www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 03, March 2025, pp : 1804-1808

e-ISSN : 2583-1062
Impact Factor : 7.001

ADVANCED ATM SECURITY SYSTEM USING INTEGRATED FINGERPRINT AND IRIS RECOGNITION

Swetha[1], B. Ganesh[2], S. Sathwik Reddy[3], P. Sampath Kumar[4]

[1,2,3,4]Assistant Professor, Information Technology, ACE Engineering College, India. Information Technology, ACE Engineering College, India.

DOI: https://www.doi.org/10.58257/IJPREMS39229

ABSTRACT

Automated Teller Machines (ATMs) have become an essential part of modern banking, offering customers uninterrupted financial services. However, these services are often vulnerable to security threats such as card skimming, PIN theft, and unauthorized transactions. Traditional security measures like PIN authentication and physical ATM cards have limitations that make them susceptible to fraud. This project focuses on integrating fingerprint and iris recognition technology to enhance ATM security, ensuring that only authorized users can access their accounts. By utilizing a dual biometric authentication approach, the system provides an extra layer of security, reducing fraudulent activities and improving user confidence. The project also includes the development of hardware and software components to support seamless transactions. This paper discusses the design, implementation, and potential benefits of this innovative security system, highlighting its role in safeguarding financial transactions in the banking sector.

Keywords: Biometric authentication, ATM security, Fingerprint recognition, Iris recognition, Multi-factor authentication.

1. INTRODUCTION

Automated Teller Machines (ATMs) serve as convenient self-service banking terminals, allowing customers to perform various financial transactions, including cash withdrawals, balance inquiries, and fund transfers. However, the widespread use of ATMs has led to an increase in security threats, with fraudsters constantly developing new ways to bypass traditional authentication methods. The most common vulnerabilities in ATM security systems include card skimming, PIN theft through shoulder surfing, and identity fraud. To address these challenges, biometric authentication has emerged as a promising solution. Biometric authentication uses unique physiological traits, such as fingerprints and iris patterns, which are nearly impossible to replicate or steal. Fingerprint recognition is widely used but has limitations, such as potential wear and tear on the skin and susceptibility to external environmental conditions. On the other hand, iris recognition is highly accurate and provides consistent authentication under various conditions. By integrating these two biometric authentication methods, this project aims to develop a secure and efficient ATM system that minimizes fraud risks while maintaining user convenience

2. LITERATURE SURVEY

Several studies have explored the implementation of biometric authentication systems in banking and financial transactions. Traditional ATM security mechanisms primarily rely on PIN-based authentication, which has proven to be highly vulnerable to cyber-attacks and fraudulent activities. Previous research has shown that fingerprint recognition provides a convenient and effective authentication method, but it is not foolproof, as factors such as cuts, dirt, or damage to the skin can affect recognition accuracy. Iris recognition has been identified as one of the most reliable biometric authentication methods due to the uniqueness and stability of iris patterns over time. However, the adoption of iris recognition in ATM systems has been limited due to high implementation costs. Studies have demonstrated that a multimodal biometric authentication system combining fingerprint and iris recognition can provide enhanced security, reducing the likelihood of fraudulent access while ensuring a seamless user experience. This project builds on these findings by integrating both fingerprint and iris recognition into an ATM security system, offering a comprehensive solution that addresses the limitations of single-mode authentication methods.

3. EXISTING SYSTEM

The existing ATM security systems primarily rely on traditional authentication methods, including PIN-based verification and physical ATM cards. These methods, while functional, have significant drawbacks that make them susceptible to fraudulent activities. Card skimming is one of the most prevalent security threats, where fraudsters install skimming devices on ATM card slots to capture users' card details. Additionally, PIN theft through methods such as shoulder surfing and phishing attacks poses a major risk. Attackers can easily obtain a user's PIN by observing them during transactions or through malicious software installed on compromised ATMs. Another issue with the existing system is the reliance on physical ATM cards, which can be lost, stolen, or cloned. If a card falls into the wrong hands

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 03, March 2025, pp : 1804-1808
e-ISSN : 2583-1062
Impact Factor : 7.001

along with the corresponding PIN, unauthorized access to the user's bank account becomes effortless. While some ATMs have implemented fingerprint authentication as an added layer of security, these systems still face limitations due to environmental factors such as dirt, moisture, or fingerprint wear, which can lead to authentication failures. Furthermore, iris recognition, although highly secure, is not widely adopted in commercial ATMs due to high costs and limited infrastructure. Consequently, the existing system lacks a reliable, multi-layered authentication mechanism, making financial transactions vulnerable to security breaches.

4. PROPOSED SYSTEM

The proposed system introduces an advanced security framework that integrates fingerprint and iris recognition to overcome the limitations of existing ATM authentication methods. By employing a dual biometric authentication approach, the system ensures that only authorized users can access ATM services, significantly reducing the risk of fraud. During user registration, biometric data, including fingerprints and iris scans, are securely captured and stored in an encrypted database. When accessing an ATM, the system first prompts the user to provide their fingerprint, followed by an iris scan for additional verification. The authentication process utilizes advanced image processing techniques and machine learning algorithms to enhance accuracy and speed. The integration of these two biometric modalities ensures that even if one method fails due to external factors, the second modality serves as a backup, enhancing overall security and reliability. Furthermore, the system employs robust encryption techniques to protect stored biometric data from potential cyber threats, preventing unauthorized access or data breaches. The implementation of real-time fraud detection mechanisms further strengthens the security of ATM transactions by identifying suspicious activities and alerting the banking authorities immediately. The proposed system not only improves the accuracy and reliability of ATM authentication but also enhances user convenience by eliminating the need for PINs and physical cards. With this innovative approach, financial institutions can provide customers with a secure and seamless banking experience while minimizing the risks associated with traditional authentication methods.

5. METHODOLOGY

The proposed system follows a structured methodology to ensure a secure and efficient ATM authentication process. Initially, users must register their biometric credentials, including fingerprints and iris scans, which are securely stored in an encrypted database. During authentication, the system captures real-time biometric data and matches it with the stored records to verify the user's identity. If both fingerprint and iris authentication are successful, the user gains access to the ATM services. The system architecture consists of multiple components, including biometric scanners, a secure database, and a web-based user interface for transaction management. Advanced encryption techniques are employed to protect stored biometric data from potential cyber threats. Additionally, machine learning algorithms can be integrated to improve authentication accuracy and detect fraudulent activities in real time. The methodology ensures a balance between security and user convenience, making the ATM authentication process both seamless and highly secure.

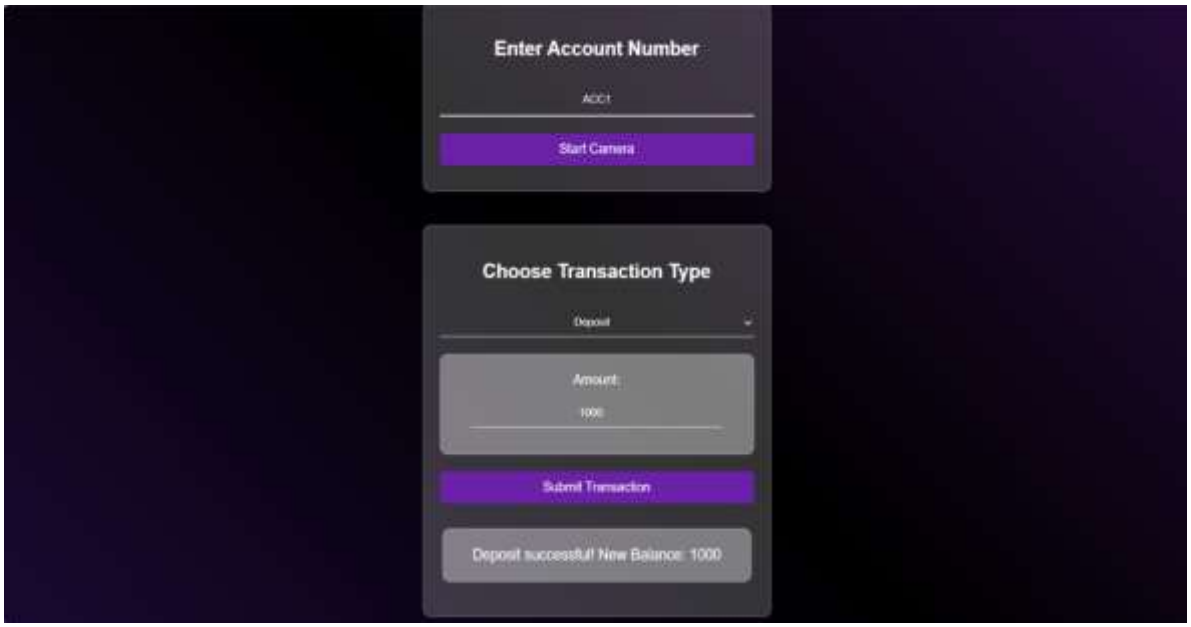
6. MODELING AND ANALYSIS

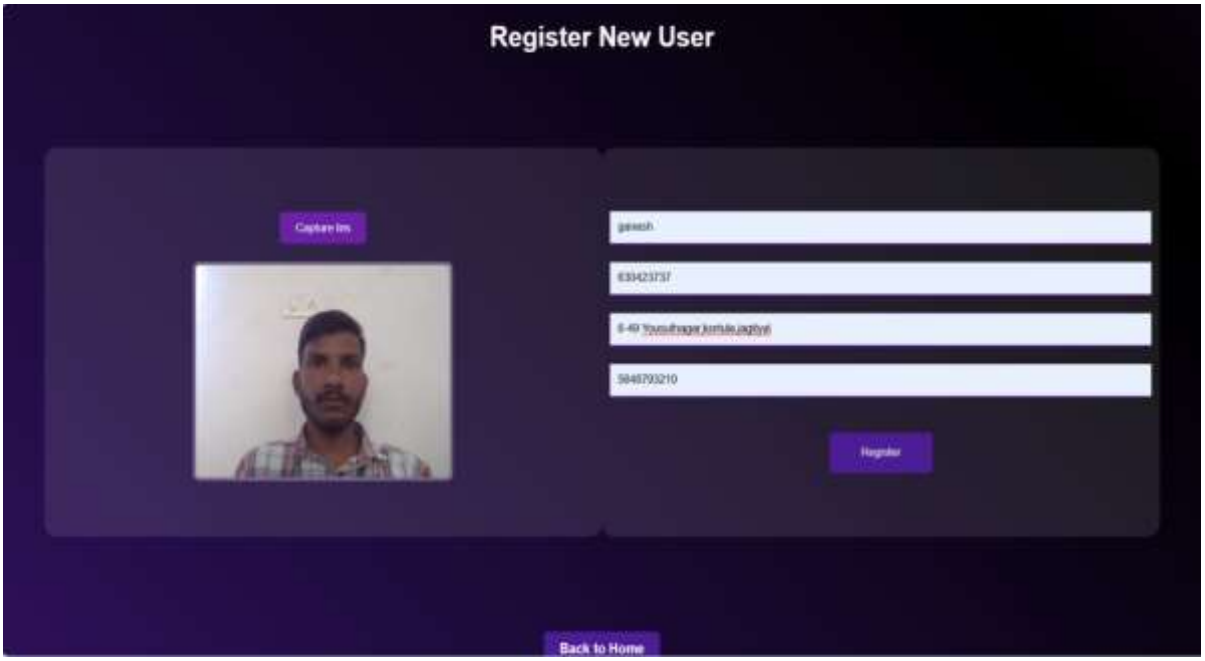
```python
# Admin login
@app.route('/admin/login', methods=['POST'])
def admin_login():
    data = request.json
    if data['username'] == 'admin' and data['password'] == 'admin123':
        return jsonify({'message': 'Admin logged in successfully!'}), 200
    return jsonify({'message': 'Invalid credentials!'}), 401

# View all users (admin-only)
@app.route('/admin/users', methods=['GET'])
def view_users():
    # Check if admin is authenticated
    if not request.headers.get('Authorization') == 'Bearer admin_token':
        return jsonify({'message': 'Unauthorized access!'}), 403

    users = User.query.all()
    user_list = [
        {
            'account_number': user.account_number,
            'name': user.name,
            'balance': user.balance
        } for user in users
    ]
    return jsonify(user_list), 200
```

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 03, March 2025, pp : 1804-1808

e-ISSN : 2583-1062
Impact Factor : 7.001





7. FUTURE WORK

Future advancements in ATM security systems could focus on integrating artificial intelligence and deep learning techniques to enhance fraud detection and improve authentication accuracy. The implementation of AI-driven behavioral analysis could help identify anomalies in user behavior, preventing potential fraud attempts. Additionally, expanding the system to support voice recognition could provide another layer of security, making ATM transactions even more secure. Mobile banking integration may also be explored, allowing users to authenticate transactions remotely using biometric data. Enhancing the system's adaptability to different environmental conditions, such as varying lighting conditions for iris recognition, will further improve reliability. These enhancements will ensure that ATM security continues to evolve, keeping pace with emerging threats and technological advancements.

8. CONCLUSION

The integration of fingerprint and iris recognition into ATM security systems marks a significant advancement in banking security. This project demonstrates that a dual biometric authentication system effectively mitigates fraud risks, enhances user convenience, and improves transaction security. The implementation of encryption techniques ensures data privacy, while real-time fraud detection mechanisms add an extra layer of protection. The proposed system offers a scalable and reliable solution for financial institutions seeking to enhance ATM security. With future advancements in AI and biometric authentication, this system can further evolve to provide even greater security and efficiency in banking transactions.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 03, March 2025, pp : 1804-1808

e-ISSN : 2583-1062
Impact Factor : 7.001

9. REFERENCES

[1] Pandey, S., & Rajeswari, K. (2013). "A Study on Intelligent Question Generation for Technical Assessments. International Journal of Computational Intelligence and Applications." International Journal of Advanced Computer Research.

[2] Liu, D., Wang, J., & Zheng, L. (2013). "Automatic Test Paper Generation Based on Ant Colony Algorithm." Journal of Software.

[3] Chavan, A., et al. (2016). "Automated Question Paper Generator System Using Apriori Algorithm and Fuzzy Logic." International Journal for Innovative Research in Science & Technology.