

E-DEPARTMENT

Assistant Professor DR.A.S.Selva Reegan, Aslin Stephy.D.M , Aswathy.N.S, Babisha.N, Sneha.R.
Stella Mary's College of Engineering

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%.

Index Terms—ATM, Automated Teller Machine, cash withdrawal, security, debit card fraud, identity theft, computer vision, biometric identification, facial recognition, Deep Convolutional Neural Network.

I. INTRODUCTION

UTOMATED Teller Machines (ATMs) have revolutionized banking by enabling self-service transactions without requiring customers to visit bank branches. Since the first ATM was installed in 1967 at a Barclays branch in London, these machines have become ubiquitous, providing 24/7 access to banking services such as cash withdrawals, deposits, fund transfers, and balance inquiries. Despite their convenience, ATMs have become vulnerable to various fraudulent activities. As of 2021, debit card fraud was the most reported form of identity theft, with approximately 270,000 reported cases. Common fraudulent techniques include skimming, shimming, cash-out schemes, and jackpotting, all of which compromise the security of ATM users and their accounts. The conventional security measure of using a Personal Identification Number (PIN) has proven inadequate, especially for users who struggle to memorize [1]their PINs or fear card theft. This security gap necessitates more robust authentication methods. Nowadays, crimes at ATMs have become an alarming issue. Security for the customer's account is not guaranteed by PIN. Many people,

who aren't familiar with the concept of PIN are unlikely to memorize and recognize it. There are many people who mistrust PIN, such as, if they have lost their card, they would feel unsafe that their account could be accessed by others and they would lose all their money.



fig.1 ATM machine.

The integration of Artificial Intelligence with Internet of Things (AIoT) presents a promising solution. By combining biometric identification techniques with deep learning algorithms, specifically Deep Convolutional Neural Networks, ATM security can be significantly enhanced. Facial recognition technology, similar to applications already in use for crime investigation and office attendance, can verify the identity of ATM users by matching their faces with stored data. This approach eliminates the possibility of fraud resulting from card theft or PIN compromise, as biometric features cannot be replicated. The proposed facial recognition system achieves 97.93% accuracy on real-time datasets, demonstrating superior performance compared to existing security methods. Additionally, the system incorporates liveness-detection technology to prevent fraud attempts using photographs, videos, or masks.

to attackers. This research revealed that banks' heavy investments in PIN security through Hardware Security Modules (HSMs) may be undermined by poorly positioned surveillance cameras, which can create side-channels exposing sensitive information. Card-less ATM transactions offer promising security enhancements. Yadav et al. (2020) proposed a mobile app system generating time-limited security codes that can function without network connectivity. This three-level security approach verifies user identity at login, through app-based authentication at the ATM, and via user-generated reference numbers for specific transactions, effectively addressing card cloning vulnerabilities. QR code technology represents another innovative approach to ATM security. Research by Patil et al. (2019) developed the "GetNote" Android application that generates encrypted QR codes containing credentials such as card number, amount, PIN, and CVV. The ATM scans and decrypts these codes, authenticating the information against the bank's database. This system offers superior security by eliminating the need for users to manually enter PINs during transactions. Dual identification systems combining traditional PINs with additional authentication factors have shown significant potential. Kale and Jajulwar (2019) designed a system requiring users to choose between fingerprint verification or OTP authentication after entering their PIN. This approach effectively counters common ATM fraud techniques such as skimming, shoulder surfing, and card trapping by introducing biometric verification or time-limited codes sent via GSM module. Biometric recognition technologies are increasingly central to ATM security innovation. Tyagi et al. (2019) explored iris recognition for ATM authentication, noting its stability over time, uniqueness, and high reliability. Similarly, research on fingerprint recognition using minutiae feature extraction algorithms has been integrated with message authentication techniques and location tracking through GPS to identify fraudulent transaction attempts. NFC technology offers promising advances in ATM security. Mahansaria and Roy (2019) proposed replacing physical ATM cards with smartphones operating in NFC Card Emulation mode. Their system maintained strong security through data encryption and secure channels while eliminating physical cards entirely, with security analysis and threat modeling confirming the approach's robustness against common vulnerabilities. Novel approaches include user-defined Personal Identification Numbers (UDPINs) communicated through mobile phones to GSM modules embedded in ATMs. Swathi et al. (2018) demonstrated this method's advantage in allowing dynamic PIN changes for each transaction, reducing concerns about card loss and eliminating the need for immediate deactivation. More advanced biometric approaches include authentication through electrocardiogram signals based on emotional states.

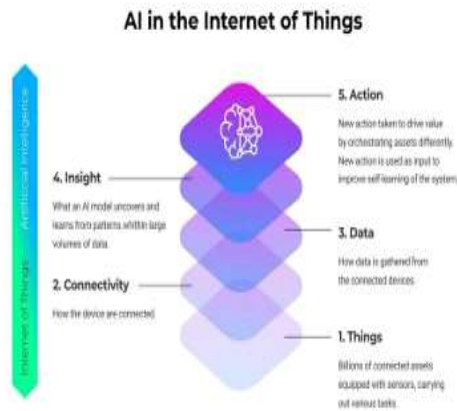


Fig:2 AI in the Internet Of Things

Face-based authentication can function as either a primary verification method or as a secondary measure alongside traditional PINs. The touchless nature of facial recognition adds convenience while maintaining security, as the system automatically locks access when the authenticated user moves away from the ATM camera. This comprehensive security model protects users' accounts and enhances the overall ATM experience through improved usability and transaction efficiency[2].

II. LITERATURE SURVEY

Video surveillance systems in ATM environments inadvertently create security vulnerabilities that can compromise PIN confidentiality. A 2020 study by Seneviratne et al. demonstrated that PINs could be inferred from video footage even when both keypad and fingertips are not visible

Gupta and Chowdhary (2017) proposed a framework that analyzes ECG signals to differentiate between normal anxiety and threat conditions, enabling ATMs to block transactions when users appear to be under duress. Comprehensive anti-theft modules for ATM machines have also been developed using Raspberry Pi systems. These modules integrate fingerprint authentication for ATM center access with accelerometers, cameras, and automatic shutters to detect and respond to theft attempts. When suspicious activity is identified, the system can automatically alert police, lock down the facility, and provide real-time video monitoring through web servers. These diverse research directions demonstrate significant advances in ATM security beyond traditional card-and-PIN systems, with biometric verification, mobile integration, and emotional analysis emerging as particularly promising approaches to counter evolving security threats.

III. EXISTING SYSTEM

The existing ATM authentication landscape relies primarily on traditional password-PIN systems combined with physical access cards. These cards typically feature magnetic stripes or chips that store account information, with a fixed Personal Identification Number serving as the verification mechanism[3]. When chips fail, magnetic stripes often function as backup identification methods, creating redundancy but also potential security vulnerabilities. Recent innovations have introduced QR-based cash withdrawal systems that allow customers to bypass physical cards entirely. These systems require ATMs equipped with QR code scanners that can detect and decrypt information stored within the codes. Applications like 'GetNote' generate encrypted QR codes containing essential credentials including card number, transaction amount, PIN, and CVV number. The ATM authenticates these details against the bank's database before dispensing cash, while maintaining traditional withdrawal options for customers who prefer conventional methods[4].

Some financial institutions have implemented more robust security architectures that incorporate biometric verification alongside traditional PIN-based authentication. These systems combine fingerprint recognition with standard PIN verification to establish dual-factor authentication. Fingerprint verification typically employs minutiae feature extraction algorithms to identify unique patterns. Additionally, some systems integrate GSM technology to enable transaction confirmation through mobile approval messages. Location tracking via GPS provides another security layer, with automatic card blocking triggered when unauthorized usage is detected and immediate notifications sent to the legitimate cardholder. The biometric authentication components of these

systems employ various algorithmic approaches including Gaussian Mixture Models, Artificial Neural Networks, Fuzzy Expert Systems, and Support Vector Machines. Dimensional reduction techniques like Linear Discriminant Analysis and Principal Component Analysis help process biometric data efficiently[5]. These systems can authenticate identity by comparing new biometric measurements against stored data profiles, with matches confirming the user's claimed identity. Despite these advances, current systems face significant limitations. Authentication accuracy remains below 100%, with face detection and training data processes operating somewhat slowly. Detection range is limited, and systems cannot replay live video to capture missed facial recognition opportunities. Manual intervention is still required for instructor and training set management. Unimodal biometric implementations struggle with various challenges including noisy data, variations within the same class, restricted degrees of freedom, non-universality issues, vulnerability to spoofing attacks[6], and unacceptable error rates. Additional practical drawbacks include the requirement for users to carry mobile phones with specific applications installed, creating potential accessibility barriers for some banking customers.

IV. PROPOSED SYSTEM

This project proposes an innovative automatic teller machine security model that combines traditional physical access cards with electronic facial recognition powered by Deep Convolutional Neural Networks. The system leverages deep learning, a subset of machine learning within artificial intelligence, to achieve greater accuracy in facial recognition compared to traditional machine learning approaches. The deep facial recognition system follows a systematic process beginning with face detection to localize faces, followed by alignment to normalized canonical coordinates, and culminating in the facial recognition module[7]. This module incorporates anti-spoofing technology to distinguish between live and fake faces, processes facial variations such as poses and ages, utilizes various architectures and loss functions to extract discriminative features during training, and employs face matching methods for feature classification after deep feature extraction from test data.

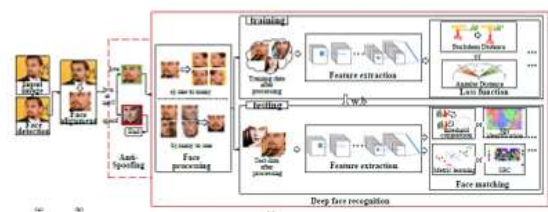


Fig:3 Deep face recognition.

The CNN face recognition implementation uses 32 filters in the first layer to capture various image features such as sharp edges, color variations, and outlines, with subsequent layers increasing filter counts by powers of two. A 5×5 pixel sliding window serves as the kernel size, moving at a rate of 1×1 pixels across the entire image. Input images are preprocessed to 64×64×3 dimensions, representing RGB color channels. The network employs uniform kernel initialization, ReLU activation functions, and the Adam optimizer. Training occurs in batches of 10 rows over 10 epochs to optimize the network’s weight adjustments. When the stored facial image and captured image do not match, indicating an unauthorized user, the system generates a Face Verification Link. This link is sent to the account holder to verify the unauthorized user’s identity through dedicated artificial intelligent agents that provide remote certification. Based on this verification, the system either authorizes the transaction or signals a security violation alert to the banking security protocol. The system architecture follows a structured workflow from initial account creation and face enrollment to transaction processing. When a user attempts an ATM transaction, their face is captured and verified against stored datasets. For authorized users, the transaction proceeds normally[8]. For unmatched faces, the Unknown Face Forwarder Link is activated, requiring the legitimate account holder to either accept or reject the transaction. If rejected, the card is blocked to prevent unauthorized access. This facial biometric authentication system offers numerous advantages: uniqueness for each user, fraud reduction, prevention of theft and criminal activities, trustworthy authentication, secure lifestyle infrastructure, unauthorized access prevention, and fast, accurate prediction. The face verification system ensures that biometric features cannot be replicated, providing enhanced security over traditional PIN-based systems. The implementation includes various modules such as an ATM Simulator for testing XFS-based ATMs and a comprehensive Face Recognition Module[9]. This module encompasses face enrollment, image acquisition, preprocessing steps (grayscale conversion, resizing, noise removal, binarization), face detection using Region Proposal Networks (RPN), and feature extraction to identify key facial characteristics for classification

V. SYSTEM ANALYSIS

Software testing is an essential part of the development process, with several distinct methodologies. Unit testing examines individual components of source code to verify their correctness, using automated test scripts that check if each section meets design requirements and behaves as expected. Python’s built-in unittest framework makes this process more efficient. Integration testing evaluates how multiple parts of

an application work together, identifying defects in their interactions. System testing validates the complete software product, ensuring it meets end-to-end specifications through methods like black box and white box testing[10]. Hardware and software specifications are crucial for proper system implementation. The recommended hardware includes an Intel Core i5 processor at 2.60 GHz with 8 GB of RAM and 320 GB of disk space, supporting Windows 10, macOS, or Linux operating systems. Software requirements specify Python 3.7.4 for server-side programming, HTML/CSS/Bootstrap for client-side development, Flask 1.1.1 as the IDE, MySQL 5 for the backend database, and Wampserver 2i as the server platform.

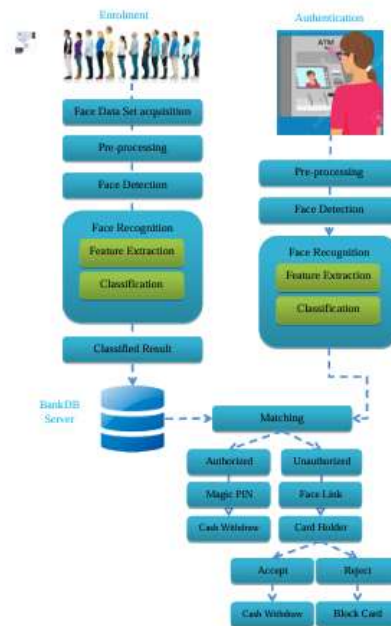


Fig. 4 system flow.

Python 3.7.4 is a versatile high-level programming language created by Guido van Rossum, designed to be highly readable with English keywords rather than punctuation. It supports both object-oriented and procedural programming paradigms and is widely used by major technology companies. Python’s extensive standard libraries support various applications including machine learning, GUI development, web frameworks, image processing, web scraping, and scientific computing. Several specialized Python libraries enhance its functionality. TensorFlow provides an end-to-end platform for machine learning with intuitive APIs. Keras, running on TensorFlow, enables fast experimentation with deep learning models. Pandas offers powerful data analysis and

manipulation tools with flexible data structures. NumPy facilitates high-performance array processing for mathematical operations.

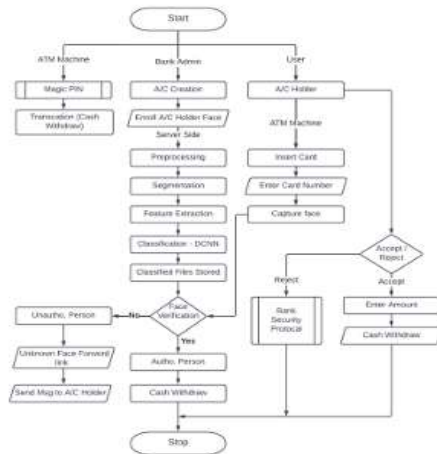


Fig:5 Flowchat.

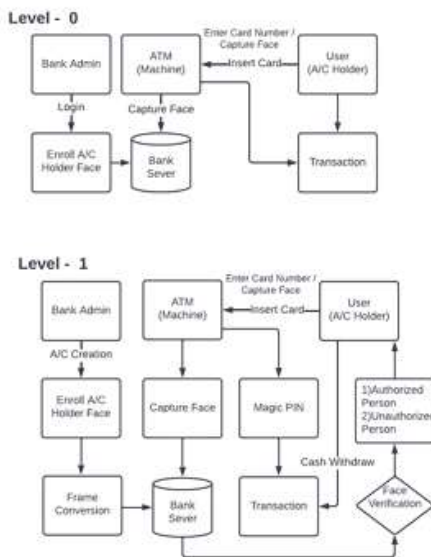


Fig:6 ATM-Data flow diagram.

Matplotlib creates static, animated, and interactive visualizations. Scikitlearn supplies machine learning algorithms that interoperate with NumPy and SciPy. Pillow and OpenCV handle image processing and computer vision tasks respectively. MySQL, an open-source relational database management system, manages database records through SQL

queries. It's popular for its scalability, ease of use, and compatibility with PHP for web applications. WampServer provides a Windows web development environment that integrates Apache2, PHP, and MySQL with PhpMyAdmin for database management. Bootstrap 4, a free and open-source framework, creates responsive websites with cross-browser compatibility. Flask, a micro web framework for Python, offers tools and libraries for building web applications ranging from simple blogs to commercial websites, emphasizing simplicity and extensibility.

VI. CONCLUSION

To evaluate the performance of our method, we compare our method against the state-of-the-art methods in Fddb. The evaluation indicators include: recall rate is used to evaluate the proportion of the detected face to the total face of the sample mark; false positive is the number of errors in the detected face. These two indicators are expressed by the ROC (Receiver Operating Characteristic) curve. The results are shown in FIGURE 1(a) and FIGURE 1(b). The ROC curve detection results show that the traditional face detection method VJ recall rate is only 66.6%, the detection method based on deep learning has been greatly improved. Our method achieves state-of-the-art performance in terms of both the discrete ROC curve and continuous ROC curve. Our discrete ROC curve is superior to the MTCNN. We also obtain the best true positive rate of the discrete ROC curve at 2000 false positives (96.1%). In addition, the possible influencing factor is that our method is not very effective in detecting the side face. The ROC curve does not clearly indicate which method is better, so another indicator AUC is used to illustrate the pros and cons of the method. AUC represents the area proportion under the ROC curve and the value is between 0 and 1. The higher the AUC value is, the better the method performance will be. Then test on the WIDER FACE dataset, WIDER FACE is a more challenging benchmark than Fddb in face detection. It is very encouraging to see that our model consistently achieves the competitive performance across the three subsets. It has higher robustness for faces with large occlusion and angle change, which is basically consistent with the evaluation results in the Fddb dataset. 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. Some potential future enhancements for the Real Time Secure Clickbait and Face Biometric ATM User Authentication and Multiple Bank Transaction System could include: improved accuracy, where the system could be further optimized to improve the accuracy of face recognition and verification, reducing the likelihood of false positives or false negatives; integration with additional security features, where the system could be integrated with additional security features, such as biometric authentication or OTP verification, to further enhance the security of ATM transactions; and multi-factor authentication, where the system could be expanded to support multi-factor authentication, requiring users to provide additional forms of authentication in addition to facial recognition, such as a password or a fingerprint scan. Other potential enhancements include real-time alerts, where the system could be configured to send real-time alerts to bank administrators or security personnel in the event of a security breach or suspicious activity; integration with mobile banking, where the system could be integrated with mobile banking applications to enable users to perform transactions and account management tasks using their mobile devices; support for multiple languages, making it more accessible to users who are not fluent in the system's default language; and support for additional transaction types, where the system could be expanded to support additional types of transactions, such as account transfers or bill payments, to provide users with a more comprehensive banking experience. Overall, these enhancements could help to further improve the security, accessibility, and functionality of the Real Time Secure Clickbait and Face Biometric ATM User Authentication and Multiple Bank Transaction System, providing users with a more secure and convenient banking experience.

REFERENCES

- [1] 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. Mammour, "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. 716719, doi: 10.1109/ISdea.2012.400.
- [4] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, "RaspberryPi 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. Kadir-Talha, F. Abtahi, M. Attari, and F. Seoane, "Full impedance cardiography measurement device using raspberryPI3 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, and W. 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 anti-spoofing 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. 14.