevent any serious tragedy.

In this paper, the proposed model uses Biometric authentication which includes fingerprint and face recognition authentication. The drawback of the prevailing authentication Pattern in ATM is the usage of PIN as password. Here the PINs are replaced with the randomly generated OTP sent through IoT services. In case of any robbery, the vibrations on the ATM are sensed by the sensor, the surrounding will be alerted by a buzzer and the door of ATM room will close immediately and also a fainting gas is pumped inside the ATM to make the thief unconscious.

2.LITERATURE SURVEY

[1] **Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar (2018)**. In this paper, the authors had proposed the concept of Finger-shield ATM, a biometric identification in the form of the fingerprint is implemented along with ATM which is integrated with smart card and database server. Despite the fact that user has to go through additional authentication time for fingerprint verification, the security was much improved and guaranteed by their system. Firstly, a smartcard is inserted into the reader, the program will ask for PIN from the user through the keypad. On successful PIN authentication, the program

will then prompt fingerprint input. After successful fingerprint authentication, the user will proceed further or authentication will fail.

[2] **Indranil Banerjee, Sjivangam Mookherjee, Sayantan Saha, Souradeep Ganguli, Subham Kundu, Debduhita Chakravarti (2019).** In this paper, the authors had proposed a double layer security check. Firstly, the user inserts the RFID card after that user gives a fingerprint which is verified if there is a mismatch a message is sent to the user. If it's a match, the system further goes on with the level-2 security check i.e., the IRIS scanner. IRIS is the only part of our body that doesn't change from birth till our death. Iris scan is one of the most secured biometric systems it further increases the level of security along with the fingerprint and RFID card that acts as the secondary security check.

[3] **Murugesan M, Santhosh M, Sasi Kumar T, Sasiwarman M, Valanarasu (2020).** This paper represents the security of ATMs using facial recognition. The authors had used an RFID reader instead of an ATM card reader to identify the account details of the user. CCTV is used to recognize the face using haar cascade and local binary pattern and if the face will match to the database, then after entering the pin, the transaction will proceed otherwise the system will send the link to the account holder it will show the snap of the person who is currently using his card and also enables three options for the user to choose one option – 'it's me', 'accept', 'decline'. If the user clicks on it's me then it will allow updating the image of an account holder and if an account holder clicks on accept then the system will allow the transaction and if the user clicks on the decline, it will terminate the transaction.

[4] **Darwin Nesakumar A, T Suresh, Nivedha T, K Nivedha, Priyadharshini G, P Mugilan (2020).** In this paper, the author had proposed a system using facial recognition and fingerprint. After inserting an ATM card and entering a pin, the card reader collects the details stored in the card and after capturing the face and fingerprint system will compare with the database, if all the information is matched then it will allow for transaction otherwise it will send a one- time password along with the suspect's image to the account holder's mail and after entering the correct OTP system will allow the transaction.

[5] **Shivani Shukla, Anjali Helonde, Sonam Raut, Shubhkirti Salode, Jitesh Zade (2018).** In this paper, the author had proposed a security text-based word and graphical password for the transaction system which uses facial recognition for detection of the face in the second stage. As soon as the user has entered the system, the user will land on the Random keypad page. If the user is not registered then the user can click on the registration link which will on the same page. After clicking on the registration link, the registration form will be opened which includes fields like user name, account number, date of birth, address, contact number, and gender. Once the form is submitted, the user will be registered with the system. If the user is already registered then the user can enter the pin using a random keypad where the numbers would be a random sequence. After entering the PIN, it will proceed for facial recognition. If the match is found then the user can perform their operations like balance inquiry, pin change, withdrawal. This system overcomes the shoulder surfing attack.

[6] **Prakash Chandra Mondal, Rupam Deb, and Md. Nasim Adnan (2017).** The author proposed a system that uses behavioural biometrics for authentication with more security. In this system, authentication is performed using three steps which include online handwriting signature verification, chip-based card, and PIN verification. This method does not involve the need for further enhancement like using physical biometrics (fingerprint, face images, etc).

[7] **Rasib Khan, Ragib Hasan, and Jinfeng Xu (2015).** In this paper, the authors had proposed the system in which Secure PIN Authentication as a service (SEPIA) is used for authentication of the PIN for ATMs which uses cloud-connected personal mobile and wearable devices. The process gets started when the user interacts with the screen and this initiates a request message to the ATM server. As a response, a QR code is generated on the screen and this QR code can be scanned using wearable devices like Google glass from which the user's details can be retrieved and verified. After the verification, the user needs to enter the PIN received via phone number. After the authentication, the user can perform the transaction.

3.METHODOLOGY

Existing System

The drastic increase in the usage of ATM motivates the researchers to research the development, security, and enhanced facilities of ATM. Gokul. S, Kukan. S, and Meenakshi. K replaced ATM cards with RFID cards which contain the card number of the customer and instead of using the PIN, the fingerprint of the customer was used for authorization. V. Prasanan, R. Sandeep Kumar, and C. Deepak proposed a system

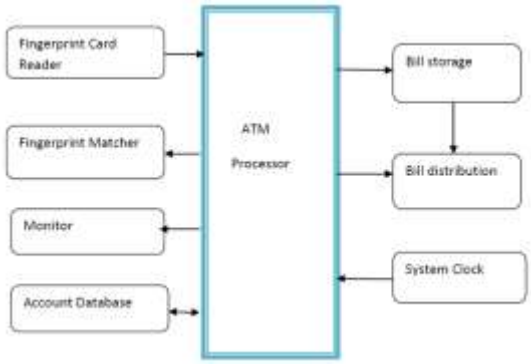
that uses a vibration sensor, light sensor, smoke sensor, and temperature sensor.

If any person attempts to damage the ATM or break the ATM, it is detected employing a vibration sensor and the door is immediately locked. V. Arun kumar and Vasanth Kumar. V used the face recognition technique for user authorization. The system compares the face input of the individuals with the face details of the users in the database and decides whether or not a match is found. The system provides a ranked list of matches by comparing the data of the individual given with all the other individuals in the database. Abhinav Muley and Vivek used fingerprint identification that accelerated the transaction and improved the level of security. The proposed system replaces the existing ATM transaction card system with a biometric fingerprint. Biometrics helps to classify an individual uniquely with the aid of the person's biological characteristics and proposed a new approach to detect Anomalous behaviour in ATM's. In, Authors gave a face recognition based new generation ATM machine, followed by had iris and fast fingerprint verification and which had added message authentication system.

Proposed System

We have posited a new concept that enhances the overall experience, usability, security, and convenience of the transaction at the ATM. First, the face and fingerprint of the customer should be received and uploaded to the MySQL database. To achieve interaction with the customer, a user interface is created using Python GUI. The whole transaction will be shown through the user interface. The image of the face and fingerprint of the customer is coded into digital data and then it gets stored in the database. While registering biometric details, the customer will be provided with a bank account and balance. They also want to provide a username and a password while registering their account to the administrator of the corresponding bank. When a customer wants to access ATM, he/she firstly place their finger on the fingerprint module. After acceptance, they should show their face to the camera that is before them. Both biometric details are converted into digital code. Now, this digital data is checked against the list of registered customer's biometric data. If data matches, then the system will send an OTP to the corresponding account holder's mobile phone through IoT, as shown in the figure 5. If the provided data not matched, then the system won't allow the further process. The system asks to enter OTP to the customer. After entering OTP, the system checks it with the corresponding data. On breaching three reattempts the account will be blocked. If all three authentication match then the customer asks to select a Bank from the given option. After this selection customer allows to make the transaction in the respective Bank account. Users can ingress any bank account of his/her, but it should be linked with their ID. Here customers can do some of the ATM functions like account details, withdrawal, deposit, money transfer. And also, they can view their previous transaction with that account. After completing a successful Proceeding, the user can either continue or exit. This system has been designed with Python-DBMS along with the use of hardware Peripherals to provide a cheap ATM system. Accesses to multiple bank's accounts are also supported in this system.

4.SYSTEM ARCHITECTURE:



System Architecture

UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of Object-Oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML. The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing Object-Oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

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.

Figure :Use Case Diagram

CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling 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.

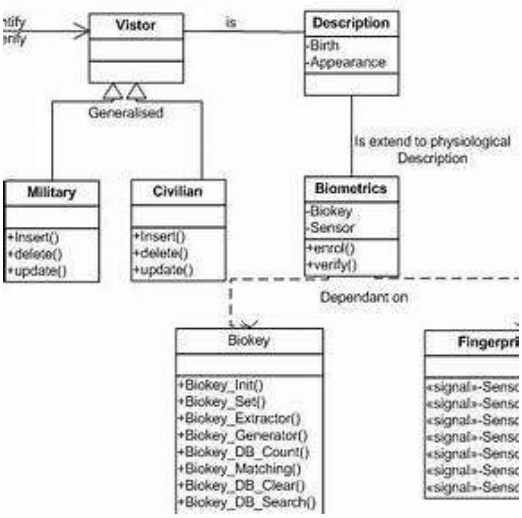


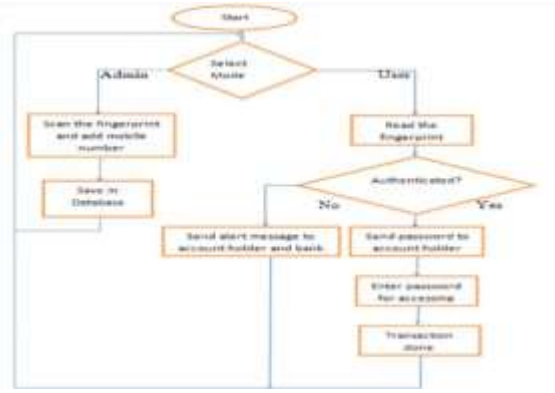
Figure 3.1.3 : Class Diagram

SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling 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, event scenarios, and timing diagrams.

ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling 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.



Activity Diagram

SYSTEM STUDY

FEASIBILITY STUDY

The feasibility of the project is analyzed 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.

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.

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/Procedure: 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.

System Testing

System testing ensures that the entire integrated software system meets requirements. It tests a

configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

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, 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.

MODULES USED

Tensorflow

TensorFlow is a free and open source software library for dataflow and differentiable programming across a range of tasks. It is a symbolic math library, and is also used for machine learning applications such as neural networks. It is used for both research and production at Google.

TensorFlow was developed by the Google Brain team for internal Google use. It was released under the Apache 2.0 open source license on November 9, 2015.

Numpy

Numpy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.It is the fundamental package for scientific computing with Python. It contains various features including these important ones:A powerful N-dimensional array object**,** Sophisticated (broadcasting) functions**,** Tools for integrating C/C++ and Fortran code**.**Useful linear algebra, Fourier transform, and random number capabilities. Besides its obvious scientific uses, Numpy can also be used as an efficient multi-dimensional container of generic data. Arbitrary data-types can be defined using Numpy which allows Numpy to seamlessly and speedily integrate with a wide variety of databases.

Pandas

Pandas is an open-source Python Library providing high-performance data manipulation and analysis tool using its powerful data structures. Python was majorly used for data munging and preparation. It had very little contribution towards data analysis. Pandas solved this problem. Using Pandas, we can accomplish five typical steps in the processing and analysis of data, regardless of the origin of data load, prepare, manipulate, model, and analyse. Python with Pandas is used in a wide range of fields including academic and commercial domains including finance, economics, Statistics, analytics, etc.

Matplotlib

Matplotlib is a Python 2D plotting library which produces publication quality figures in a variety of hardcopy formats and interactive environments across platforms. Matplotlib can be used in Python scripts, the Python and IPython shells, the Jupyter Notebook, web application servers, and four graphical user interface toolkits. Matplotlib tries to make easy things easy and hard things possible. You can generate plots, histograms, power spectra, bar charts, error charts, scatter plots, etc., with just a few lines of code. For examples, see the sample plots and thumbnail gallery.

For simple plotting the pyplot module provides a MATLAB-like interface, particularly when combined with IPython. For the power user, you have full control of line styles, font properties, axes properties, etc, via an object oriented interface or via a set of functions familiar to MATLAB users.

Scikit – learn

Scikit-learn provides a range of supervised and unsupervised learning algorithms via a consistent interface in Python. It is licensed under a permissive simplified BSD license and is distributed under many Linux distributions, encouraging academic and commercial use.

5.ACKNOWLEDGEMENT:

The members of the research project want to sincerely thank our guide Head of the Department Mrs. A. Nagaraju and the Department of Information Technology, Malla Reddy Institute of Technology and Science, India for their encouragement and support for the completion of their work.

6.CONCLUSION AND FUTURE SCOPE CONCLUSION

CONCLUSION: As the result of fraudulent activities increased in the card-based system, this proposed ATM system uses biometric. The card-less system provides more secured cash transactions compared to a card-based system. The biometric authorizations include both fingerprint and face recognition, in which the fingerprint of every individual is uniquely identified.

FUTURE SCOPE

Several potential future enhancements could be applied to fingerprint-based ATM systems to improve security, user experience, and functionality:

i. Multi-factor Authentication: Combine fingerprint recognition with additional authentication factors, such as facial recognition, iris scanning, or palm vein recognition, for even stronger security.

ii. Behavioral Biometrics: Implement systems that analyze user behavior patterns (like typing speed, touchscreen gestures, or navigation habits) to add an extra layer of authentication, making it more difficult for unauthorized users to access accounts.

iii. Blockchain Integration: Incorporate blockchain technology for secure data storage, ensuring the integrity of the biometric data and transaction records.

iv. AI-Powered Fraud Detection: Utilize AI algorithms to continuously monitor and analyze usage patterns, identifying anomalies in transactions and behavior that might indicate fraud.

v. Dynamic Security Codes: Generate dynamic, time-sensitive security codes that must be validated alongside the fingerprint scan, ensuring real-time verification.

vi. Biometric Encryption: Use biometric encryption techniques that convert biometric data into an encrypted code, adding an extra layer of security to the stored fingerprint information.

vii. User Customization: Offer users the ability to set personalized security preferences, such as transaction limits or specific usage timeframes, enhancing control over their accounts.

viii. Biometric Data Privacy: Implement strict policies to protect and govern the use of biometric data, ensuring it's stored and processed securely, compliant with privacy regulations.

ix. Voice Recognition Integration: Combine fingerprint recognition with voice recognition for multi-modal biometric authentication, further enhancing security.

7.REFERENCE

[1] Pranali Ravikant Hatwar and Ravikant B Hatwar, BioSignal based Biometric Practices, International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp. 1-9, 2013.

[2] Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning,
Available at: https://www.sans.org/readingroom/whitepapers/authentic ati on/biometric- scanningtechnologies-finger-facial-retinal-sca nning-1177.

[3] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern
Recognition, 2004, 37:543-553.

[4] N. Selvaraj and G. Sekar, A Method to enhance the Safety Level of the ATM Banking industry using AES Algorithm, International Journal of Computer Applications, Vol. 3, No. 6, pp. 5-9,2010.

[5] A. Haldorai and A. Ramu, Security and channel noise management in cognitive radio
networks, Computers & Electrical Engineering, vol. **87**, p. 106784, Oct. 2020.doi:10.1016/j.compeleceng.2020.106784.

[6] A. Haldorai and A. Ramu, Canonical Correlation Analysis Based Hyper Basis Feedforward Neural Network Classification for Urban Sustainability,Neural Processing Letters, Aug. 2020.doi:10.1007/s11063-020-10327-3.

[7] J. Yang N. Xiong, A.V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie and Y. Yang.
A Fingerprint Recognition Scheme supported Assembling Invariant Moments for Cloud
Computing Communications, IEEE Systems Journal, Vol. 5, No. 4, pp. 574-583, 2011.

International Journal of Advanced Science and Technology. 29. 255-260.