Vol. 3 No. 4
Scientific Voyage: ISSN: 2395-5546
Government College of Engineering and Ceramic Technology, West Bengal, India

STUDY ON TWO STAGE AUTHENTICATION FOR ONLINE TRANSACTION IN MOBILE DEVICES

Sudipta Roy[1,*], **Papri Majumder**[2], **Sneha Chatterjee**[3], **Abhik Chakraborty**[4], **Mayank Shekhar**[5], **Sayantan Chakraborty**[6], **Pranab Gharai**[7], and **Soumit Chowdhury**[8]

[1-6]*Department of Information Technology, B. P. Poddar Institute of Management and Technology, Kolkata*

[7]*Department of Computer Science, Brainware University, Kolkata*

[8]*Department of Computer Science, Government College of Engineering and Ceramic Technology, Kolkata*

[**]`sudipta.1706@gmail.com`

Received: Nov 09, 2023
Revised: Nov 23, 2023
Accepted: Dec 08, 2023

ABSTRACT

In recent years with remarkable development in technology, single factor authentication e.g., passwords are no longer considered secure. The widespread adoption of online financial transactions has raised concerns about the security of digital payment systems. Multi-factor authentication is a security mechanism that entails employing additional techniques in addition to the usual login and password to verify a user's identity. The use of two stage authentication has emerged as a critical security technique to reduce the risks of unauthorized access and fraudulent activities. This paper looks at how two stage authentications might improve the safety of online financial transactions. The paper examines the efficacy of two stage authentication in avoiding unauthorized access and financial fraud through a thorough analysis of recent literature and case studies. It explores numerous two stage authentication techniques, highlighting their advantages and disadvantages. These techniques include SMS-based codes, biometric verification, and hardware tokens. To overcome the shortcomings of the existing technique, we proposed a system that includes fingerprint authentication along with PIN at the time of money transaction to avoid unauthorized access.

Keywords: Two Stage Authentication, Online Transaction, Mobile Banking, PIN, Transaction Security, Fingerprint Authentication, Bio metrics, Internet Banking

1 INTRODUCTION

The emergence of the digital age has fundamentally changed how we carry out financial transactions. Our everyday lives have become completely reliant on online banking, e-commerce, and mobile payment apps, which provide unmatched ease. In this context, the security of financial transactions is of paramount importance. Financial data, personal information, and transactions themselves are prime targets for malicious actors seeking to exploit vulnerabilities in the digital ecosystem. To protect against these attacks, two stage authentication is a crucial protection measure. Users are required to supply two separate factors—typically something they know, like a password, and something they have, like a mobile device—to confirm their identity when using two stage authentication These elements working together considerably improve security by lowering the possibility of unwanted entry. Two stage authentication is a crucial tool for safeguarding the confidentiality, integrity, and authenticity of financial data since it makes it harder for hostile actors to access financial accounts. The growing concerns regarding the vulnerability of financial data and personal information in the digital space is the motivation behind this research work.

Utilizing a secret password is the most popular method of user authentication. The password is, however, susceptible to different cyber-attacks. Therefore, it becomes vital to secure sensitive information of online transactions in mobile devices. The paper [11] discusses identity theft and prevention against it. Identity theft poses a significant and genuine threat to everyone. By using two stage authentications with random codes, the Secure Online Transaction Algorithm (SOTA) seeks to address this. SOTA utilizes mobile devices and an application for logging into card accounts, generating unique codes. This approach significantly reduces the risk of unauthorized users exploiting someone else's information for fraudulent activities. A robust approach for authentication in mobile banking involves integrating user ID and password with fingerprint recognition is discussed in paper [8]. Increased dependability is provided by this combination approach, guaranteeing safe access to private financial data and transactions. The paper [11] introduces a segment-based online signature verification approach for securing mobile transactions. It identifies invariant segments in a user's signature, leveraging touch screen data to extract geometric layout and behavioral characteristics. Additionally, it employs a quality score during enrollment for robust user signature profile construction, ensuring reliable verification despite geometric distortions on touch screens.

Paper [10] explains the implementation of facial recognition techniques for login and banking purposes which is aimed at enhancing security measures. The proposed system uses a multi-level approach, integrating traditional username and password verification with advanced facial recognition capabilities. Additionally, users are required to input a PIN to successfully complete the transaction process. The solution delivers a strong and trustworthy security framework, protecting sensitive financial data, and preventing unwanted access by utilizing these combined authentication techniques. Paper [9] explains the value of Virtual Private Networks (VPNs) for gaining access to data resources on cloud servers. It suggests a unique architecture with a Multi-Factor Authentication (MFA) system to boost security by using biometrics and low-entropy passwords. Mobile devices, authentication servers, and banking servers are some of the components of the suggested model. It makes use of voice recognition as a crucial factor in authentication. The effectiveness and efficiency of the system is analyzed, and it is found to be protected against various attacks. The proposed system can improve the security functions by protecting the credentials in the database of the authentication server. The Paper [3] discusses the increasing number of ATM users and the associated security risks, particularly the threat of financial losses due to stolen ATM cards and PINs. It emphasizes the advantages of biometric technology, with a focus on fingerprint recognition, as a more secure and efficient means of authentication. Fingerprint recognition is highlighted for its simplicity, non-stored image data, and resistance to misuse, making it a promising solution to enhance ATM security and protect users from potentially fraudulent activities. Fraud attacking the automated teller machine (ATM) has increased over the decade. The Paper [3, 7] describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint and iris authentication. The Socket Secure version 5 (SOCKS V5) protocol describes the password-based authentication to provide authentication services to the initial SOCKS protocol. In this system, the request transmits the password in simple text and thus, it is not recommended due to security reasons. In this paper, we proposed a two-stage authentication system that uses fingerprints along with PIN to enable online payments. The primary objective of this paper is to fortify security measures by implementing a robust two stage authentication system, thereby reducing the risk of unauthorized access, and safeguarding sensitive information. The paper aims to prioritize user experience by adopting user-friendly two stage authentication methods, ensuring minimal user inconvenience. The paper recognizes the critical necessity of reinforcing the security of online transactions, particularly with regards to the protection of sensitive financial data and the prevention of unauthorized access.

The remaining paper is arranged as follows: We will first go through the existing technique on two factor authentication in Section 2. Then we will discuss the enhancement of the existing system in Section 3. After that we will describe our proposed model in Section 4. Section 5 deals with the future scope of the two-stage authentication. At the end we will conclude our work in Section 6.

2 EXISTING TECHNIQUE

In conventional systems, system resources are available for a predetermined amount of time or until the user logs out explicitly once their identification has been confirmed. which assumes that the user's identification remains unchanged for the duration of the session and that a single verification at the start of the session is sufficient.

In existing system [11], the authors proposed a technique using two stage authentications along with One-Time Password. This framework utilizes a smartphone application that is registered to a specific credit card. The code needed to authenticate the purchase the customer is trying to make will be sent via the application, which will act as the transmission device. The consumer's purchase is validated and confirmed if they enter the correct code, else the transaction will be rejected. After choosing the desired product, the consumer proceeds to checkout. If they choose a credit card secured with this framework, the Online Retailer Employs Public Key Infrastructure Advanced Encryption Standard (PKI AES) Encryption to securely transmit consumer data to the Credit Card Company. Upon verification, the Credit Card Company utilizes Secure Hash Algorithm (SHA-256 hash) to send an eight-digit number to the Online Retailer and a corresponding one-time password (OTP) to the consumer's credit account smartphone application via PKI. The online retailer completes the transaction if the hashed code input by the customer and the hashed code supplied to them by the credit card company match.

A strong approach for authentication in mobile banking integrating it with user ID, password, and fingerprint identification to improve security and reduce risks is explained in paper [8]. The most common biometric modality, the fingerprint, is scanned, improved, and turned into a template by a mobile device's scanner. In terms of dependability and fraud prevention, biometrics outperforms conventional techniques like PINs and passwords because it uses an individual's physiological or behavioral characteristics for automatic identification. The money will be sent to the appropriate categories, such as Net Banking, Credit Card Payment, and Wallet, upon successful fingerprint authentication.

In paper [12], signature verification is used for securing mobile transactions. The proposed system normalizes signatures by generating concentric circles (R1 and R2) to establish scaling, constraining signature coordinates to [-1, 1]. Normalized signatures are interpolated to ensure uniform length. The feature extraction component captures geometric layout and user characteristics. Signature quality evaluation yields a score balancing inconsistency and distinctiveness for user profile construction. Critical segment extraction identifies stable feature segments reflecting intrinsic signing behaviors. Utilizing the similarity score, our system determines acceptance or rejection of the user.

Paper [9], proposed a model that comprises a mobile device, authentication server, banking server, and users with valid low entropy passwords and biometric identities. Its scalability allows for multiple users and banking servers. User accesses Banking server by registering a low entropy password and unique biometric identity, especially their distinct voice. Users initially register with the authentication server using a low entropy password and International Mobile Subscriber Identity (IMSI) number, while biometric users generate a key pair for registration. The authentication server verifies the digital signature and IMSI, granting a ticket to the user, facilitating communication with the banking server. During authentication, the user provides the low entropy password and unique voice, verifying identity. The user's password undergoes an authentication check, prompting the user device to send a login message to the authentication server. Upon successful verification, the authentication server grants a session key, ensuring secure user access to the Banking server.

A facial recognition system is a technological tool that can compare a digital image or video frame containing a human face to a database of faces. An approach using facial authentication is explained in paper [10]. The face authentication system operates in three stages: image acquisition, model training, and recognition. Image acquisition requires high-quality images for effective face detection and recognition. For each user, 100 images of 136×136 pixels are acquired via a webcam and converted to grayscale, separating the luminance from the chrominance planes. These images are then transformed into matrices and labeled accordingly. A Local Binary Pattern Histogram (LBPH) face recognizer model is created, trained with the image matrices and their corresponding labels, and saved during the process. Face recognition involves the use of the Haar cascade classifier and the trained recognizer. If the confidence scores meet the set criteria, the user is authenticated; otherwise, they are classified as unknown. Python, along with the OpenCV library, is employed for the face recognition system, while MySQL is utilized for the bank record management.

Paper [3], proposed a system which integrates fingerprint into ATM alongside PIN numbers. Using this framework, users can feel at ease knowing that their accounts are safe from unauthorized access. After fingerprint verification, a specialized fingerprint module generates a 4-digit code which is sent to the user's registered mobile number. Customers are guaranteed additional security measures during ATM transactions because access is authorized based on the validation of this code.

A Two Factor Authentication channel based on steganography in the QR code is proposed in [2]. The main technique used is steganography, specifically steganographic insertion and extraction, to hide mTAN in QR codes. Additionally, AES encryption ensures the security of mTAN during transmission. This combination of techniques is intended to enhance the security of the 2FA system.

In Paper [6] a new authentication protocol that could be used on mobile devices allowing more secure authentication between mobile users and SOCKS proxy server is proposed. In addition, authentication is also provided between SOCKS proxy server and application server. Furthermore, the proposed protocol also generates secure session keys between mobile user and proxy server, and proxy server and application server.

Paper [1] doesn't specifically highlight the technology used in the research. However, it can be inferred that the technology used for data collection and analysis includes data extraction from publicly available sources, as well as tools and software for assessing the compliance, robustness, and complexity of MFA protocols. The research likely utilized various cybersecurity and analytical tools for assessing MFA security and complexity.

Paper [4] presents a comprehensive analysis of authentication techniques, encompassing single-factor and multi-factor methods. Notably, the study reveals that smart card-based authentication stands out as the most extensively researched single-factor technique. Furthermore, the combination of text passwords and smart cards emerges as the most investigated approach in multi-factor authentication. The research underscores the paramount criteria for evaluating and selecting authentication schemes, which primarily include usability, security, and cost-effectiveness. This systematic review underscores the extensive research efforts in the domain of authentication while highlighting the need for further exploration in various application contexts.

In paper [5], a two-level integrated authentication mechanism (2L-IAM) was proposed. At the first level, the user will be authenticated using their fingerprint or personal identification number, and at the second level, face recognition (FR) will be used to authenticate them. The justification for the suggested 2L-IAM is that FR-based second level authentication ensures the genuine identification of the authorized IB user.

3 ENHANCEMENTS OF EXISTING TECHNIQUE

As technology advances, so do cyber criminals' strategies. Report shows that nearly 15 billion credentials were taken from 1000000 data breaches. Possessing these credentials, fraudsters can access medical records, bank accounts, trade secrets of companies, and much more. This shows that the existing system and username and password combination is liable to risk.

In paper [11], during transmission, if one bit is changed, then the hashed data will not match the other hashed data. This, in turn, will not authenticate the user and will prevent the purchase from being completed. Besides this, credit card companies will have to pay a certain amount to adopt this approach. Facial authentication that is used in [10] is subject to facial spoofing which means a fraudster may attempt to bypass a facial authentication system by presenting a false image.

The implementation of steganography in the QR-code for two factor authentication [2] can be complex and may require specific software. The adoption of this technique by users and organizations may require time and effort.

To overcome all the drawbacks of the above-mentioned system, we proposed a system using fingerprint to authenticate the user. At the time of payment, the user is required to enter PIN and authenticate the fingerprint to make the payment.

In Paper [1] there are some parameters, Comprehensive Evaluation: The research provides a detailed evaluation of MFA solutions in online banking by considering multiple criteria, including compliance, security, and usability. Global Perspective: The study covers banks from different countries, offering a global perspective on the state of MFA adoption in the banking sector. Novel Complexity Metric: The introduction of a novel metric to assess the complexity of MFA protocols provides a unique contribution to the field. Regulatory Impact: The research identifies the potential influence of regulations, like the Regulatory Technical Standard (RTS), on improving the security of MFA protocols in online banking.

In Paper [4] the researchers conducted a comprehensive analysis of various authentication techniques. Their study revealed that single-factor authentication methods are diverse, with smart card-based authentication being the most extensively researched. Furthermore, the study found that multi-factor authentication techniques often combine different single-factor methods, and the combination of text-passwords and smart cards emerged as the most widely studied approach. When comparing and selecting authentication schemes, the researchers noted that usability, security, costs, and contextual factors played pivotal roles. Notably, the research identified a gap in the existing literature as no framework was found that provided an in-depth analysis of both single-factor and multi-factor authentication techniques for decision-making processes.

To overcome all the drawbacks of the above-mentioned system, we proposed a system using fingerprints to authenticate the user. At the time of payment, the user is required to enter PIN and authenticate the fingerprint to make the payment.

4 PROPOSED WORK AND ITS IMPLEMENTATION

This paper's main goal is to increase online transaction security, realizing how important it is to protect sensitive financial data and guard against illegal access. We have created a novel hybrid authentication system that combines various layers of verification throughout the transaction process to achieve this goal. This hybrid system's incorporation of both conventional and biometric authentication techniques ensures a strong and thorough approach to user verification.

4.1 REGISTRATION PROCESS

STEP 1: Open the app and enter email id and password.

STEP 2: The email id is verified by sending an OTP via mail.

STEP 3: Enter the OTP sent via email.

STEP 4: If verification fails, repeat step 1.

STEP 5: Upon successful verification, set PIN and enroll fingerprint biometric.

STEP 6: Store the information in the database.

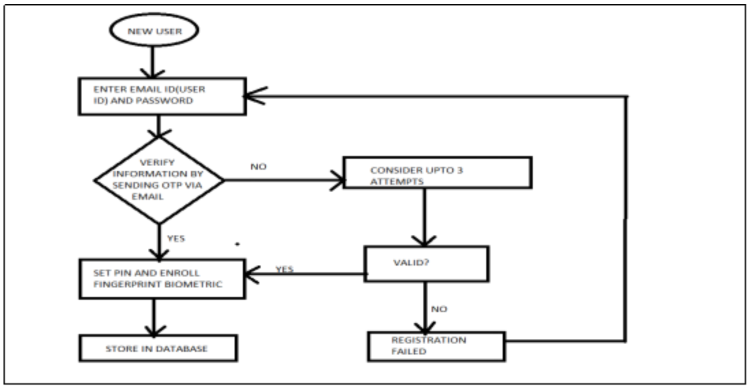
NEW USER
ENTER EMAIL ID(USER ID) AND PASSWORD
VERIFY INFORMATION BY SENDING OTP VIA EMAIL
NO
CONSIDER UPTO 3 ATTEMPTS
YES
SET PIN AND ENROLL FINGERPRINT BIOMETRIC
YES
VALID?
NO
STORE IN DATABASE
REGISTRATION FAILED

Fig. 1. User Enrollment Process

4.2 TRANSACTION PROCESS

STEP 1: Open the app and enter email id and password.

STEP 2: Choose operation.

STEP 3: For transaction, choose payee and enter the amount.

STEP 4: Next enter the PIN.

STEP 5: If valid, proceed to fingerprint authentication.

STEP 6: If PIN does not match, repeat step 3 (only 3 attempts allowed)

STEP 7: If fingerprint authentication fails, repeat step 4 (only 3 attempts allowed)

STEP 8: If fingerprint authentication is successful, the transaction will be successful.

Our hybrid approach includes a second level of protection by using fingerprint authentication which aims to enhance the security of online transactions while offering seamless and user-friendly experience. Since fingerprint patterns are unique to everyone, the user is asked to verify their identity using fingerprint authentication. The two factors process not only improves the overall security posture but also increases user trust in the transaction system.

The implementation can be done using mobile integrated development environment. Since the system depends on the built-in fingerprint sensors used in mobile phones to function, external hardware won't be required. This method uses the built-in capabilities of mobile devices to provide a simple and easily accessible solution without requiring the inclusion of new hardware. The development will be optimized for Android systems, offering a productive and easy-to-use interface. The integration of inbuilt fingerprint sensors enhances the system's security and convenience, aligning with the widespread availability of this technology in modern smartphones.

5 FUTURE SCOPE

As a future scope we are planning to implement iris recognition to our proposed system. The main reason of using iris recognition

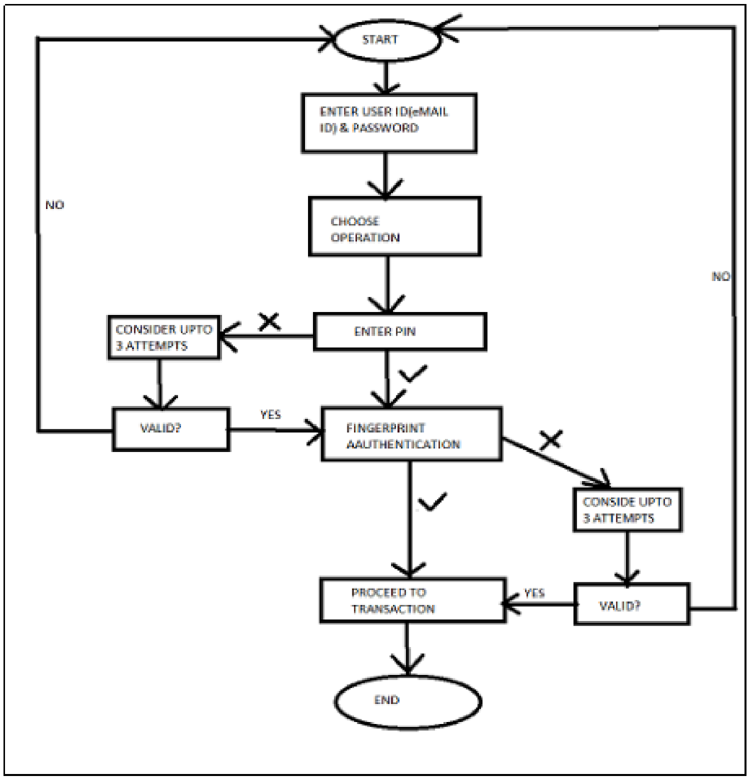

Fig. 2. Process before Transaction

is its speed of matching and extreme resistance to false matches. Besides this, we are planning to integrate it with the banking sector and create a real-time application for the industry where transactions happen instantaneously. Therefore, our goal is to make the system more trustworthy, easy to use, and safe for transferring money.

6 CONCLUSION

The implementation of a two-stage authentication system in an organization or application will represent a significant step forward in bolstering security and safeguarding sensitive information. The project is expected to successfully achieve its objectives of strengthening security by reducing the risk of unauthorized access, enhancing the user experience through user-friendly two stage authentication methods, ensuring compliance with relevant security standards and regulations, and establishing ongoing monitoring and improvement processes. The paper's success is expected to be measured by the reduced incidence of account compromises and increased user adoption. This implementation is intended to stand as a testament to our dedication to security and the protection of our organization's assets and user data.

Declaration: The authors declare no conflicts of interest.

REFERENCES

[1] Sinigaglia, F., Carbone, R., Costa, G., & Zannone, N. (2020). A survey on multi-factor authentication for online banking in the wild. Computers & Security, 95, 101745.

[2] Kouraogo, Y., Orhanou, G., & Elhajji, S. (2020). Advanced security of two-factor authentication system using stego QR code. International Journal of Information and Computer Security, 12(4), 436-449.

[3] Dutta, M., Psyche, K. K., & Yasmin, S. (2017). ATM transaction security using fingerprint recognition. Am J Eng Res (AJER), 6(8), 2320-0847.

[4] Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. Information and Software Technology, 94, 30-37.

[5] Bah, C. U., Seyal, A. H., & Yahya, U. (2021). Combining PIN and Biometric Identifications as Enhancement to User Authentication in Internet Banking. arXiv preprint arXiv:2105.09496.

[6] Garg, R., Gupta, M., Amin, R., Patel, K., Islam, S. H., & Biswas, G. P. (2015, December). Design of secure authentication protocol in SOCKS V5 for VPN using mobile phone. In 2015 International Conference on Trends in Automation, Communications and Computing Technology (I-TACT-15) (pp. 1-6). IEEE.

[7] Soares, J., & Gaikwad, A. N. (2016, September). Fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) (pp. 409-414). IEEE.

[8] Sharma, L., & Mathuria, M. (2018, January). Mobile banking transaction using fingerprint authentication. In 2018 2nd International Conference on Inventive Systems and Control (ICISC) (pp. 1300-1305). IEEE.

[9] Prabakaran, D., & Ramachandran, S. (2022). Multi-factor authentication for secured financial transactions in cloud environment. CMC-Computers, Materials & Continua, 70(1), 1781-1798.

[10] Jain, A., Arora, D., Bali, R., & Sinha, D. (2021). Secure authentication for banking using face recognition. Journal of Informatics Electrical and Electronics Engineering (JIEEE), 2(2), 1-8.

[11] Gualdoni, J., Kurtz, A., Myzyri, I., Wheeler, M., & Rizvi, S. (2017). Secure online transaction algorithm: securing online transaction using two-factor authentication. Procedia computer science, 114, 93-99.

[12] Ren, Y., Wang, C., Chen, Y., Chuah, M. C., & Yang, J. (2019). Signature verification using critical segments for securing mobile transactions. IEEE Transactions on Mobile Computing, 19(3), 724-739.