IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205018 |

A Novel Pin Generation and Face Recognition Methods in Online Banking

S. Kiran[1], G. Shriram[2], R. Athiruban[3], R. Vasanthakumar[4], Mrs. V. Dhavamani[5]

UG Student, Dept. of CSE., Sir Issac Newton College of Engg. & Technology, Nagapattinam, Tamil Nadu, India[1-4]

Assistant Professor, Dept. of CSE., Sir Issac Newton College of Engg. & Technology, Nagapattinam, Tamil Nadu, India[5]

ABSTRACT: Online banking has become an essential part of modern banking. Many attacks are successful in accessing social network accounts since the current password-based authentication paradigms are not efficient and robust enough as well as vulnerable to automated attacks. The simplest alternative is complementing the single factor (password-based) authentication process with additional identification elements, such as one-time PIN codes, generated by the user's own device (e.g., the smartphone) or received via SMS. To improve the security of online banking transactions, real-time face recognition technology can be used as a biometric authentication technique. This technology provides a reliable and convenient way of verifying the identity of customers in real-time. The aim of this project is to develop an online banking system that uses real-time face recognition technology for customer authentication. The system will be designed to provide a secure and user-friendly interface that allows customers to carry out banking transactions such as funds transfer, bill payments, and balance inquiries.

KEYWORDS: Online Banking, Face recognition, Security, Biometric authentication, Smartphone.

I. INTRODUCTION

Face recognition uses AI algorithms and ML to detect human faces from the background. The algorithm typically starts by searching for human eyes, followed by eyebrows, nose, mouth, nostrils, and iris. Once all the facial features are captured, additional validations using large datasets containing both positive and negative images confirm that it is a human face. Some of the common techniques used for facial recognition are feature-based, appearance-based, knowledge-based, and template matching. Each of these methods has its advantages and disadvantages. Feature-based methods rely on features such as eyes or nose to detect a face. The outcomes of this method could vary based on noise and light. Further, appearance-based methods use statistical analysis and machine learning to match the characteristics of face images. In a knowledge-based approach, a face is recognized based on predefined rules. This could be challenging considering the efforts needed to define well-defined rules. Whereas template-matching methods compare images with previously stored face patterns or features and correlate the results to detect a face. However, this method fails to address variations in scale, pose, and shape.

II. LITERATURE SURVEY

1) Title: A Blockchain based key revocation access control for open banking
Author: Riad, Khaled and Mohamad elhoseny
Year: 2022
Objective: Implement the smart contract's functions on the Ethereum platform and test the contract's code on the KovanTestnet before deploying it to the Mainnet. Although the customer is authenticated to open banking, his keys can be revoked according to the status response of the bank branch.

2) Title: Classification and analysis of security techniques for the user terminal area in the internet banking service.
Author: Lee, Kyungroul Lee and Kangbinyim.
Year: 2020
Objective: Classify the security technologies in the user terminal domain into secure keyboard program, PKI applications, E2E encryption, anti-hacking program, personal firewall, removable media security, and anti-reverse engineering technique and describe detailed and key techniques of each security technology.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205018 |

3) Title: Identification of non typical international transaction on bank cardsof individuals using machine learning methods.
Author: Domashova, jenny, and Elend Kripak
Year: 2021
Objective: Develop an algorithm for detecting atypical transfers; implement the developed algorithm and evaluate the quality of its work.

4) Title: Usage of machine learning methods for early detection of money laundering schemes.
Author: :Domashova,jenny,andNatailaMikhailia.
Year: 2021
Objective: Proposes an enhanced Credit Card Risk Identification (CCRI) method based on the features selection algorithm as Random Forest Classifier and Support Vector Machine to detecting fraud risk.

III. EXISTING SYSTEM

A. *Existing System:*

Online security remains a challenge to ensure safe transacting on the internet. User authentication, a human-centric process, is regarded as the basis of computer security and hence secure access to online banking services. The increased use of technology to enforce additional actions has the ability to improve the quality of authentication and hence online security, but often at the expense of usability. Today, there are a number of technologies in use to combat fraud in the banking industry. One of these is the use of One Time Passwords (OTPs), which is a fraud prevention technology specific for e-banking transactions. The problem is that all existing security measures present one challenge or the other. Transaction monitoring is a different type of approach that comes from an adaptation of credit/debit card fraud prevention systems.

B. *Disadvantages:*

- Key exchange scheme provides low community and high computation complexity.
- Running time of the client is about ten times of that at the server end.
- Guessing attack and Online dictionary attack can be occurred.
- SMS based OTP only provide for current transactions, difficult to know the specific persons.

IV. PROPOSED SYSTEM

A. *Proposed System:*

Online banking is now very popular among consumers because it provides a convenient way to perform transactions from anywhere using smart devices. Now a day thief is using high tech methods to gain access to user information such as passwords, PINs and security questions. This project aims at enhancing the security of Internet banking system with additional face biometric Authentication combination. Internet banking now uses Static User ids and passwords along with OTP-One-time Passwords to mobile number. Although this is the best security feature available to date, this security method is still vulnerable and it is very important to enhance the existing security. The term biometrics refers to the emerging field of technology devoted to the identification of individuals using biological behaviors. Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information. Biometrics is not into Internet banking applications yet. It is because of the practical difficulties and it is very expensive to implement and execute this technology. But, now with technology advancement and cost of Biometric devices coming down, we have probabilities to integrate Biometric Technology to Online Banking. Face biometric can be used to provide cost effective rather than other biometric features such as fingerprint, iris and other features.

B. *Advantages:*

- Solve transaction attacks in banking interface.
- Without primary user knowledge, no one perform fraud activities.
- High level authentication steps for access financial transactions.
- Immediately send notification about transactions.
- No need to implement additional sensors.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205018 |

C. System Architecture:

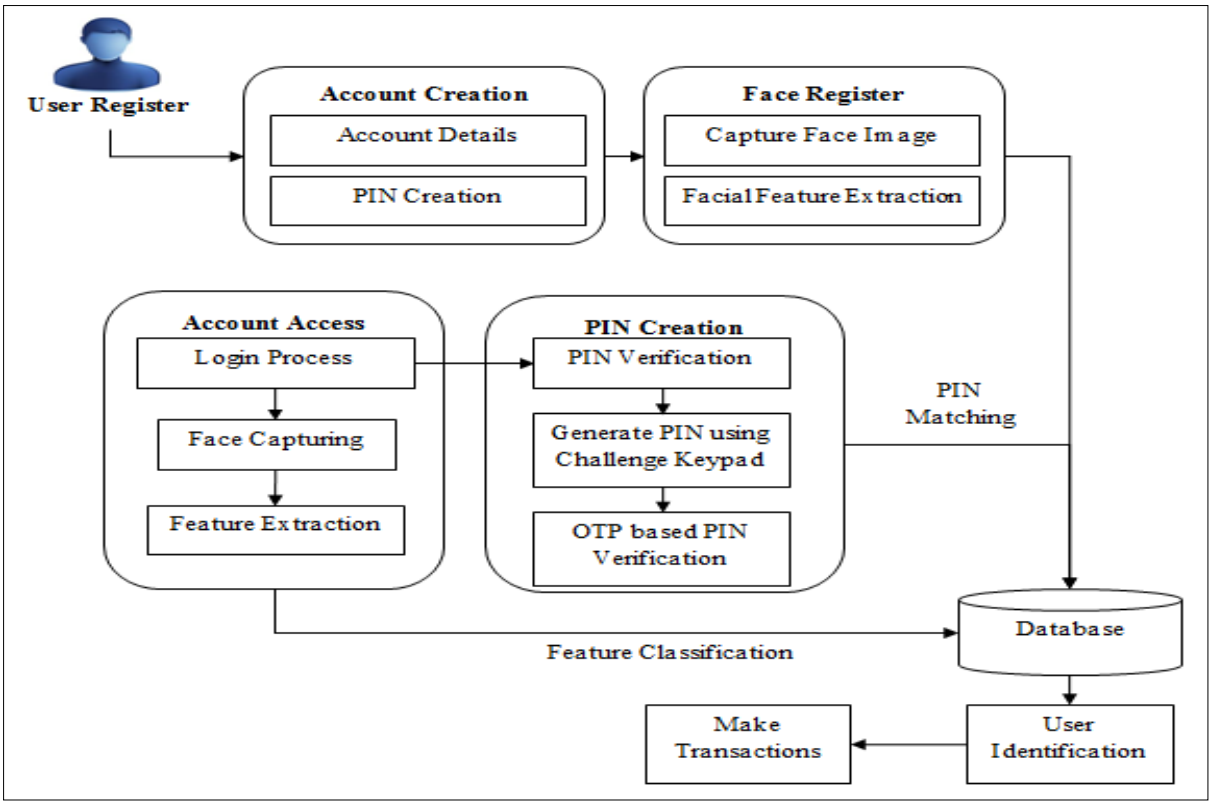

Fig 1: System Architecture

V. CONCLUSION AND FUTURE WORK

Real-time face recognition with OTP verification methods implemented for enhancing the security of online banking systems. By using facial recognition technology, the system can verify the identity of the user in real-time and provide an additional layer of security to prevent unauthorized access. This technology can help prevent fraud, protect sensitive information, and give users peace of mind when banking online. The new OTP based PIN verification process is another layer of security that can prevent fraudulent activities. An indirect input PIN-entry method using OTP has been proposed to defeat shoulder-surfing, video-recording, and spyware attacks. This process prevents hackers from gaining access to the account even if they somehow manage to bypass the facial recognition system. This technology can help protect user data and prevent fraudulent activities, giving users greater confidence in banking online.

In future, can extend the framework to implement an ATM security by using face recognition and Multi Party Access system took advantages of the stability and reliability of secure ATM access. Additionally, the system also contains the original verifying methods which were inputting owner's password which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded system which makes the system more safe, reliable, and easy to use.

REFERENCES

1. Riad, Khaled, and Mohamed Elhoseny. "A Blockchain-based key-revocation access control for open banking." Wireless Communications and Mobile Computing 2022 (2022).
2. Lee, Kyungroul, Sun-Young Lee, and Kangbin Yim. "Classification and Analysis of Security Techniques for the User Terminal Area in the Internet Banking Service." Security and Communication Networks 2020 (2020): 1-16.
3. Domashova, Jenny, and Elena Kripak. "Identification of non-typical international transactions on bank cards of individuals using machine learning methods." Procedia Computer Science 190 (2021): 178-183.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205018 |

4. Domashova, Jenny, and Natalia Mikhailina. "Usage of machine learning methods for early detection of money laundering schemes." Procedia Computer Science 190 (2021): 184-192.
5. Rtayli, Naoufal, and Nourddine Enneya. "Selection features and support vector machine for credit card risk identification." Procedia Manufacturing 46 (2020): 941-948.
6. Veena, K., K. Meena, Yuvaraja Teekaraman, Ramya Kuppusamy, and Arun Radhakrishnan. "C SVM classification and KNN techniques for cyber-crime detection." Wireless Communications and Mobile Computing 2022 (2022): 1-9.
7. Kabir, M. Monjirul, Nasimul Hasan, Md Khalid Hassan Tahmid, Tanjil Ahmed Ovi, and Victor Stany Rozario. "Enhancing smartphone lock security using vibration enabled randomly positioned numbers." In Proceedings of the International Conference on Computing Advancements, pp. 1-7. 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details