International conference on Advanced Techniques in Communication Networking and Automation

RESEARCH ARTICLE OPEN ACCESS

FACE RECOGNITION BASED MULTIFACTOR AUTHENTICATION METHOD FOR ONLINE BANKING SERVICE

1. K.VIGNESHWARAN 2.K.R.NAVIN KUMAR 3.B.BHARATH 4.Mr.N.KANNAN,M.TECH.

1,2,3 Final Year Student, 4 Assistant professor
Department of Computer Science and Engineering
E.G.S Pillay Engineering College(Autonomous),Nagapattinam.

Abstract— the importance of security in the authentication process as well as the increase in threat level posed by such malware has attracted many researchers to the field. 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. 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 enter the PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. Second layer based on OTP verification in reverse order. Third layer based on real time authentication system using face biometrics for authorized the person for Net banking system, which provides new solutions to address the issues of security and privacy. 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.

Index Terms—**Bank Interface Creation, User Registration, Hybrid PIN and Brightness Password Verification, Face Verification, Multi Party Access System, Alert System.**

I. INTRODUCTION

1.1 CLOUD COMPUTING

Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. Cloud computing has become an essential part of modern computing infrastructure, and it is being used by individuals and organizations of all sizes to solve their computing needs.

There are three primary types of cloud computing services:

Infrastructure as a Service (IaaS): This service provides virtualized computing resources, such as servers, storage, and networking, over the internet. Customers can use these resources to build their own IT platforms, and they are responsible for managing and maintaining their own applications and operating systems.

Platform as a Service (PaaS): This service offers a complete platform for developing, testing, and deploying web applications, without the need for customers to manage the underlying infrastructure. Customers can focus on developing their applications, while the cloud provider takes care of the rest.

Software as a Service (SaaS): This service provides customers with access to software applications that are hosted by the cloud provider. Customers can access these applications through a web browser or a mobile app, and they do not need to manage the underlying infrastructure or software.

Cloud computing services offer several advantages, including cost savings, scalability, flexibility, and reliability. They also enable organizations to focus on their core business functions, rather than spending time and resources on IT infrastructure management.Face Recognition.

1.2 CLOUD BASED BIO-METRIC AUTHENTICATION SYSTEM

Biometric authentication services using cloud computing have become increasingly popular in recent years. Biometric authentication is a method of verifying a person's identity by using unique biological traits, such as fingerprints, facial recognition, voice recognition, and iris scans. Cloud computing provides an ideal platform for biometric authentication services because it offers a secure, scalable, and flexible infrastructure that can handle large volumes of data and traffic.

There are several ways in which biometric authentication services can be deployed using cloud computing:

Cloud-based biometric authentication: In this approach, biometric data is collected and processed on the cloud. Users can access the authentication service through a web-based application, and the biometric data is matched against a database of known users to verify their identity.

Hybrid biometric authentication: In this approach, biometric data is collected and processed on the user's device, such as a smartphone or tablet. The data is then sent to the cloud for verification against a database of known users.

Cloud-enabled biometric authentication: In this approach, biometric data is collected and processed on the user's device, but the cloud is used to provide additional processing power and storage capacity. This approach enables faster and more accurate biometric authentication.

Cloud-based biometric authentication services offer several benefits over traditional authentication methods, such as passwords and PINs. They are more secure, as biometric data is unique and difficult to replicate. They are also more convenient for users, as they eliminate the need to remember complex passwords or carry around physical tokens. Additionally, they can be easily integrated into existing systems and applications, making them ideal for use in a wide range of industries, including finance, healthcare, and government.

1.3 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. In a patron server atmosphere, the authentication schemes are the depended on add-ons in an effort to shield the touchy expertise towards a malicious adversary by way of providing variety of services equivalent to user credentials privateness, comfy mutual authentication, and SK protection. In the true-life functions, two-factor authentication (the password together with a wise card) turns into a easy approach for authentication in protection-valuable applications comparable to e-banking, e-tailing and e-well-being services.

1.4 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. A face recognition based online banking application typically involves a user taking a selfie or video of their face, which is then analyzed by an algorithm that extracts unique facial features, such as the distance between the eyes, the shape 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] presented a banking fraud detection method using Artificial Intelligence technologies. The only viral thing today is the Covid 19 virus, which has severely disrupted all the economic activity around globe because of which all the businesses are experiencing irrespective of its domain or country of origin. One such major paradigm shift is contactless business, which has increased digital transaction. This in turn has given hackers and fraudsters a lot of space to perform digital scams line phishing, spurious links, malware downloads etc. These frauds have become undesirable part of increased digital transactions, which needs immediate attention and eradication from the system with instant results. In this pandemic situation where, social distancing is key to restrict the spread of the virus, digital payments are the safest and most appropriate payment method, and it needs to be safe and secure for both the parties. Findings of the study suggest that inclusion of AI did bring a change in the business environment. AI used for entertainment has become an essential part in business. Transfiguration from process to platform focused business. The primary requirement of AI is to study the customer experience and how to give a better response for improving the satisfaction. But recently AIs are used not only for customer support, but it's been observed that businesses have taken it as marketing strategy to increase demand and sales.

Surekha, et.al [2] banking sector contributes to 70% of Indian Gross Domestic Product (GDP) and for India to meet its economic aspirations; it should enable this vivacious sector to grow at 8–10 times of its current pace, in the next ten years. This pace of active growth requires a double engine of sophisticated technology and a tech enabled, scalable, and a secured banking system. Implementing Blockchain Technology (BCT) in the banking sector, provides a realistic solution which when coupled with devices connected by the Internet of Things (IoT), will result in secured, fast-paced, cost effective, and transparent growth of the sector. The prevalence of personalized banking, secured banking, connected banking, and digital banking are use cases, made possible through interface with IoT. This chapter delves into the opportunities in the banking sector to be explored and challenges to be met in the BCT-IoT implementation process. BCT- and IoT-based opportunities such as peer-to-peer lending, Know Your Customer (KYC) updation, Cross-border transfer payments, syndicate lending, fraud reduction are some of the banking operations that are elaborated.

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. It has, however, exposed the institutions to a growing number of cyber security threats and vulnerabilities. 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] to maintain stakeholders, particularly, end user's security, protecting the data from fraudulent efforts is one of the most pressing concerns. A set of malicious programming code, scripts, active content or intrusive software that is designed to destroy intended computer systems and programs or mobile and web applications is referred to as malware. According to a study, naive users are unable to distinguish between malicious and benign applications. Thus, computer systems and mobile applications should be designed to detect malicious activities towards protecting the stakeholders. A number of algorithms are available to detect malware activities by utilizing novel concepts including Artificial Intelligence, Machine Learning, and Deep Learning. In this study, we emphasize Artificial Intelligence (AI) based techniques for detecting and preventing malware activity. We present a detailed review of current malware detection technologies, their shortcomings, and ways to improve efficiency. Our study shows that adopting futuristic approaches for the development of malware detection applications shall provide significant advantages. The comprehension of this synthesis shall help researchers for further research on malware detection and prevention using AI.

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

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 most basic method displays a time-dependent code that a user is required to input into the banking interface. Smart cards and USB tokens are other security measures employed by banks that work by verifying the user through their possession of a smart card or USB device. 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. This approach analysis the sender and receiver of the transaction and compares with identified fraud patterns. This approach requires no additional hardware for the user as all analysis is done in the background. However, this too comes with its disadvantages, as there will be a loophole in the system when new fraud patterns occur before they are detected. Also, occasionally genuine transactions will be forwarded to call centers which then inconvenience customers.

IV. ONLINE BANKING SECURITY USING HYBRID PIN METHODS WITH FACE RECOGNITION 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. 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. Hybrid 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 enter the PIN, while the attacker who is looking at the device from a bigger distance is seeing only 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. Based on this analysis, it seems practically almost impossible for a surveillance camera to capture the PIN of a smartphone user when hybrid keypad is in use. Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information. 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. And also extend the process to implement the system with multiparty access. The user of the account is considered as primary user. The primary user provides the permission to access account to other persons considered as secondary users. 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. Session time analysis can be used prevent from infrequent access.

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. Commonly used techniques include Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA).
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 thus changing the way people shop and how retailers operate. There is a steep 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.

User Registration

Before a user can be authenticated to the system, he has to be registered with the system for the first time. This step is called registration. So, for a new user, he has to get registered with a system and then authenticated before he can request services. 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 encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. In this module we can implement authentication phase. After registration, user enters into the system using login setting. At first, face image capture and recognize the face. Here we use two types of PIN authentication. 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 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.

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. MPA requires that a second authorized user approve an action before it is allowed to take place. This pro-actively protects data or systems from an undesirable act. 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.

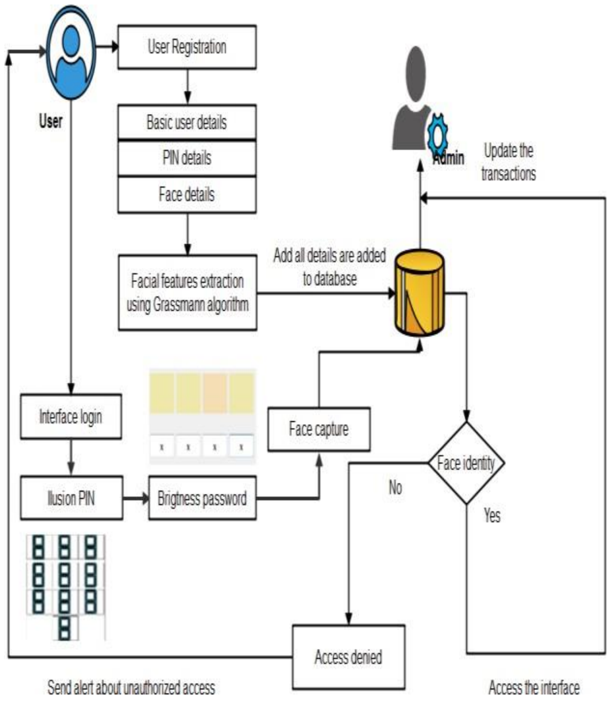

Fig 1. Architecture for Proposed Work

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 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. In this project we are using biometric security measure in the online banking system. The proposed system explains a hybrid keypad and Bright password are implemented in an ATM application. The main goal of our work was to design a PIN-based authentication scheme that would be resistant against shoulder surfing attacks. To this end, we 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.

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.