Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 12, Issue. 5, May 2023, pg.7 – 11

ONLINE BANKING SECURITY WITH REAL TIME FACE RECOGNITION APPROACH

Arunadevi R[1]; Haresh R[2]; Shyam Jerold G[3]

[1]Department of Computer Science and Engineering & Parisutham Institute of Technology & Science, Thanjavur, India
[2]Department of Computer Science and Engineering & Parisutham Institute of Technology & Science, Thanjavur, India
[3]Department of Computer Science and Engineering & Parisutham Institute of Technology & Science, Thanjavur, India
[1] aruna.ap.cse.pits@gmail.com; [2] hareshraina152@gmail.com; [3] shyamjerold74@gmail.com

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i05.002

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. The system will incorporate a Grassmann Learning algorithm that is capable of capturing and analyzing a customer's facial features in real-time. The algorithm will compare the facial features of the customer with those in the bank's database to verify the customer's identity. Second level verification based on OTP verification in reverse order. The system will provide a secure and user-friendly interface for customers to carry out banking transactions in real-time. In this proposed net banking application notifications are sending to the user regarding banking interface access and amount transaction.

I. INTRODUCTION

Face recognition-based online banking with One Time Password verification is a system that uses biometric technology to verify the identity of customers accessing their bank accounts online. This system utilizes a combination of facial recognition technology and One Time Password verification to enhance security and protect against fraudulent activities. The system works by first capturing an image of the customer's face using a

camera or webcam connected to their device. The Grassmann Learning technology then compares this image to a database of previously stored images to determine if there is a match. During transaction, the customer is prompted to enter a unique OTP sent to their registered mobile number or email address. The OTP verification provides an additional layer of security and ensures that only the legitimate customer with access to their registered mobile number or email can log in to their account. Here customers have to enter their OTP in reverse order. Once the OTP is verified, the customer can access their account and perform transactions such as checking their account balance, transferring funds, paying bills, and more.

II. LITERATURE SURVEY

Face recognition-based online banking with One Time Password verification is a system that uses biometric technology; this paper aims to verify the identity of customers accessing their bank accounts through online. The main appearance aims at the Online banking to provide addition security to the users and helps to reduce the third party access activity. This system utilizes a combination of facial recognition technology and OTP verification to enhance security and protect against fraudulent activities. The system works by first capturing an image of the customer's face using a camera or webcam connected to their device. The paper presents the implementation of new algorithm of Grassmann Learning technology then compares this image to a database of previously stored images to determine if there is a match. During transaction, the customer is prompted to enter a unique OTP sent to their registered mobile number or email address. Here, we additionally propsed the Reverse OTP instead of normal OTP. The structure of proposed Reverse OTP verification method provides an additional layer of security and ensures that only the legitimate customer with access to their registered mobile number or email can log in to their account. Once the OTP is verified, the customer can access their account and can perform their activities they want to perform here.

III. 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 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. Face biometric can be used to provide cost effective rather than other biometric features such as fingerprint, iris and other features using Grassmann learning algorithm. The OTP based password can be send at the time transactions. Finally SMS alert send to primary user with detail description of user name, time of access, amount details.

IV. SYSTEM ARCHITECTURE

System Architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability.

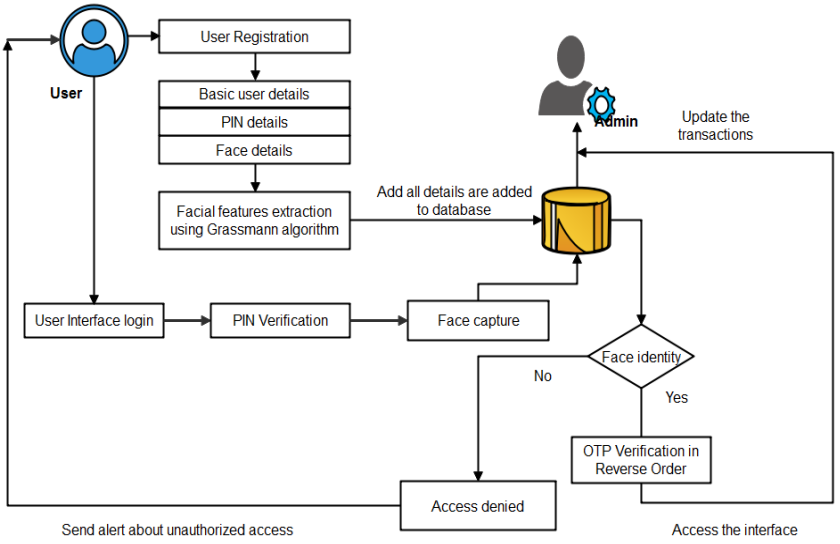

Fig.1 Architecture Diagram

V. MODULE DESCRIPTION

A. Banking Interface Creation

Online banking is thus changing the way people shop and how retailers operate. There is a step decline in traditional payment methods such as cash and cheque and people are choosing the emerging digital payment technologies as they render convenient and flexible methods for conducting cashless financial transactions. It has led to a new breed of fraud perpetrators that use sophisticated technologies to hack into personal devices and corporate networks. Traditional techniques such as password or tokens are no match to their attacks. To overcome, these attacks, we can design the interface for online transactions in banking system. In this module, admin and user interface created. Admin can be view the details of users, accounts details and so on. The user can be performing various operations such as net banking, credit card transactions, and debit card transactions and on. After that user can give their basic details in the user registration and set a verification password in it.

B. Face Verification using Grassmann Learning algorithm

After registration, user can set password using face capture process. At first, camera is enabling in system for capture the face. Face identification is a one-to-many matching process that compares a query face image against all the template images in a face database to determine the identity of the query face. The identification of the test image is done by locating the image in the database that has the highest similarity with the test image. Here feature vector is made from important values. of the image from each filter Energy, mean and standard deviation forming a 40 value feature vector for every image. The input facial features are matching with

database using grassmann learning algorithm. Then the captured image will have the following process like Image pre-processing, Future extraction.

C. Reverse OTP Verification

A One Time Password is a string of characters or numbers automatically generated to be used for one single login attempt. One Time Passwords can be sent to the user's phone via SMS is used to protect web-based services, private credentials and data. OTP's will minimize the risk of fraudulent login attempts and come in all shapes and sizes, but always add an extra layer of authentication. The risk of fraud is drastically reduced if the user doesn't only have to fill in his user name and password but also needs OTP have to complete the login. Here user should enter their OTP in reverse order. This will enhance the efficiency compared with existing OTP based authentication system.

D. Account Access

Users are allowed to access banking application, when they are completing password and face verification. Admin has permission to view user details and user transaction details. The user should select the receiver name and the account number. Then, the amount to be transferred should be entered. The transaction details will be reflected in the corresponding accounts. So, by have all this process our account will have a improved security and the user will have a enough protection for their account.

VI. CONCLUSION AND FUTURE WORK

Real-time face recognition with reverse 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 reverse OTP verification process is another layer of security that can prevent fraudulent activities. By sending a one-time password (OTP) to the user's mobile device, the system ensures that only the authorized user can access the account. 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. Additional, 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]. Ajish, S., and K. S. Anil Kumar. "Secure Mobile Internet Banking System Using QR Code and Biometric Authentication." In Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021, pp. 791-807. Singapore: Springer Nature Singapore, 2022.

[2]. Estrela, Priscila Morais Argôlo Bonfim, Robson de Oliveira Albuquerque, Dino Macedo Amaral, William Ferreira Giozza, and Rafael Timóteo de Sousa Júnior. "A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications." Sensors 21, no. 12 (2021): 4212.

[3]. Faruk, Md Jobair Hossain, Hossain Shahriar, Maria Valero, Farhat Lamia Barsha, Shahriar Sobhan, Md Abdullah Khan, Michael Whitman et al. "Malware detection and prevention using artificial intelligence techniques." In 2021 IEEE International Conference on Big Data (Big Data), pp. 5369-5377. IEEE, 2021.

[4]. Kang, Dongwoo, Jaewook Jung, Hyoungshick Kim, Youngsook Lee, and Dongho Won. "Efficient and secure biometric-based user authenticated key agreement scheme with anonymity." Security and Communication Networks 2018 (2018).

[5]. Sinha, Mudita, Elizabeth Chacko, and Priya Makhija. "AI Based Technologies for Digital and Banking Fraud During Covid-19." In Integrating Meta-Heuristics and Machine Learning for Real-World Optimization Problems, pp. 443-459. Cham: Springer International Publishing, 2022.

[6]. Shanmugapriyan, J., R. Parthasarathy, S. Sathish, and S. Prasanth. "Secure Electronic Transaction Using AADHAAR Based QR Code and Biometric Authentication." In 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), pp. 1-4. IEEE, 2022.

[7]. Srinivas, Jangirala, Ashok Kumar Das, Neeraj Kumar, and Joel JPC Rodrigues. "Cloud centric authentication for wearable healthcare monitoring system." IEEE Transactions on Dependable and Secure Computing 17, no. 5 (2018): 942-956.

[8]. Surekha, Nayak, Rangasamy Sangeetha, Chellasamy Aarthy, Rajamohan Kavitha, and R. Anuradha. "Leveraging blockchain technology for internet of things powered banking sector." In Blockchain based Internet of Things, pp. 181-207. Singapore: Springer Singapore, 2022.

[9]. Yuan, Chengsheng, Xingming Sun, and QM Jonathan Wu. "Difference co-occurrence matrix using BP neural network for fingerprint liveness detection." Soft Computing 23, no. 13 (2019): 5157-5169.

[10]. Xia, Zhihua, Chengsheng Yuan, Rui Lv, Xingming Sun, Neal N. Xiong, and Yun-Qing Shi. "A novel weber local binary descriptor for fingerprint liveness detection." IEEE Transactions on Systems, Man, and Cybernetics: Systems 50, no. 4 (2018): 1526-1536.

