e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707110 |

Real Time Secure Clickbait and Biometric ATM User Authentication and Multiple Bank Transaction System

Dr T. Geetha MCA, M.Phil Ph.D., Mr. E. Enbaraj MCA

HOD, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

PG Student, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

ABSTRACT: ATM or Automated Teller Machines are widely used by people nowadays.Performing cash withdrawal transaction with ATM is increasing day by day. ATM is very important device throughout the world. The existing conventional ATM is vulnerable to crimes because of the rapid technology development. A total of 270,000 reports have been reported regarding debit card fraud and this was the most reported form of identity theft in 2021. A secure and efficient ATM is needed to increase the overall experience, usability, and convenience of the transaction at the ATM. In today's world, the area of computer vision is advancing at a breakneck pace. The recent progress in biometric identification techniques, including finger printing, retina scanning, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. Specifically, the goal of this project is to give a computer vision method to solve the security risk associated with accessing ATM machines. This project proposes an automatic teller machine security model that uses electronic facial recognition using Deep Convolutional Neural Network. If this technology becomes widely used, faces would be protected as well as their accounts.Face Verification Clickbait Link will be generated and sent to bank account holder to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification. However, it obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of account safety making it possible for the actual account owner alone have access to his accounts. This eliminates the possibility of fraud resulting from ATM card theft and copying.The experimental results on real-time datasets demonstrate the superior performance of the proposed approach over state-of-the-art deep learning techniques in terms of both learning efficiency and matching accuracy.By using this real time dataset, the proposed system achieves the highest accuracy with 97.93%.

KEYWORDS: ATM Machine, Face Recognition, Deep Conventional Neural Network.

I. INTRODUCTION

Automated Teller Machines, popularly referred to as ATMs, are one of the most useful advancements in the banking sector. ATMs allow banking customers to avail quick self-serviced transactions, such as cash withdrawal, deposit, and fund transfers.ATMs enable individuals to make banking transactions without the help of an actual teller. Also, customers can avail banking services without having to visit a bank branch. Most ATM transactions can be availed with the use of a debit or credit card. There are some transactions that need no debit or credit card. Over the last two decades, automated teller machines (ATMs) have become as much a part of the landscape as the phone booths made famous by Superman. As a result of their ubiquity, people casually use these virtual cash dispensers without a second thought. The notion that something could go wrong never crosses their minds. Most ATM scams involve criminal theft of debit card numbers and personal identification numbers (PINs) from the innocent users of these machines. There are several variations of this confidence scheme, but all involve the unknowing cooperation of the cardholders themselves.ATM fraud is described as a fraudulent activity where the criminal uses the ATM card of another person to withdraw money instantly from that account. This is done by using the PIN. The other type of ATM fraud is stealing from the machine in the ATM by breaking in skimming. This type of ATM scam involves a skimmer device that criminals place on top of or within the card slot. To record your PIN number, the criminals may use a hidden camera or an overlay that covers the original PIN pad. Using the card numbers and PIN's they record; thieves create duplicate cards to withdraw money from consumers' accounts. Unlike losing your debit card or having it stolen, you won't realize anything is amiss until unauthorized transactions take place. Take a look at these so you know how to detect

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707110 |

ATM skimmer This is the latest update to skimming. Instead of reading your card number, criminals place a shimming device deep inside the ATM to record your card's chip information. The end result is the same as skimming because thieves use the stolen chip data to create "cloned" versions of your debit card Cash-out This scam targets multiple accounts from the same financial institution. Armed with a hacked bank employee's credentials, the criminal alters account balances and withdrawal limits. Using stolen debit card numbers captured from a separate skimming attack, they can "cash out" the ATM until it's out of money Jackpotting While there are multiple types of jackpotting attacks, typically, these incidents involve gaining physical access to the inside of the machine. The criminals may replace hardware or install malicious software giving them control of the cash dispensing function. Jackpotting is similar to a cash out scam, but it does not require the criminal to have any customer account details or stolen debit card information.

II. EXISTING SYSTEM

Existing systems of ATM authentication primarily rely on traditional methods such as card-based authentication and PIN entry. However, advancements in technology have led to the adoption of additional authentication mechanisms to enhance security and user convenience. Here are some existing systems of ATM authentication **Card and PIN Authentication**: This is the most common method used in ATM authentication. Users insert their ATM card into the card reader slot and enter their Personal Identification Number (PIN) using the keypad. The system verifies the entered PIN against the one stored on the card's chip or magnetic stripe. **Biometric Authentication**: Some ATMs incorporate biometric authentication methods such as fingerprint recognition or iris scanning. Users can register their biometric data with the bank, and the ATM system verifies their identity by matching the biometric data captured at the time of authentication. **Two-Factor Authentication (2FA)**: In addition to the traditional card and PIN authentication, some ATMs implement two-factor authentication. This involves combining something the user knows (PIN) with something the user has (e.g., a mobile device or token). For example, users may receive a one-time password (OTP) on their registered mobile phone that they need to enter along with their PIN for authentication **Near Field Communication (NFC)**: NFC technology allows users to authenticate transactions using contactless methods such as mobile wallets or contactless cards. Users can tap their NFC-enabled device or card on the ATM reader to initiate a transaction, eliminating the need for physical insertion of the card. **Mobile Authentication** Some banks offer mobile banking apps with built-in authentication features. Users can authenticate transactions at the ATM by scanning a QRcode displayed on the ATM screen using their mobile banking app. The app then prompts the user to authorize the transaction on their mobile device. **Token-Based Authentication**: Some banks issue physical or virtual tokens to customers for authentication purposes. These tokens generate one-time passwords (OTPs) that users need to enter along with their PIN to complete transactions at the ATM.

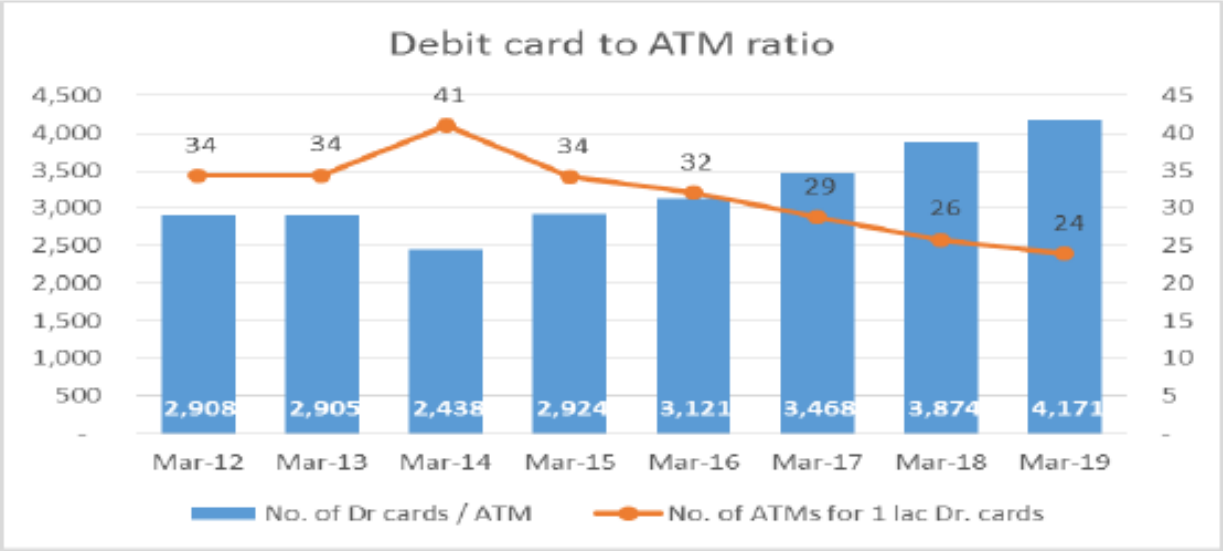
III. LITERATURE SURVEY

A literature survey on ATM machines reveals a multifaceted exploration into their evolution, technological advancements, security concerns, and user experience. Early studies focused on usability and interface design, emphasizing the importance of intuitive interactions to enhance user satisfaction and operational efficiency. Security remains a predominant theme, with extensive research on fraud detection, biometric authentication, and encryption protocols aimed at safeguarding transactions and user data. Technological advancements, such as the integration of AI and machine learning, have further transformed ATM functionality, enabling predictive maintenance and personalized user experiences. Future research directions underscore the need for continuous innovation in security measures and user-centric design to meet evolving technological challenges and user expectations in the digital banking era. The system design of the Real-Time Secure Clickbait and Biometric ATM User Authentication and Multiple Bank Transaction System encompasses a sophisticated architecture aimed at revolutionizing ATM security and user authentication. Leveraging advanced technologies such as facial recognition and biometric authentication, the system is designed to address the growing concerns of ATM-related fraud and identity theft. By seamlessly integrating innovative security measures and real-time authentication methods, the system aims to enhance the overall security, usability, and convenience of ATM transactions for users. This introduction provides an overview of the system design's objectives and highlights its key components and functionalities, setting the stage for a comprehensive exploration of the project's architecture and implementation details.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707110 |



IV. PROPOSED SYSTEM

The proposed system for the ATM User Face Identification project involves integrating facial recognition technology into the existing ATM infrastructure. Here's an overview of the key features and components.The Facial Recognition Module integrates advanced facial recognition technology, leveraging a Convolutional Neural Network (CNN) trained on a dataset of facial images. This module is responsible for accurately detecting and analyzing facial features captured by the ATM's high-resolution camera during transactions. Upon initiation of a transaction, the user's face is captured and processed to extract facial features. These features are then compared with pre-existing facial templates stored in the system's database to verify the user's identity. The CNN continually learns and adapts to improve accuracy and performance over time. Unknown Face Verification System In cases where the user's face is not recognized or matches with an unknown identity, the Unknown Face Verification System is activated. This system generates a unique Face Verification Link and securely transmits it to the user's registered mobile number. The Face Verification Link serves as an additional authentication step, allowing the user to confirm their identity by clicking on the link and completing further verification steps, such as entering a one-time code or confirming the transaction details. This process enhances security and provides users with an alternative verification method. The Notification Module is designed to deliver real-time transaction updates and security alerts to users. Users receive notifications via their preferred communication channels, including SMS, email, or in-app alerts. Transaction details, such as withdrawal amounts, account balances, and transaction confirmations, are promptly communicated to the user to ensure transparency and security. Additionally, the Notification Module alerts users of any suspicious activities or security breaches, enabling them to take immediate action, such as contacting their bank or reporting the incident. This proactive approach enhances user awareness and helps mitigate potential risks associated with ATM transactions.

Face Recognition: The process begins with actively creating a comprehensive dataset by recording a live video of the account holder's face for approximately 30 seconds. This dynamic dataset serves as the bedrock for training the subsequent face recognition model. It ensures a diverse collection of facial expressions, angles, and lighting conditions for robust model training. Frame Conversion Post dataset acquisition, the system seamlessly converts video frames into individual images. This step is pivotal for simplifying subsequent image processing and analysis. It enables the system to work with discrete frames, facilitating more efficient handling and manipulation during pre-processing. Pre-processing This pre-processing module encompasses multiple steps to optimize images for subsequent analysis. Grey Scale Conversion The conversion to greyscale simplifies image representation, reducing complexity. Noise Filter The application of mean or Gabor filtering minimizes noise, enhancing the clarity of facial features. Binarize Converting images to binary format further streamlines feature extraction. These steps collectively contribute to creating a standardized and enhanced image dataset.

Face Detection: Leveraging a Region Proposal Network (RPN), this module identifies potential face regions within the pre-processed images. RPN excels at proposing regions likely to contain facial features, laying the groundwork for

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707110 |

subsequent processing. It streamlines the computational effort by focusing on regions of interest, enhancing efficiency in face recognition.

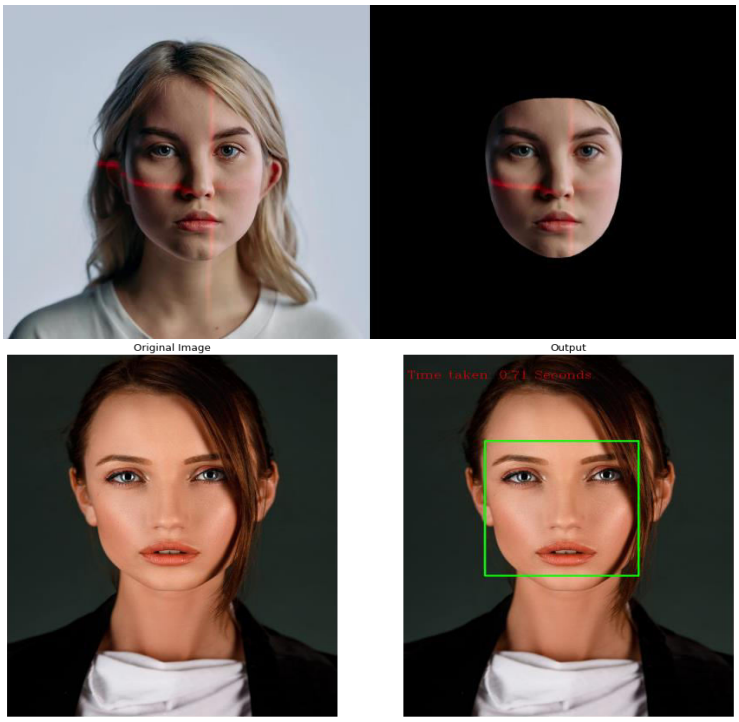


Fig 1 Face Detection

Face Feature Extraction: This module focuses on extracting relevant features from the detected face regions using Gray Level Co-occurrence Matrix (GLCM). GLCM captures statistical information about pixel intensity relationships, offering a rich set of features for subsequent classification. It serves as a robust method for characterizing facial textures and patterns.

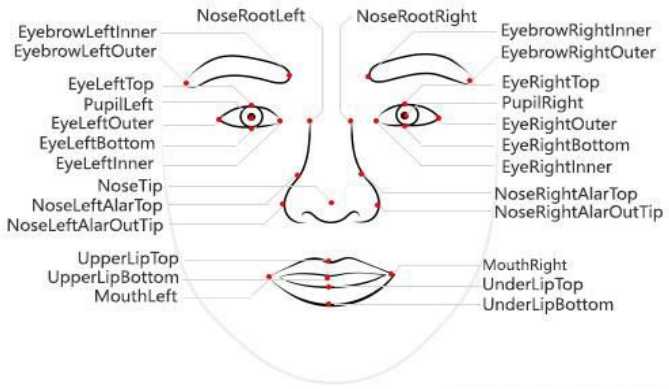


Fig 2 Face Feature Extraction

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707110 |

V. RESULT

SCREENSHOT

Fig 3 Admin page

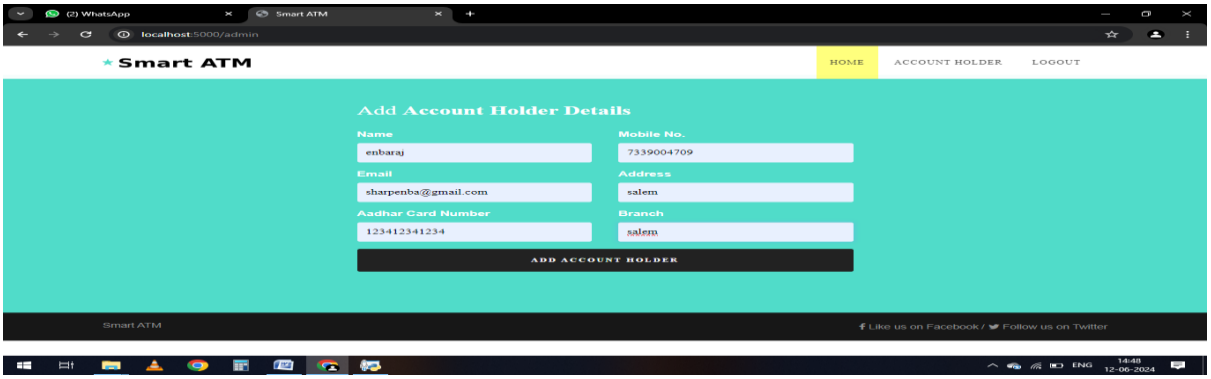


Fig 4 Account Holder Page

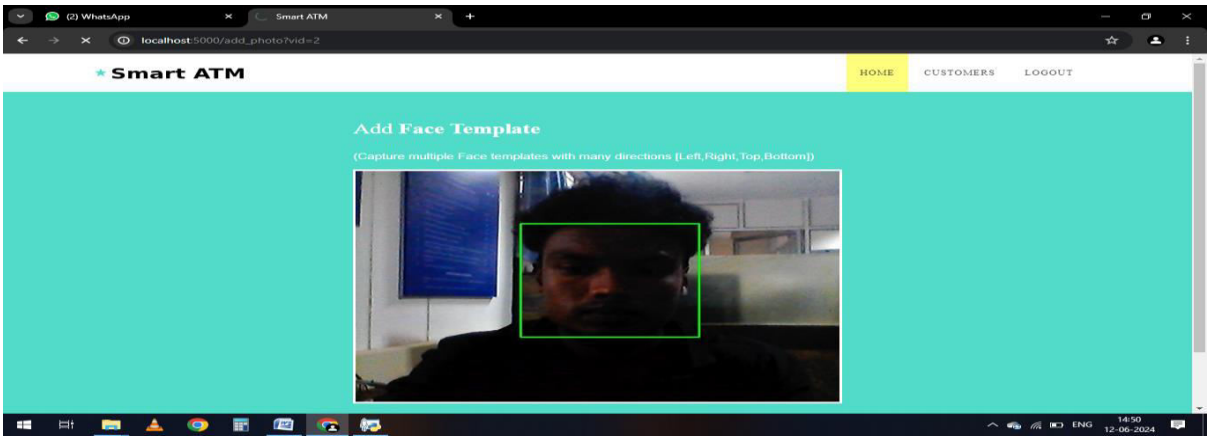


Fig 5 Face Template Page

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707110 |

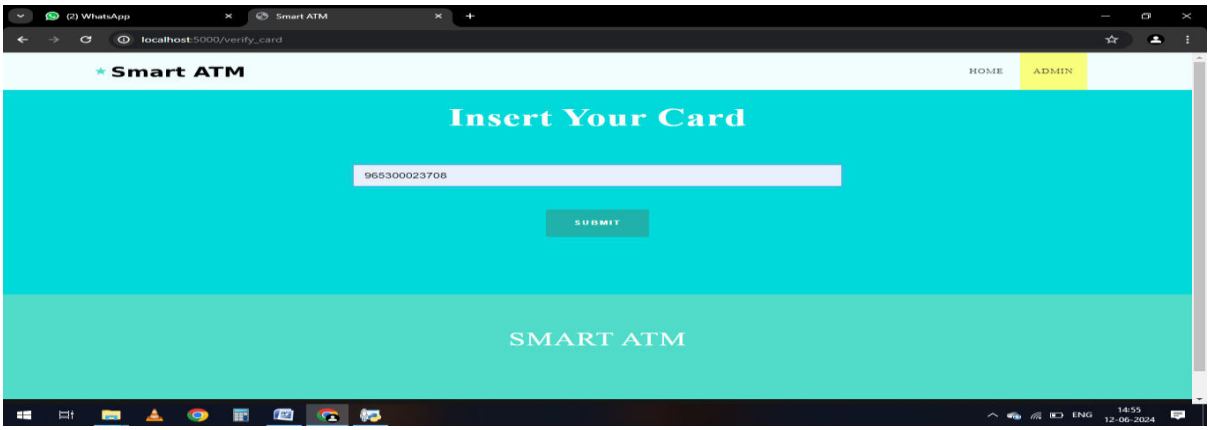


Fig 6 Insert Number Page

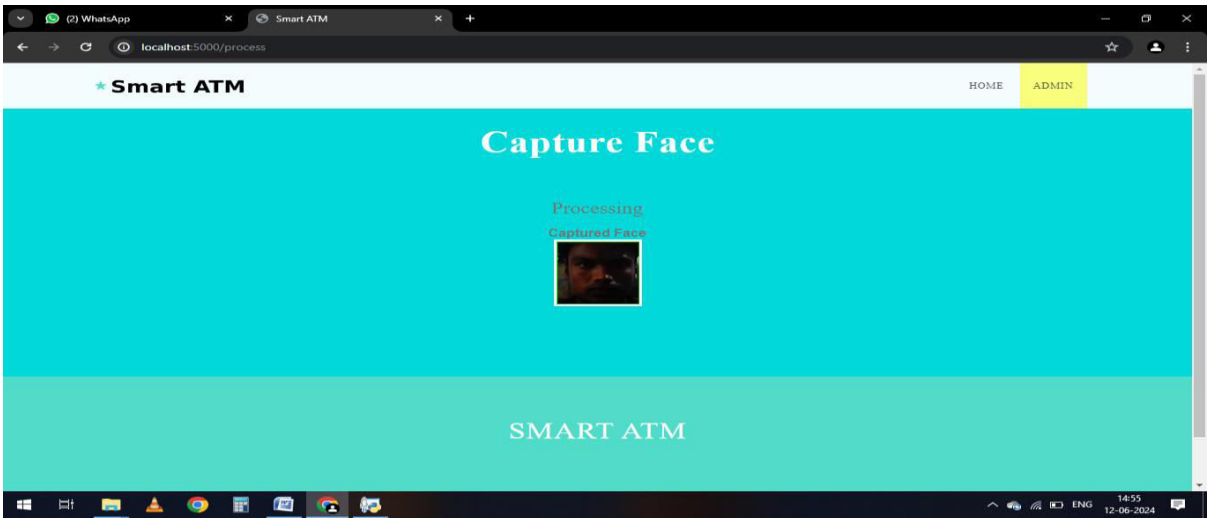


Fig 7 Capture Face page

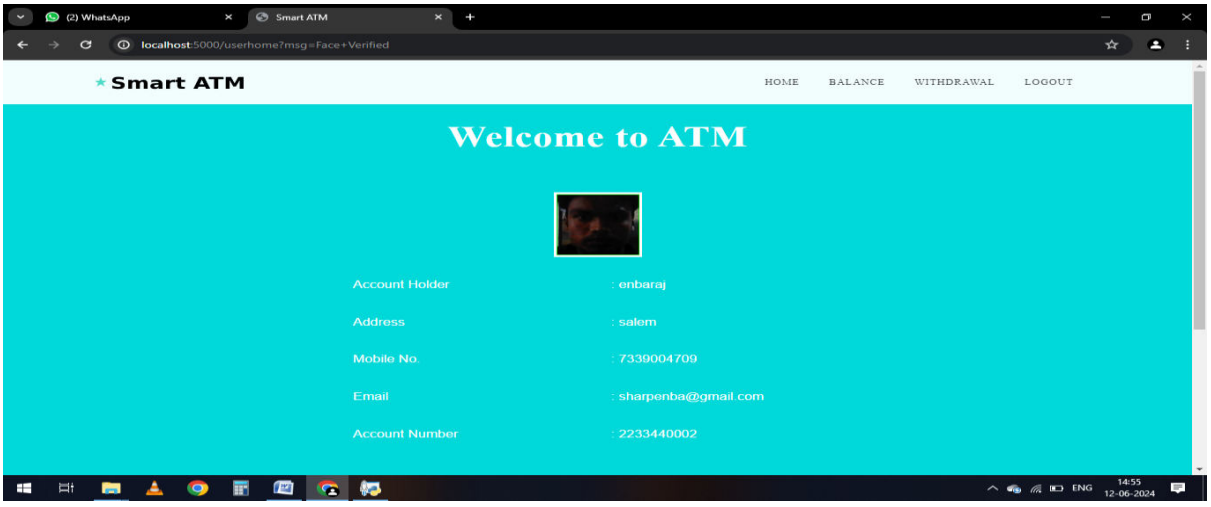


Fig 8 View User Detail

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707110 |

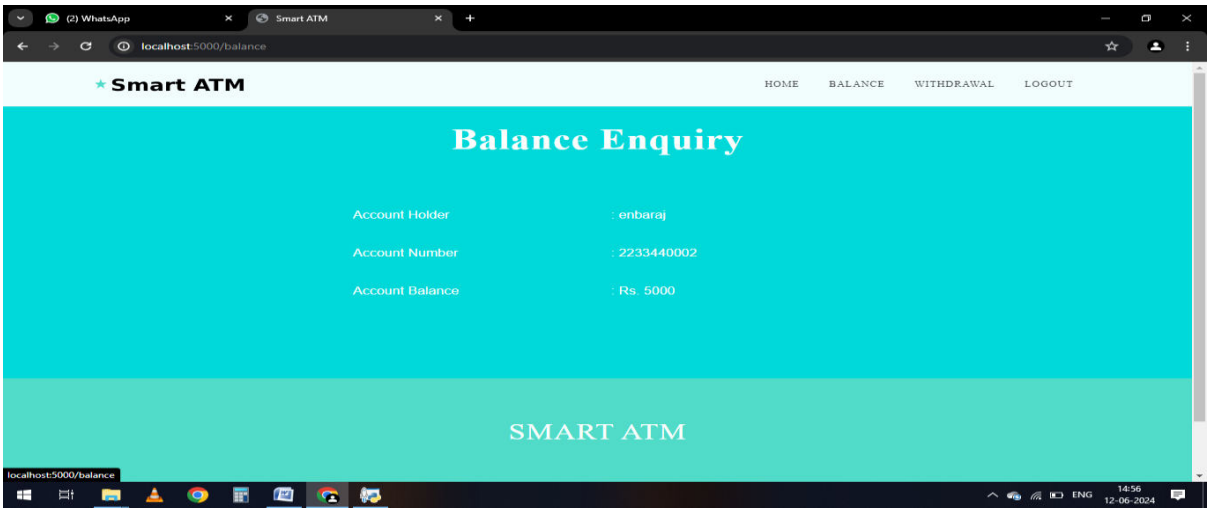


Fig 9 Balance Enquiry Page

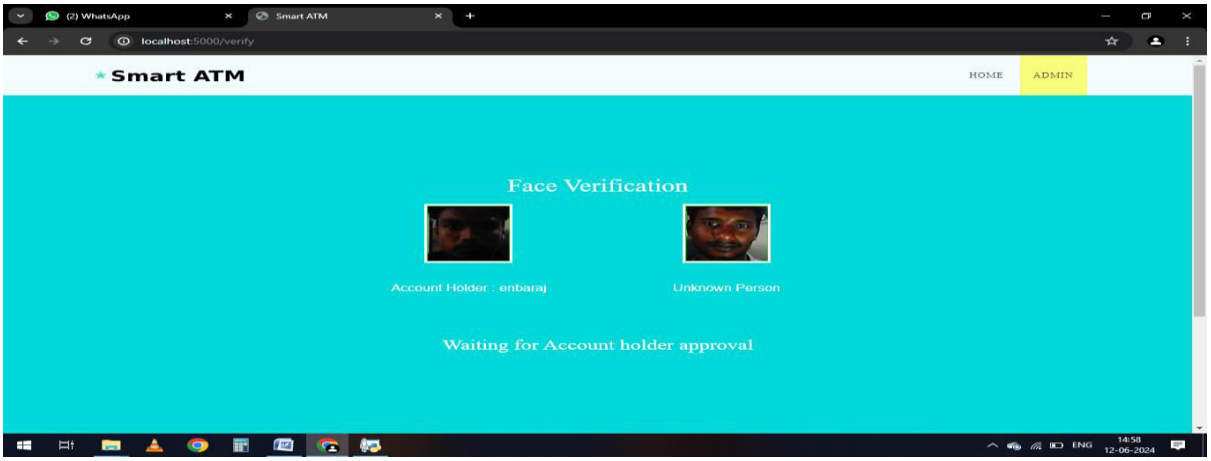


Fig 10 Get Approval

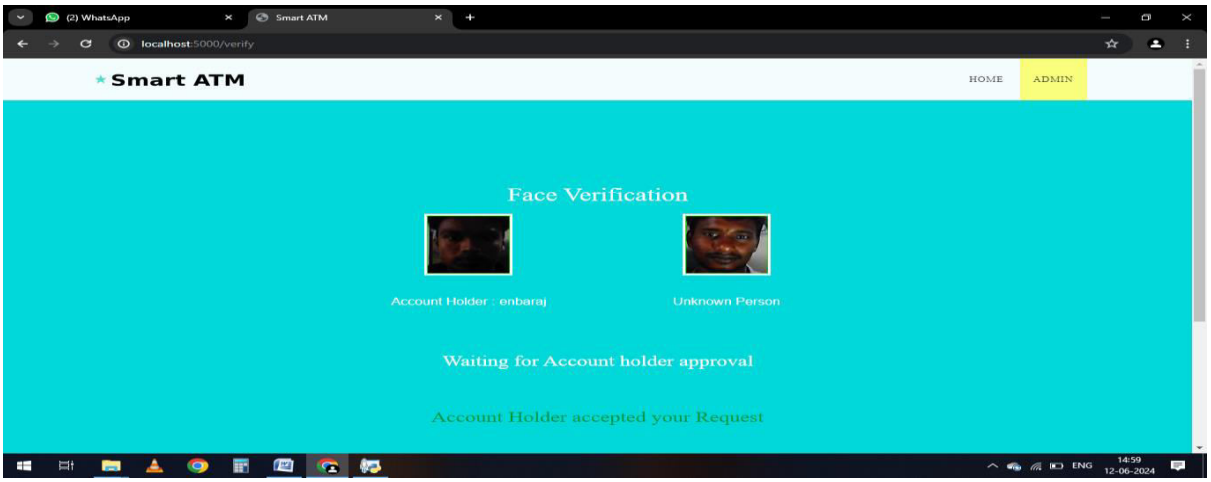


Fig 11 Accept Approval

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707110 |

OUTCOMES: Face biometric-based ATM user authentication systems have shown promising outcomes in enhancing security and user convenience. Research indicates that such systems significantly reduce the risk of fraud by providing a robust layer of authentication that is difficult to replicate or spoof. Users benefit from a streamlined and faster authentication process, eliminating the need for physical cards or PINs, which can be lost or stolen. Moreover, face biometrics offer a non-intrusive and user-friendly experience, accommodating diverse user demographics. Implementation studies have demonstrated high accuracy rates in verification, bolstering confidence in the technology's reliability. Challenges persist, particularly regarding environmental factors like lighting conditions and angle variations, yet ongoing advancements in facial recognition algorithms and hardware continue to improve system performance and broaden its application across the banking sector.

VI. CONCLUCTION

Agricultural farm security is widely needed technology nowadays. In order to accomplish this, Biometrics as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. In this project, we have developed to proffer a solution to the much-dreaded issue of fraudulent transactions through Automated Teller Machine by biometrics and Unknown Face Forwarder that can be made possible only when the account holder is physically or far present. Thus, it eliminates cases of illegal transactions at the ATM points without the knowledge of the authentic owner. Using a biometric feature for identification is strong and it is further fortified when another is used at authentication level.The ATM security design incorporates the possible proxy usage of the existing security tools (such as ATM Card) and information (such as PIN) into the existing ATM security mechanisms. It involves, on real-time basis, the bank account owner in all the available and accessible transactions

REFERENCES

[1] J. Liang, H. Zhao, X. Li, and H. Zhao, ``Face recognition system based on deep residual network," in Proc. 3rd Workshop Adv. Res. Technol. Ind. (WARTIA), Nov. 2017, p. 5.
[2] I. Taleb, M. E. Amine Ouis, and M. O. Mammar, ``Access control using automated face recognition: Based on the PCA & LDA algorithms," in Proc. 4th Int. Symp. ISKO-Maghreb, Concepts Tools Knowl. Manage. (ISKO-Maghreb), Nov. 2014, pp. 1-5.
[3] X. Pan, ``Research and implementation of access control system based on RFID and FNN-face recognition," in Proc. 2nd Int. Conf. Intell. Syst. Design Eng. Appl., Jan. 2012, pp. 716-719, doi: 10.1109/ISdea.2012.400.
[4] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``Raspberry Pi and computers-based face detection and recognition system," in Proc. 4th Int. Conf. Comput. Technol. Appl. (ICCTA), May 2018, pp. 171-174.
[5] A. Had, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane, ``Full impedance cardiography measurement device using raspberry PI3 and system-on-chip biomedical instrumentation solutions," IEEE J. Biomed. Health Informat., vol. 22, no. 6, pp. 1883-1894, Nov. 2018.
[6] A. Li, S. Shan, andW. Gao, ``Coupled bias-variance tradeoff for cross-pose face recognition," IEEE Trans. Image Process., vol. 21, no. 1, pp. 305-315, Jan. 2012.
[7] C. Ding, C. Xu, and D. Tao, ``Multi-task pose-invariant face recognition," IEEE Trans. Image Process., vol. 24, no. 3, pp. 980-993, Mar. 2015.
[8] J. Yang, Z. Lei, D. Yi, and S. Li, ``Person-specific face antispoofong with subject domain adaptation," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 797-809, Apr. 2015.
[9] H. S. Bhatt, S. Bharadwaj, R. Singh, and M.Vatsa, ``Recognizing surgically altered face images using multi objective evolutionary algorithm," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.
[10] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring system using RFID and IOT using cloud," in Proc. Online Int. Conf. Green Eng. Technol. (IC-GET), Nov. 2016, pp. 1-4.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com