IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306226|

Securing Net Banking Transactions: Using Face Recognition and Blockchain Technology

J. Santhana Krishnan[1], Biju Balakrishnan[2]

Student, Department of MCA, Hindusthan College of Engineering and Technology, Coimbatore, India[1]

Assistant Professor, Department of MCA, Hindusthan College of Engineering and Technology, Coimbatore, India[2]

ABSTRACT: Blockchain technology provides robust security for banking by decentralizing transaction verification and storage, reducing costs, and eliminating the need for intermediaries. By implementing blockchain, we ensure data integrity and resilience against failures, as each node holds a complete transaction ledger linked through the SHA-256 algorithm. This project integrates blockchain with face detection to secure net banking transactions, ensuring only authenticated users can perform operations. This combination enhances trust and reliability in the banking industry, offering a secure, decentralized, and transparent solution for transaction management.

KEYWORDS: Blockchain technology, Face detection, Decentralized ledger, Banking transactions.

I. INTRODUCTION

1.1 OVERVIEW

The security measures aims to enhance internet banking security by integrating face biometrics with traditional authentication methods. During enrolment, a template is stored either on a card or in a database. During matching, the obtained template is compared with existing ones using algorithms like Hamming distance. The application requires the user to input a username, password, and face image via their device camera. The system pre-processes the iris image and scans the database for authentication. If all credentials match, the user is authenticated. This approach aims to provide a more secure and reliable method than traditional username and password alone, leveraging the unique and stable characteristics of facial features. Cued click point selection for face recognition further enhances security.

1.2 PROBLEM DESCRIPTION

Traditional internet banking authentication methods, relying solely on usernames and passwords, are vulnerable to various security threats such as guessing, phishing, and identity theft. These methods do not provide robust security as passwords can be easily compromised. Additionally, the growing sophistication of cyber-attacks necessitates more secure authentication mechanisms. The challenge is to develop a system that can ensure secure user authentication while being user-friendly and efficient. Face biometrics, with its unique and stable features, offers a promising solution. Integrating biometric authentication can significantly reduce the risk of unauthorized access. Thus, there is a need to implement an advanced security system for internet banking that combines facial recognition with traditional methods.

1.3 OBJECTIVE

The primary objective of this project is to develop an application that enhances the security of internet banking transactions by using face biometrics in conjunction with traditional username and password authentication. The system will capture and pre-process a user's face image for authentication. It aims to reduce the risk of unauthorized access by leveraging the unique and stable characteristics of facial features. The project also seeks to implement cued click point selection to further enhance security. By doing so, it aims to offer a more reliable and user-friendly authentication method. The objective is to create a secure and efficient system that can be widely adopted in the banking industry. Ultimately, the project aims to protect users from identity theft and other cyber threats.

1.4 SCOPE

The scope of this project includes designing and developing a secure internet banking application that integrates face biometrics with traditional authentication methods. It involves creating a system for capturing and processing facial images for user authentication. The project will implement algorithms for template matching and cued click point selection. The system will be tested for performance, reliability, and user-friendliness. Additionally, considerations will include sensor and device availability, computational time, and cost. The application will be designed to deter identity

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306226|

theft and unauthorized access. The project will focus on ensuring the robustness and social acceptability of the biometric system. Finally, it aims to provide a scalable solution suitable for widespread adoption in the banking industry.

II. SYSTEM SPECIFICATION

2.1 SOFTWARE REQUIREMENTS

- Operating system : Windows OS
- Front End : .NET
- Back End : SQL SERVER
- Application : Web Application
- Tool : Visual Studio 2010

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

Ensuring safe online transactions remains a significant challenge, with user authentication being crucial for secure access to online banking services. While technology can enhance authentication quality and online security, it often compromises usability. Various technologies, such as One Time Passwords (OTPs), are employed to combat banking fraud but come with their own set of challenges. Transaction monitoring, inspired by credit/debit card fraud prevention, analyzes transactions for fraud patterns without requiring additional user hardware. However, this method also has drawbacks, including vulnerabilities to new fraud patterns and the potential for false positives. Genuine transactions may be flagged and forwarded to call centers, causing inconvenience to customers. Overall, existing security measures each present unique challenges, underscoring the need for more effective solutions. Balancing security and usability in online banking remains a critical issue.

Disadvantages

- Conventional methods of authentication via usernames and passwords are no longer sufficient.
- Guessing attack and Online dictionary attack can be occurred.
- Difficult to analyze the original users.
- Multi-person access may be fraudulent.
- SMS alert only provide for current transactions, difficult to know the specific persons.

3.2 PROPOSED SYSTEM

The proposed project aims to enhance the security of internet banking systems by incorporating face biometric authentication alongside existing methods. Currently, internet banking uses static user IDs, passwords, and OTPs sent to mobile numbers. Although this is a strong security feature, it remains vulnerable, necessitating further enhancements. Biometrics, which identifies individuals using biological behaviours, is a promising technology for securing valuable information but is not yet widely used in internet banking. In this system, the primary user can grant account access to secondary users, setting limits for their access. During login, face recognition will identify whether the user is primary or secondary. Users must select a click-point within a highlighted portion of their face image; if unable, they can shuffle to the next highlighted area. This method encourages the creation of more random and difficult-to-guess passwords. Additionally, OTP-based passwords will be sent during transactions. Finally, SMS alerts will notify the primary user of access details, and session time analysis will help prevent infrequent access.

Advantages

- Overcome the guessing attacks and dictionary attacks
- Without primary user knowledge, no one perform fraud activities
- No need to implement additional sensors
- SMS alert to know about transactions details up to date
- Multi-party access with improved security

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

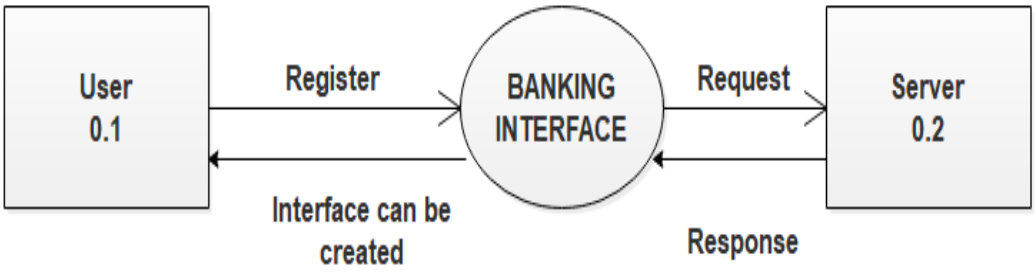
|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306226|

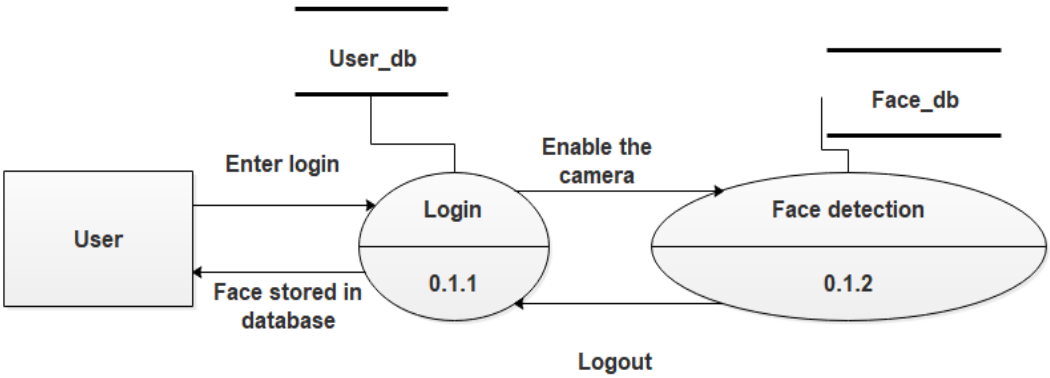
IV. SYSTEM DESIGN

4.1 DATA FLOW DIAGRAM

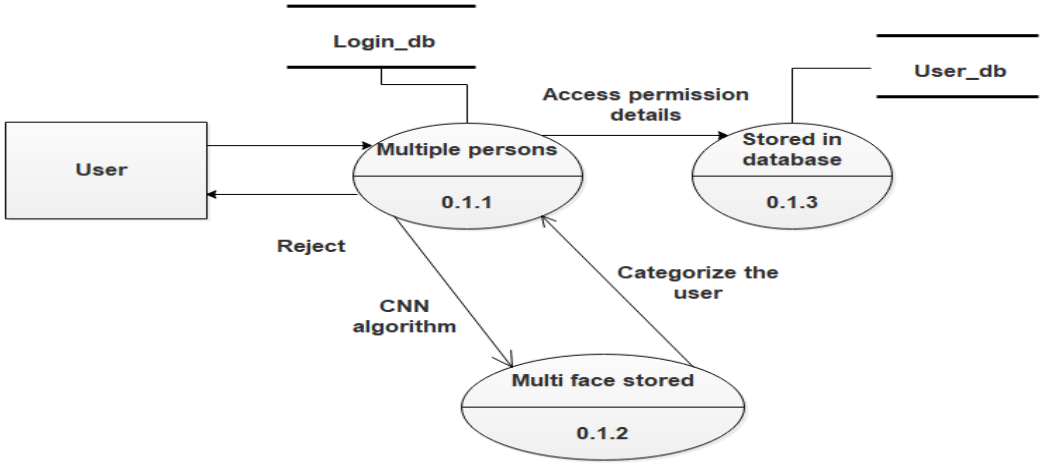
LEVEL 0



LEVEL 1



LEVEL 2



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

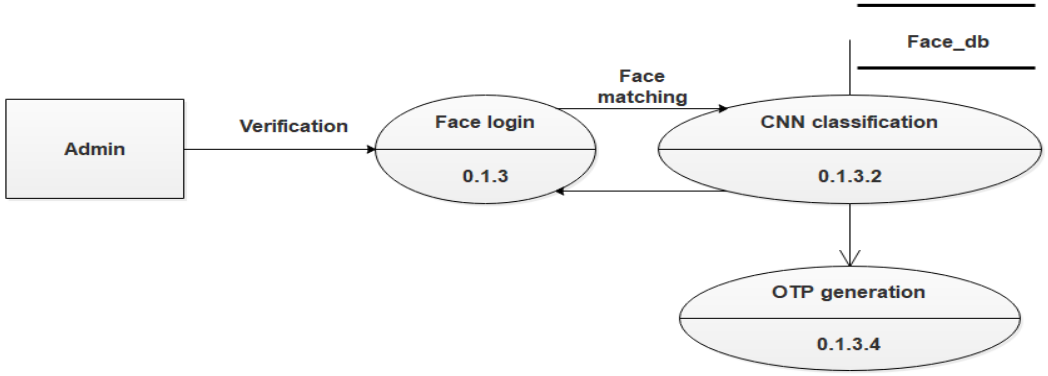
Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

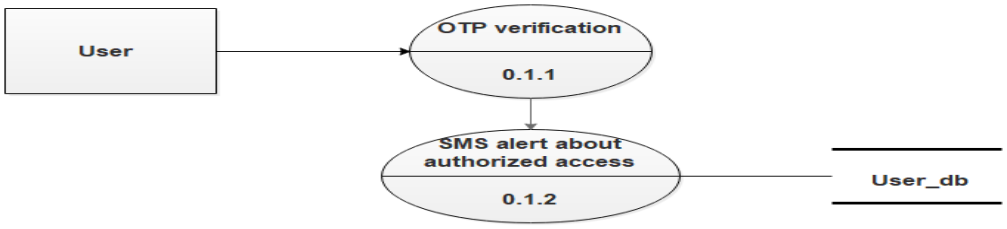
|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306226|

LEVEL 3



LEVEL 4



4.2 PROJECT EXPLANATION

4.2.1 BANK INTERFACE CREATION

User interfaces are crucial in computing systems, especially in contexts like Internet Banking where customers access services globally. Traditional security measures such as passwords and tokens are increasingly vulnerable to sophisticated attacks. Dissatisfied customers might resort to actions like spreading rumors of service failures or withdrawing patronage. Hence, designing secure and user-friendly interfaces is paramount. These interfaces facilitate various operations such as net banking, credit card transactions, and debit card transactions. They must adhere to best practices and high standards to mitigate risks effectively. While no single Internet Banking System reigns supreme globally, contemporary and customer-centric design principles are essential. System designers play a pivotal role in ensuring interfaces are innovative and robust against evolving threats. Admin interfaces enable management of user details and account information, enhancing operational efficiency and security. By prioritizing secure interface design, Internet Banking systems can better protect against malicious activities and maintain customer trust worldwide.

4.2.2 FACE DETECTION

Face recognition is a complex task within image analysis and computer vision, posing significant challenges. As information security grows increasingly crucial, innovative approaches are needed to enhance detection accuracy. This module focuses on implementing a features-based method to identify facial components like nose, lips, eyes, and cheeks. It utilizes the iterative closest point algorithm to refine and align these features accurately. By employing this method, the system aims to improve overall facial recognition performance and robustness. Such advancements are pivotal in developing more secure and reliable systems for various applications requiring facial recognition technology.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306226|

4.2.3 FACE VERIFICATION

This module focuses on implementing a Convolutional Neural Network (CNN) algorithm for verifying multiple users, leveraging its effectiveness in various competitions and research. CNNs are renowned for their ability to enhance training performance by reducing the number of parameters through spatial convolution, minimizing the need for extensive data preprocessing. The network structure of CNNs involves input data passing through successive layers, each equipped with convolutional kernels that extract crucial data characteristics. This hierarchical processing ensures that the most significant features are identified and utilized for user verification tasks. The development of CNNs has revolutionized image analysis and pattern recognition, providing robust solutions for complex datasets and user authentication systems. Researchers continually refine CNN architectures to optimize accuracy and adaptability across diverse applications. CNNs' capacity to autonomously learn and extract features directly from raw data distinguishes them as powerful tools for tasks requiring high precision and efficiency. As CNN algorithms evolve, they promise ongoing advancements in user verification and broader applications in artificial intelligence and machine learning domains

4.2.4 OTP GENERATION

One-time passwords (OTPs) are unique passwords valid for a single session or transaction, contrasting with static passwords by preventing replay attacks. Once an OTP is used, it becomes invalid, thwarting attempts by intruders to reuse intercepted codes. This security feature ensures that compromised OTPs cannot be exploited to access services or conduct transactions. Another advantage is that using the same or similar password across multiple systems does not expose all accounts if one OTP is compromised. OTP systems often incorporate unpredictable session data to further reduce interception and impersonation risks, bolstering overall security.

By generating fresh authentication codes for each login attempt, OTPs significantly enhance account security in digital environments. They provide robust protection against unauthorized access and cyber threats, making them ideal for securing sensitive transactions and user logins. As organizations prioritize stronger authentication measures, OTP adoption continues to grow due to its effectiveness in safeguarding user information. Overall, OTPs offer a reliable solution to mitigate risks associated with static password vulnerabilities in today's interconnected digital landscape.

4.2.5 SMS NOTIFICATION

SMS notifications are sent in response to events or transactions, serving purposes beyond marketing by enhancing organization and public safety. They are particularly valuable for providing timely transaction alerts to primary users, containing essential details such as username, timing, amount, payment mode, and more. This ensures users are promptly informed about transaction specifics, promoting transparency and up-to-date awareness. SMS alerts play a crucial role in keeping users informed and engaged, enabling them to monitor transactions effectively and maintain security. This feature not only enhances user experience but also supports organizational efficiency and public safety initiatives through timely communication

4.2.6 BLOCK CHAIN TECHNOLOGY

Blockchain technology utilizes cryptography, decentralization, and consensus mechanisms to create a secure data structure. Data is organized into blocks where each block contains transactions. These blocks are cryptographically linked in a chain, making tampering extremely difficult. Transactions undergo validation through a consensus process, ensuring their accuracy and reliability. This approach guarantees trust in the transactional integrity of blockchain and distributed ledger technologies (DLT), making them robust solutions for secure and transparent record-keeping. Blockchain's decentralized nature and cryptographic security principles enhance trust among participants, fostering innovation in various industries reliant on secure data management and transaction verification.

V. IMPLEMENTATION

5.1 WORKING

5.1.1 Frontend

The user interface for the internet banking application is developed using .NET framework. The interface includes login and transaction screens that prompt users for their username, password, and face image.

5.1.2 Backend

A backend server is set up using .NET to handle authentication requests and transactions. The database, implemented

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306226|

using SQL Server, stores user data, facial templates, and transaction records.

5.1.3 Face Recognition

Face detection and recognition are implemented using .NET properties for image capturing and comparison. The system captures facial images during the enrollment phase and stores them securely in the database. During the login phase, the system captures and processes the user's face image, comparing it with stored templates using .NET's built-in image processing features.

5.1.4 Blockchain Integration

The blockchain component, implemented using the Ethereum platform, records transaction logs and ensures data integrity. Smart contracts automate the transaction verification process, providing an immutable and transparent transaction ledger.

5.1.5 Authentication Workflow

Enrolment Phase

- Capture and process the user's face image using .NET properties.
- Store the facial template in the SQL Server database.
- Login Phase
- Capture and process the user's face image using .NET properties.
- Match the captured template with stored templates.
- Verify the username and password.
- Implement cued click points for additional security.
- Transaction Phase
- Send OTP to the registered mobile number.
- Require face recognition for transaction approval.
- Log transaction details in the blockchain.

VI. RESULT ANALYSIS

61 Performance Metrics

- The face recognition system achieves high accuracy in identifying legitimate users using .NET's image processing capabilities.
- The average response time for face recognition and transaction processing is within acceptable limits, ensuring a smooth user experience.
- User surveys indicate high satisfaction with the ease of use and perceived security of the new authentication method.

6.2 Security Metrics

- Penetration testing reveals the system's resilience to face spoofing and OTP interception, with no significant vulnerabilities detected.
- The system demonstrates strong resistance to common cyber-attacks, including phishing and man-in-the-middle attacks.
- Blockchain technology effectively ensures the integrity and immutability of transaction logs, preventing unauthorized alterations.

6.3 Comparative Analysis

- The biometric authentication system shows a marked improvement in security and user satisfaction compared to traditional methods relying solely on usernames, passwords, and OTPs.
- There is a significant reduction in fraud incidents following the implementation of biometric authentication, highlighting its effectiveness.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306226|

VII. CONCLUSION

Biometric technology represents a robust and convenient approach to enhancing security in online banking applications. By integrating face recognition systems, banks can significantly improve authentication processes, ensuring that only authorized individuals access sensitive information. Unlike traditional methods, such as passwords or IDs, biometrics offer a higher level of security as physical characteristics are unique to each individual and cannot be easily stolen or replicated. The addition of click point identification further enhances security by introducing a dynamic element to the authentication process. Moreover, implementing multi-person access control strengthens security measures, allowing tailored access privileges while maintaining robust protection against unauthorized access attempts. Real-time alert systems provide immediate notifications of any suspicious activities, enabling prompt responses to potential security breaches. As biometric technology continues to evolve and gain mainstream adoption, its integration into banking systems promises to safeguard sensitive transactions and uphold stringent security standards effectively.

VIII. FUTURE ENHANCEMENT

In the future, the framework can be expanded to include ATM security systems using fingerprint recognition and GSM modems. Fingerprint recognition leverages the stable and reliable characteristics of fingerprints, enhancing security significantly. The system also integrates traditional verification methods, such as inputting a password sent by the controller, to further ensure owner identification. Built on embedded system technology, the entire system prioritizes safety, reliability, and user-friendliness. This technological foundation not only strengthens security measures but also enhances the system's overall robustness. By combining fingerprint recognition with existing security protocols, the system provides a comprehensive approach to ATM security. Future advancements may focus on refining these features to meet evolving security standards and user expectations in banking environments.

REFERENCES

1. ASP.NET Core in Action, Second Edition Annotated Edition by Andrew Lock, 2021.
2. An Atypical ASP.NET Core 6 Design Patterns Guide: A SOLID adventure into architectural principles and design patterns using .NET 6 and C# 10, 2nd Edition 2nd ed. Edition, 2022, by Carl-Hugo Marcotte (Author), Abdelhamid Zebdi (Foreword)
3. ASP.NET Core 5 and React: Full-stack web development using .NET 5, React 17, and TypeScript 4, 2nd Edition 2nd ed. Edition, 2021, by Carl Rippon
4. C# 9 and .NET 5 – Modern Cross-Platform Development: Build intelligent apps, websites, and services with Blazor, ASP.NET Core, and Entity Framework Core using Visual Studio Code, 5th Edition 5th ed. Edition, 2020, by Mark J. Price
5. Essential ASP.NET Web Forms Development: Full Stack Programming with C#, SQL, Ajax, and JavaScript 1st ed. Edition, 2020, by Robert E. Beasley

WEBSITE REFERENCE

6. www.csharpcornar.com
7. www. Microsoft.com/sql
8. www.databasejournal.com
9. www.microsoft.com/vcsharp

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details