IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Fortifying Online Banking: Advanced Security Measures Using Mobile Phone

Harshavardhan D[1], Saisree K[2], Ragavarshini S[3]

[1] Department of CSE, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
https://orcid.org/0009-0009-5426-7724. 3010harsha@gmail.com
[2] Department of CSE, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
https://orcid.org/0009-0004-1695-4017. saisreekota7@gmail.com
[3] SRM Institute of Science and Technology, Ramapuram, Department of CSE, Chennai, India. sr6623@srmist.edu.in,
https://orcid.org/0009-0002-6583-0198

ABSTRACT

This study delves into enhancing the security of mobile banking, a prominent platform post-ATM banking. Mobile banking apps like G-pay and Paytm are susceptible to hacking, necessitating robust protection mechanisms. These include fingerprint and facial recognition, as well as distress detection, to safeguard user accounts. When a hacker gains access to an account, they initiate a money transfer, requiring essential information like account number, IFSC number, transfer limits, balance, alternative accounts, and the transaction amount. The server verifies this data against its database for validity. If the amount is within the allowed limit, it demands the account holder's fingerprint for confirmation. If the amount exceeds the limit, the authentication process intensifies with facial recognition, a 360-degree scan, and iris scanning and distress detection. Any signs of distress or discomfort prompt further scrutiny, involving a secondary account holder. Transaction details are shared with the bank manager and the cyber-crime branch. The final transfer depends on the secondary account holder's approval. If fraud is suspected, the cybercrime department is alerted. All these authentication measures are done using the users mobile phone, thus making the transaction handy to the users.

Keywords: Banking Security, Post Entry Authentication in Banks, Fingerprinting, Face Recognition, Iris Scanning, Depression Detection and 360^0 environmental checkup using device camera.

INTRODUCTION

Cyber security is a process of defending or protecting our computers, mobile devises, servers and electronic systems from any sort of malicious attacks by unauthorised user. The cyber-attack can occur in various sectors like online shopping sectors, through call apps, company which handles huge amount of data and in banks. Now a days it plays major role in banking sector at various levels.

Generally, bank follows some basic authentication methods when it comes to online bank transaction. Those authentication methods that bank follows are: passwords, PIN numbers, OTPs, and knowledge-based identification of the actual user. The authentication methods are followed to set a secure bank transaction for the bank account holder. This authentication mechanism is a corner stone in the banking system as it ensures whether the correct user is accessing the requested sensitive information or transaction. The online bank transaction authentication is basically done by acquiring user-name and password, in some cases OTPs are sent to the intended user for confirmation on whose phone number the particular bank account is registered on.

Password based authentication system is the traditional practice of authentication mechanism. It involves the providing the personal key-word as an authentication tool to provide confirmation. It is a preliminary process in any authentication process in banking sector.

PERSONAL IDENTIFICATION NUMBER is a numerical code used in computerized financial transactions. Payment cards are often allocated personal identification numbers, which may be required to complete a purchase. It increases the security of electronic financial transactions.

ONE TIME PASSOWRD is also a higher end authentication mechanism which is used in two-step authentication process. In the first step it follows a basic login credentials and the second step involves generating a dynamic one-time password.

KNOWLEDGE BASED AUTHENTICATION MECHANISM also known by acronym KBA is basically a series of knowledge questions that are used to identify person's identity in order to prevent unauthorised users form accessing the transact.

Electronic banking systems like this pave the way for tracing fraudulent transactions more readily. Hearing about a bank account going bust because of unauthorized withdrawals is becoming a typical occurrence. This may occur if a close friend, family member, or an outsider learned personal information about the user and his account without his knowledge or permission. The issue with mobile phone transactions like G-pay, Paytm, Pay-mini, and others is that if an unauthorized third party obtains knowledge of the account password, they may simply make purchases using the account of the legitimate account user. The account holder's problems are broken down into their component parts, and from there, a solution is produced that can prevent the fraudulent usage of mobile transactions. Authentication systems now a days have also evolved with the developing cyber-attacks to prevent them. Now a days, the improved authentication steps involve finger printing, face recognition, iris scanning etc, in online banking system. Usually, scammers crack the basic authentication mechanisms to access the confidential information of the legitimate user.

In this work, the banking sector is to provide security for the bank account holder, even if their bank and personal details are stolen for retrieving their money from bank in online mode. Now a days, its common that we face cyber-attacks and loss money. Cyber-attacks occur when we click on to any unauthorised link, attend any unauthenticated calls, and even through Bluetooth. So, the main idea of the work is not to prevent this links or calls or Bluetooth problems instead this focus on providing a very strong authentication process to prevent the scammer from not able to withdraw money from our account even if he is able to access our confidential information.

The proposed frame work improve the reliability, accuracy and integrity of diagnosis by using various Artificial Intelligence algorithms. This algorithm supports secure banking transaction while maintaining the accessibility.

The section-2 in this paper covers the related work that serves as a remainder. Section 3 defines the framework for the proposed work technology and algorithm. Section 4, describe the step wise procedure for the proposed work. Section 5, discuss comparison with the existing models. Section 6, present the conclusion.

METHODS

The following section describe the working principles of the proposed algorithm with an illustration in order to find and prevent the unauthorized bank transaction. This work is applicable for banking sector.

2.1. Issues

Today, many banks provide excellent banking app options for mobile users. As more technology options become accessible in the banking industry, customers' expectations and wants are shifting rapidly. Customers in the banking industry have grown to expect seamless, multi-channel customer care interactions. Today's youth, however, make excellent use of mobile banking. The advent of mobile banking has been made possible by the rapid development of technology in recent years. The government and financial institutions are encouraging customers to switch to mobile banking rather than physically visiting a bank or a store. Customers have faith that their financial information is secure while using online/mobile banking. Users have reported that they find it simple to operate. According to the research, the most often utilized mobile banking function is checking balances and account details. Most mobile banking customers believe that the fees they incur for using the service are fair. According to the findings, most financial institutions have room for advancement in the realm of mobile banking. The business community is the biggest user of mobile banking. The vast majority of customers are pleased with the mobile banking service. There are a number of banking services available, but automated teller machines, online banking, and mobile banking are the most popular. Security concerns and a general lack of technical knowledge prevent many people from using mobile banking. But thanks to the development of mobile banking, the consumer may now save time on financial affairs while still enjoying the convenience of this service.

Nowadays, it's typical to hear of bank accounts going bankrupt as a result of financial transactions made without the supposed consent of the account owners.

Another issue with mobile payment systems like G-Pay, Paytm, Pay Mini, and others is that if the account password is known or compromised by an unidentified third party, he or she can easily conduct transactions from the account of the actual account holder. Therefore, today, any kind of bank transaction is susceptible to theft and hacking. Thus, it is becoming hand-in for the unauthorized user to retrieve money from a legitimate user.

2.2. Frame Work

This method is dependent on the account holder data that is kept in the specific bank's database. A basic money transaction is initially verified by the account holder via finger printing, which is regarded as the primary security system in this implementation. The client will be questioned about the Minimum Transaction Limit while opening an account with the specific bank (MTL). The client would need to enter the amount he wishes to withdraw before proceeding with the mobile transaction services. The bank server now compares the amount of money entered by the user with the database's minimum transaction limit. The comparison would reveal the current condition of the transaction, whether simple or complex. The logic moves immediately to the fingerprinting for confirmation in his or her mobile phones if the amount submitted is less than the minimum transaction limit. The transaction starts when the appropriate fingerprint is given.

However, if the amount submitted exceeds the minimum transaction limit, a complicated process is initiated to determine the transaction's course and to uphold the process if it turns out to be an unlawful one. Here, the primary and secondary security systems collaborate. The fingerprint will be the first method of verification. It is regarded as the fundamental and first phase. When the fingerprint is provided, it looks to see if it matches the fingerprint of the client that is stored in the database. The process continues by asking for facial recognition if the fingerprint matches the client's fingerprint.

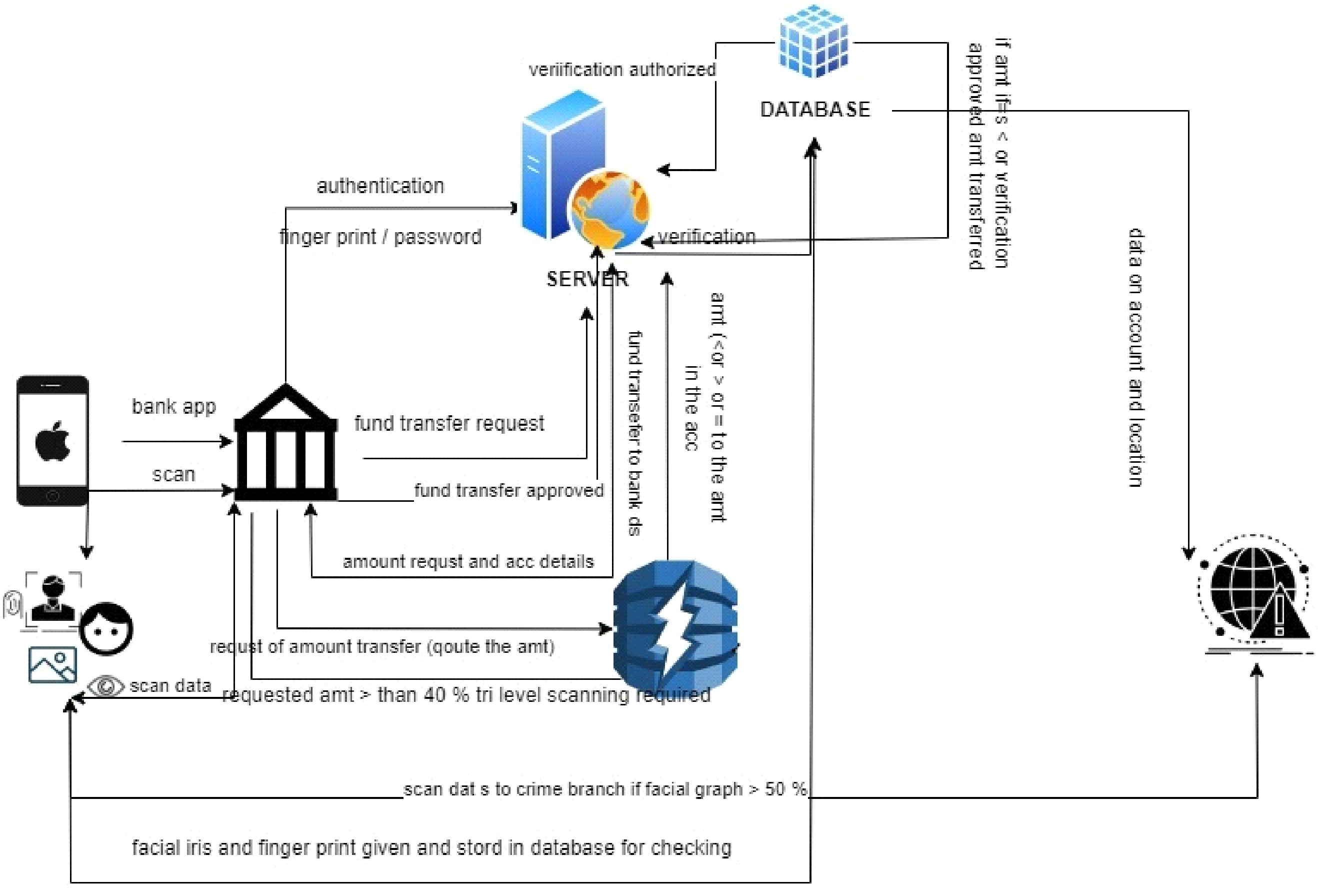
veriification authorized
DATABASE
if amt if=s < or verification approved amt transferred
authentication
finger print / password
verification
SERVER
data on account and location
amt (<or > or = to the amt in the acc
fund transefer to bank ds
bank app
scan
fund transfer request
fund transfer approved
amount requst and acc details
request of amount transfer (qoute the amt)
scan data
requested amt > than 40 % tri level scanning required
scan dat s to crime branch if facial graph > 50 %
facial iris and finger print given and stord in database for checking

Figure 3.2 Frame work of EAGLE GLOURY ALGORITHM

Face recognition is regarded as the secondary security measure that forms the basis of bank safety. Following accurate fingerprinting, the client must provide a facial scan. There are two main mechanisms involved in facial recognition:360^0 scanning, Iris scanning.

Facial recognition is used in the 360^0 scanning to scan the area for safety. It comes to a conclusion about the transaction's complexity based on how safe the client's immediate surroundings are. Iris scanning is used to precisely locate risks or discomfort that have occurred to the client but are difficult to find through any other method. Iris scanning examines the person's iris to determine the scenario as it actually is. The authentication is sent to the client's alternate account (which may be to any account holder more nearby to this particular account holder) and access is delayed if the scenario is determined to be stressful or the client is determined to be in distress. The fund transfer is cancelled if the alternate account holder does not authenticate the transfer of funds within a certain amount of time. The fund transfer will be successful if the alternate account holder gives the authentication. Information regarding the transaction pathway would be sent to the CYBER SECURITY AND BANK-MANAGER because this process has gone through the distress process.

The cyber security division and the bank manager will both receive information on the substitute account holder. In the event of any fraud, the bank manager can alert the cybercrime branch right away and halt any transactions or freeze the account to prevent money loss. In order to help with future searches, information about the transaction pathway will also be saved in the databases of both the bank manager and the cyber security agency if the alternate account holder refuses to grant access to money transfers. The fund transfer occurs successfully and without any problems if the face recognition technology does not detect any anxiety or stressful situations around.

2.3 Algorithm

Here, this work is an Eagle glory algorithm (modified hybrid approach) which helps to prevent unauthorized bank transaction. The identification of finger-print is used by AFIS algorithm, the identification of face recognition patterns is used by SVM and DBM algorithms which helps to recognise the stress level of human and iris detection is used for deriving optimal solution.

2.3.1 Eagle Glory Algorithm:

Step 1: General authentication steps before entering into the banking platform.

Step 2: Enter the amount to be withdrawn.

Step 3: Verification process in the server

Step 3.1: Compares the money entered by the user with the Minimum Transaction limit (MTL) and Minimum Number of Transactions (MNT).

Step 3.2: if amount entered is less than MTL. Go to 3.3 other-wise go to 3.4.

Step 3.3: Proceed with the Press-Pattern algorithm.

Step 3.4: If the entered amount is greater than MLT.

Step 3.5: Start with Press-Pattern algorithm. If successful go to 3.6

Step 3.6: Then proceed with Face-press algorithm.

Step 3.7: If in the future any report of fraudulence then the accounts to which the money is transferred, is blocked and money is retrieved.

Step 4: Stop.

2.3.2 Press-Pattern Algorithm (Finger-Print):

Step 1: Request for finger-print for authentication.

Step 2: Acquire the finger-print from the user.

Step 3: Check for the unique patterns from the finger-prints.

Step 4: Perform singularity detection, Segmentation, Enhancement and minute extraction for the finger-print patterns.

Step 5: Compare the procured finger-print while transaction with the analysed patterns in data-base.

Step 6: If matched the transaction successful.

Step 7: If the user finger-print not available.

Step 8: We request authentication from alternate account.

Step 9: If authenticated, money transferred to the concerned account and transaction is successful.

Step 10: Else transaction failed.

2.3.3 Face-Press Algorithm (FP-Algorithm):

Step 1: Request for face recognition for authentication.

Step 2: Acquire the facial pose of the user.

Step 3: Check the unique pattens from the acquired face pose.

Step 4: Perform extraction task.

Step 5: Along with the face-muscle enhancement, perform iris-scanning, distress detection and 360^0 environmental scanning.

Step 6: If face recognition process is successful.

Step 7: We go for iris scanning. If this fails then transaction fails.

Step 8: If iris scanning successful. Transaction proceeds with 360^0 scanning for environmental check-up.

Step 9: Then distress detection is performed.

Step 10: If any distress detected or any problem detected during 360^0 scanning, then go to 4.2.11

Step 11: The transaction is performed successfully and the transaction pathway is sent to the database of cyber-crime department and bank manager.

The algorithm states the general authentication steps after we enter into the banking platform and before any amount transaction.

Here, the bank generally asks for the amount to be entered. When we enter the amount, now the verification step starts. Here, the algorithm compares the entered amount with the MTL. If the entered amount is less than MTL and MNT then fingerprint authentication is procured from the legitimate user. If the finger print provided by the user does not match with the saved fingerprint patterns in the users database, then the transaction fails. If the user is not able to provide the fingerprint, then authentication from the alternate trusted account holder is acquired if even this alternate account holder fails to authenticate then transaction fails.

Similarly, if the amount entered is greater than MTL or number of transactions is greater than MNT or both, then first the fingerprint authentication proceeds as a primary step in the authentication. Then if the fingerprint authentication is successful then it proceeds to face recognition. In this face recognition process where a set of 3 authentication takes place simultaneously, which are iris scanning, 360^0 environmental checkup and distress detection along with the face scanning. In case if the user is unable to provide his face recognition authentication, then an alternate account holder can authenticate for the transaction to occur by providing his/her face recognition process. If iris scanning is successful than 360^0 degree environmental scanning and distress detection takes place. If any distress is detected then the transaction path is reported to the database of the cybercrime department and the bank manager. In case of future report about any fraudulence then the path of transaction will be traced and will be halted for retrieving the money back.

RESULT AND DISCUSSION

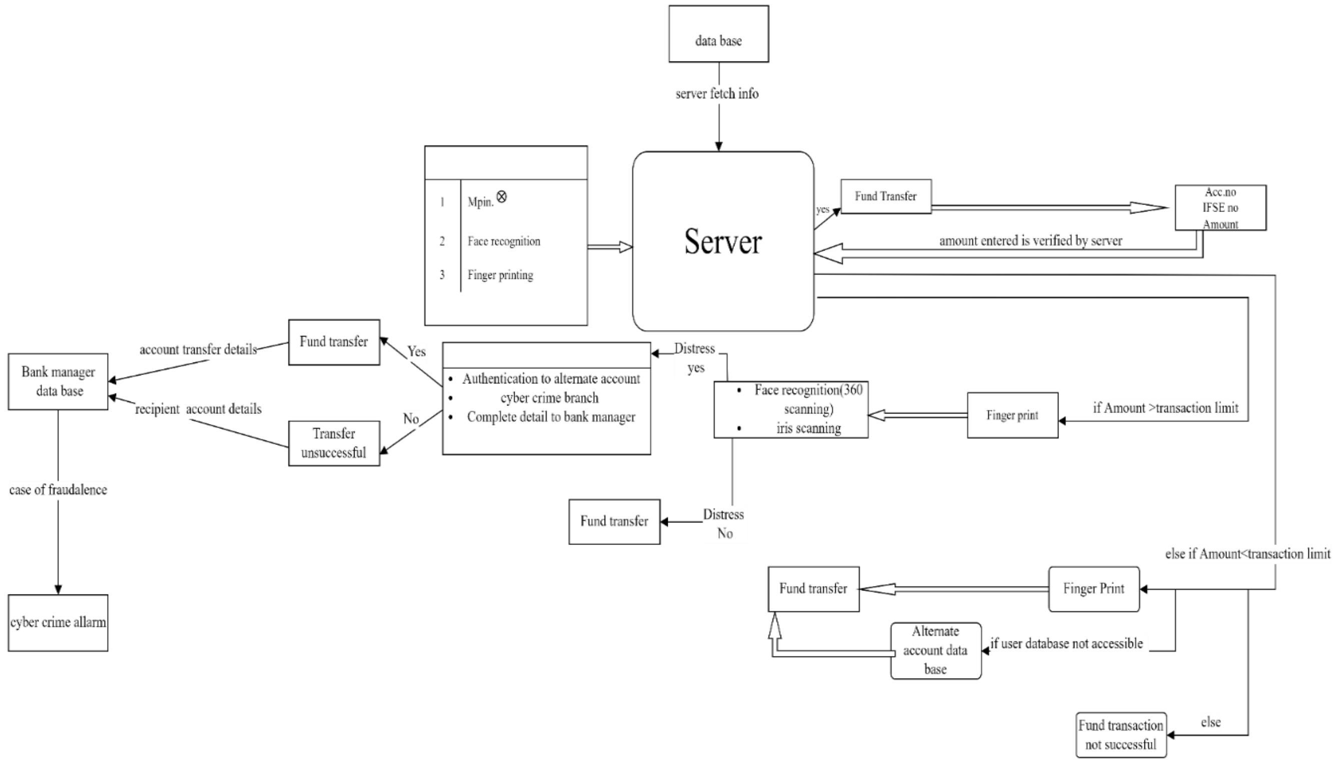

Figure 5. Representing the Flow diagram of the Eagle Glory Algorithm.

This method is dependent on the account holder data that is kept in the specific bank's database. A basic money transaction is initially verified by the account holder via finger printing, which is regarded as the primary security system in this implementation. The client will be questioned about the Minimum Transaction Limit while opening an account with the specific bank (MTL). The client would need to enter the amount he wishes to withdraw before proceeding with the mobile transaction services. The bank server now compares the amount entered by the user with the database's minimum transaction limit. The comparison would reveal the current condition of the transaction, whether simple or complex. The logic moves immediately to the fingerprinting for confirmation in his or her mobile phones if the amount submitted is less than the minimum transaction limit. The transaction starts when the appropriate fingerprint is given.

However, if the amount submitted exceeds the minimum transaction limit, a complicated process is initiated to determine the transaction's course and to uphold the process if it turns out to be an unlawful one. Here, the primary and secondary security systems collaborate. The fingerprint will be the first method of verification. It is regarded as the fundamental and first phase. When the fingerprint is provided, it looks to see if it matches the fingerprint of the client that is stored in the database. The process continues by asking for facial recognition if the fingerprint matches the client's fingerprint.

Face recognition is regarded as the secondary security measure that forms the basis of bank safety. Following accurate fingerprinting, the client must provide a facial scan. There are two main mechanisms involved in facial recognition:360^0 scanning, Iris scanning Facial recognition is used in the 360^0 scanning to scan the area for safety. It comes to a conclusion about the transaction's complexity based on how safe the client's immediate surroundings are. Iris scanning is used to precisely locate risks or discomfort that have occurred to the client but are difficult to find through any other method. Iris scanning examines the person's iris to determine the scenario as it actually is. The authentication is sent to the client's alternate account (which may be to any account holder more nearby to this particular account holder) and access is delayed if the scenario is determined to be stressful or the client is determined to be in distress. The fund transfer is cancelled if the alternate account holder does not authenticate the transfer of funds within a certain amount of time. The fund transfer will be successful if the alternate account holder gives the authentication. Information regarding the transaction pathway would be sent to the CYBER SECURITY AND BANK-MANAGER because this process has gone through the distress process.

The cyber security division and the bank manager will both receive information on the substitute account holder. In the event of any fraud, the bank manager can alert the cybercrime branch right away and halt any transactions or freeze the account to prevent money loss. In order to help with future searches, information about the transaction pathway will also be saved in the databases of both the bank manager and the cyber security agency if the alternate account holder refuses to grant access to money transfers. The fund transfer occurs successfully and without any problems if the face recognition technology does not detect any anxiety or stressful situations around.

There are totally 4 scenarios in the working of the model:

SCENARIO 1 (Fingerprinting): This occurs when the entered amount is lesser than the MTL and MNT. Here the user will be asked for his fingerprint which he has to enter for the transaction to occur. Here, the finger print processing considers various features like short break, spur, dotted ridges, delta, bifurcation, core of ridges, ridge ending, ridge enclosure, crossover, pore, island, scanning. If the finger print matching is not successful then transaction fails.

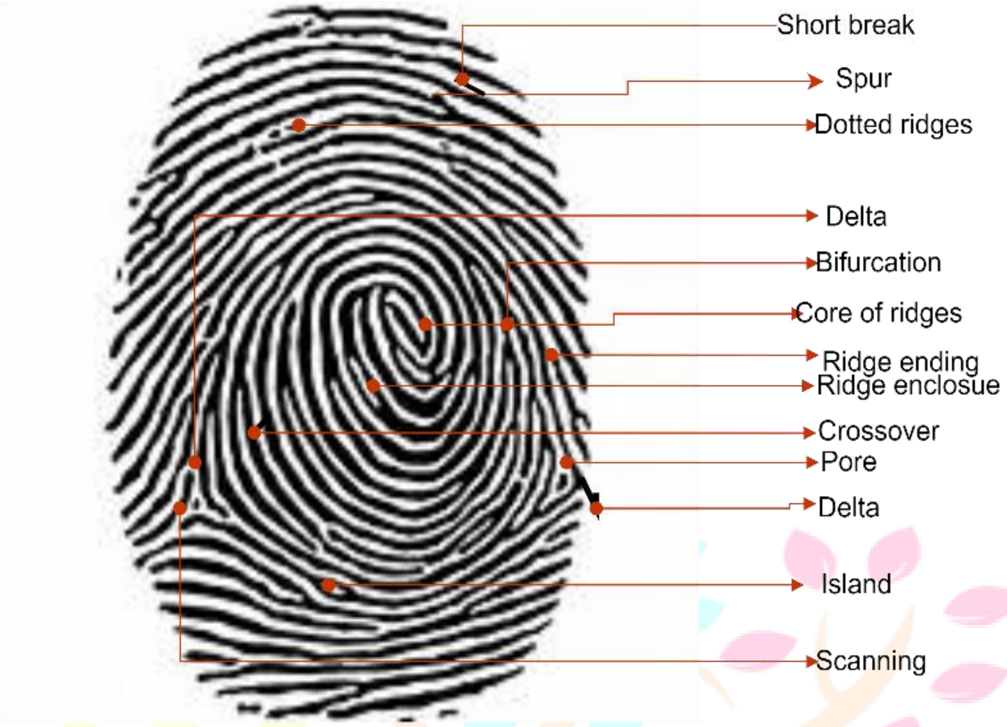

Figure 5.1 stating the various features of finger-print

The finger print also follows certain process to deduce certain patterns to recognise the finger print. They are:

1) Pre- Processing stage: Image Enhancement, Image Binarization, Image Segmentation
2) Minutia Extraction stage: Thinning, Minutiae Marking
3) Post Processing stage: Removal of False Minutiae, Fingerprint Matching

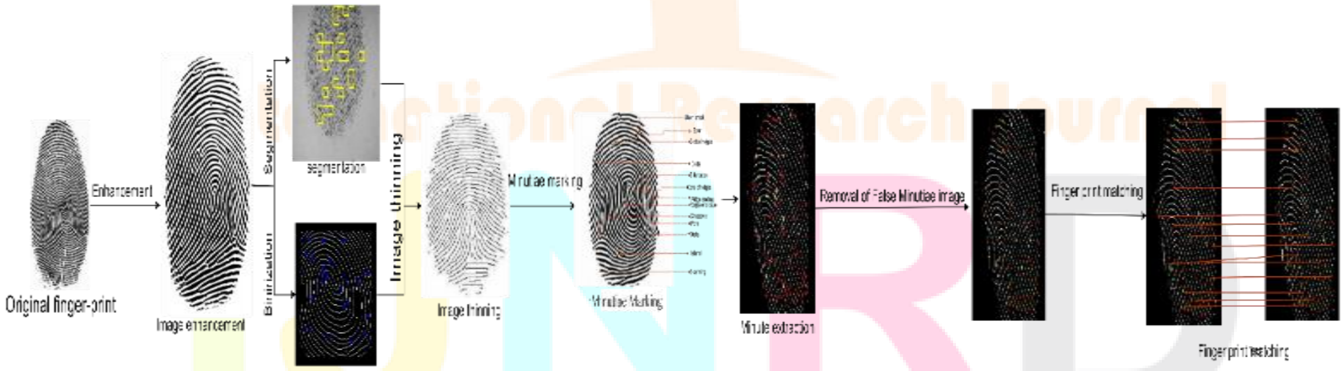

Figure 5.2 Stating the finger print extraction and recognition process

SCENARIO 2 (Face recognition): This occurs when the entered amount is greater than the MTL and MNT. In this situation first fingerprint authentication proceeds as stated above, following this face recognition occurs. Here certain stages are considered those are Enrolment Module, Database, Identification Module. Here, as soon as face is scanned it is checked with the database for confirmation whether face in enrolled and database match or not. As the face is scanned and matches are confirmed the process proceeds to iris scanning. If the iris scanning matches with the iris of the legitimate user in database, then it proceeds through distress detection and 360^0 scanning.

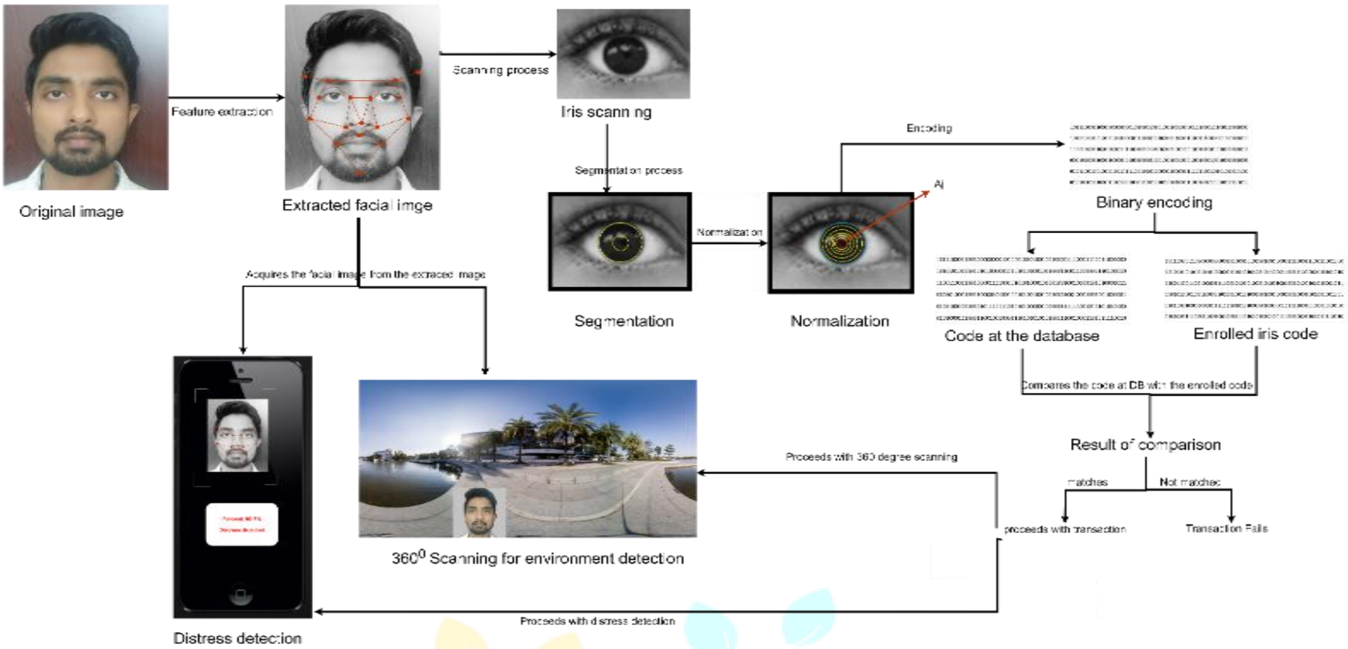

Figure 5.3 representing the second scenario that represent the face, iris, distress-detection and 360^0 scanning process for feature detection and authentication.

SCENARIO 3 (Distress detection): This occurs when the face is recognised with distress or anxiety or dismay. Here, in this situation the information about the amount transaction pathway is sent to data base of cybercrime department and bank manager as an alert message and alternate account holder is asked for authentication. The transaction occurs any way without fail.

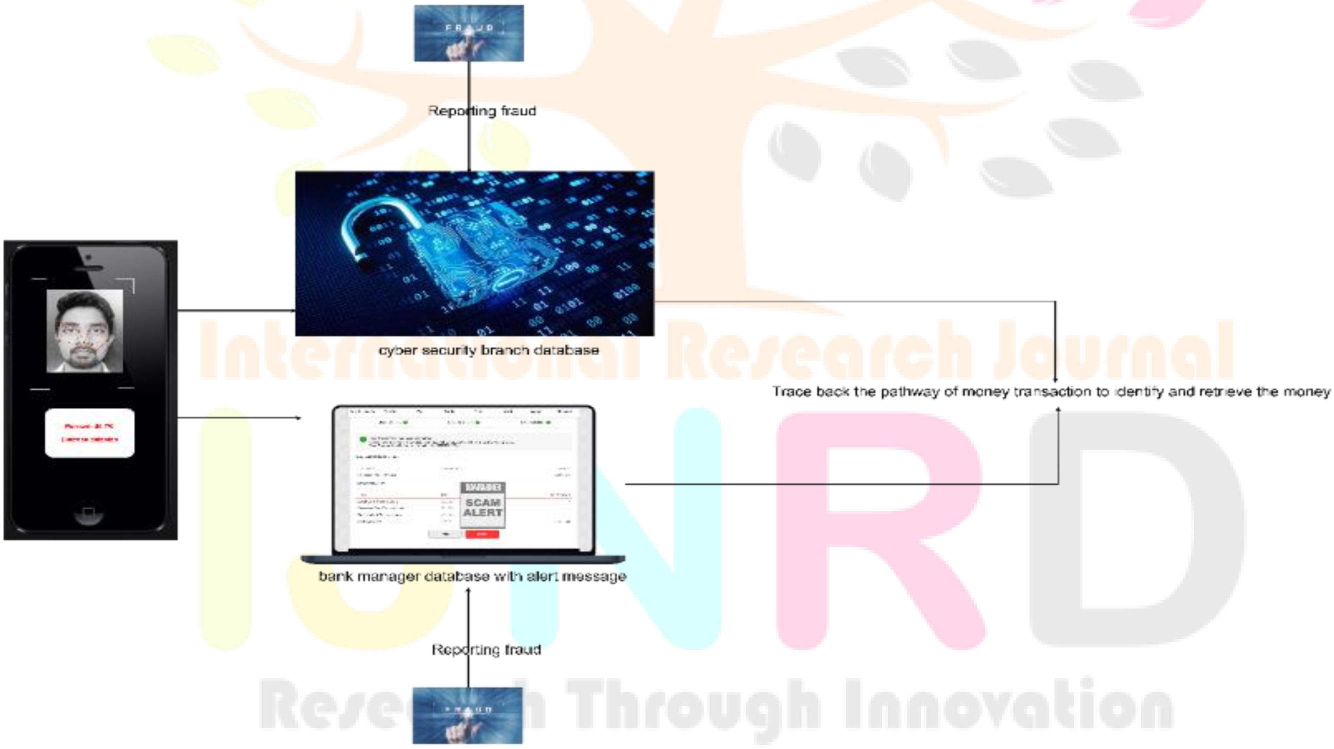
FRAUD
Reporting fraud
cyber security branch database
Trace back the pathway of money transaction to identify and retrieve the money
SCAM ALERT
bank manager database with alert message
Reporting fraud
FRAUD

Figure 5.4 Representing the process after the user is detected with distress, the later part shows the steps after the fraudulence is reported.

CONCLUSION

In conclusion, the project's primary objective is to fortify the security of online banking services through a multi-level authentication system. By prioritizing the protection of users' financial assets and sensitive information, it not only reduces the risk of unauthorized access but also fosters trust in digital banking. The project encompasses the full development and deployment of this robust security solution, positioning it as a key defence against potential breaches and affirming the commitment to safeguarding

REFERENCES:

1. O. P. Chaurasia, "An Approach to Fingerprint Image PreProcessing," Amity School of Engineering and Technology, Amity University, Noida, India, pp. 1-7, 2012.

2. Alaa Ahmed Abbood, Ghazali Sulong, Sabine U. Peters, "A Review of Fingerprint Image Pre-processing," Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia. College of Education, The Florida State University Tallahassee, Florida 32306, pp. 1-7, 2014.

3. A M Mahmud Chowdhury and Masudul Haider Imtiaz, "Contactless Fingerprint Recognition Using Deep Learning—A," Journal of Cybersecurity and Privacy, pp. 1-17, 2022.

4. Vivek Hilal Mahale , Pravin Yannawar , Ashok Gaikwad , Mouad M.H. Ali, "Overview of Fingerprint Recognition System," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)At: DMI College of Engineering, Palanchur, Nazarethpet, Chennai, Tamil Nadu, India, pp. 1-5, 2016.

5. P. Gnanasivam, S. Muttan, "An efficient algorithm for fingerprint preprocessing and feature extraction," ICEBT 2010, pp. 1-10, 2010.

6. Jashanpreet Kaur, Akanksha, Harjeet Singh, "Face detection and Recognition: A review," Conference: 6th International Conference on Advancements in Engineering & Technology (ICAET-2018),ISBN No. 978-81-924893-3-9At: Sangrur (Punjab)-India, pp. 1-3, 2018.

7. Ben Wycliff Mugalu, Rodrick Wamala , Jonathan Serugunda, Andrew Katumba, "Face Recognition as a Method of Authentication in a Web-Based System," arXiv:2103.15144v1 [cs.CV] 28 Mar 2021, pp. 1-7, 2021.

8. Natalya Minakova & Alexander Mansurov , "Implementing Open Source Biometric Face Authentication for Multi-factor Authentication Procedures," Conference paper:Part of the Communications in Computer and Information Science book series (CCIS,volume 1526), First Online: 17 January 2022, pp. 1-9, 2022.

9. Hassan Soliman, Ahmed Saleh, Eman Fathi, "Face Recognition in Mobile Devices," International Journal of Computer Applications (0975 – 8887) , Vols. Volume 73– No.2, July 2013, pp. 1-8, 2013.

10. Rehmat Ulla , Hassan Hayat, Afsah Abid Siddiqui, Uzma Abid Siddiqui, Jebran Khan , Farman Ullah, Shoaib Hassan, Laiq Hasan, Waleed Albattah , Muhammad Islam, and Ghulam Mohammad Karam, "A Real-Time Framework for Human Face Detection andRecognition in CCTV Images," Article ID 3276704, "https://doi.org/10.1155/2022/3276704", vol. Volume 2, pp. 1-12, 2022.

11. Laxmisha Rai, Zhiyuan Wang, Amila Rodrigo, Zhaopeng Deng, Haiqing Liu, "Software Development Framework for Real-Time Face Detection and Recognition in Mobile Devices," International Journal of Interactive Mobile Technologies (iJIM) 14(04):103, Vols. volume-14, pp. 1-18, 2020.

12. Arun Misra, Rahul Kumar Dev, Mr. M. Rajasekaran, "Secured payment system using face recognition technique," 4TH INTERNATIONAL CONFERENCE ON THE SCIENCE AND ENGINEERING OF MATERIALS: ICoSEM2019, pp. 1-9, 2020.

13. Timesler, "Face Recognition Using Pytorch," https://github.com/timesler/facenet-pytorch#quick-start, 2023.

14. Prabu Sevugan, Swarnalatha, Magesh Gopu, Ravee Sundararajan, "IRIS RECOGNITION SYSTEM," International Research Journal of Engineering and Technology (IRJET), vol. Volume: 04, no. Issue: 12, pp. 1-5, 2017.

15. Nadia Othman, Bernadette Dorizzi, Sonia Garcia-Salicetti, "OSIRIS: An open source iris recognition software," https://www.sciencedirect.com/science/article/pii/S0167865515002986, Vols. Volume 82, Part 2, pp. 1-7, 2016.

16. Jie Sun, Shipeng Zhao, Sheng Miao, Xuan Wang, Yanan Yu, "Open-set iris recognition based on deep learning," https://doi.org/10.1049/ipr2.12493, vol. volume 16, no. issue 9, pp. 1-12, 2022.

17. D. Xezonaki, G. Paraskevopoulos, A. Potamianos, S. Narayanan , "Affective Conditioning on Hierarchical Attention Networks applied to," pp. 1-5, 2020.

18. Faming Yin, Jing Du, Xinzhou Xu, ORCID and Li Zhao , "Depression Detection in Speech Using Transformer and Parallel Convolutional Neural Networks," https://doi.org/10.3390/electronics12020328, pp. 1-12, 2023.

FINANCING:

The authors did not receive financing for the development of this research

CONFLICT OF INTEREST:

The author declare that there is no conflict of interest

AUTHORSHIP CONTRIBUTION:

1. Conceptualization: Harshavardhan D, Saisree K, Ragavarshini S
2. Data curation: Harshavardhan D
3. Formal analysis: Harshavardhan D
4. Acquisition of funds: None
5. Research: Harshavardhan D, Saisree K, Ragavarshini S
6. Methodology: Harshavardhan D, Saisree K, Ragavarshini S
7. Project management: Harshavardhan D, Saisree K, Ragavarshini S
8. Resources: Harshavardhan D, Saisree K, Ragavarshini S
9. Software: Harshavardhan D, Saisree K, Ragavarshini S
10. Supervision: Saisree K
11. Validation: Ragavarshini S
12. Display: Harshavardhan D, Saisree K, Ragavarshini S
13. Drafting- original draft: Harshavardhan D
14. Writing-proofreading and editing: Harshavardhan D