

## FACE RECOGNITION WITH HYBRID PIN BASED AUTHENTICATION METHOD FOR ONLINE BANKING USING IOT

Vijayalakshmi Murugan\*<sup>1</sup>

\*<sup>1</sup>Dept. Of CSE, Sir Isaac Newton College Of Engineering And Technology, India.

DOI : <https://www.doi.org/10.56726/IRJMETS45040>

### ABSTRACT

Many researchers have entered the field due to the significance of security in the authentication process and the rise in threat level provided by such viruses. Since the current password-based authentication paradigms are not effective and robust enough and are also susceptible to automated attacks, many attacks are successful in gaining access to social network accounts. The simplest option is to add other identity components, like one-time PIN numbers, created by the user's own device (like a smartphone) or received via SMS, to the single factor (password-based) authentication procedure. In this project, a novel method using multi-layer-based authentication is proposed to address the problem of shoulder-surfing attacks on authentication schemes. So, implement multiple level different authentication methods in Net banking application to satisfy the privacy requirements. First layer based on Illusion PIN-based authentication method that operates on Net banking Application. Illusion keypad uses the technique to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to input the PIN whereas the attacker, who is viewing the device from a greater distance, can only see one keypad. OTP verification in reverse order is used as the second layer. Using facial biometrics as a third layer of real-time authentication, which offers fresh approaches to the privacy and security problems, the person is authorized to use the Net banking system. Also provides multi authority based access system. Primary account holder can add secondary user to access banking application. The multi-layer authentication process enabled when user login into the application and also when a transaction is done with multiparty access system.

**Keywords:** Bank Interface Creation, User Registration, Hybrid PIN And Brightness Password Verification, Face Verification, Multi Party Access System, Alert System.

## I. INTRODUCTION

### 1.1 ARTIFICIAL INTELLIGENT

Artificial intelligence (AI) is a field of technology that uses machines to replicate the cognitive processes of human intellect. AI has opened up a new world of utilizing technology, from self-driving cars to recognizing faces on mobile lock screen. A key component of SAS software and many other applications is artificial intelligence. Image recognition, audio recognition, natural language creation, sentiment analysis, and chatbots are just a few of the often used applications. AI offers a wide range of qualities that seem promise for tomorrow's products. AI can learn from and discover from data to automate repetitive, high-volume processes. Second, it gives products in the fields of automation, conversational platforms, intelligent robots, and bots more intelligence. Thirdly, it has the ability to learn by itself via algorithms by identifying patterns and regularities. In order to make it easier to construct sophisticated solutions like fraud detection systems, AI performs a deep dive on the data sets next. Deep learning is also used by AI to ensure astounding accuracy by gradually analysing the inputs. Last but not least, artificial intelligence supports firms in monetizing data to stay ahead of the curve.

#### 1.1.1 AI with Machine Learning

Machine learning is a branch of artificial intelligence that primarily focuses on using data and algorithms to simulate human learning. It applies statistical techniques to teach classification or forecasting algorithms, and even offers insights into data mining initiatives. In the industry, terms like deep learning, machine learning, and occasionally neural networks are frequently used interchangeably. But these technologies differ in relatively small ways.

Deep learning is the process of training algorithms with little to no human input. Through a procedure called dimensionality reduction, it transforms unstructured data into processable groupings. The input layer, several hidden layers, and an output layer are the node layers that make up neural networks, often known as artificial

neural networks. Each node is connected to the others and has a corresponding weight and threshold. Basically, data is forwarded to the network's next layer if the value of any output layer exceeds its threshold. Deep neural networks and simple neural networks are the two forms of neural networks. A deep neural network has more layers than the basic neural network, which only has two or three levels.

Natural language processing, which converts spoken words into text, is frequently employed in automatic voice recognition. Furthermore, voice search on mobile devices is made possible through speech recognition. Second, by responding to frequently asked questions like pricing, shipping, delivery, comments, and refunds, it is becoming more and more popular as a touchpoint for customers on websites and applications. Additionally, ML is employed in voice assistants and virtual assistants to carry out menial chores. In computer vision, ML is used to extract important insights from pictures, movies, and other visual inputs, particularly in the areas of radiology and self-driving automobiles. To create cross-selling strategies and make recommendations to customers on e-commerce platforms, marketing uses machine learning to analyse consumer behaviour patterns.

### **1.1.2 Face Recognition**

AI and ML algorithms are used in face recognition to identify human faces in the backdrop. Usually, the algorithm looks for human eyes first, then for brows, nose, mouth, nostrils, and iris. After all the facial features have been recorded, further verifications utilizing sizable datasets with both positive and negative photos help to validate that the image is indeed of a human face. Facial recognition methods that are frequently employed include feature-based, appearance-based, knowledge-based, and template matching. Each of these approaches has benefits and drawbacks.

In order to identify a face, feature-based approaches rely on traits like the eyes or nose. The results of this procedure could differ depending on the noise and light. Additionally, appearance-based techniques match the properties of face photos using machine learning and statistical analysis.

A face is recognized using a knowledge-based approach using pre-established principles. Given the work required to develop clear norms, this might be difficult. A face can be found using template-matching techniques, which compare photos to previously saved face patterns or traits. This approach, however, does not account for changes in scale, position, and shape.

## **1.2 AUTHENTICATION METHODS**

With the rapid development of Wi-Fi conversation networks and e-commerce applications akin to e-banking, transaction-oriented application, protecting customers' anonymity in the safety-valuable functions could be very critical. Within the contemporary years, several transactions for cellular devices exist on the web or Wi-Fi networks due to the portability of the cellular contraptions similar to laptops, shrewd playing cards and wise telephones. By offering a number of services including user credential privacy, comfortable mutual authentication, and SK protection, authentication methods are relied upon add-ons in a client-server environment to secure the sensitive technology from a malevolent opponent. In the true-life functions, two-factor authentication (the password together with a wise card) turns into an easy approach for authentication in protection-valuable applications comparable to e-banking, e-tailing and e-well-being services.

### **1.3 FACE RECOGNITION BASED ONLINE BANKING APPLICATION**

Face recognition technology is a biometric authentication method that has become increasingly popular in recent years. Online banking applications that incorporate face recognition technology can offer enhanced security and convenience to customers, making it easier for them to access their accounts while keeping their personal information safe. An algorithm is used to analyse a user's selfie or video of their face in a face recognition-based online banking application in order to extract distinctive facial traits such the space between the eyes, the contour of the jawline, and the curvature of the lips. This information is then compared to a database of known users to verify the user's identity and grant access to their account.

However, it is important to note that face recognition technology is not foolproof and can be subject to errors and false positives. Therefore, it is important to implement additional security measures, such as multi-factor authentication, to ensure the security of online banking applications.

## II. RELATED WORK

Sinha, et.al [1] provided a technique for detecting banking fraud using artificial intelligence. The only thing that is currently contagious is the Covid 19 virus, which has seriously disrupted global economic activity and is causing problems for all firms, regardless of their industry or place of origin. Contactless business, which has boosted digital transaction, is one such significant paradigm shift. As a result, hackers and scammers now have a lot of room to carry out online scams including phishing, dubious links, malware downloads, etc. Due to the rise in digital transactions, these scams have become an undesired component that requires rapid attention and complete removal from the system. Digital payments are the safest and most appropriate payment method in this pandemic circumstance because social distance is essential to limiting the transmission of the virus, and it needs to be safe and secure for both the parties. The study's conclusions imply that the corporate environment did change as a result of the integration of AI. Artificial intelligence (AI) utilised for entertainment has become crucial to business. changing a business's focus from processes to platforms. Studying customer experience and how to provide a better reaction to increase satisfaction is the fundamental demand of AI. However, it has been seen that businesses are now using AIs as a marketing technique to boost demand and sales, not just for customer assistance.

Surekha, et.al [2] in order for India to achieve its economic goals, it must allow the banking industry, which accounts for 70% of the country's GDP, to expand by 8–10 times its current rate over the next ten years. This rate of active expansion necessitates a dual engine of advanced technology and a banking system that is tech enabled, scalable, and secure. Implementing Blockchain Technology (BCT) in the banking industry offers a practical solution that, when combined with IoT-connected equipment, will lead to the sector's growth being secure, quick, affordable, and transparent. Personalized banking, secure banking, linked banking, and digital banking are all common use cases that the Internet of Things has enabled. This chapter explores the potential in the banking industry that should be investigated and the difficulties that must be overcome during the BCT-IoT deployment process. Peer-to-peer lending, Know Your Customer (KYC) updates, cross-border transfer payments, syndicate lending, and fraud reduction are just a few of the banking operations that are detailed as being dependent on BCT and IoT.

Garg, et.al [3] Implement application of AI in Indian banking sector and different results achieved through it. The author has stated few models that could be implemented in banks such as predictive and knowledge flow models. As per research banks like HDFC, ICICI, Axis, SBI banks used artificial intelligence for online banking and chatbots to provide better customer experience. AI could improve employee performance and customer satisfaction and has a tendency to fully empower human resources in banking sector reducing efforts and humanly errors. AI could provide an edge to banks by risk identification, assessment and risk mitigation strategies. Artificial intelligence provides numerous advantages for the banking industry. In India's banking sector and artificial intelligence is transforming corporate operations and customer-end services. It's also utilized to act in accordance with regulations, prevent frauds, and assess individual creditworthiness. Artificial intelligence (AI) has the potential to improve company operations, provide tailored services, and aid with wider aims like financial inclusion. However, it has exposed the institutions to an increasing number of cyber security risks and weaknesses. In order to create an active defence system against cybercrime, banks are increasingly looking to emerging technologies such as block chain and analytics.

Faruk, et.al [4] protecting the data from fraudulent attempts is one of the most urgent considerations to preserve stakeholders, particularly end users' security. Malware is a collection of harmful programming code, scripts, active content, invasive software, or mobile and web applications that are intended to damage target computer systems, programmes, or mobile and web applications. A study found that novice users can't tell the difference between dangerous and good software. Therefore, malicious activity detection should be built into computer systems and mobile applications to safeguard stakeholders. There are several techniques to identify malware activity that make use of cutting-edge ideas like artificial intelligence, machine learning, and deep learning. In this study, focus on AI-based strategies for identifying and thwarting malware activity. An in-depth analysis of current malware detection systems, their drawbacks, and solutions to increase effectiveness is provided in this paper. Proposed study demonstrates that employing futuristic methods for the creation of malware detection programmes will offer important benefits. Understanding this synthesis will aid researchers in their future work on AI-based malware identification and prevention.

Priya. G, et.al [5] implemented machine Learning Algorithms in fraud detection, since the algorithms can be trained by using the test data set to give quick, accurate and efficient result. This need complete life cycle approach which consists of monitoring, learning, detecting, preventing and improving in real time decision making. In order to stay ahead of the fraudsters, organizations should come forward to share fraudulent historical activities instead of restricting themselves within a boundary as per the proposed model. A centralized fraud management platform is the need of the hour to facilitate a shared fraud prevention approach. Proposal is to develop an operating platform to bring organizations across the globe to leverage this framework through adhering to its standards and hence share and leverage fraud patterns to proactively alert and be alerted on fraudulent transactions there by building a strong layer of protection for their applications. This centralized structure can be implemented in across all the sectors like financial sector, telecom industry, stock market, online sector and social engineering area. Today's industry needs to create a dynamic, intelligence driven approach to cyber risk management not only to prevent, but also detect, respond to, and recover from the potential damage that results from these attacks.

### III. EXISTING METHODOLOGIES

To ensure secure online transactions, online security continues to be a difficulty. The foundation of computer security and, thus, secure access to online banking services is thought to be user authentication, a human-centered process. The potential to improve authentication quality and subsequently online security through expanded use of technology is possible, but frequently at the sacrifice of usability. A variety of technologies are used nowadays to combat fraud in the banking sector. One such measure is the application of One Time Passwords (OTPs), a fraud prevention solution designed specifically for online banking transactions. The simplest technique simply shows a time-dependent code that must be entered into the banking interface by the user. The issue is that each and every one of the current security solutions has certain drawbacks. A different sort of method that results from the application of credit/debit card fraud prevention systems is transaction monitoring. This method examines the transaction's sender and recipient and compares the results with known fraud trends. Since all analysis is carried out in the background, this method doesn't require any additional hardware from the user. However, this too has drawbacks since when new fraud patterns emerge before they are discovered, the system will have a flaw. Additionally, call centres may occasionally receive legitimate transactions, which cause customers to suffer.

### IV. ONLINE BANKING USING FACE RECOGNITION WITH HYBRID PIN

Online banking has become increasingly popular among customers, because it offers a convenient option to conduct transactions utilizing smart devices from anywhere. Nowadays, thieves use high-tech techniques to obtain user data like passwords, PINs, and security questions. With the use of face biometric authentication, this initiative seeks to increase the security of online banking. Static user names and passwords are now used with online banking, along with OTPs—one-time passwords—to mobile numbers. A hybrid keyboard and Brightness based password authentication methods is implementing to address the problem of shoulder-surfing attacks on authentication schemes. This is a PIN-based authentication method that operates on touch screen devices. A hybrid keypad combines two keypads with distinct digit orderings so that the user who is close to the device sees one keypad to enter the PIN while the attacker who is viewing the device from a greater distance sees the other keypad. In brightness password system, if the brightness value is high, the user must insert a correct PIN digit. Whenever it looks dark to the user, user is required to enter a misleading lie digit. In this way, only the legitimate user and the SE know the real PIN digits along with its positions in the currently generated sequence. According to this investigation, it appears to be essentially impossible for a surveillance camera to record a smartphone user's PIN when a hybrid keypad is in use. User's most important information may be protected and secured using the potent science and technology combo known as biometrics. This proposed approach provides the chances of integrating biometric technology with online banking since that technology is advancing and the cost of biometric equipment is decreasing. Face biometric can be used to provide cost effective rather than other biometric features such as fingerprint, iris and other features. And also extend the process to implement the system with multiparty access. The user of the account is considered as primary user. Other users who are regarded as secondary users are given access to the account by the primary user. The primary user set the limit for secondary access. At the time of login verification, face can be

recognized as whether it is primary or secondary. 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. Infrequent access can be avoided via session time analysis.

#### METHODOLOGY

The Grassmann algorithm is a mathematical technique that is often used in face recognition to analyze and compare facial features. Here are the basic steps involved in using the Grassmann algorithm for face recognition:

**Feature extraction:** The first step is to extract facial features from the images of the faces to be recognized. Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) are two often employed approaches.

**Face representation:** Next, the extracted facial features are represented as points in a high-dimensional space. This space is often referred to as a feature space or a face space.

**Grassmann manifold:** The Grassmann manifold is a mathematical space that represents all possible subspaces of a fixed dimension in a high-dimensional space. The Grassmann algorithm uses this manifold to compare the subspaces that represent the facial features of different faces.

**Subspace projection:** Each face is represented as a subspace in the feature space. The Grassmann algorithm then projects these subspaces onto the Grassmann manifold to create a set of points that can be compared.

**Distance computation:** Finally, the distance between the subspaces is computed using a distance metric such as the Grassmann distance. The distance metric takes into account the geometry of the Grassmann manifold and provides a measure of how similar or dissimilar the subspaces are.

**Classification:** The computed distances are then used to classify the faces into known or unknown individuals. This step typically involves setting a threshold value for the distance metric, above which a face is considered to be unknown.

Overall, the Grassmann algorithm is a powerful technique for face recognition that can handle variations in lighting, pose, and facial expressions. It is particularly useful when the number of training samples is small, as it can effectively capture the variability of facial features in a low-dimensional space.

#### PROCEDURE

##### Bank interface creation:

Online banking is altering the way of consumers shop and how businesses run. Traditional payment methods like cash and cheques are drastically declining, and more consumers are opting for the convenient and adaptable options provided by emerging digital payment technology. A new breed of fraudsters has emerged as a result, using cutting-edge technology to break into business networks and personal computers. Traditional methods, like passwords or tokens, are ineffective against these attacks. Here create the interface for online banking system transactions to prevent these assaults. Admin and user interface were created in this module. 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.

##### User Registration

Before a user can be authenticated to the system, they have to be registered with the system for the first time. This step is called registration. In order to request services, a new user must first register with a system and then be authenticated. In a basic authentication process, a user presents some credentials like user ID and some more information to prove that the user is the true owner of the user ID. This process is simple and easy to implement.

##### Hybrid PIN & Bright Pass Verification

Authentication is the process of determining whether a user should be allowed to access to a particular system or resource. User can't remember strong password easily and the passwords that can be remembered are easy to guess. A password authentication system should promote memorable, secure passwords that are strong and less predictable. While allowing for user discretion, this password authentication scheme encourages users to choose stronger passwords. Here implement the authentication process in this module. After registration, user enters into the system using login setting. At first, face image capture and recognize the face. Two different PIN

authentication types are used in the proposed method. One is Illusion PIN setup and another one is BrightPass setup. After successful PIN verification, users allow to capture face for further authentication.

**Face Verification**

After completion of registration, the user can create a password using face recognition. 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. Finding the image in the database with the greatest similarity to the test image is how the test image is identified. 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.

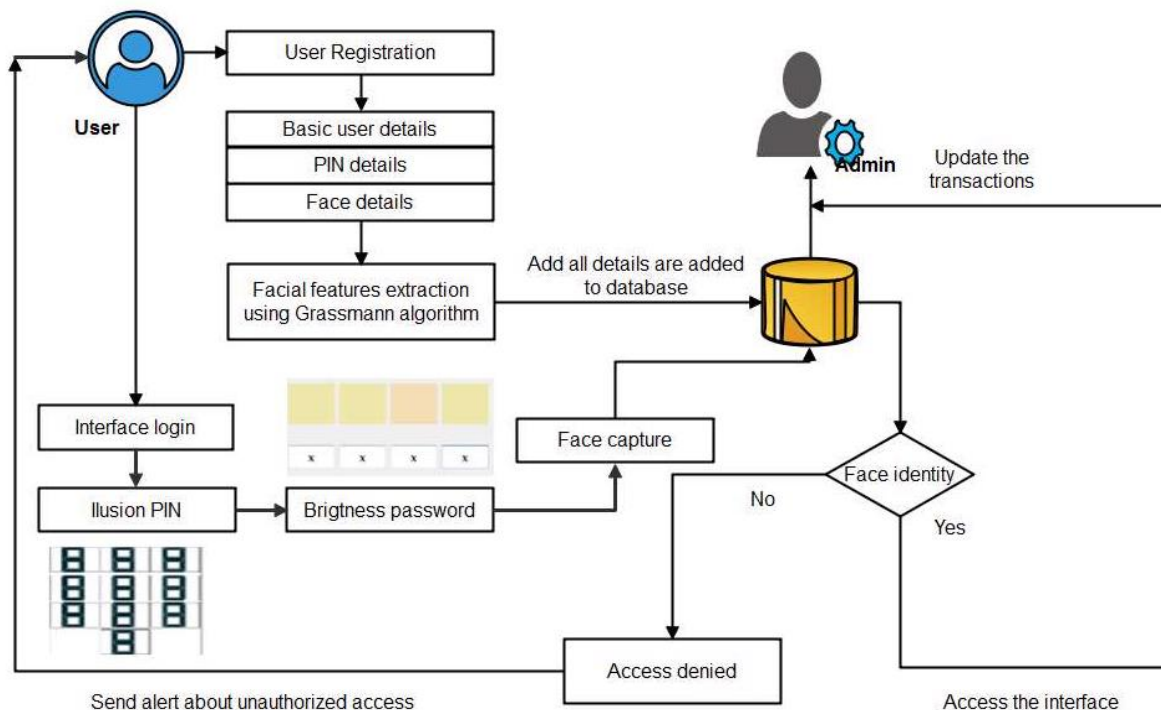
**Multiparty Access System**

Multi-party authorization (MPA) is a process to protect online transactions from undesirable acts by a malicious insider or inexperienced technician acting alone. A second authorized user must give their consent in order for MPA to allow an activity to proceed. This prevents an undesirable act from happening to data or systems in advance. In this module, user of account specified as primary user. In this module, primary user provides access permission to secondary users with predefined threshold values. Admin can store details of secondary users with relationship information.

**Alert System**

Finally provide SMS alert to primary users about the transactions. The details of the transactions has user name of account access, timing details, amount details, mode of payments and so on. Based on these details, primary user easily knows the transactions details up to date.

**PROPOSED SYSTEM ARCHITECTURE**



**Fig 4.1:** Architecture for Proposed Work

**The benefits of face recognition technology in online banking applications include:**

**Improved security:** Face recognition technology is more secure than traditional authentication methods, such as passwords and PINs, which can be easily compromised. Facial features are unique and difficult to replicate, making it more difficult for fraudsters to gain access to a user's account.

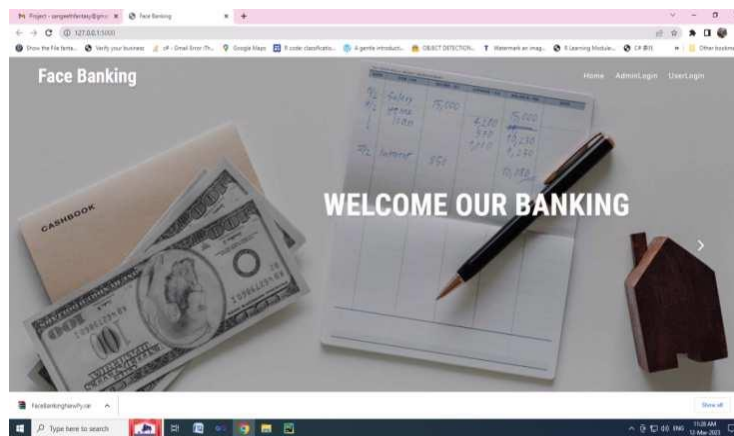
**Greater convenience:** Face recognition technology eliminates the need for users to remember complex passwords or carry around physical tokens, making it easier for them to access their accounts.

**Enhanced user experience:** Face recognition technology provides a seamless and intuitive user experience, allowing users to access their accounts quickly and easily.

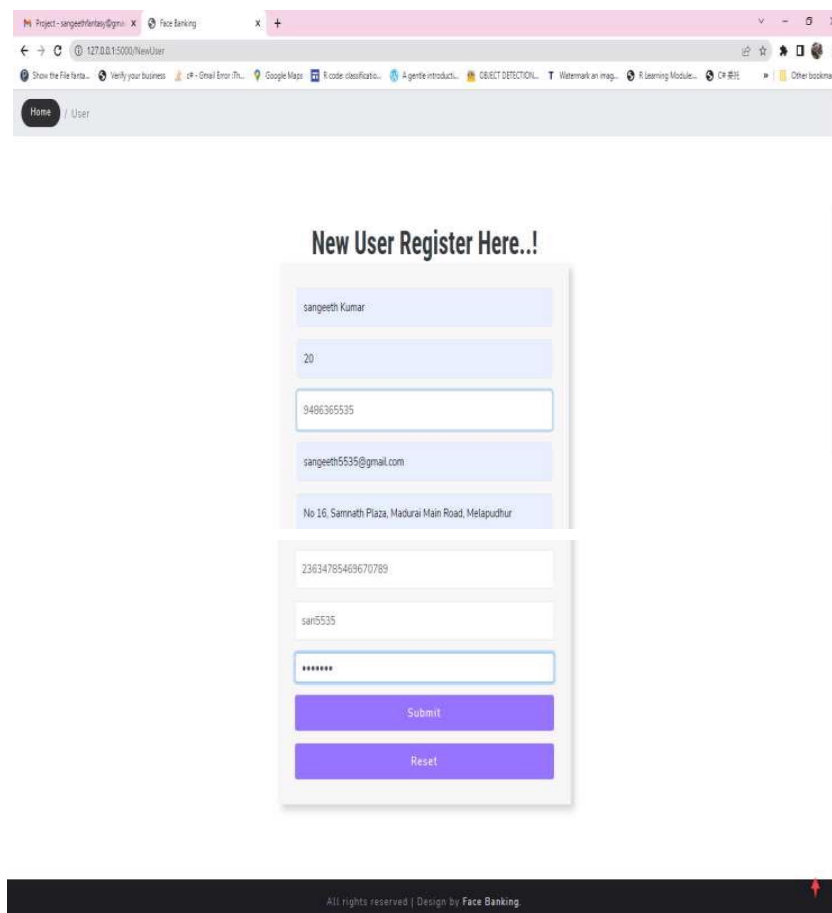
## V. EXPERIMENTAL RESULTS

The experimental results of the studies indicate that face recognition-based authentication has several advantages over traditional authentication methods, including improved security, convenience, and user experience. The proposed online banking system implemented using python as front end and MySQL as back end.

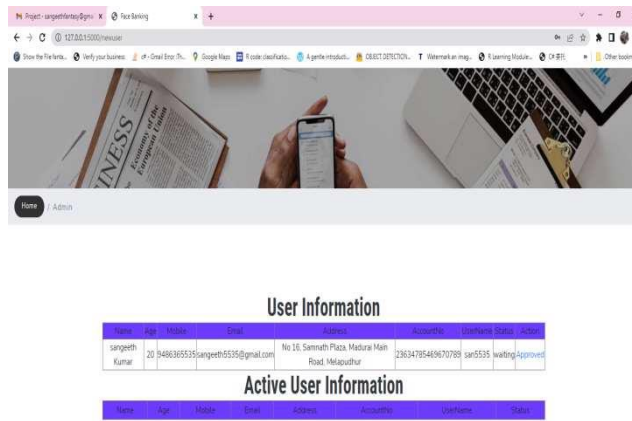
### Home Page



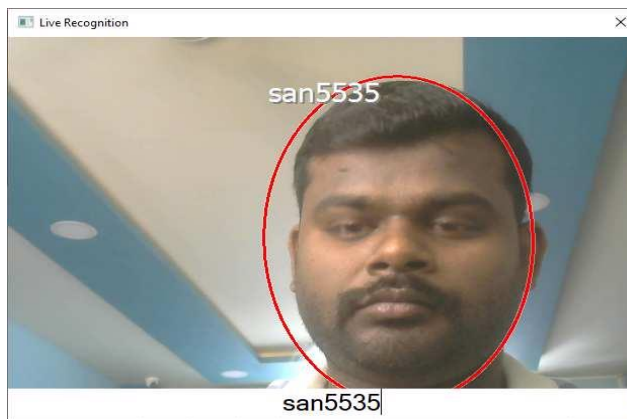
### User Register



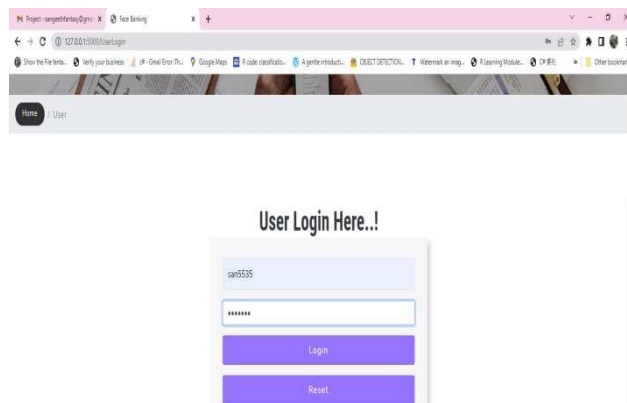
**Admin Approve User Details**



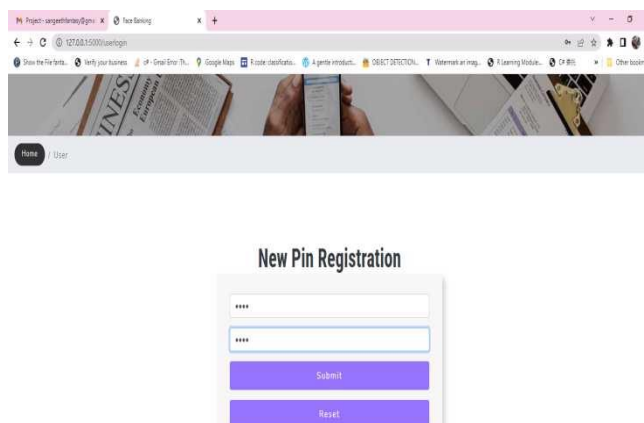
**Face Capture and Register**



**User Login**

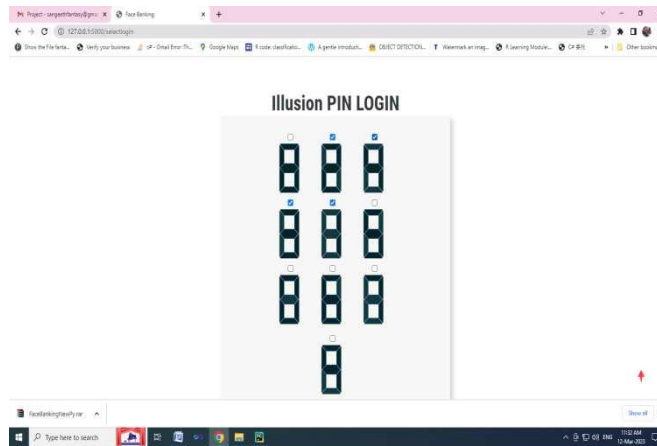


**Secret PIN Creation**





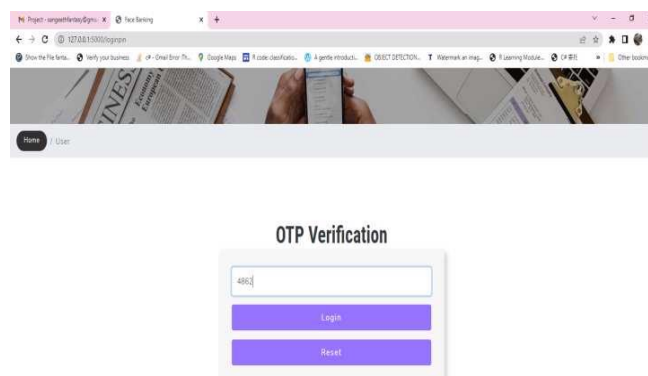
### Digital PIN method



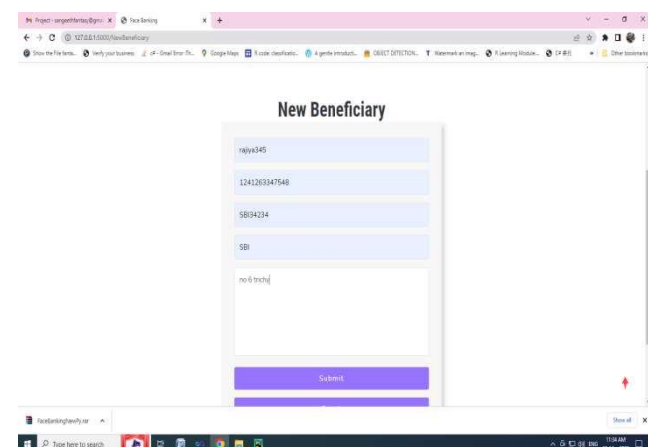
### Face Capture and Verification



### OTP Verification

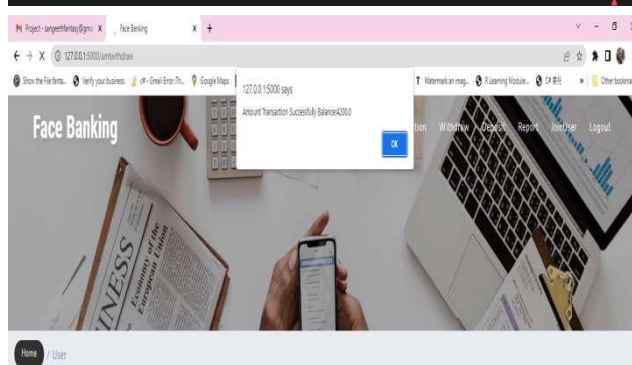
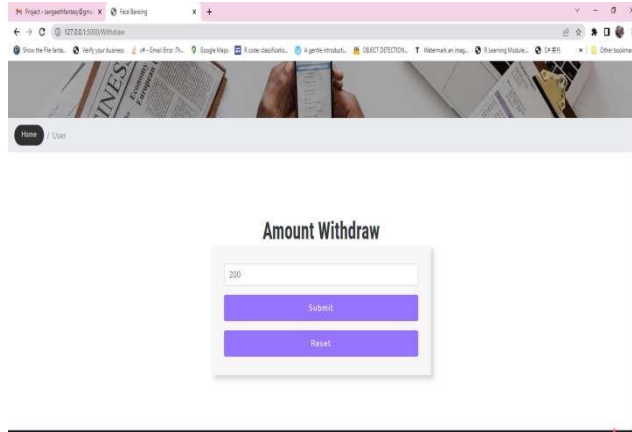


### Add Beneficiary

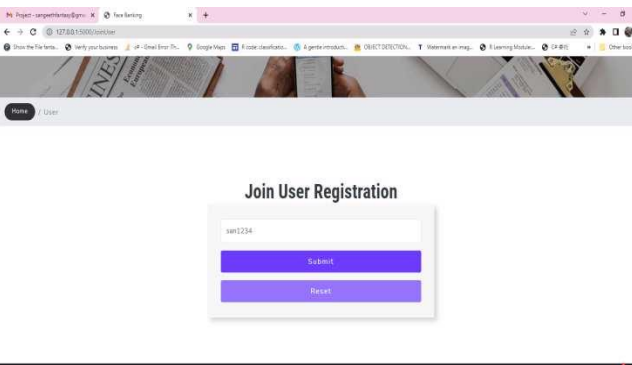




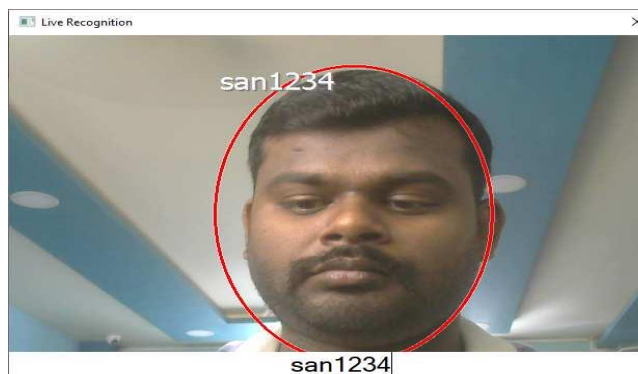
### Amount Withdrawal

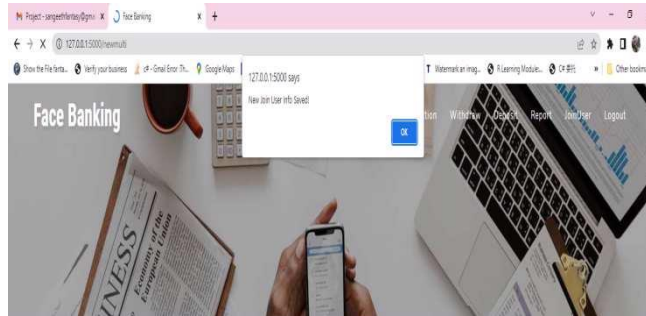


### Create Join User

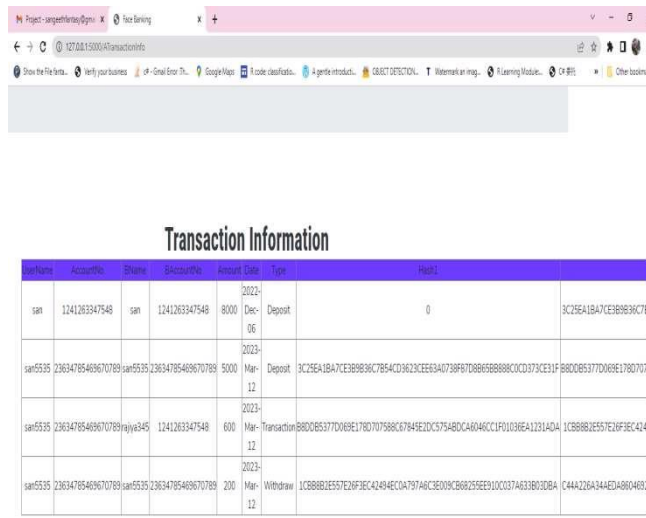


### Capture Joint user Face Image and Register





**View Transaction Details**



Name	Account No	Phone	Branch	Amount	Date	Type	Hash
san	1241263347548	san	1241263347548	8000	2022-12-06	Deposit	0
san5535	23634785469670789	san5535	23634785469670789	5000	2023-12-12	Deposit	3C29EA1BA7CE3B8936C7854CD3623CE63A0738967D866588888C0C0373CE1F8600B5377D069E17807075
san5535	23634785469670789	san5535	1241263347548	600	2023-12-12	Transaction	880DB5377D069E1780707588C87849E20C5754BDC46040CC1F01036EA121A0A1C8B8882E557E28F3EC4248
san5535	23634785469670789	san5535	23634785469670789	200	2023-12-12	Withdraw	1C8B882E557E28F3EC42484ECC0A797A8C3E009C86825EE310CC37A631803D0BA1C44A226A344E3A8804892C

**VI. CONCLUSION**

The main goal and importance of the online banking system using face image is to provide security. To overcome the challenges of the technology it can be combined with more secure features. This proposed application implemented biometric security measure in the online banking system. The proposed system explains a hybrid keypad and Bright password are implemented in an online banking application. The main goal of proposed work was to design a PIN-based authentication scheme that would be resistant against shoulder surfing attacks. To this end, proposed work created Illusion PIN and bright password system. The proposed system has quantified the level of resistance against shoulder-surfing by introducing the notion of safety distance. Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based security systems. And also provide multi-person access control to provide access privileges to users with improved security. Real time alert system proposed for unauthorized access and multi person access.

**VII. REFERENCES**

- [1] Sinha, Mudita, Elizabeth Chacko, and Priya Makhija. "AI Based Technologies for Digital and Banking Fraud during Covid-19." Integrating Meta-Heuristics and Machine Learning for Real-World Optimization Problems. Springer, Cham, 2022. 443-459.
- [2] Surekha, Nayak, et al. "Leveraging Blockchain Technology for Internet of Things Powered Banking Sector." Blockchain based Internet of Things. Springer, Singapore, 2022. 181-207.
- [3] Garg, Yashika, And Kanika Sachdeva. "Artificial Intelligence In Indian Banking Sector: A Game Changer." DogoRangsang Research Journal, Vol-12 Issue-08 No. 05 August 2022.
- [4] Jobair Hossain Faruk, Md, et al. "Malware Detection and Prevention using Artificial Intelligence Techniques." arXiv e-prints (2022): arXiv-2206.
- [5] Priya, G. Jaculine, and S. Saradha. "Fraud detection and prevention using machine learning algorithms: a review." 2021 7th International Conference on Electrical Energy Systems (ICEES). IEEE, 2021.

- 
- [6] Bojjagani, Sriramulu, et al. "Systematic survey of mobile payments, protocols, and security infrastructure." *Journal of Ambient Intelligence and Humanized Computing* (2021): 1-46.
- [7] Albalooshi, Fatema A., et al. "Facial Recognition System for Secured Mobile Banking." *KnE Engineering* (2018): 92-101.
- [8] Albalooshi, Fatema A., et al. "Facial Recognition System for Secured Mobile Banking." *KnE Engineering* (2018): 92-101.
- [9] Manju, V., and S. Madhumathi. "Improving net banking security with face recognition based bio-metric verification." *Int J Sci Res Comput Sci Eng Inform Technol* 5.3 (2019): 82-91.
- [10] Dhoot, Anshita, A. N. Nazarov, and Alireza Nik Aein Koupaei. "A security risk model for online banking system." *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*. IEEE, 2020.