Leveraging Face Recognition Technology for Secure ATM Transaction

Mehfooz Ur Rehman[1] **and H Jayamangala**[2]
PG Student, Department of Computer Applications[1]
Assistant Professor, Department of Computer Applications[2]
Vels Institute of Science Technology and Advanced Studies, Pallavaram, Chennai, India
22304260@vistas.ac.in and jayamangala.scs@velsuniv.ac.in

Abstract: *ATM or Automated Teller Machines are widely used by people nowadays. Performing cash withdrawal transactions with ATMs is increasing day by day. ATMs are a 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 fingerprinting, 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 holders to verify the identity of unauthorized users through some dedicated artificial intelligent agents, for remote certification. However, it is 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 to 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*

Keywords: ATM card

I. INTRODUCTION

Automated Teller Machines have revolutionized the banking sector by providing easy access to customers and loading off the burden from bank officials. Some of the uses of an ATM are- The most common uses of an Automated Teller Machine include withdrawing money, checking balance, transferring money, or changing the PIN (Personal Identification Number) Newer and advanced ATMs also provide options to open/withdraw a Fixed Deposit (FD), or to apply for a personal loan. You can also book railway tickets, pay the insurance premiums, income tax & utility bills, recharge mobile, and deposit cash. Some of these facilities require you to register at the bank branch. Customers can now do money transactions at their convenience. ATMs today are installed in public spaces, highways, malls, market places, railway/airport stations, hospitals, etc. Automated Teller Machines provide 24×7 access anywhere. ATMs help to avoid the hassle of standing in long queues at the bank even for simpler transactions like withdrawing money. It has also helped in reducing the workload of the bank officials.

II. LITERATURE SURVEY

Ghostface Nets: Lightweight Face Recognition Model from Cheap Operations by Mohammad Alansari; Oussama Abdul Hay. (Year 2023) Algorithms/Techniques: CNN. To develop a new set of lightweight architectures named Ghostface Nets. Ghostface Nets are effective for applications with minimal computational complexity

DOI: 10.48175/IJARSCT-18406

constraints. Ghost face nets, also known as low-visibility face detection networks, are specialized convolutional neural networks (CNNs) designed to detect faces in challenging conditions such as low light, fog, or smoke. These networks are trained on diverse datasets that include images with varying degrees of visibility to ensure robustness in real-world scenarios. By adapting architectures and training strategies, ghost face nets excel at recognizing facial features even in obscured or low-contrast environments.

Design for Visitor Authentication Based on Face Recognition Technology Using CCTV By Hyung-Jin Mun; Min-Hye Lee (Year: 2023). Algorithm/Techniques: YoLoV3. To present a visitor authentication technology that uses CCTV with a Jetson Nano and webcam. Although the system was applied to two representative microprocessors, the Raspberry Pi and the Jetson Nano, it was difficult to apply in real life because the operation was very slow and the desired result. Install CCTV cameras at entry points. Employ computer vision for real-time face detection. Utilize a face recognition algorithm to verify visitors against a database. Authenticate entry based on recognized faces.

III. METHODOLOGY

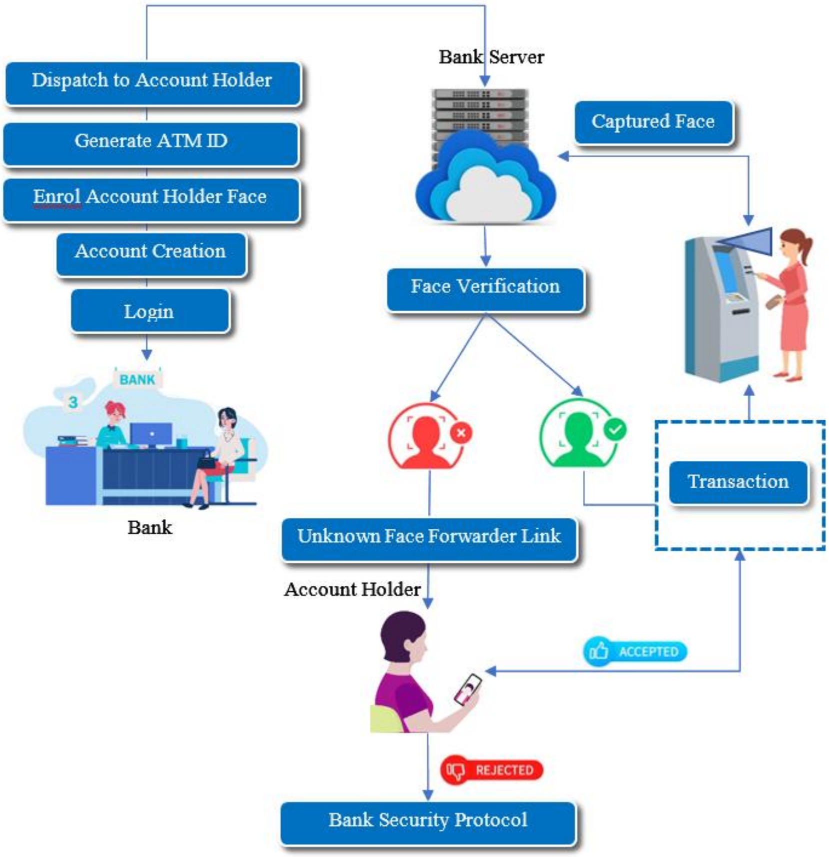

Fig.1 System architecture

Dataset:

Table Name: Customer Account Creation					
S.no	**Field**	**Data Type**	**Field Size**	**Constraint**	**Description**
1	Id	Varchar	20	Null	Id
2	Name	Varchar	20	Null	Name

DOI: 10.48175/IJARSCT-18406

3	Address	Varchar	50	Null	Address
4	Mobile number	Bigint	20	Null	Mobile number
5	Email	Varchar	50	Null	Email
6	Account number	Varchar	30	Null	Account number
7	Debit card number	Varchar	30	Null	Debit card number
8	Bank Name	Varchar	20	Null	Bank Name
9	Branch Name	Varchar	20	Null	Branch Name
10	Deposit amount	Double	500	Null	Deposit amount
11	Customer id	Int	11	Primary key	Customer id
12	Password	Varchar	20	Null	Password
13	Create date	Timestamp	Timestamp	Null	Create date

Fig.2 Dataset

IV. EXPERIMENTAL RESULTS

IoT is the data “supplier”, while machine learning is the data “miner”. To make the data supplied by IoT work, it needs to be refined. Dozens of IoT sensors and external factors are producing a myriad of data points. The “miner’s” task here is to identify correlations between them, extract meaningful insight from these variables and transport it to the storage for further analysis.

TensorFlow: TensorFlow is an open-source machine learning framework used for building and training neural network models, including

Convolutional Neural Networks (CNNs) for facial recognition

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 holders to verify the identity of unauthorized users through some dedicated artificial intelligent agents, for remote certification. However, it is 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 to 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%.

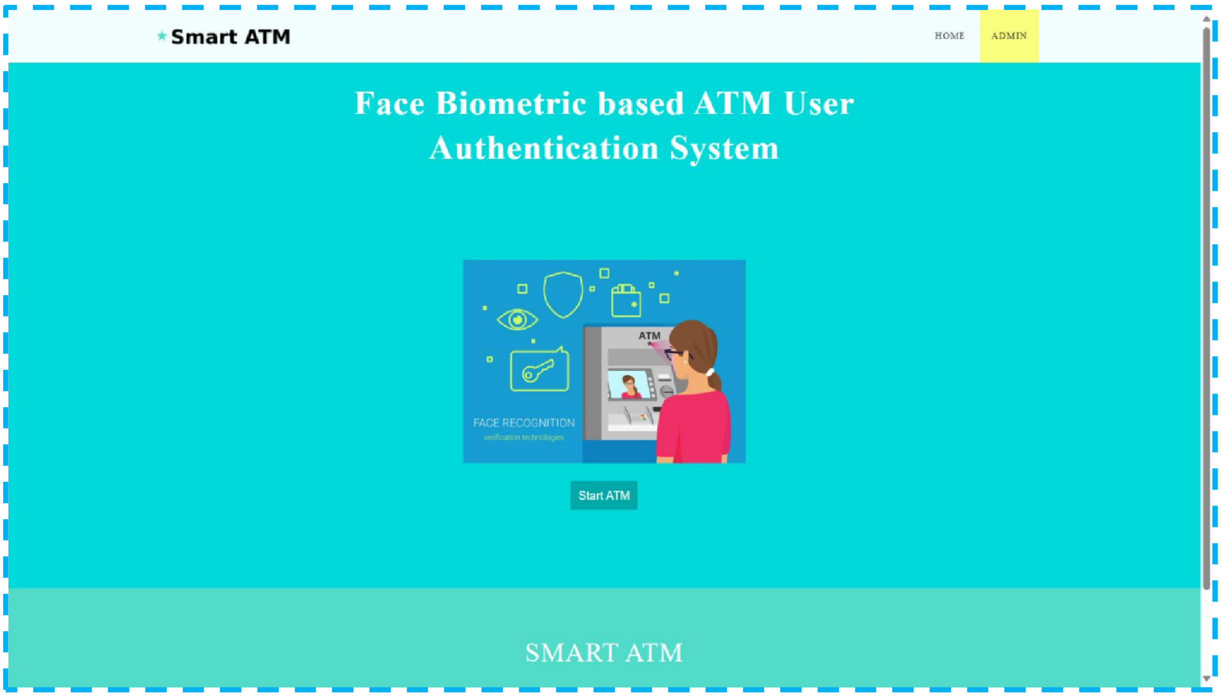
Smart ATM
HOME
ADMIN
Face Biometric based ATM User Authentication System
ATM
FACE RECOGNITION
verification technologies
Start ATM
SMART ATM

Fig. 3 Home page

V. CONCLUSION

The ATM User Face Identification System using CNN and a face verification link is a sophisticated and innovative solution that enhances the security of ATM transactions. It is designed to authenticate users' identities by detecting and recognizing their faces, which ensures that only authorized users can access their accounts. Moreover, in the event of an unauthorized access attempt, the system sends a face verification link to the authorized account holder's mobile number to confirm the transaction, thus preventing fraudulent activities.In conclusion, the implementation of the ATM User Face Identification System using CNN and a face verification link using Python Flask and MySQL is a significant step towards enhancing the security of ATM transactions.It provides a reliable and robust solution that ensures the safety of users' data and transactions, thus enhancing user trust and confidence in the banking system. By integrating facial recognition technology, it enhances security while providing convenience to users. With its ability to accurately identify individuals, it mitigates the risk of unauthorized access and fraudulent transactions. Moreover, its user-friendly interface streamlines the authentication process, ensuring a seamless and efficient banking experience. Overall, this system represents a significant advancement in ATM security, prioritizing both safety and usability for customers. It elevates the authentication process to new heights of accuracy and reliability. This system not only fortifies defenses against identity theft and fraudulent activities but also enhances user experience through its intuitive interface. Its implementation signifies a proactive approach by financial institutions towards safeguarding customer assets and maintaining trust in digital banking services. As technology continues to evolve, such innovative solutions pave the way for a safer and more seamless banking landscape, ensuring the protection of both individuals and their financial assets. The ATM User Face Identification System represents a pivotal advancement in banking security, embodying the fusion of cutting-edge technology with the imperative need for enhanced user authentication. By harnessing the power of facial recognition, it sets a new standard for safeguarding customer transactions against unauthorized access, fraudulent activities. This system underscores a commitment to customer-centricity by streamlining the authentication process, fostering a frictionless user experience at ATMs worldwide. As financial institutions embrace digital transformation, the integration of such innovative solutions not only bolsters trust and confidence among consumers but also heralds a new era of secure, accessible, and user-friendly banking services in the digital age.

DOI: 10.48175/IJARSCT-18406

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 antispoofing 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 algorithms,'' 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.