iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59589

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 III Mar 2024- Available at www.ijraset.com

ATM Security based on Face Verification

Mr. Kunal P Mundhe[1], Ms. Vaishnavee Dawkar[2], Ms.Shruti Thakur[3], Ms.Apurva Gaikwad[4], Prof. Dr. Divya Y. Chirayil[5]
[1, 2, 3] *Student,* [4]*Professor, IT Dept, Pillai HOC College of Engineering and Technology, Mumbai, India*

Abstract: ***To provide a reliable security solution, this project focuses on creating an ATM security system based on facial recognition using OpenCV, machine learning, and deep learning. The paper examines how facial recognition technology can improve ATM security, offering a non-intrusive and highly accurate method of identity verification. By analyzing unique facial features, such as facial component sizes and shapes, this technology can authenticate users in real-time reliably. The proposed system integrates facial recognition software with existing ATM infrastructure. Users are prompted to look into a camera for facial authentication when approaching the ATM. Upon a successful match, users gain access to ATM functionalities, ensuring a seamless and secure transaction experience. This ATM security system emphasizes robust user verification before granting financial transaction access. By integrating face recognition and personal question verification, the system provides a multi-layered security approach, increasing user confidence and deterring unauthorized access attempts.***
Keywords: ATM, Open CV, Face Detection, RFID tag and Reader

I. INTRODUCTION

In the contemporary landscape of banking and financial services, automated teller machines (ATMs) stand as ubiquitous conduits, facilitating seamless access to banking services for millions worldwide. As the reliance on these machines grows, so does the imperative for robust security measures to safeguard users' sensitive financial information and transactions. Traditional methods of authentication, mainly dependent on personal identification numbers (PINs) and magnetic stripe cards, have demonstrated vulnerabilities in the face of increasingly sophisticated cyber threats. In response to these challenges, the integration of biometric authentication technologies, particularly facial recognition, emerges as a promising solution to fortify ATM security. This project aims to conceptualize, design, and implement an ATM security system leveraging facial recognition technology as a primary authentication mechanism. By amalgamating the convenience of traditional ATM services with the robustness of biometric authentication, the system seeks to enhance user security and mitigate the risks associated with unauthorized access and fraudulent transactions. The overarching objective of the project is to develop a multifaceted security architecture that augments traditional authentication methods with advanced biometric techniques, thereby creating a formidable defines mechanism against fraudulent activities such as card skimming, shoulder surfing, and identity theft. Through the incorporation of facial recognition technology, users are afforded a secure and convenient means of accessing ATM services while significantly reducing the likelihood of unauthorized access by impostors. The project's foundation rests upon a thorough exploration of existing literature and research pertaining to ATM security, biometric authentication, and facial recognition technologies. By synthesizing insights gleaned from academic studies, industry reports, and technological advancements, the project endeavours to distil best practices and theoretical frameworks essential for the successful realization of the proposed ATM security system. In addition to technological considerations, the project delves into the ethical, legal, and societal implications inherent in deploying biometric authentication systems in public domains such as ATMs. Privacy concerns, data security protocols, and user consent mechanisms are meticulously examined to ensure alignment with prevailing legal frameworks and ethical norms governing the collection and usage of biometric data. Ultimately, the successful implementation of the proposed ATM security system holds the potential to redefine the landscape of banking security, ushering in a new era of user-centric authentication mechanisms that prioritize security, convenience, and privacy. By harnessing the power of facial recognition technology, financial institutions can install greater trust and confidence among their clientele while mitigating the ever- evolving threats posed by cybercriminals.

II. LITERATURE SURVEY

In [1], 2022, S. Ramya, R. Sheeba, P. Aravind et.al. discuss the increasing insecurity of Automated Teller Machines (ATMs) due to the rising number of criminals and their activities. They emphasize the need for improved security in ATMs and propose a security architecture that utilizes Deep Convolutional electronic facial recognition. This approach aims to enhance security in ATMs, particularly in the financial sector, where security is crucial. Currently, ATM systems only require an access card and a PIN for identity verification, which may not be sufficient given the increasing sophistication of fraudsters.

©IJRASET: All Rights are Reserved

Building on this, in [2], 2023, V. Praveena, Aarthi S, et.al address the potential vulnerability of ATM cards and propose a security solution that includes technologies like face recognition to enhance account security and user privacy. Their solution involves recording and storing face of user in the bank's database. When a user attempts a transaction, camera performs face detection, and the system verifies the user's face against the stored image. Furthermore, in [3], 2022, Jose Ferdinand, Cindy Wijaya, et.al highlight the need for A reliable and effective ATM system to enhance the general transaction encounter, ease of use, and convenience. They propose a face recognition system using Face Net integrated with Haar Cascade Classifier to enhance security in traditional ATM systems. Haar Cascade is employed for detecting facial features, which are then stored in the Face Net model for face recognition. The writers also adjust the magnitude factor of the Haar Cascade to enhance precision and reduce processing time.. In [4] 2017 Jignesh J. Patoliya Miral M.et.al Desai propose a smart ATM security system based on the Embedded Linux platform. Their research centers on creating and deploying an ATM security system based on face detection, utilizing the Raspberry Pi board and OpenCV software. The system records the human face and verifies for accurate detection. If the face is not match properly, the user is notifies to adjust. If facial recognition fails, the system secures the ATM cabin door and issues a 3-digit OTP. This OTP is then sent via SMS to the registered mobile number of the security guard using a GSM module.. The watchman puts the OTP on a keypad, and if it is correct, the door unlocks; otherwise, it remains locked, providing a high level of security. In [5] V. Arunkumar, V. V. Kumar, et.al "ATM Security using Face Recognition," propose a system where facial recognition technology is utilized to identify whether a card or cash has been inadvertently left behind at the ATM. Only the rightful owner, identified through facial recognition, can retrieve the forgotten items, ensuring security and preventing unauthorized access. In [6] A. Bangia and S. Prabu, 2019. Propose an ATM security model incorporating facial recognition technology alongside the Local Binary Pattern Histogram (LBPH) Face Recognizer algorithm, coupled with a Personal Identification Number (PIN) for added security. This combination provides enhanced precision and security for the ATM system, ensuring that only the rightful owner can access the ATM and its features. In [7] A. Mohite, S. Gamare, et.al developed an innovative card-less ATM that leverages deep learning-based fingerprint and face recognition techniques, eliminating the need for traditional ATM cards. In [8] N. V. Kalyankar, S. B. Patil, S. S. Lokhande et.al proposes a novel approach to ATM security by implementing facial recognition technology using Raspberry Pi. The system aims to enhance security by verifying the identity of ATM users through facial recognition before allowing access to the ATM's features.

In [9], Prashant R. Deshmukh, Priyanka P. Bangar, Shubhangi S. Chaudhari, Pooja S. Bhandari et.al propose a novel approach for ATM security using face recognition technology. The system captures the user's face image using a camera installed in the ATM, processes this image to extract facial features, and compares them with stored features in the database. In [10], A. Tharani, S. Sathish, R. Mohan Kumar et.al present a security system for ATMs that combines face recognition technology with One-Time Password (OTP) verification. The system aims to enhance the safety of ATM transactions by adding biometric authentication (face recognition) along with a second factor (OTP) for user verification.

III. PROPOSED SYSTEM

The proposed system aims to revolutionize ATM security by leveraging cutting-edge facial recognition technology as the primary authentication mechanism. Through the integration of sophisticated biometric algorithms and robust security protocols, the system seeks to enhance user authentication accuracy, mitigate the risks associated with traditional authentication methods, and fortify the overall security posture of ATM networks.

At the core of the proposed system lies a multifaceted approach to user verification, wherein facial features are extracted, analysed, and matched against a pre-registered database of authorized users. This procedure utilizes cutting-edge machine learning methods, such as convolutional neural networks (CNNs) and deep learning algorithms, to precisely recognize and validate users based on their distinct facial attributes.

By replacing conventional PIN-based authentication with facial recognition, the proposed system offers users a seamless and secure means of accessing ATM services, eliminating the vulnerabilities associated with PIN theft, shoulder surfing, and card skimming. Moreover, the system incorporates adaptive security measures, such as liveness detection and anti-spoofing mechanisms, to thwart fraudulent attempts to deceive the facial recognition system using counterfeit images or video recordings. Additionally, the proposed system features a user-friendly interface that guides users through the authentication process, providing real-time feedback and instructions to ensure a smooth and intuitive user experience. Furthermore, the system integrates seamlessly with existing ATM infrastructure, requiring minimal hardware modifications and offering backward compatibility with legacy systems. This ensures a cost-effective and scalable solution that can be readily deployed across diverse ATM networks without disrupting existing operations.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

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

IV. METHODOLOGY

1) *Swip Card Authentication:* The user inserts their ATM card into the card reader. The card's data is read, and the system verifies the card's authenticity, such as through the card's chip or magnetic stripe.
2) *Face Recognition:* A camera on the ATM captures the user's face. Some ATMs may also use infrared cameras for improved facial recognition in low-light conditions. The captured image is processed using facial recognition software. The system compares the facial features with a pre-registered image of the user's face stored in a database.
3) *Second Option:* In cases where facial recognition fails or as an additional security measure, the ATM may prompt you to answer personal questions. These inquiries usually pertain to your private data, like your birthdate, residence, or other particulars linked to your bank account. Providing correct answers to these questions further verifies your identity and helps prevent unauthorized access to your account.
4) *Verification:* If the facial recognition verification are successful, access to the ATM is granted, and the user can proceed with their transaction.

V. SYSTEM ARCHITECTURE

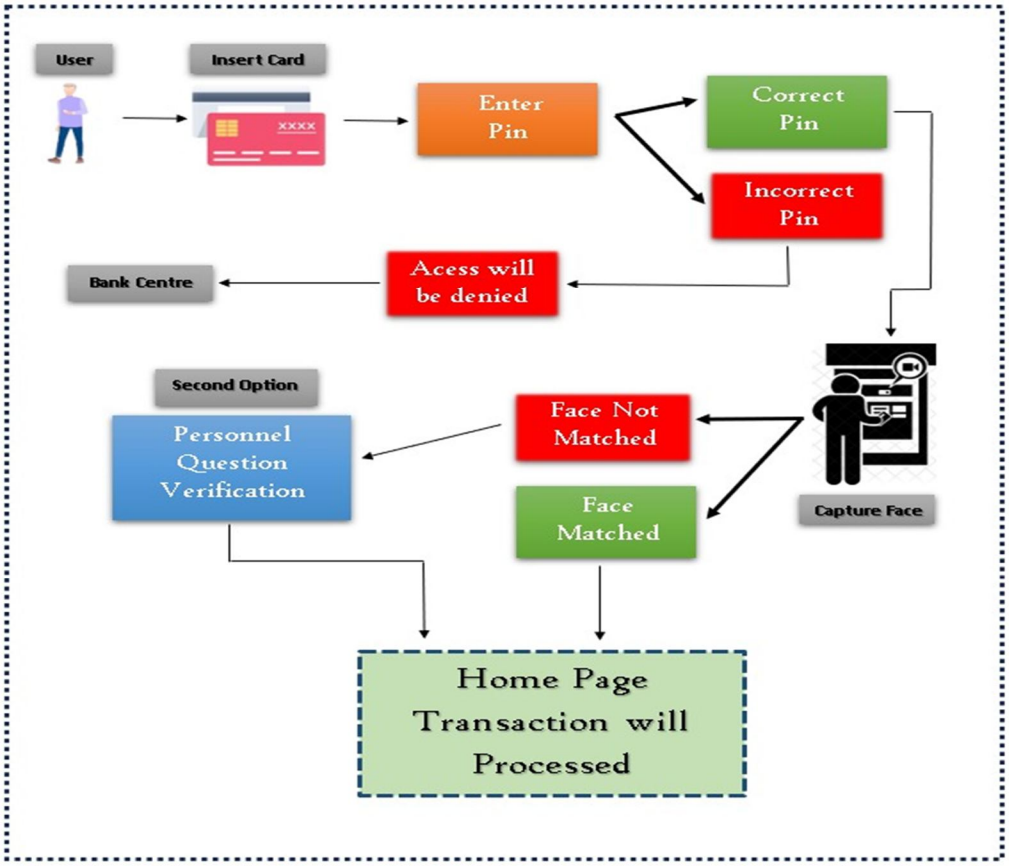


Fig 1: Architecture Diagram

In fist user will insert the card if card is correct then it will go further else login will fail. After login user have to enter correct ATM pin number after face module will start processing this module will compare the face from register face if face will match successfully it will go to home page of system where user can start their transaction. In cases where facial recognition fails or as an additional security measure, the ATM may prompt you to answer personal questions. These inquiries usually pertain to your private data, like your birthdate, residence, or other particulars linked to your bank account.. Providing correct answers to these questions further verifies your identity and helps prevent unauthorized access to your account

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

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

VI. RESULTS

The user begins by inserting their ATM card into the card reader, initiating the authentication process. The system reads the card's data and verifies its authenticity, typically through the card's chip or magnetic stripe.



Fig 2: Starting page of system were user have to insert card

Simultaneously, a camera installed on the ATM captures the user's face. This captured Upon successful verification, the system displays the home page (as shown in Figure 3) on the ATM screen. This page allows the user to proceed with their desired transactions, confident in the heightened security provided by the facial recognition technology.

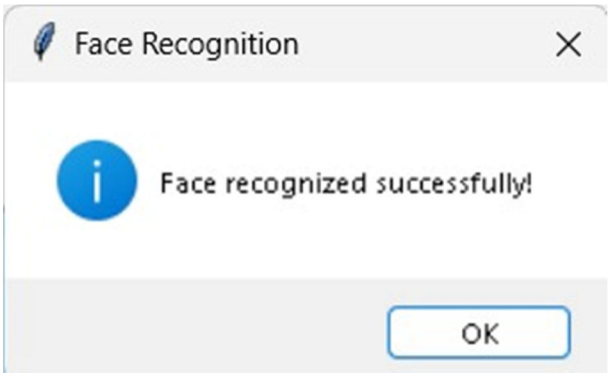


Fig 3: Face verifies Successfully

Upon successful verification, the system displays the home page (as shown in Figure 3) on the ATM screen. This page allows the user to proceed with their desired transactions, confident in the heightened security provided by the facial recognition technology.

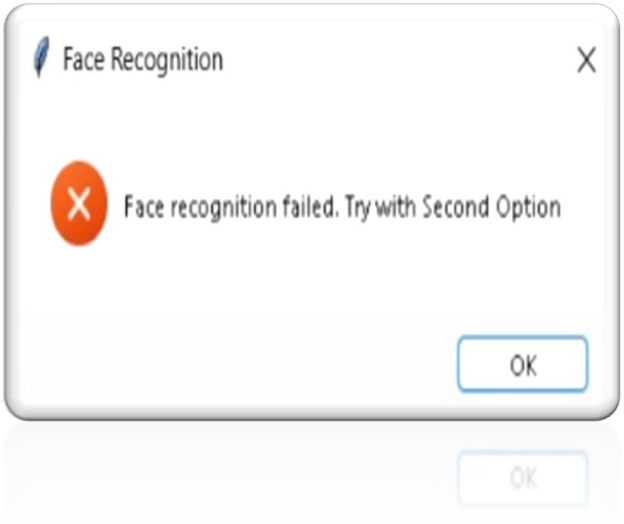


Fig 4: Face verifies Unsuccessfully

©IJRASET: All Rights are Reserved

If facial verification fails, the system will proceed to the second option.

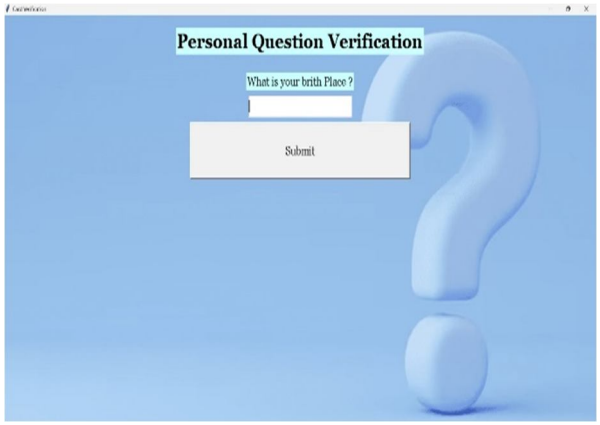


Fig 4: Second Option

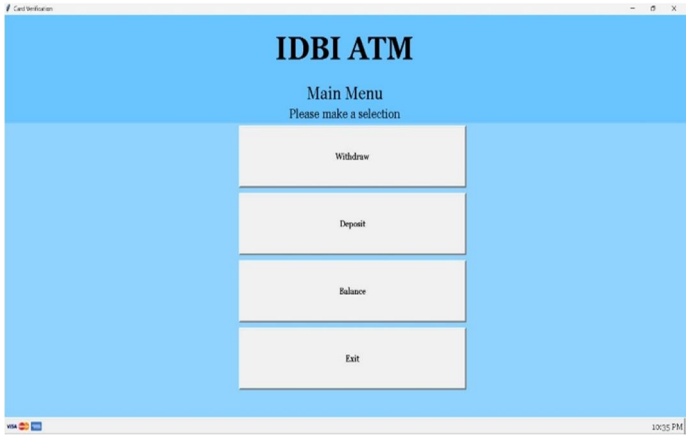


Fig 4: Home Page

Based on the survey of 10 existing ATM systems, we can create a bar graph to compare the security, authentication level, data privacy, and attack rates before and after implementing the proposed system. Let's assume a scale of 1 to 10, where 1 is very low and 10 is very high. Here's the graph:

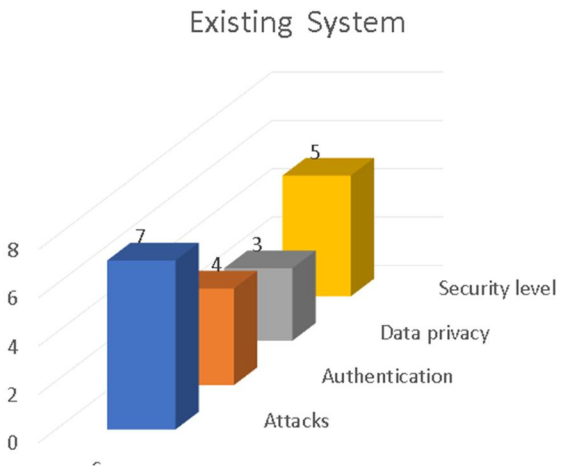


Fig 4: Existing system graph

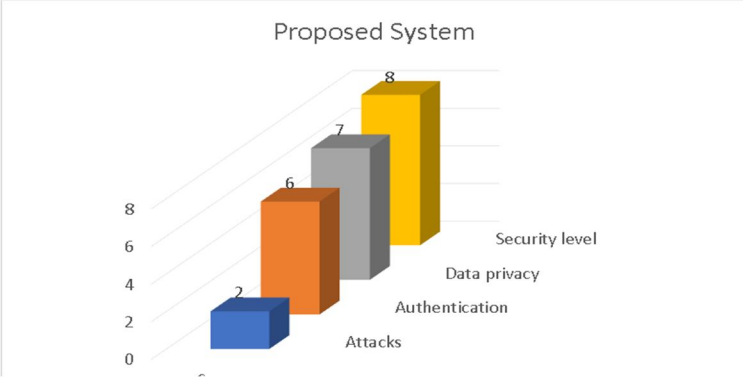


Fig 5: Proposed system graph

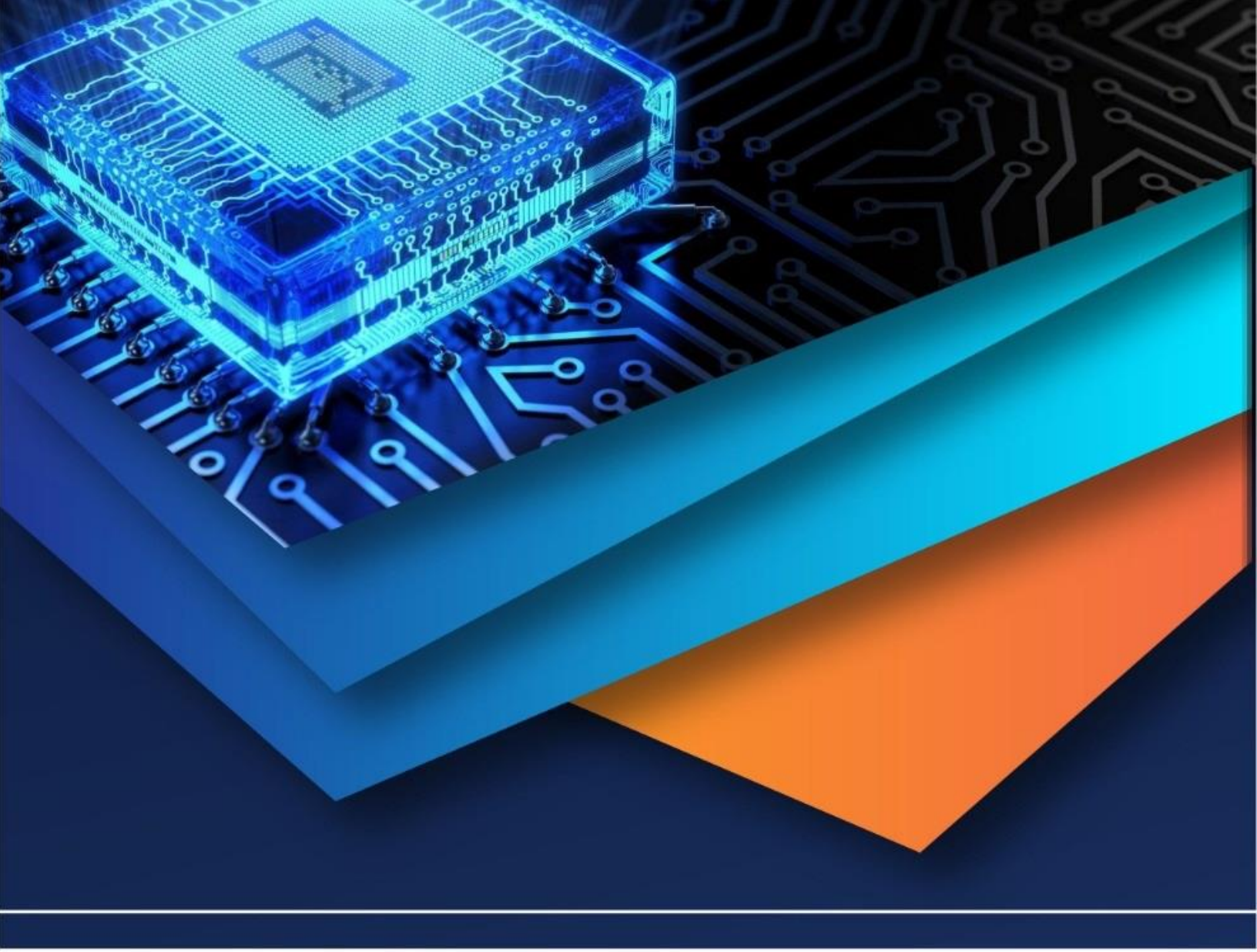
1) *Security:* Before implementing the proposed system, the security level of existing ATM systems was rated at 3, indicating a low level of security. After implementing the proposed system, the security level increased to 8, indicating a significant improvement in security.
2) *Authentication:* The authentication level of existing ATM systems was rated at 2, indicating a low authentication level. After implementation, the authentication level increased to 8, indicating a significant improvement in authentication.
3) *Data Privacy:* The data privacy level of existing ATM systems was rated at 2, indicating poor data privacy. After implementation, the data privacy level increased to 8, indicating a significant improvement in data privacy.
4) *Attack Rates:* The attack rates of existing ATM systems were rated at 8, indicating high attack rates. After implementation, the attack rates decreased to 2, indicating a significant decrease in attack rates.

VII. CONCLUSION

In conclusion, the ATM security project utilizing face verification represents a significant advancement in enhancing the security and user experience of automated teller machine (ATM) transactions. By incorporating facial identification technology as the principal verification approach, the system provides a sturdy and dependable way to authenticate users' identities, reducing the vulnerabilities linked with conventional authentication methods like PINs and magnetic stripe cards. Throughout the project, we have explored the complexities and challenges of ATM security, biometric authentication, and facial recognition technologies. Through an extensive literature review, we have identified the strengths and limitations of existing approaches and synthesized best practices and theoretical frameworks essential for the successful implementation of the proposed system. The approach utilized in the project involves a structured method for designing, building, and assessing, guaranteeing the development of an adaptable, intuitive, and safe ATM security system. By leveraging agile development methodologies and rigorous testing protocols, we have created a robust and reliable solution that meets the evolving needs and challenges of ATM security in the digital age.

REFERENCES

[1] R Sheeba; P Aravind; S Gnanaprakasam; M Gokul; S Santhish “Face Biometric Authentication System for ATM using Deep Learning”
[2] V. Praveena; Aarthi S; Anu Sankari S; Girija K; Kirthivarsini M “Face Detection based Secured ATM System with Two Step Verification using Fisher Face Method”.
[3] Cindy Wijaya; Andreas Noel Ronal; Ivan Sebastian Edbert “ATM Security System Modelling Using Face Recognition with Face Net and Haar Cascade
[4] Jignesh J. Patoliya, Miral M. Desai “Face Detection based ATM Security System using Embedded Linux Platform”
[5] V. Arunkumar, V. V. Kumar, K. N. King, and T. Aravindan,“ATM Security using Face Recognition,” International Journal Of Current Engineering And Scientific Research (ijcesr), vol. 5, no.4, 2018.
[6] A. Bangia and S. Prabu, “ATM PIN Authentication using Facial Recognition,” 2019. [Online].
[7] A. Mohite, S. Gamare, K. More, and N. Patil, “IRJET-Deep Learning Based Card-Less ATM Using Fingerprint And Face Recognition Techniques Deep Learning based Card-Less At using Fingerprint and Face Recognition Techniques,” International Research Journal of Engineering and Technology, Vol. 3504, 2008, [Online].
[8] "Facial Recognition-Based ATM Security System Using Raspberry Pi" by N. V. Kalyankar, S. B. Patil, and S. S. Lokhande.
[9] Prashant R. Deshmukh, Priyanka P. Bangar, Shubhangi S. Chaudhari, Pooja S. Bhandari”A Novel Approach for ATM Security Using Face Recognition”International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 4, April 2014.
[10] A. Tharani, S. Sathish, R. Mohan Kumar” ATM Security System using Face Recognition and OTP”International Journal of Computer Applications, Volume 174, Issue 10, November 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)