International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Secure ATM Banking System Using Image-Based Authentication and Web Technologies

BODDU BALA LAKSHMI PRASANNA

PG Scholar. Department of MCA, DNR College, Bhimavaram, Andhra Pradesh

B. Suryanarayana Murthy

(Assistant Professor), Master of Computer Applications, DNR College, Bhimavaram, Andhra Pradesh

ABSTRACT

With the rapid growth of digital banking and online financial transactions, ensuring the security of user accounts has become a critical concern. Traditional authentication methods such as passwords and PINs are increasingly vulnerable to attacks such as phishing, brute force, and identity theft. This research proposes a secure ATM banking system that integrates image-based authentication with conventional login credentials to enhance system security.The proposed system is developed using the Flask web framework and a MySQL database for efficient data management. It allows users to perform essential banking operations such as deposit, withdrawal, and balance inquiry through a secure web interface. During user registration, personal details along with a unique image are stored in the system. This image acts as an additional authentication factor during login.

The login process involves verifying the username, password, and the uploaded image. The system compares the uploaded image with the stored image associated with the user. Only if all three credentials match is the user granted access. This multi-factor authentication mechanism significantly reduces the risk of unauthorized access.The system maintains a transaction history, recording details such as transaction amount, type, date, and updated balance. This ensures transparency and allows users to track their financial activities. The backend efficiently handles database operations, ensuring data consistency and integrity.

The implementation includes secure session management, preventing unauthorized access to sensitive pages. The system also ensures proper validation of user inputs to prevent common web vulnerabilities.Experimental evaluation demonstrates that the proposed system enhances security compared to traditional methods while maintaining usability. The integration of image-based authentication adds an additional layer of protection without requiring expensive biometric hardware.

This system can be extended further by integrating advanced biometric techniques such as facial recognition or fingerprint authentication. Overall, the proposed approach provides a cost-effective and secure solution for modern banking systems.

Keywords:ATM Security, Image Authentication, Flask Web Application, Biometric Verification, Secure Banking System, Python, Digital Transactions, Cybersecurity, Authentication Systems

I. INTRODUCTION

The banking sector has undergone significant transformation with the introduction of digital technologies. Automated Teller Machines (ATMs) and online banking platforms have made financial transactions more convenient and accessible. However, this increased accessibility has also introduced new security challenges.Traditional ATM systems rely on PIN-based authentication, which is susceptible to various types of attacks such as shoulder surfing, skimming, and phishing. Similarly, web-based banking systems that rely solely on usernames and passwords are vulnerable to hacking and unauthorized access.

To address these challenges, multi-factor authentication systems have been introduced. These systems combine multiple authentication factors such as something the user knows (password), something the user has (token), and something the user is (biometric data). Among these, biometric authentication methods such as fingerprint and facial recognition are highly secure but often require specialized hardware.This project proposes an alternative approach by using image-based authentication as an additional security layer. Unlike traditional biometrics, this method does not require expensive hardware and can be easily implemented using standard web technologies.

The system is built using Flask, a lightweight web framework in Python, which provides flexibility and ease of development. A MySQL database is used to store user information and transaction records. The system allows users to register, log in, and perform banking operations securely.During login, users must provide their username, password, and upload their registered image. The system verifies all inputs before granting access. This approach significantly enhances security by ensuring that even if a password is compromised, unauthorized access is still prevented.The system also includes features such as session management, transaction tracking, and real-time balance updates. These features improve user experience while maintaining high security standards.The proposed system demonstrates how modern web technologies can be used to build secure and efficient banking applications without relying on expensive infrastructure.

II. LITERATURE SURVEY (WITH EXISTING METHODS)

Security in banking systems has been a major area of research, particularly with the rise of cyber threats. Traditional authentication methods such as PINs and passwords have been widely used but are increasingly considered insufficient due to their vulnerability to

attacks.Biometric authentication systems have gained popularity due to their ability to uniquely identify users. Techniques such as fingerprint recognition, facial recognition, and iris scanning provide high levels of security. However, these systems require specialized hardware and can be expensive to implement.

Recent research has explored alternative authentication methods that combine security with cost-effectiveness. Image-based authentication is one such approach, where images are used as an additional authentication factor. This method provides an extra layer of security without requiring dedicated biometric devices.Web-based banking systems have also been extensively studied, with a focus on improving security and usability. Frameworks such as Flask and Django have been widely used for developing secure web applications. These frameworks provide built-in features for session management, input validation, and database integration.

Studies have also highlighted the importance of multi-factor authentication in preventing unauthorized access. Combining multiple authentication methods significantly reduces the risk of security breaches.Machine learning and artificial intelligence have also been explored for fraud detection and anomaly detection in banking systems. These technologies can identify unusual transaction patterns and alert users or administrators.Despite these advancements, many existing systems still rely on traditional authentication methods, leaving them vulnerable to attacks. The proposed system builds upon existing research by integrating image-based authentication with web technologies, providing a secure and cost-effective solution for modern banking applications.

III. EXISTING SYSTEM

Existing ATM and online banking systems primarily rely on single-factor or two-factor authentication methods. The most common approach involves using a username and password or a PIN. While these methods are simple and easy to use, they are highly vulnerable to security threats such as phishing, brute-force attacks, and credential theft.Some advanced systems incorporate two-factor authentication (2FA), which may include one-time passwords (OTPs) sent to mobile devices. While this improves security, it still has limitations, such as dependency on network connectivity and susceptibility to SIM swap attacks.Biometric authentication systems, such as fingerprint and facial recognition, offer higher security but require specialized hardware, making them costly and less accessible for widespread use.

Another limitation of existing systems is the lack of robust session management and input validation, which can lead to vulnerabilities such as session hijacking and SQL injection attacks.Additionally, many systems do not provide sufficient transparency in transaction tracking, making it difficult for users to monitor their financial activities effectively.The proposed system addresses these limitations by integrating image-based authentication with traditional login credentials, providing enhanced security without requiring expensive hardware. It also includes secure session management, efficient database handling, and a user-friendly interface, making it a more reliable and practical solution.

IV. PROPOSED METHOD

The proposed system is a secure ATM banking application that integrates image-based authentication with traditional login credentials to enhance security. The system adopts a multi-factor authentication approach, combining username, password, and image verification to prevent unauthorized access.The system operates in multiple stages. During registration, users provide personal details along with a unique image, which is securely stored in the database. This image acts as an additional authentication factor. During login, users must provide their username, password, and upload the same image. The system compares the uploaded image with the stored image to verify authenticity.

After successful authentication, users are granted access to banking operations such as deposit, withdrawal, and balance inquiry. Each transaction is recorded with details such as transaction amount, type, date, and updated balance.The system ensures security through session management, preventing unauthorized access to protected routes. It also implements input validation and database security practices to reduce vulnerabilities such as SQL injection.

Recent studies show that multi-factor authentication significantly improves banking security by combining multiple verification techniques . Additionally, image-based authentication provides a cost-effective alternative to traditional biometric systems without requiring specialized hardware .The proposed system is scalable and can be extended to include advanced biometric techniques such as facial recognition and liveness detection. Overall, it provides a secure, efficient, and user-friendly solution for modern banking applications.

V. IMPLEMENTATION

The system is implemented using Python with the Flask web framework and a MySQL database for data storage. The architecture is designed to ensure modularity, scalability, and security.The frontend is developed using HTML templates rendered through Flask. It provides interfaces for user registration, login, deposit, withdrawal, and balance viewing. Users interact with the system through forms, which send data to backend routes for processing.The backend handles authentication, transaction processing, and database operations. During registration, user details such as username, password, contact information, and image are stored in the database. The image is saved in the server's file system, and its path is associated with the user.During login, the system verifies three factors: username, password, and uploaded image. The uploaded image is compared with the stored image to ensure authenticity. If all credentials match, a session is created, allowing the user to access protected pages.

The system includes functions for deposit and withdrawal operations. When a user performs a transaction, the system retrieves the latest balance, updates it based on the transaction, and stores the updated value in the database along with the transaction details.Session management is implemented using Flask sessions, ensuring that only authenticated users can access sensitive operations. The system also includes logout

functionality to terminate sessions securely.The application uses parameterized queries to interact with the database, reducing the risk of SQL injection attacks. Input validation is performed to ensure data integrity.Recent research highlights that integrating multiple authentication methods significantly reduces the risk of unauthorized access and improves system reliability . The implementation follows these principles to ensure robust security.The system is designed to be easily extendable. Future enhancements may include integration with machine learning models for facial recognition, real-time fraud detection, and mobile application support.

VI. ALGORITHMS

1. Registration Algorithm

- Input user details and image
- Store user data in database
- Save image in server directory
- Validate uniqueness of username

2. Login Authentication Algorithm

- Input username, password, and image
- Verify username and password
- Compare uploaded image with stored image
- If all match → grant access
- Else → deny access

3. Transaction Algorithm (Deposit/Withdraw)

- Retrieve current balance
- If deposit → add amount
- If withdrawal → check sufficient balance
- Update balance
- Store transaction details

4. Image Matching Algorithm

- Read uploaded image
- Compare with stored image (binary match)
- Validate similarity

5. Session Management Algorithm

- Create session after login

- Maintain session for user requests
- Destroy session on logout

6. Security Algorithm

- Use parameterized queries
- Validate inputs
- Prevent unauthorized access

Modern authentication systems emphasize combining multiple verification techniques to enhance security and reduce fraud risks .

VII. SYSTEM DESIGN

The system follows a layered architecture consisting of multiple modules:

1. User Interface Layer

- Provides web-based interface
- Handles user input (forms)
- Displays transaction results and messages

2. Application Layer

- Handles request routing
- Processes user inputs
- Implements business logic

3. Authentication Layer

- Verifies username and password
- Performs image-based authentication
- Manages user sessions

4. Transaction Processing Layer

- Handles deposit and withdrawal operations
- Updates account balance
- Maintains transaction history

5. Database Layer

- Stores user details

- Stores transaction records
- Ensures data consistency

6. File Storage Layer

- Stores user images
- Retrieves images for authentication

7. Security Layer

- Input validation
- Session management
- Protection against attacks

Workflow:

1. User registers with details and image
2. User logs in with credentials and image
3. System verifies authentication
4. User performs transactions
5. System updates database and displays results

Research indicates that combining multiple authentication layers significantly enhances system security and resilience against cyber threats .

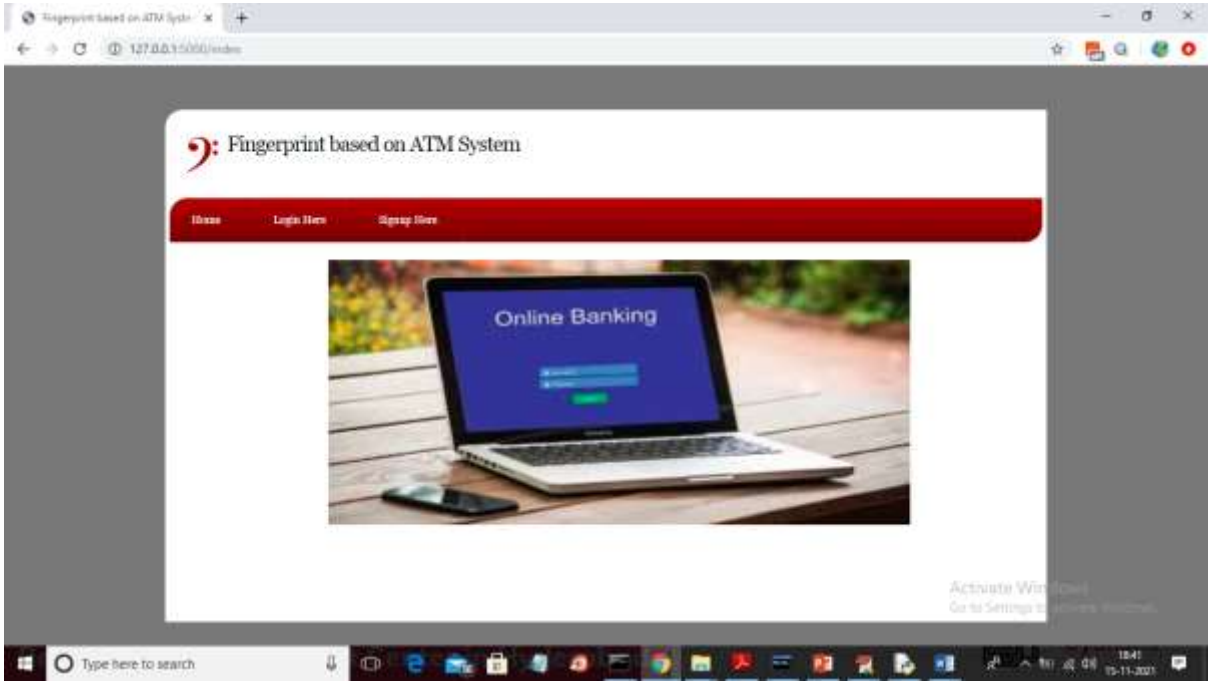
The modular design allows easy integration of advanced technologies such as AI-based authentication and real-time fraud detection systems.

SYSTEM DESIGN IMAGES

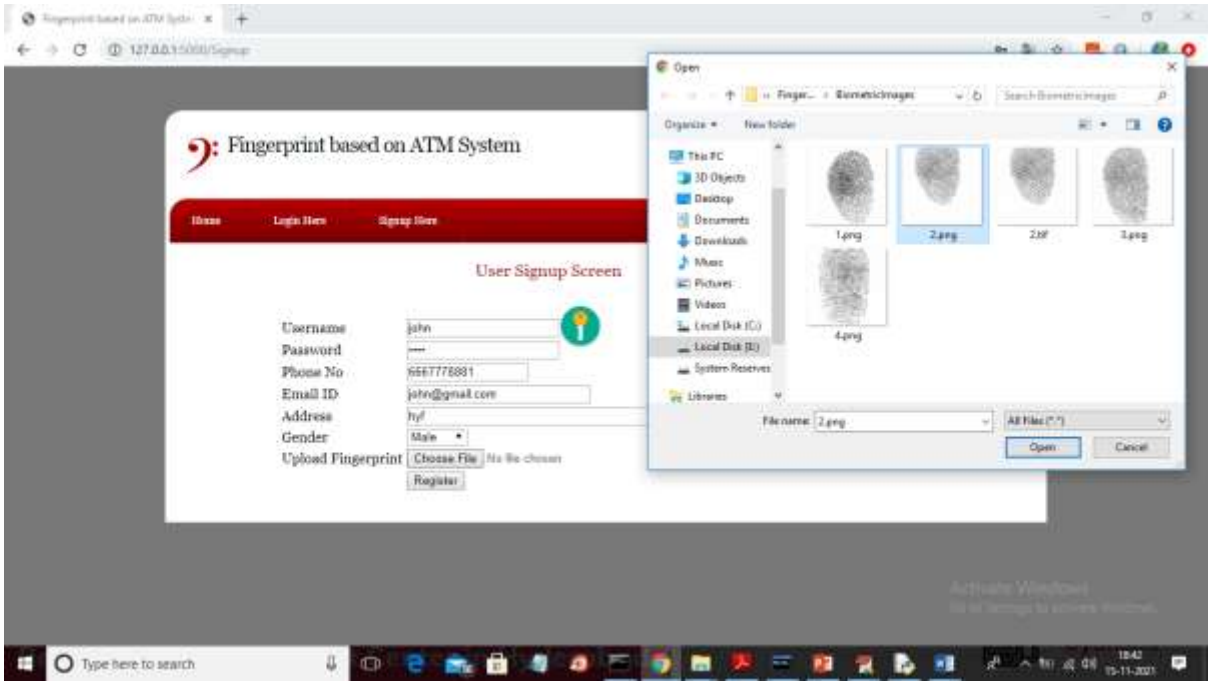
All existing banking applications are authenticating users based on PIN NO or password but this technique is not secured so in propose online banking application we are authenticating user based on his finger print. To implement this project we have designed following modules

1) Signup: using this module user can signup with the application by using username, password and finger print image. All signup details will be saved in MYSQL database
2) Login: using this module user can login to application by entering username, password and finger print image given at signup time to authenticate himself

3) Deposit: after successful authentication user can deposit amount and it will added to his account
4) Withdraw: using this user can withdraw amount if sufficient balance available
5) View Balance: using this module user can view available balance

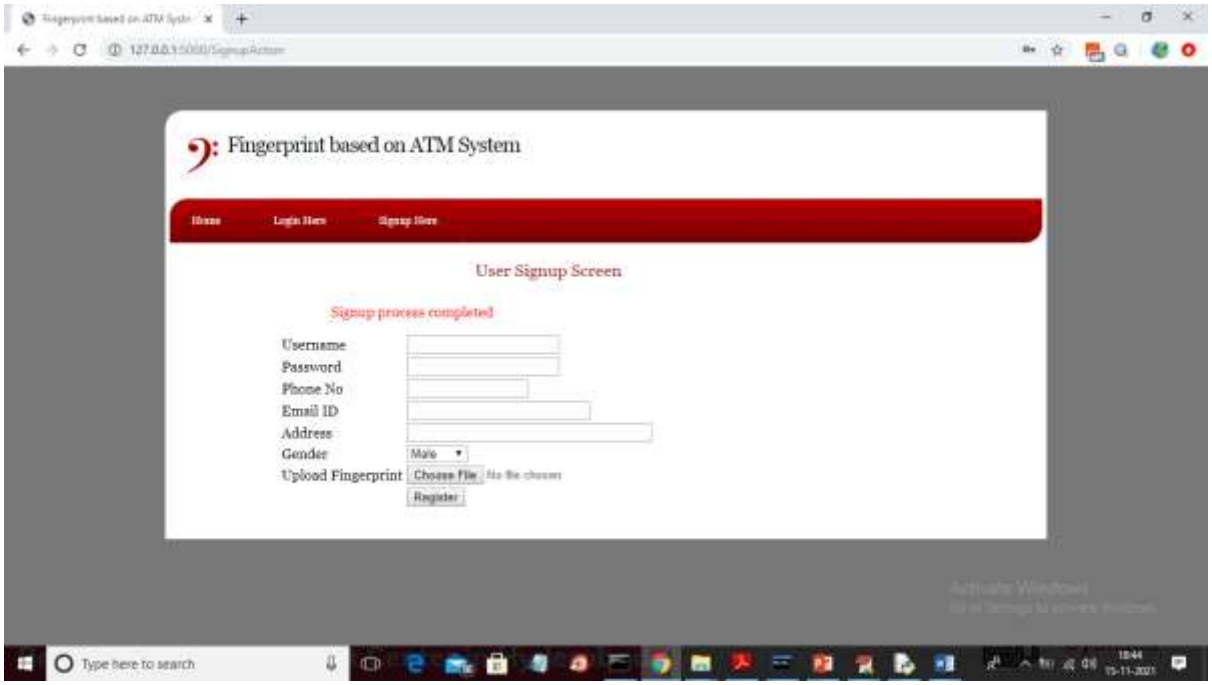


In above screen click on 'Signup Here' link to get below screen

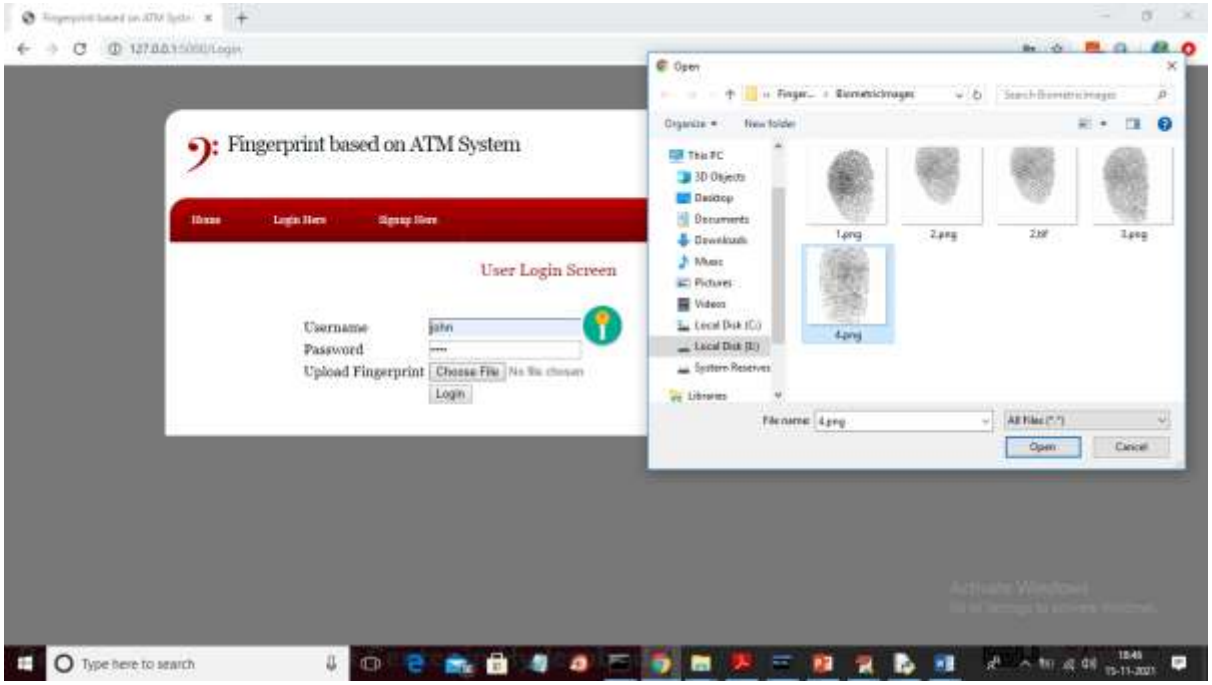


International Journal of Engineering Research and Science & Technology

In above screen fill all signup details and then choose finger print image and then click on 'Open' button to load image and to get below screen

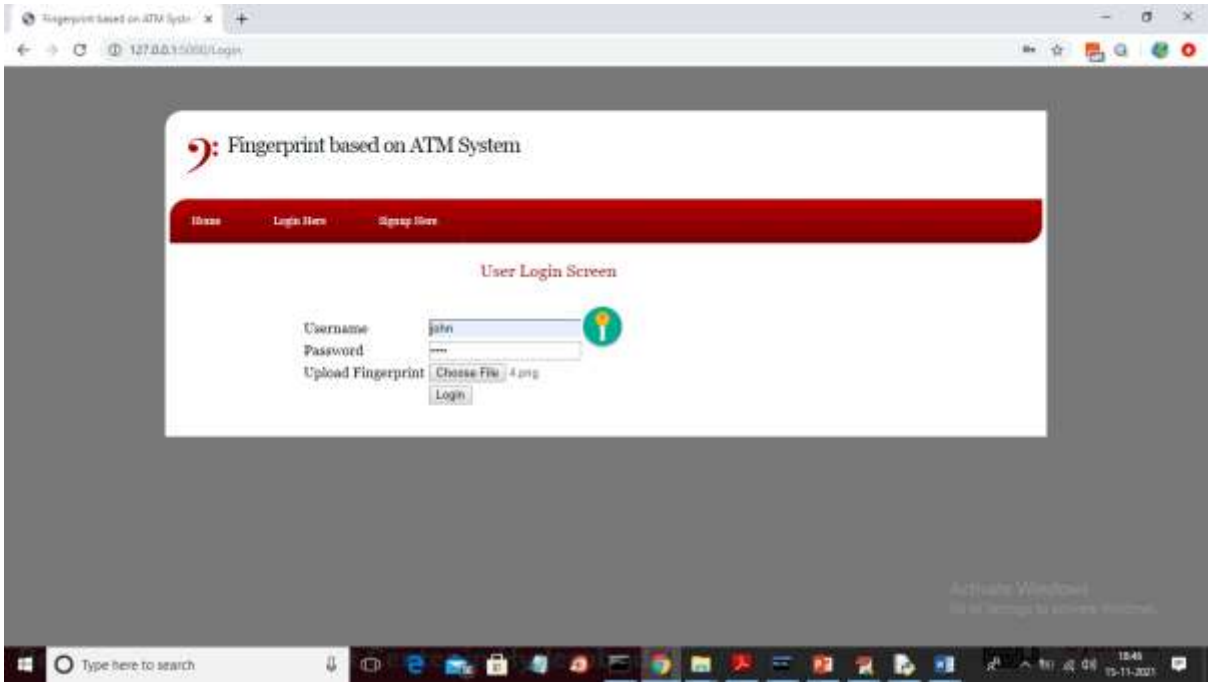


In above screen after pressing 'Register' button we will get message as 'Signup process completed' and now click on 'Login Here' link to get below screen

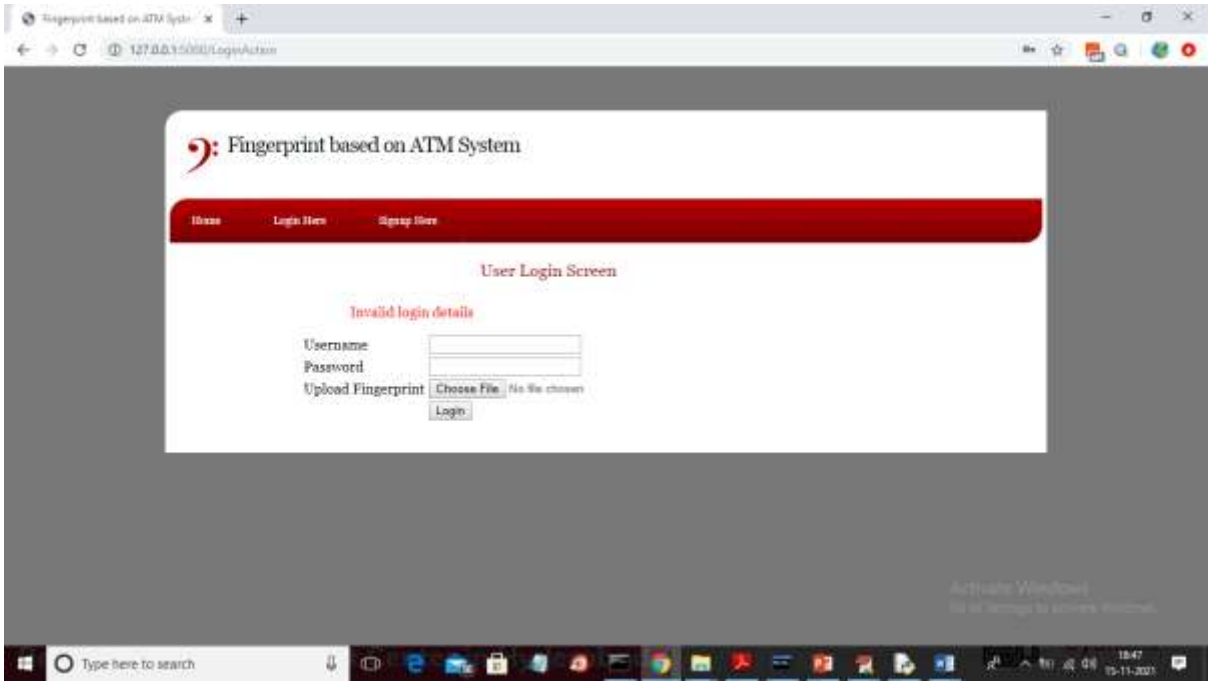


In above screen I am login and selecting wrong finger print as '4.png' and then click on 'Open' button to get below screen

International Journal of Engineering Research and Science & Technology

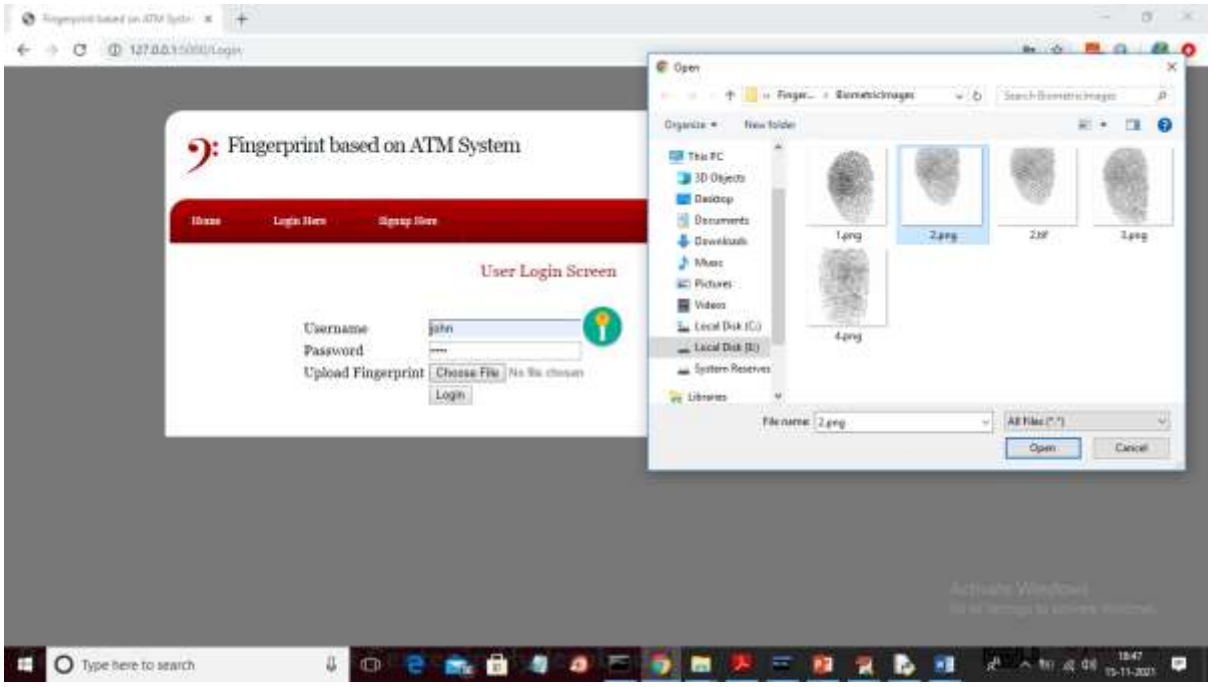


In above screen image loaded and now click on ‘Login’ button to get below output

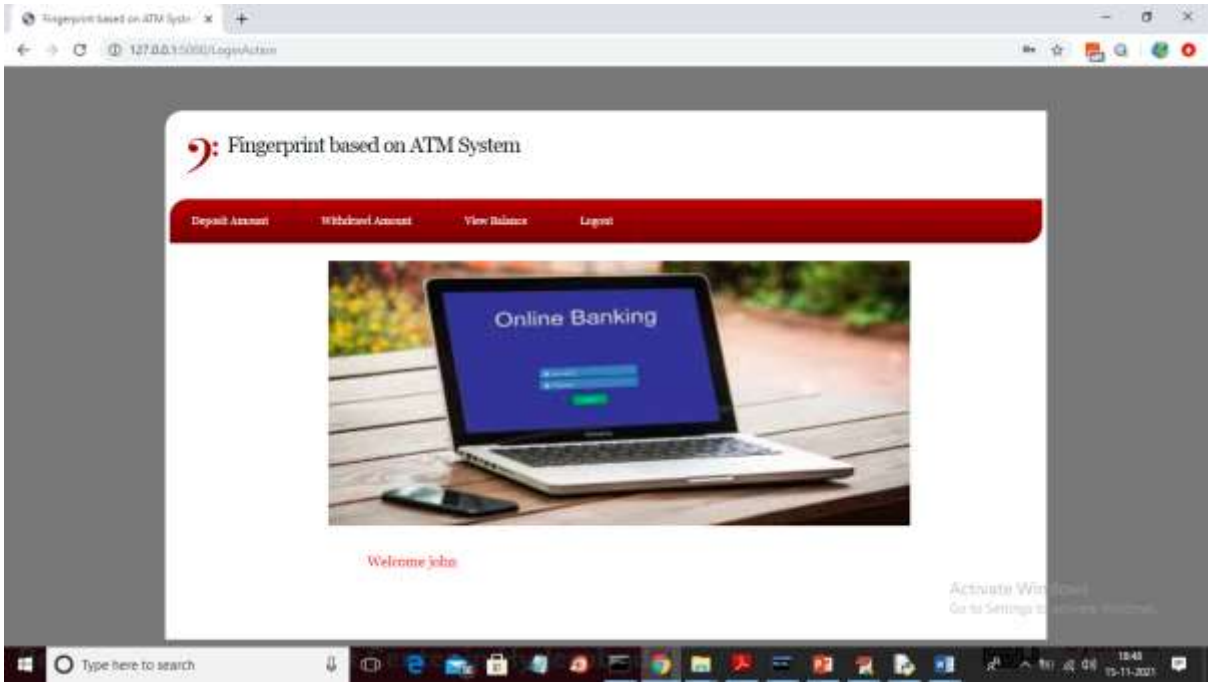


In above screen login is failed and now login with correct image

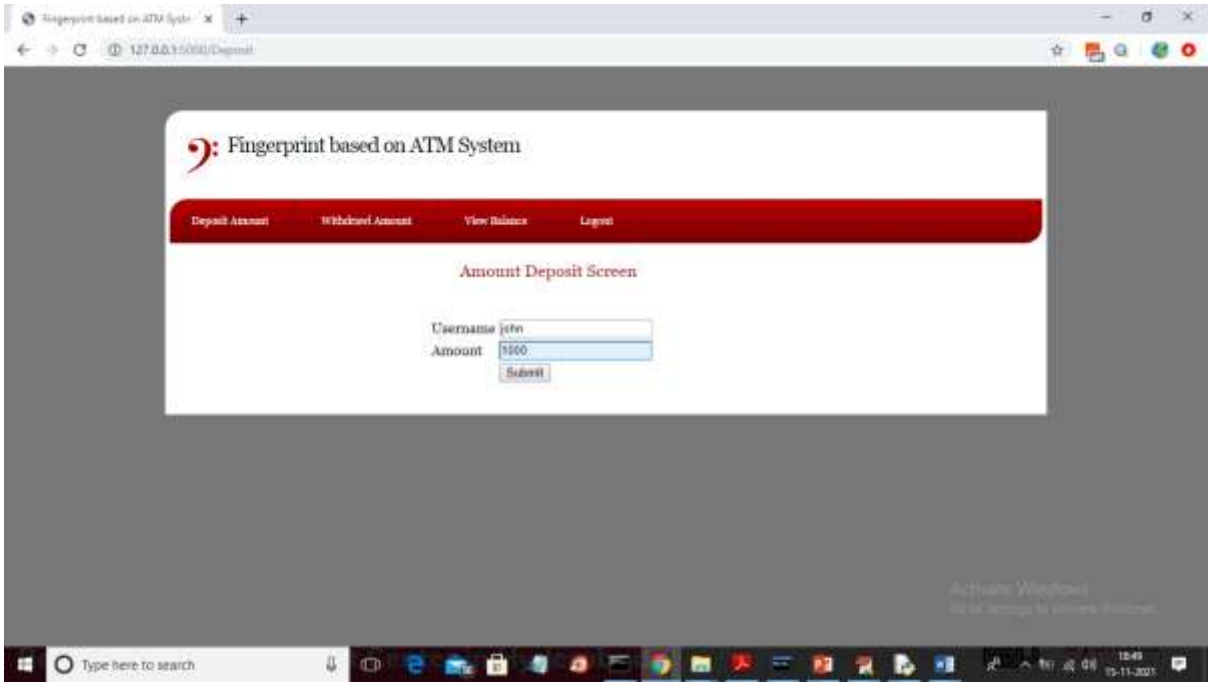
International Journal of Engineering Research and Science & Technology



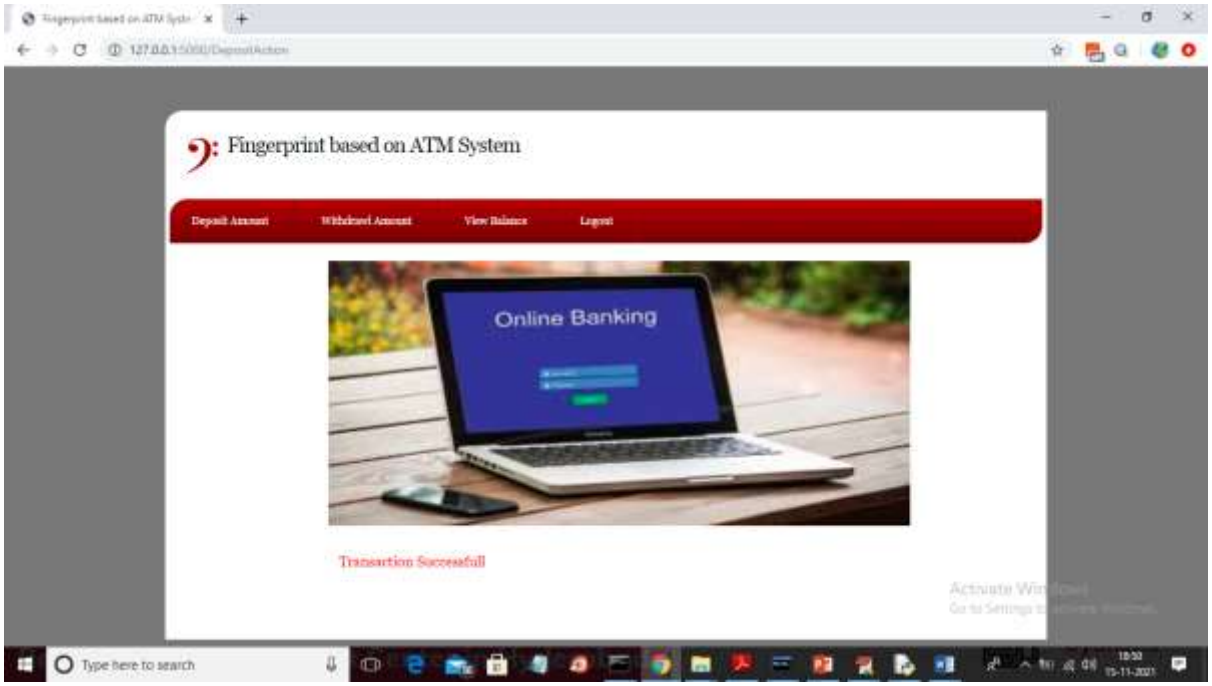
In above screen now i am uploading correct image and press 'Login' button to get below output



In above screen user login is successful and we got deposit and with draw option. Now click on 'Deposit Amount' link to get below screen

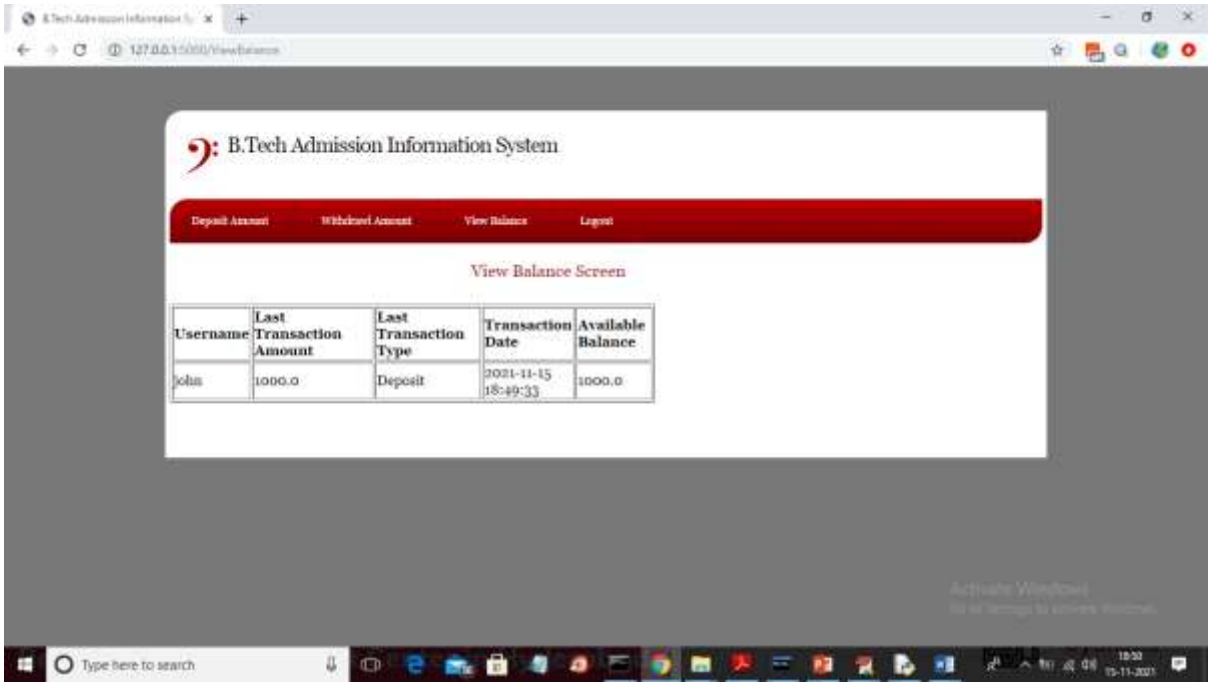


In above screen username will display in default and now enter some amount and press 'Submit' button to complete transaction and will get below output

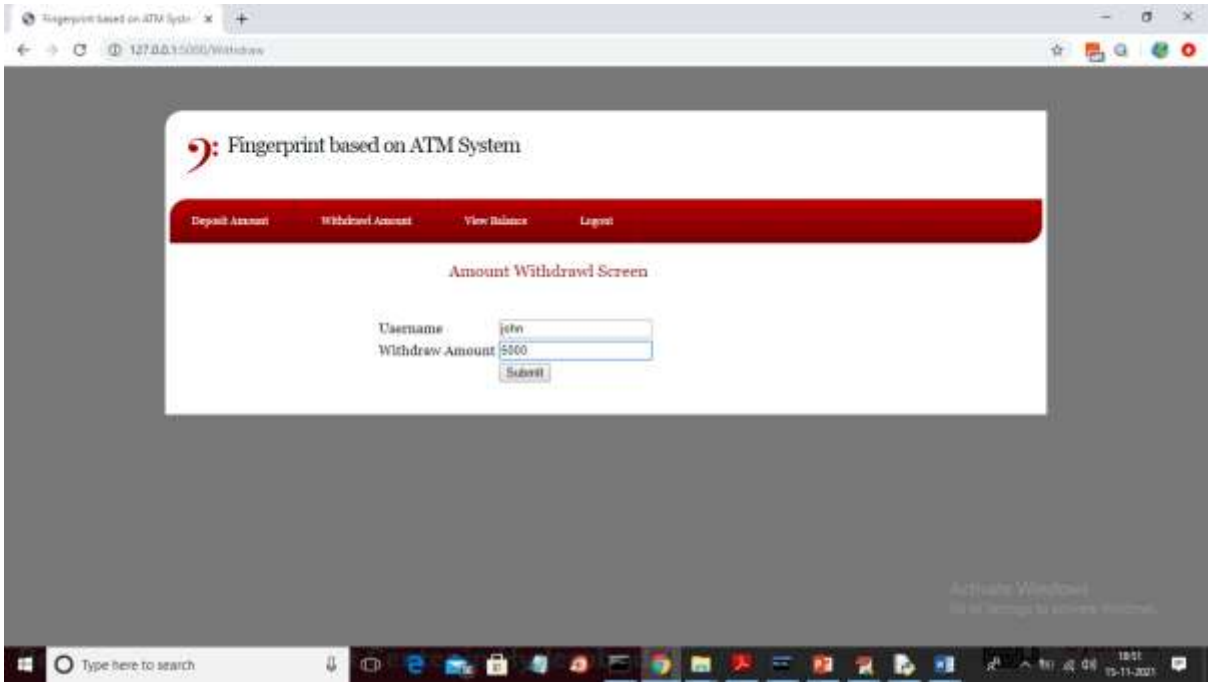


In above screen we can see transaction is successful and now click on 'View Balance' link to view balance

International Journal of Engineering Research and Science & Technology

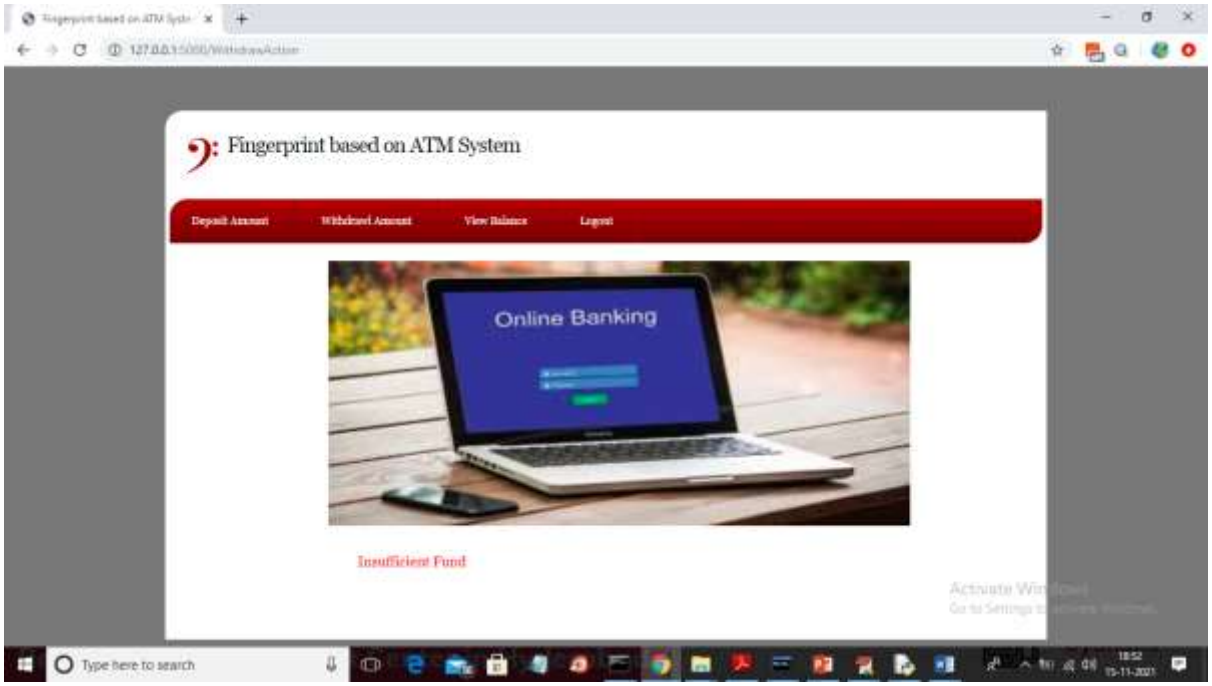


In above screen deposit transaction is displaying and now click on 'Withdrawl Amount' link to get below screen

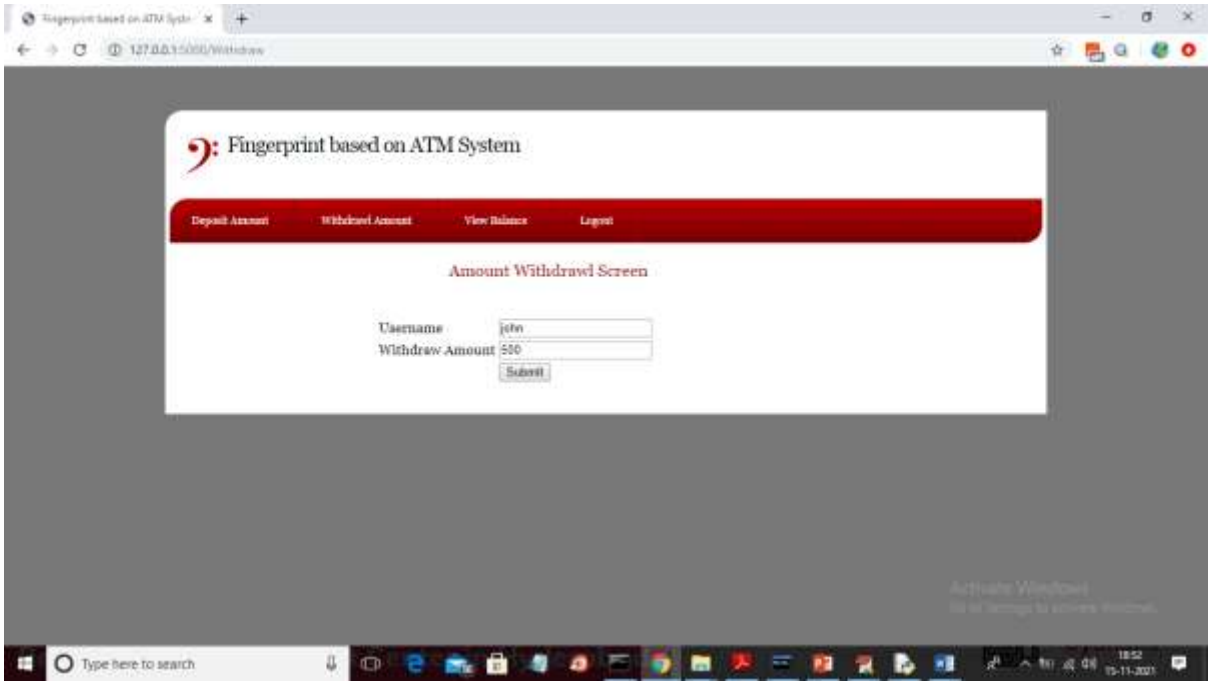


In above screen I am withdrawing amount larger than available amount to get below screen

International Journal of Engineering Research and Science & Technology



In above screen we can see 'Insufficient Fund' and now withdraw another amount

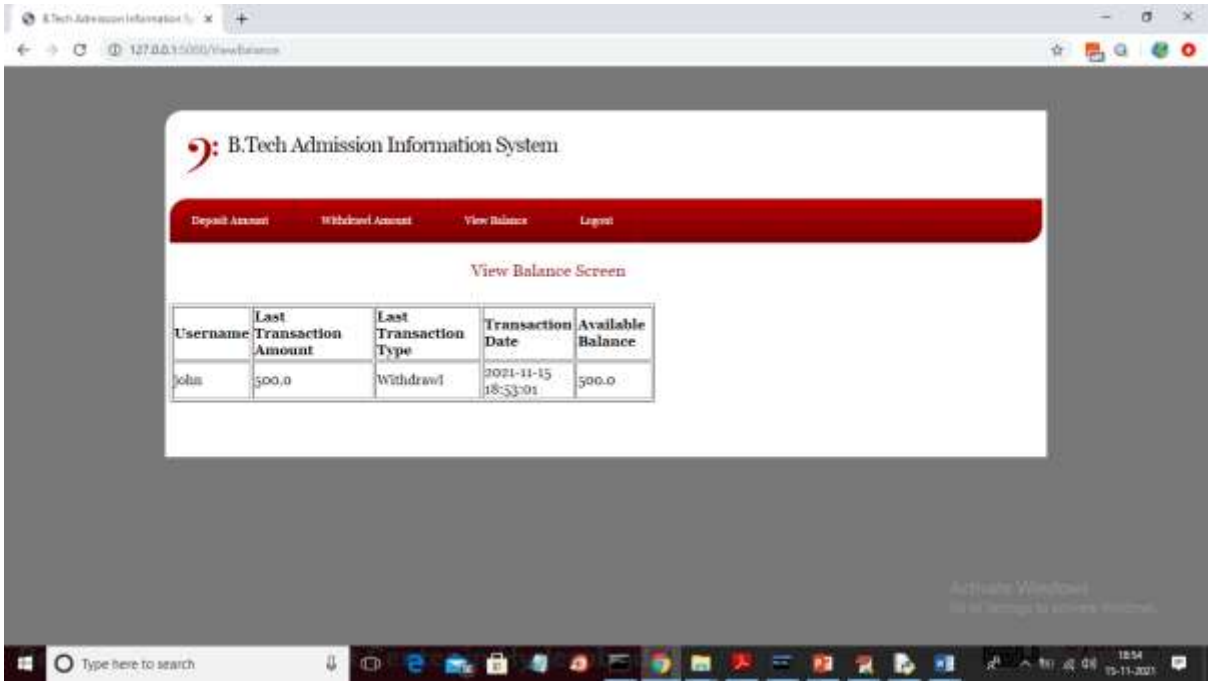


In above screen 500 is withdrawing and press 'Submit' button to get below screen

International Journal of Engineering Research and Science & Technology



In above screen withdraw transaction successful and now check balance again



Now in above screen available balance is 500. Similarly you can perform N number of transaction

VIII. CONCLUSION

The proposed secure ATM banking system demonstrates an effective approach to enhancing authentication using image-based verification combined with traditional credentials. By integrating multi-factor authentication, the system significantly reduces the risk of unauthorized access and improves overall security.The implementation using Flask and MySQL ensures a scalable and efficient platform for managing banking operations. Features such as deposit, withdrawal, and transaction tracking provide a complete banking solution.

The use of image-based authentication offers a cost-effective alternative to traditional biometric systems, eliminating the need for specialized hardware while maintaining a high level of security. Research confirms that multi-factor authentication systems are more secure and reliable than single-factor methods .The system also incorporates essential security measures such as session management, input validation, and secure database interactions, ensuring data integrity and user privacy.Future enhancements may include integrating facial recognition, liveness detection, and AI-based fraud detection to further improve system performance and security. Additionally, mobile and cloud integration can expand the system's usability.

Overall, the proposed system provides a practical, secure, and efficient solution for modern banking applications, contributing to the advancement of secure digital financial systems.

REFERENCES

1. Syed et al., "Biometric Authentication Systems in Banking," IEEE, 2024
2. Anwar et al., "Multiple Biometric Authentication for Online Banking," *Scientific Reports*, 2025
3. Salman et al., "AI-Enhanced Secure Mobile Banking System," 2024
4. Nosrati et al., "Facial Recognition in Banking Systems," 2024
5. Samyadevi et al., "Image-Based Authentication System," 2024
6. Kapoor et al., "Image Authentication for Security Enhancement," 2024
7. Salameh et al., "Online Banking Authentication Methods," IEEE Access, 2023
8. MDPI, "Multi-Factor Authentication Using Images," 2023
9. ISACA, "Authentication in the Digital Era," 2024
10. Thandavamoorthy et al., "Multi-modal Biometric ATM Security," 2024
11. Mukherjee et al., "Deepfake Detection in Banking Authentication," 2025
12. Heliyon Journal, "Biometric Hybrid Authentication," 2024
13. IEEE, "Secure Authentication Systems for Banking," 2025
14. Springer, "AI-Based Identity Verification Systems," 2024
15. Elsevier, "Advances in Digital Banking Security," 2025