iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61104

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Enhance the Security of ATM Machine Access with Face and Fingerprint Recognition

Asst. Prof. Borude K.M[1], Aditya Gaikwad[2], Vaishnavi Bundele[3] , Diksha Borade[4] , Sayali Nannaware[5]
[1, 2, 3, 4, 5]*Computer Department, Adsul's Technical Campus, Savitribai Phule Pune University Ahmednagar, Maharashtra, India.*

Abstract: ***The project introduces an innovative approach to enhance the security and accessibility of Automated Teller Machines (ATMs). In this era where financial transactions are increasingly digital and essential, safeguarding ATM access is of paramount importance. This project leverages the power of biometric authentication, combining fingerprint and face recognition technologies to create a robust and reliable access control system. The proposed system allows ATM users to authenticate their identity with a seamless and secure process. Fingerprint recognition provides a high-precision, individualized identification method, while face recognition adds an additional layer of security, ensuring the users identity matches the stored biometric data. This dual-biometric approach significantly reduces the risk of unauthorized access and fraudulent activities at ATMs. Beyond enhancing security, the project contributes to user convenience by streamlining the authentication process, eliminating the need for traditional ATM cards or PINs. Users can access their accounts swiftly and securely, thereby improving the overall ATM experience. Furthermore, the project's incorporation of state-of-the-art biometric technologies underscores its potential to set a standard for secure ATM access not only in the financial sector but also in various other domains where access control is critical.***

Keywords: ***Automated Teller Machines (ATMs), Face Recognition, Fingerprint Sensor, CSS, Python, SQLite, flask, dlib, Convolutional Neural Network (CNN), etc***

I. INTRODUCTION

In the ever-evolving landscape of financial technology, the quest for heightened security measures in Automated Teller Machines (ATMs) has taken a significant stride with the integration of biometric authentication.(Khan, 2015) This innovative project introduces a robust and secure ATM Access Control System, combining state-of-the-art fingerprint and face recognition technologies. Traditional methods of authentication, relying on cards and Personal Identification Numbers (PINs), are susceptible to various security vulnerabilities.(Karovaliya et al., 2015) Recognizing the pressing need for a more resilient and user-friendly approach, this project endeavours to redefine ATM security by harnessing the power of biometrics. Fingerprint and face recognition, as pivotal components of the proposed system, promise not only to fortify the authentication process but also to deliver a seamless and efficient experience for users. This introduction sets the stage for exploring the intricacies and advancements that underpin the novel biometric approach to ATM access control, contributing to a paradigm shift in the domain of financial transaction security.

II. LITERATURE SURVEY

(Peter et al., n.d.) [1]	We have adopted the notion of facial recognition verification in ATMs, with the differentiation between identification (matching against a database) and verification (confirming an individual's identity).
(Gujar et al., 2022) [2]	With a focus on three main stages—face detection, feature extraction, and generating an effective representation of facial features for recognition—we have integrated the Viola-Jones approach for real-time face detection and recognition.
(Patoliya & Desai, 2017) [3]	We've combined ideas like employing Embedded Linux with the Raspberry Pi board to create an ATM security system that detects faces. In this system, faces are photographed, their detection confirmed, and a high-level security mechanism is used, which includes locking the ATM door and using a GSM module attached to the Raspberry Pi to generate an OTP for additional SMS verification.

(Karovaliya et al., 2015) [4]	We have implemented the idea of using features like face recognition and One-Time Passwords (OTPs) to improve ATM security and usability. By using facial recognition technology to identify each user uniquely, the possibility of ATM card fraud due to theft or duplication is decreased. Furthermore, OTPs are produced at random to improve security and do away with the requirement for users to memorize PINs.
(Sasipriya et al., n.d.) [5]	We have integrated the concept of an advanced ATM system that utilizes facial recognition technology to substitute ATM cards with RFID tags. High-quality face photos are used by the system for authentication; the images are compared to a database, and the findings are sent to a control unit for additional processing. Using a Raspberry Pi microcontroller and facial verification software improves security and lowers the possibility of forced transactions.
(Jain, 1999) [6]	We have integrated a system to identify faces in humans from individual photos in a vast collection, tackling issues such picture fluctuation in terms of size, position, expression, and posture. The system makes use of unique bunch graph extraction techniques and image graphs with fiducial points represented by wavelet components. Comparing these image graphs is the basis for recognition; studies using databases such as FERET and Bochum have included recognition in a variety of positions.
(Khan, 2015) [7]	One-Time Passwords (OTPs) are a notion that we have incorporated as an additional layer of protection for ATM transactions. To assure uniqueness, OTPs are generated with the help of cryptographic hash functions and a number of other variables, including time, account number, cell number, location, and IMEI number. The research also proposes biometric security as a substitute for OTPs in application-based issues, offering strong security safeguards for ATM transactions.
(Omkar et al., 2022) [8]	We have integrated the design of an OTP (One-Time Password) system and a facial detection technology to create a secure ATM. By doing away with easily copied magnetic cards and static PINs, the goal is to combat the rising fraud in ATM transactions. By integrating facial detection and OTP authentication for cardless transactions, the suggested solution seeks to improve security while simultaneously improving usability.
(Mahesh et al., n.d.) [9]	We involves developing an ATM security system where customers' fingerprints and mobile numbers are collected by the bank during account opening. Customers can access the ATM machine by placing their finger on the fingerprint module, which generates a different 4-digit code sent as a message to their mobile through a GSM modem connected to a microcontroller. The customer enters this code on the ATM screen, and the system verifies its validity to allow further access.
(Ranjitham et al., 2018) [10]	We have emphasizes using biometrics, specifically Face ID and Fingerprint, for authentication instead of relying on PINs and ATM cards. The combination of these two biometrics is considered highly secure for identification and verification purposes. The system identifies the user's fingerprint and verifies their face image to grant authentication. Additionally, the prototype of the system utilizes a Raspberry Pi microcontroller.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

III. COMPONENTS

1) Web Camera:

Fig 1 :- Webcam

A web camera is a device which helps to take pictures and video often used for video chatting and video and image capturing for authentication and verification process. In our prototype, the Logitech camera is used for this process. It is one of the cheapest yet a good web camera available in the market. Other cameras can also be used for face capturing. The Lapcare camera supports 720p video recording and 5MP image capturing. 5MP image is more than enough for a good Face identification.

2) Fingerprint Scanner:

Fig 2 :- Fingerprint Scanner

- The main component of the project is the fingerprint sensor. Facial recognition technology is also used to identify people, even though fingerprints play a significant role in identification. Think about a situation where the twins' faces collide because they have the same fingerprints, yet their fingerprint ID helps to identify the account.
- These days, gesture identification is also used to distinguish between individuals with identical faces; however, fingerprint identification is more trustworthy than gesture identification. Two people cannot have the same fingerprints since each fingerprint is unique and is created by a combination of elements.
- Until the finger is destroyed, the fingerprint cannot be destroyed. Even a scratch or bruise on a fingerprint heals to return to its original appearance.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

IV. TECHNOLOGY

1) Image Processing:

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the buildup of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.

2) Computer Vision:

A branch of digital image processing called computer vision uses several sets of algorithms to interpret images and extract information from the surrounding world. Face identification, another subset of computer vision, was used in our project. Many software tools, including MATLAB, OpenCV, and others, can be used for face identification. Nonetheless, OpenCV is the most useful tool to utilize because it offers many easily accessible modules and is fully open source. Python libraries that are available on the OpenCV website are utilized in the project to access the OpenCV modules. As its name suggests, OpenCV is available for computer vision in addition to face recognition. And it might be among the most effective instruments for developing artificial intelligence.

3) Python (Programming Language) :

- Python is a general-purpose, high-level programming language. With a strong emphasis on indentation, its design philosophy prioritizes code readability.
- Python uses garbage collection and dynamic typing. It is compatible with various programming paradigms, such as object-oriented, functional, and structured (especially procedural).

4) CNN Algorithm :

- A Convolutional Neural Network (CNN) is a type of deep learning algorithm specifically designed for image processing and recognition tasks. Compared to alternative classification models, CNNs require less preprocessing as they can automatically learn hierarchical feature representations from raw input images.
- Convolutional neural networks are known for their superiority over other artificial neural networks, given their ability to process visual, textual, and audio data. The CNN architecture comprises three main layers: convolutional layers, pooling layers, and a fully connected (FC) layer.

5) Eye-blink Algorithm :

- The eyes are detected to be either open or closed at a particular period by using thresholding and equations regarding the symmetry of human face.
- The eye region is processed to ascertain certain attributes of eyelid movement. .These intensities cross during the eyelid closing and opening.

V. IMPLEMENTATION

The implementation of the "Fingerprint & Face Recognition ATM Access Control System" involved a meticulous process, starting with the selection of appropriate hardware and software components. High-quality fingerprint sensors and cameras were integrated into the ATM hardware infrastructure to capture biometric data effectively. On the software front, Python programming language and the OpenCV library were utilized for developing the biometric recognition algorithms, while SQlite served as the database management system for storing encrypted biometric templates and user information securely. The biometric algorithms were fine-tuned and optimized to achieve high accuracy and efficiency in real-time user authentication. User-friendly interfaces were designed to guide users through the enrolment process, ensuring seamless integration of fingerprint and face data into the system. Rigorous testing and validation procedures were conducted to evaluate the system's performance, including accuracy, speed, and robustness against spoofing attempts. Throughout the implementation phase, a focus on security, reliability, and user experience remained paramount, culminating in a robust and efficient ATM access control system poised to elevate the standards of banking security and convenience.

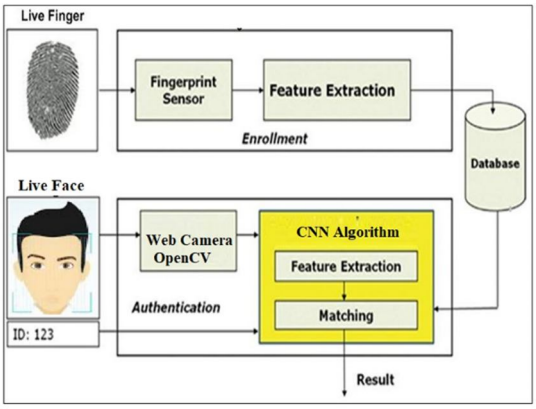
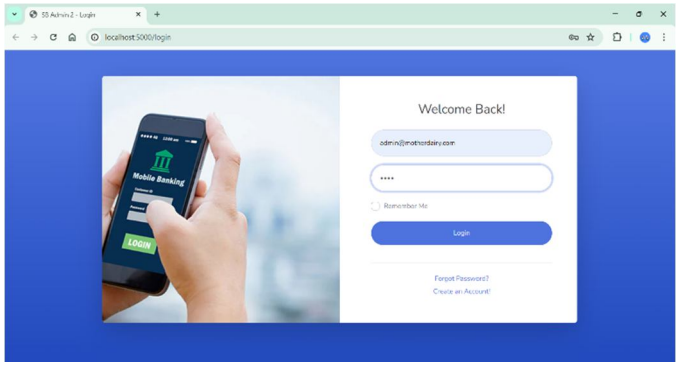
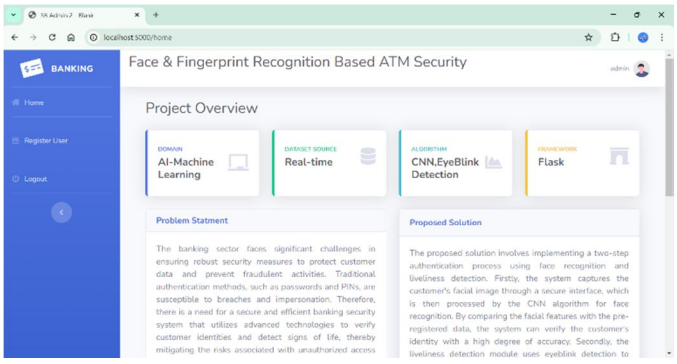


Figure 1 : Proposed Architecture of System

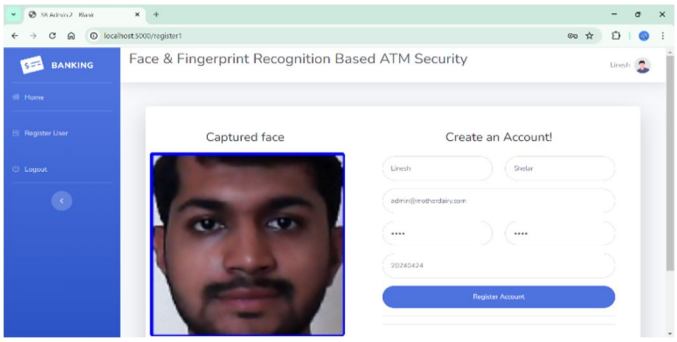
VI. RESULTS



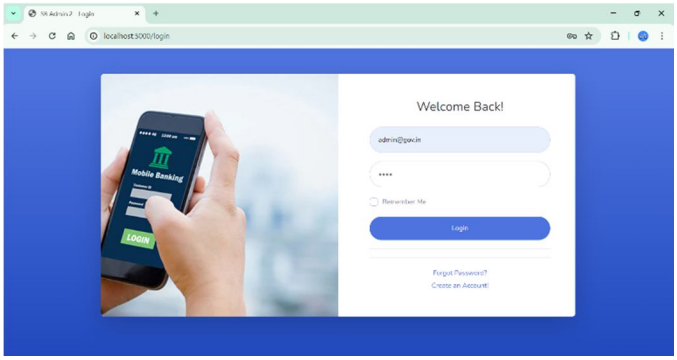
1 :Admin Login for User Registration.



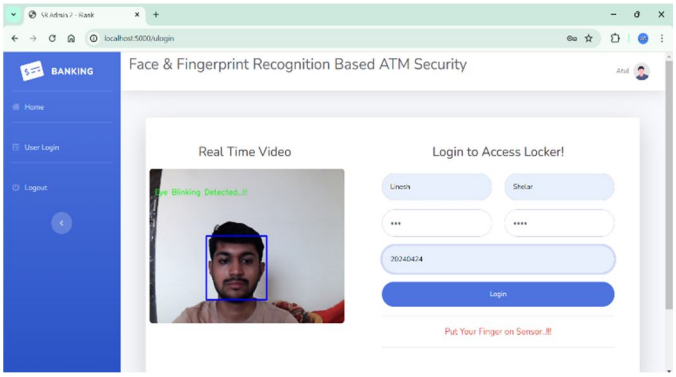
2: Home Page.



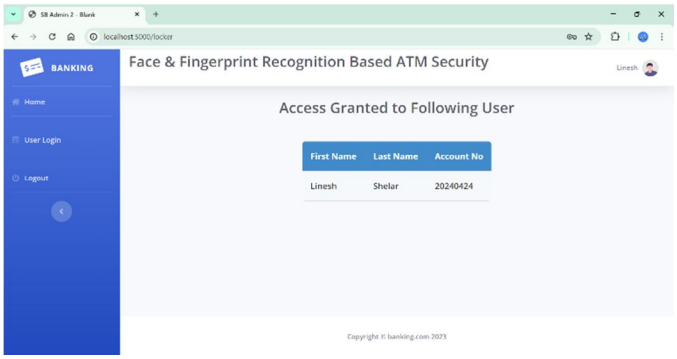
3: User Registration.



4 : Admin Login For User Security.



5 : User Login.



6 : Access Granted.

VII. CONCLUSIONS

The development and implementation of the "Fingerprint & Face Recognition ATM Access Control System" represent a significant stride towards redefining ATM security paradigms. Traditional authentication methods, prone to vulnerabilities, are surpassed by the integration of advanced biometric technologies. Throughout this project, the fusion of fingerprint and face recognition not only fortifies the security landscape but also introduces a level of user-friendly authentication unprecedented in conventional banking systems.

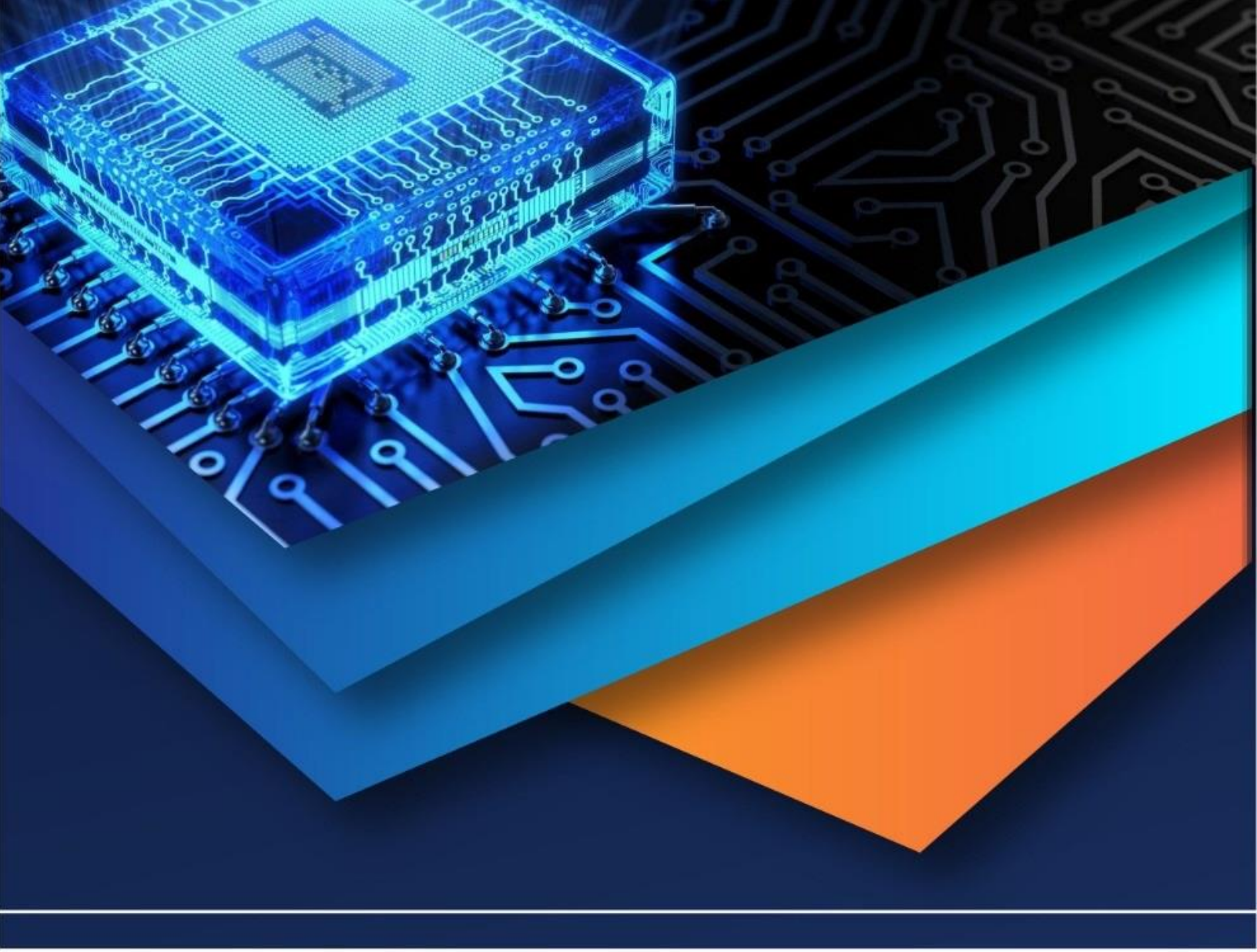
The project's success lies in its ability to seamlessly weave together intricate biometric algorithms, robust database management, and a user interface designed for accessibility. The system's efficiency is evidenced by its capability to authenticate users accurately and swiftly in real-time, mitigating risks associated with card theft, PIN compromises, and unauthorized access. Furthermore, the inclusion of liveness detection mechanisms adds an extra layer of security, safeguarding against potential spoofing attempts.

As we propel into an era where technology meets the demands of security and user experience, this project marks a pivotal moment in the evolution of ATM systems. The documented methodologies, from algorithm development to system integration, provide a blueprint for future innovations in the realm of biometric-based access control.

This project not only champions security but also envisions a future where banking interactions are characterized by efficiency, reliability, and an unwavering commitment to user privacy. The success of this endeavour underscores the transformative potential of biometric technologies in reshaping the landscape of financial security.

REFERENCES

[1] K. J. Peter, G. G. S. Glory, S. Arguman, G. Nagarajan, V. V. S. Devi, and K. S. Kannan, "Improving ATM security via face recognition," in 2011 3rd International Conference on Electronics Computer Technology, 2011.
[2] P. A. D. Gujar, N. B. Sawant, T. L. Hake, A. A. Shete, and S. M. Deshmukh, "Face recognition open CV based ATM security system," Int. J. Res. Appl. Sci. Eng. Technol., vol. 10, no. 5, pp. 1114–1119, 2022.
[3] J. J. Patoliya and M. M. Desai, "Face detection-based ATM security system using embed ded Linux platform," in 2017 2nd International Conference for Convergence in Technol ogy (I2CT), 2017.
[4] M. Karovaliya, S. Karedia, S. Oza, and D. R. Kalbande, "Enhanced security for ATM machine with OTP and facial recognition features," Procedia Comput. Sci., vol. 45, pp. 390–396, 2015.
[5] S. Sasipriya, P. M. Kumar, and S. Shenbagadevi, Face recognition based new generation ATMsystem.
[6] L. Wilskott, J.-M. Fellous, and C. Norbertkruger, "Face Recognition by Elastic Bunch Graph Matching," Chapter, pp. 355–396, 1999.
[7] M. Hamid Khan, Securing, and Biometric, "Securing ATM with OTP and Biometric"," International Journal on Recent and Innovation Trends in Computing and Communication, no. 4, pp. 2041–2044, 2015.
[8] D. Omkar, A. Sahil, K. Sahil, and S. D. Gunjal, "Cardless transaction of ATM machine with a security of facial recognition and otp with shuffle keypad,"Irjet.net.[Online].Available:https://www.irjet.net/archives/V9/i1/I RJET-V9I115.pdf. [Ac cessed: 13-Apr-2023].
[9] M.Patil, M. Sachin P Wanere, and M.Maighane, "ATMTransaction Using Biometric Fin gerprint Technology"," ATM Transaction Using Biometric Fingerprint Technology, vol. 2, no. 6, pp. 22–27.
[10] Dr.G. Ranjitham , Senthamilarasu Manoharan , Vetrivelu Murugesan , Sree Sabaresan Ravi , "Face Recognition and Fingerprint Based New Generation ATM".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY