ISSN: 0974-5823 Vol. 7 No. 8 August, 2022

*International Journal of Mechanical Engineering*

# Face Authentication ATM using Deep Learning

**S. Sam Peter**

Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.

**G. Krithik**

Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.

**M. Pratheep**

Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.

**K. Prakash**

Department of Computer Science and Engineering, Sri Krishna College of Technology,Coimbatore, India.

***Abstract* -** Nowadays, ATM scams are increasing in many countries. In India, nearly 2000 scams were recorded last year (2022). To reduce the scams and improve the security in banking, this ATM face password project can be replaced the debit or ATM cards So that the User does not need to carry their debit card everywhere. User will have their unique account number to access the ATM. After entering that unique account number, the machine will scan the User's face recognition to see if it matches the data set in the account. It executes the banking process. If not, it sends an OTP pin to the account holder's phone number by using IoT. By using the OTP PIN, the person in the ATM can withdraw the amount in that account. This system can be beneficial for the future banking system.

Index Terms – *ATM, debit card, face recognition*

## INTRODUCTION

ATMs made our life easier, introduced in 1969 in the USA. In India, the first ATM was introduced in 1987 in Mumbai by HSBC bank. Before that, everyone had to wait in their specific bank branch for a long time. If the bank branch is not in their area, they have to travel to that branch to withdraw their money. Sometimes the bank may run out of money so that the person who came for banking may return with a no withdrawal amount, but this ATM has made a big revolution in the banking field. After the introduction of ATMs, anyone can easily withdraw money from any bank inside the country just with a single swipe Card scams are occurring daily in our day-to-day lives.

There are two types of ATMs one which has the option of withdrawal, checking bank balance, transferring money online, changing PIN and the other one has the features of depositing money, checking bank balance, changing the PIN, and withdrawing money instantly. There are many different labeled ATMs. For agriculture purposes green label is used, for e-commerce transactions yellow label is used, for share transactions orange label is used, for specific queries for women pink label is used and finally, TATA groups use white label ATMs. The ATM provides 24x7 service so that people can withdraw money from anywhere and at any time.

Even though security has increased in banking, the scams also increase eventually. Using skimmers, A card can be duplicated into many cards sold in the black market, the dark web without knowing the actual cardholder. These scams are happening by using a device called card skimmers which scammers and hackers commonly use to read a card and write the copy to another card. It’s easy to purchase a card skimmer in any online store or big offline hardware store. The most common scams across the world are skimming, shimming, cash-out and jackpotting.

Shimming is nothing is the upgraded process of skimming. In this process, scammers used to read the RFID chip in the card even without the PIN anyone can withdraw money from the account holder money. In the same method of skimming the data can be made into duplicate copies and can be sold in the black market so-called dark web by selling the card details through dark web even government can't find the IP address of the seller on the dark web

Another popular method in scamming cash out in his method hackers modify the bank employee credentials and the withdrawal limit so that the stolen cards can be used to withdraw money the last famous method is jackpotting in this type of scam, which scammers used to change the hardware in the ATM so that information entered in the machine will be sent as a copy to the scammer

## RELATED WORK

The ATM plays a vital role in my world to enhance the ATMs several people have tried to find any number of ways to secure the ATM by altering the ways this section gives an overview of it

Taleb, et al.., [1] have proposed a system where the already existing security systems were upgraded to their next level by achieving facial recognition authentication using principal component analysis (PCA). With a help of an Arduino microcontroller and graphical user interface (GUI), they achieved authorization from the captured facial images verified in MatLab.

X.Pan, et al.., [3] have proposed face recognition with mainly the use of RFID technology, they introduced an intelligence access control system with an FNN algorithm.

Wazwaz et al…, [4] have proposed a computer-based face recognition and detection mainly using raspberry pi, by using boosted cascade of simple features algorithm and local binary pattern algorithm to detect human faces and recognize those faces that are detected.

Hafid et al.., [5] have proposed a paper to measurement system mainly based on two systems on chip solutions and raspberry pi. A full 3-lead ECG recorder and impedance cardiographer were implemented. Wirelessly the recordings were transmitted through Bluetooth to pc.

Li et al.., [6] have proposed a model cross pose face recognition using a regression with a coupled bias-variance tradeoff is way more stable than subspace-based face representation where recognizing faces across pose difference is a problem CMU pi and multi pi results show cross pose face recognition is better than subspace face recognition.

Ding et.al.., [7] have proposed a novel face detection framework that can manage the full range of pose variations within 90 degrees of the weave. It uses CMUPI, FERET, and MULTIPI databases. It performs a single task-based baseline. The algorithm used in this methodology is the CNN algorithm.

J.yang et.al.., [8] have proposed a face ant spoofing project. In this methodology, faces recognize with a given dataset if the person is a spoofer. By considering the fake samples for training author approached a subject domain adaption method to blend virtual features. The extensive datasets used in this are CASIA and REPLAY-ATTACK.

H.S. Bhatt et al.., [9] have proposed a multi-objective evolutionary granular algorithm that matches the faces before and after plastic surgery, firstly this algorithm generates non-disjoint face granules at multiple levels of granularity. Granular information is sensing, using, a multiobjective genetic approach, at the same time optimizing the selection of features extractor for each face granular along with the masses of individual granules.

## PROPOSED SYSTEM

Face authentication ATM is developed to replace the debit card with face authentication, It increases the security in the banking field and doesn't require any debit card to withdraw or transfer money through ATMs. This method will be more user friendly that anyone can easily withdraw and transfer money.

### 3.1 Database Module

The admin who is a bank employee has the admin permission to add or edit the database on the client-side server, by this process employee use to create a new client ATM account like in **Fig 1**

The admin creates a database for the client by adding their details like name, phone number, email, father's name, address, etc. after entering these details. Admin will capture the face of the client's face in a frame by frame manner then they are classified into different layers using the DCNN algorithm and then saved as a client database where the client will get a unique ID to access it'

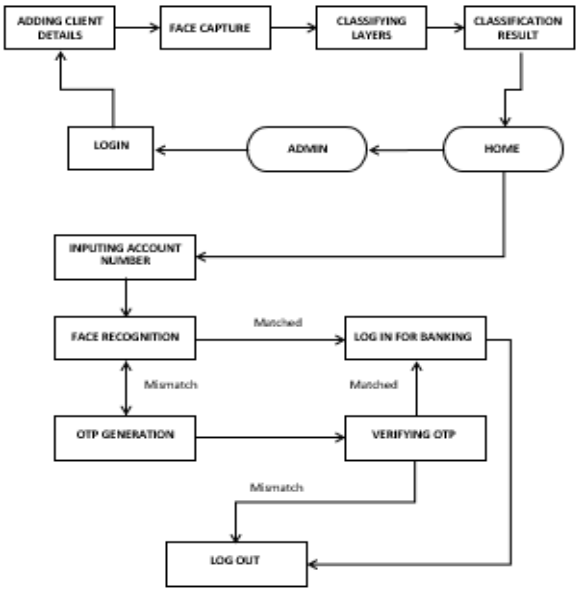


**Fig.1 Block Diagram for creating client database**

### 3.2 Face Authentication Module

In this module face during enrollment for the database the face is scanned and then using the DCNN algorithm this scanned photo is divided into five layers which in the **Fig 2** block diagram

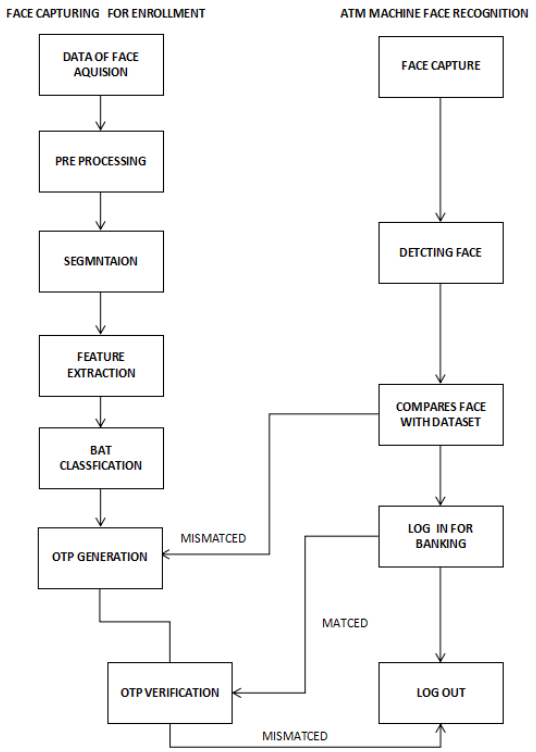


**Fig.2 Block Diagram of Face authentication**

Using the unique ID when a client opens their ATM account, the machine scans the client's face and then by using the DCNN it compares the face to the database picture if it matches it takes it to the banking site

### 3.3 IoT Module

When the face captured in the ATM doesn't match with the face in the bank database then the IoT helps here. The account holder gets a special PIN for the phone number which they registered in the bank server. Using this PIN client can enter the data in the ATM so that if the random OTP matches with the OTP in the ATM then the person receives the banking option or else the page will automatically log out, After withdrawing the amount, the account holder receives a withdrawal message through normal via text and email which have been registered in the bank server

## RESULT

In this part, the result is shown are obtained output through by implementing the DCNN algorithm in the banking sector through ATM the withdrawal money is sent through the via SMS and email

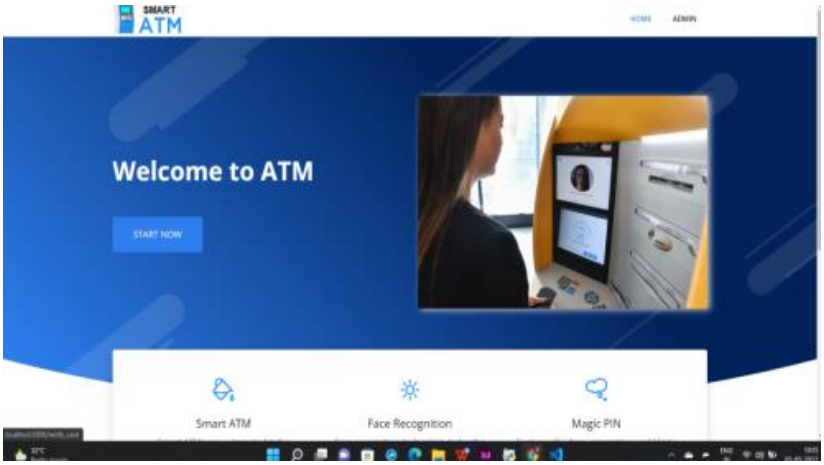


**Fig.3 home page**

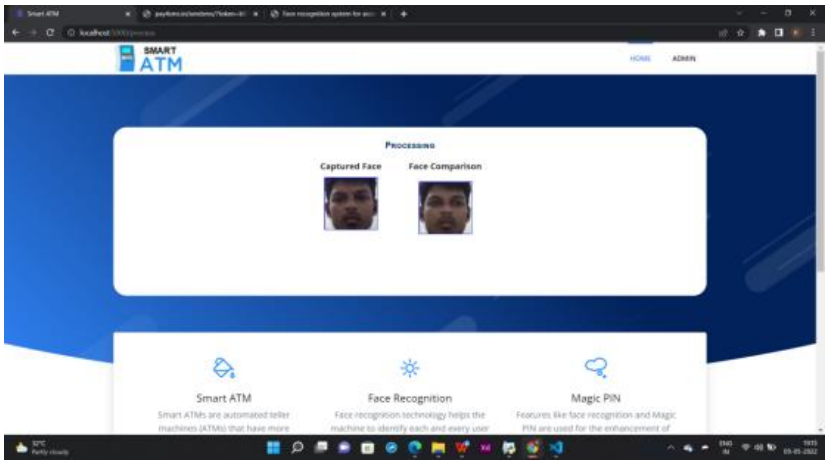


**Fig.4 Face authentication process**

This is the home page **Fig 3** of the ATM using face authentication as a password it has the basic instruction about the ATM process about how it works to start the banking client can click the start now icon displayed on the screen after that it will redirect into another URL in which the client has entered their unique ID number which was given to the client after creating their ATM face password account after entering the unique ID

number the page will redirect to a face scanner URL like in **Fig 4** in which the ATM camera scans for client's face if it matches then the client is redirected into the banking URL like **Fig 5**

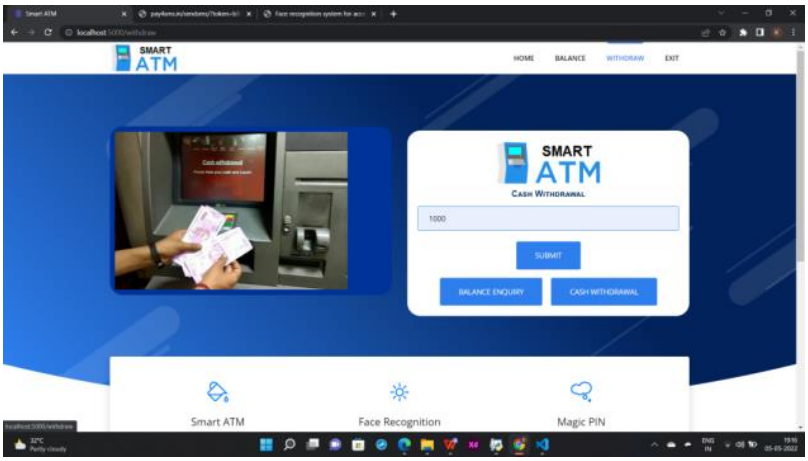


**Fig.5 Main Banking Page**

If the face doesn't match with the bank database photo then an OTP will send by ATM and redirect to a page where the client can enter the PIN if the PIN matches with the ATM OTP then the URL will redirect to the banking or it will automatically logout the user.


**Fig.6 Withdrawal statement**

After completing the withdrawal the client will receive an SMS and email so that account holders will be more aware of their withdrawal statement

## CONCLUSION

By using the DCNN algorithm the face authentication along with cloud OTP code which has been set as a password, Now the ATMs will be more secure and anyone can access their bank and withdraw the amount by using unique ATM IDs, There is no need for using the debits anymore in the ATMs so that many scams can be avoidable like skimming, cash out, jackpotting, etc. By using five layers in the DCNN algorithm it's very hard to open the account holder's money without their acknowledgment. This method is useful, In case the holder forgets to take their debit card with them during long travel they need to worry about the money to withdraw from the ATM because this methodology account holders face as their PIN to withdraw from their account in case if our face. This project can be enhanced by adding layers to the DCNN algorithm and by adding speech

recognition so that the ATMs will more secure but same time it's is difficult to recognize the voice of the account holder when they have a sore throat or any problem it can be quite hard to process the voice of the person but it's never impossible so that in future enhancement it can be added to secure the bank more efficiently.

## REFERENCES


[1] M. P. Paidoussis, *Fluid-structure interactions: slender structures and axial flow*, vol. 1. Academic press, 1998.

[2] H.-J. Bungartz and M. Schäfer, *Fluid-structure interaction: modelling, simulation, optimisation*, vol. 53. Springer Science & Business Media, 2006.

[3] A. M. S. Al-Janabi, A. H. Ghazali, Y. M. Ghazaw, H. A. Afan, N. Al-Ansari, and Z. M. Yaseen, "Experimental and numerical analysis for earth-fill dam seepage," *Sustain.*, 2020.

[4] N. S. Radhi, K. F. Morad, M. H. Hafiz, A. A. Atiyah, and A. Bouaissi, "OPTIMIZATION OF NICKEL CONTENT ON SOME PROPERTIES OF (NITI) SHAPE MEMORY ALLOY," *Knowledge-Based Eng. Sci.*, vol. 1, no. 1, pp. 40–47, 2020.

[5] C. H. Tai, K. M. Liew, and Y. Zhao, "Numerical simulation of 3D fluid–structure interaction flow using an immersed object method with overlapping grids," *Comput. Struct.*, vol. 85, no. 11–14, pp. 749–762, Jun. 2007.

[6] S. Q. Salih *et al.*, "Thin and sharp edges bodies-fluid interaction simulation using cut-cell immersed boundary method," *Eng. Appl. Comput. Fluid Mech.*, vol. 13, no. 1, pp. 860–877, 2019.

[7] T. T. Nguyen, D. Shyam Sundar, K. S. Yeo, and T. T. Lim, "Modeling and analysis of insect-like flexible wings at low Reynolds number," *J. Fluids Struct.*, vol. 62, pp. 294–317, 2016.

[8] M. R. Rasani, M. S. Aldlemy, and Z. Harun, "Fluid-structure interaction analysis of rear spoiler vibration for energy harvesting potential," *J. Mech. Eng. Sci.*, vol. 11, no. 1, pp. 2415–2427, 2017.

[9] B. Sebastian, T. Dunne, and R. Rannacher, "Numerics of Fluid-Structure Interaction," vol. 37, pp. 333–378, 2008.

[10] M. S. Aldlemy, M. R. Rasani, A. K. Ariffin, and T. M. Y. S. T. Ya, "Adaptive mesh refinement immersed boundary method for simulations of laminar flows past a moving thin elastic structure *," vol. 32, no. 1, pp. 148–160, 2020.

[11] M. S. Aldlemy, M. Rasani, T. M. Y. S. Ya, and A. K. Ariffin, "Dynamic adaptive mesh refinement of fluid structure interaction using immersed boundary method with two stage corrections," *Sci. Iran.*, p. , 2018.

[12] O. A. Alawi *et al.*, "Effects of binary hybrid nanofluid on heat transfer and fluid flow in a triangular-corrugated channel: An experimental and numerical study," *Powder Technol.*, 2022.

[13] W. A. Wall, A. Gerstenberger, P. Gamnitzer, C. Förster, and E. Ramm, "Large deformation fluid-structure interaction--advances in ALE methods and new fixed grid approaches," in *Fluid-structure interaction*, Springer, 2006, pp. 195–232.

[14] G. Hou, J. Wang, and A. Layton, "Numerical Methods for Fluid-Structure Interaction — A Review," vol. 12, no. 2, pp. 337–377, 2012.

[15] M. Aldlemy, "EFFECT OF CONDUCTIVITY IN CORROSION PROBLEM USING BOUNDARY ELEMENT METHOD AND GENETIC ALGORITHM," *Knowledge-Based Eng. Sci.*, vol. 1, no. 01, pp. 58–63, 2020.

[16] M. B. Ghomizad, H. Kor, and K. Fukagata, "A structured adaptive mesh refinement strategy with a sharp interface direct-forcing immersed boundary method for moving boundary problems," vol. 16, no. 2, pp. 1–22, 2021.

[17] W. Wall, A. Gerstenberger, and U. Mayer, "Advances in fixed-grid fluid structure interaction," in *ECCOMAS Multidisciplinary Jubilee Symposium*, 2009, pp. 235–249.

[18] O. A. Alawi, A. H. Abdelrazek, M. S. Aldlemy, and W. Ahmed, "Heat Transfer and Hydrodynamic Properties Using Different Metal-Oxide Nanostructures in Horizontal Concentric Annular Tube : An

Optimization Study," 2021.

[19] R. S. Mohammad, M. S. Aldlemy, S. Al Hassan, A. I. Abdulla, M. Scholz, and Z. M. Yaseen, "Frictional Pressure Drop and Cost Savings for Graphene Nanoplatelets Nanofluids in Turbulent Flow Environments," pp. 1–17, 2021.

[20] M. M. A. Campos *et al.*, "Determination of lead content in medicinal plants by pre-concentration flow injection analysis--flame atomic absorption spectrometry," *Phytochem. Anal. An Int. J. Plant Chem. Biochem. Tech.*, vol. 20, no. 6, pp. 445–449, 2009.

[21] M. S. Aldlemy, M. R. Rasani, T. M. Y. S. Tuan, and A. K. Ari, "Dynamic adaptive mesh re nement of uid-structure interaction using immersed boundary method with two-stage corrections," vol. 26, pp. 2827–2838, 2019.

[22] T. Lee, M. Leok, and N. H. McClamroch, "Geometric numerical integration for complex dynamics of tethered spacecraft," *Proc. 2011 Am. Control Conf.*, no. April, pp. 1885–1891, 2011.

[23] H.-J. Bungartz, M. Mehl, and M. Schäfer, *Fluid Structure Interaction II: Modelling, Simulation, Optimization*, vol. 73. Springer Science \& Business Media, 2010.

[24] T. Dunne, R. Rannacher, and T. Richter, "Numerical simulation of fluid-structure interaction based on monolithic variational formulations," *Fundam. trends fluid-structure Interact.*, pp. 1–75, 2010.

[25] C. Farhat and V. K. Lakshminarayan, "An ALE formulation of embedded boundary methods for tracking boundary layers in turbulent fluid–structure interaction problems," *J. Comput. Phys.*, vol. 263, pp. 53–70, Apr. 2014.

[26] R. Codina, G. Houzeaux, H. Coppola-Owen, and J. Baiges, "The fixed-mesh ALE approach for the numerical approximation of flows in moving domains," *J. Comput. Phys.*, vol. 228, no. 5, pp. 1591–1611, 2009.

[27] S. Liu, H. A. Afan, M. S. Aldlemy, N. Al-Ansari, and Z. M. Yaseen, "Energy analysis using carbon and metallic oxides-based nanomaterials inside a solar collector," *Energy Reports*, vol. 6, pp. 1373–1381, 2020.

[28] C. Soulaine, M. Quintard, B. Baudouy, and R. Van Weelderen, "Numerical Investigation of Thermal Counterflow of He II Past Cylinders," *Phys. Rev. Lett.*, vol. 118, no. 7, pp. 1–5, 2017.

[29] T. Wick, "Flapping and contact FSI computations with the fluid-solid interface-tracking/interface-capturing technique and mesh adaptivity," *Comput. Mech.*, vol. 53, no. 1, pp. 29–43, 2014.

[30] J. Donea, A. Huerta, and J. Ponthot, "Ph., Rodriguez-Ferran A. Arbitrary Lagrangian-Eulerian methods. Encyclopedia of computational mechanics," *Fundamentals*, vol. 1, 2004.

[31] M. S. Aldlemy, S. A. K. A. R. A. M. A. T. Ya, and R. Alebrahim, "Composite patch reinforcement of a cracked simply-supported beam traversed by moving mass," vol. 14, no. 1, pp. 6403–6416, 2020.

[32] S. Shahmiri, "A Hybrid ALE-Fixed-Grid Approach for Fluid-Structure Interaction," vol. 22, no. 22, 2014.

[33] X. YANG and M. bin LIU, "Bending modes and transition criteria for a flexible fiber in viscous flows," *J. Hydrodyn.*, vol. 28, no. 6, pp. 1043–1048, 2016.

[34] J. Baiges Aznar, "The Fixed-Mesh ALE method applied to multiphysics problems using stabilized formulations," *Mater.*, vol. 14, no. December, pp. 01–2011, 2011.