e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

A NOVAL OTP BASED PIN GENERATION AND FACE RECOGNITION METHODS IN ONLINE BANKING

Dr. N. Murali[*1], R. Kalaiselvan[*2], K. Mafrook[*3], R. Harirajan[*4]

[*1]Assistant Professor, EGS Pillay Engineering College, Nagapattinam, India.

[*2,3,4]UG Student, Department Of Computer Science And Engineering, EGS Pillay Engineering College, Nagapattinam, India.

ABSTRACT

In order to fortify the security measures of the online banking system and mitigate the risks associated with malicious access, a multilayer authentication process is proposed. This multilayer approach integrates three distinct verification methods: account number verification, face biometric verification, and OTP (one-time PIN) verification.

Account number verification is the first step in ensuring that users can only access the system with valid account credentials. Face biometric verification is the second step in adding security to the system, requiring the user to authenticate themselves using facial recognition. This reduces the likelihood of unauthorized access even in the event that account details are compromised.

By using a challenge-response method, the OTP verification increases security even more by creating a distinct, one-time PIN for every transaction or login attempt. In order to ensure that the original PIN is hidden and to make it nearly impossible for malicious users to intercept and reuse the OTP, addition mod 10 and a challenge keypad are used to generate this OTP.

Additionally, proactive notifications are implemented to alert users in real-time about any access to their banking interface or significant transactions. These notifications serve as an extra layer of security, enabling users to promptly identify and address any suspicious activity on their accounts.

By combining these multi-layered authentication methods and incorporating proactive notifications, the online banking system can significantly bolster its security posture and provide users with greater confidence in the safety of their financial transactions.

Keywords: Biometrics, Cybersecurity, PIN Entry, Password Authentication, Shoulder Surfing, OTP.

I. INTRODUCTION

The introduction of internet banking has completely changed how people handle their money, providing previously unheard-of accessibility and convenience. However, as technology has advanced, so too have security issues arisen, with fraud and cyberthreats posing serious hazards to both individuals and financial institutions. It is now critical to strengthen online financial systems' security protocols in reaction to these changing threats.

Despite being widely used, traditional authentication techniques like text passwords and static PINs have shown to be vulnerable to phishing, brute force, and credential theft attacks.

In light of this, this research suggests a novel authentication architecture designed especially for online banking platforms. It does this by combining the verification of account numbers, face biometrics, and One-Time Passwords (OTPs).

Through the introduction of dynamic and biometric based verification methodologies, the proposed framework solves the inherent constraints of conventional authentication procedures.

An extra degree of protection is added when an OTP is generated via a challenge-response method, which masks the original PIN and prevents possible eavesdropping or brute-force assaults. By giving users instantaneous alerts about account access and transaction activity, real-time notifications enhance security even more by enabling users to quickly identify and address any questionable activity.

In order to strengthen the security of online banking systems, this article outlines the proposed authentication structure and clarifies the methods used in each authentication tier. The implementation procedure, possible applications, and expected advantages of the suggested framework are also covered, highlighting how

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

important it is to reduce the dangers of unauthorized access and guarantee the integrity of financial transactions conducted online.

II. LITERATURE REVIEW

This project proposal offers a thorough way for integrating face biometric verification, account number verification, and OTP-based PIN generation with several layers of authentication to strengthen online banking security. By utilizing cutting-edge technology, the suggested solution tackles the current issues with internet security and provides a practical and economical framework for protecting financial transactions.

By using the Grassmann algorithm, face biometrics as an alternative to more conventional biometric features like fingerprint or iris scans offer a dependable and practical means of user authentication. This improves security while also making the user authentication procedure easier.

By creating distinct, one-time PINs for every transaction, OTP-based PIN verification which employs a challenge-response strategy with addition mod 10 offers an extra degree of protection. By hiding the original PIN, this technique makes it far more difficult for bad actors to intercept and utilize login credentials improperly.

In addition, the system's proactive notifications guarantee users receive alerts in real time, allowing them to quickly recognize and take action against any suspicious behaviour on their accounts.

All things considered, your project makes a substantial addition to the field of online banking security by presenting a fresh perspective that tackles current issues and offers workable solutions to improve user security and confidence in online transactions.

RELATED WORKS

A overview of the literature on PIN-entry techniques resistant to spyware, videorecording, and shoulder-surfing attacks is given in this section.

1. DIRECT INPUT TECHNIQUES

Previous studies have demonstrated that gaze input or visual distraction techniques are used in direct input methods to try to hide the observer's ability to determine the original PIN. Using a cursor camouflage [5], [6], presenting a random-digit keypad [7], [8], and input distraction techniques like aligning PIN digits together [9] or hitting the relevant number with a deep or shallow pressure [10], visual distraction methods aim to visually distract viewers. Although there are several ways to prevent shoulder-surfing assaults, visual distraction techniques are not impervious to spyware or video-recording attacks, since the attacker can still obtain the original PIN by using the recording tool.

The PIN is entered using the eyes in gaze input methods [1], [2], [3], [4], to reduce the impact of a shoulder surfing attack. These PIN-entry techniques are very impervious to attacks using shoulder surfing. They might lessen the possibility of an attack using videotape even more. However, because customers still divulge the original PIN during the authentication procedure, they are vulnerable to spyware attacks. Furthermore, because gaze interaction techniques fall short of high standards for accuracy, cost, and user pleasure, their use is overly restricted.

2. INDIRECT INPUT TECHNIQUES

In order to foil the adversary, indirect input methods are designed to stop users from disclosing the original PIN at every authentication attempt. The most common example of an indirect input technique is the challenge response strategy, in which the user receives a challenge via a visual, tactile, or aural channel. Subsequently, the user must input a reply based on the issued challenge and the initial PIN.

A number of research investigations have used haptic based [14], [15], and audio-based [11], [12], and [13] challenge-response techniques to protect against malware, video-recording, and shoulder-surfing threats. The challenge is communicated over an auditory channel in the case of audio-based methods and a haptic channel in the case of haptic based approaches. Following that, the user must respond using the original PIN and the challenge they got. As long as the channel used to convey the challenge is secure, these PIN-entry techniques can offer strong defence against spyware, video recording, and shoulder surfing. The response must be entered into an extra channel either haptic or audio in addition to the visible channel when using the audio-based and

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

haptic based techniques. However, as it goes against the PIN-entry method's compatibility criteria, needing an extra channel could hinder the acceptability and adoption of such approaches [30]. Since the focus of this study is on visual-based challenge-response systems, we won't go into further detail about these approaches.

Visual-based challenge-response is a unimodal technique where the challenge and response are transferred over the same visual channel. As a result, this may favor this approach over bimodal challenge response techniques (i.e., haptic and audio-based). For instance, [16] suggests using a visual-based challenge response technique to thwart shoulder-surfing attacks. This technique is comparable to the cognitive trapdoor game method [18], which uses colors to mask user input in place of a 4/6-numeric PIN. Put differently, individuals utilizing these techniques need to input the backdrop colors black or white that are linked to every PIN. However, the video-recording attack is not mitigated by the suggested solution. More specifically, by reviewing the recorded authentication sessions, the attacker can quickly reduce the pool of potential PINs. Furthermore, the suggested method's requirement for numerous rounds to enter PIN numbers may make it less userfriendly.

A challenge-response method with an array of digits (0–9) contrasted with an array of 10 objects was proposed by Lee. The item that is aligned with the first digit of the PIN is known as the session decision key, and it is identified by the user in the first round. The user lines up each PIN digit with the session decision key for the next round. Assume that the item that is aligned with the first digit in the first round, or 1, is , and that the user's PIN is 1234. The user must rotate the object array for the second round in order for the session decision key (i.e.,) and the second PIN digit (i.e., 2) to line up.

How you enter the third and fourth PIN digits is the same. The developed method is vulnerable to a video-recording attack with two recorded sessions, notwithstanding its effectiveness against shoulder-surfing attacks. The fact that entering the PIN requires numerous rounds is a usability constraint of this method. A challenge-response indirect input technique called Align PIN can fend off persistent shoulder-surfing attacks. To complete authentication, a user must line up each PIN number with each challenge digit in each row of a randomly selected 4 × 10 grid of cells. To put it simply, there are four digits in each grid cell: one fixed digit and three randomly selected additional digits. Every static digit has a single occurrence in every row (0, 1, 2,..., 8, 9).

A user must register a reference cell (row, column) during the registration procedure in order to identify the challenge digits while logging in. In order to match the first PIN digit with the first challenge digit in the first row, the user must use the arrow keys. To log in, he must then repeat the identical procedure for the remaining PIN numbers. Align PIN offers 18123, 2023, and VOLUME 11.

F. Binbeshr and associates: Safe PIN-Entry Technique Using One-Time PIN (OTP) to thwart attacks that leverage shoulder surfing. It is still vulnerable to video-recording attacks, though, in which a hacker can obtain the initial PIN by watching two sessions that are recorded. Furthermore, Align PIN is incompatible with the standard PIN entry technique in terms of the interface design and the stored information.

To thwart the shoulder-surfing assault, Zezschwitz et al. [17] devised the SwiPIN indirect input PIN entering method, which gives each keypad number a straightforward, random touch motion. These arbitrary motions are LEFT, RIGHT, TAB, DOWN, and UP. In order to authenticate, the user must draw the movements corresponding to his PIN numbers. The SwiPIN's security and usefulness have been assessed by the writers. Although SwiPIN performs quickly in terms of login time, as demonstrated by the evaluation results, it is vulnerable to shoulder-surfing attacks. To crack the PIN, an attacker must, in particular, be able to identify the user's drawing gestures.

III. RESEARCH METHODOLOGY

A comprehensive analysis of the literature was conducted in order to fully assess the different types of cyberattacks that target the banking industry. "A method of identifying, interpreting and evaluating all existing research related to a specific topic area, phenomenon of interest, or research questions (RQs)" is how the systematic literature review (SLR) is defined.

A. SELECTING RESEARCH DOMAIN

Research papers from a range of digital information sources were carefully examined in order to understand the idea of cybersecurity, identify issues in the field, and learn what experts have done thus far to address the obstacles.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

B. RESEARCH QUESTIONS FORMULATION

To demonstrate the impact of FinTech and biometric systems on the banking industry. Examining the main advantages that the banking sector enjoys from adopting biometrics systems is vital to improve the current system's ability to safeguard the financial sector. Research was conducted on relevant journal articles, conference proceedings, book chapters, and papers that discussed security-related issues in-depth. According to our initial research, cyber security is a major undertaking.

C. STRINGS BASED SEARCHING

The search methodology and keywords are searched as part of the search approach. A series of actions are described in the descriptions. The steps listed below have been finished in order to create keywords. Key words were identified in the recommended study areas. For efficiency, the synonyms of the main terms were eliminated.

D. THE SEARCHING PROCESSES

In order to compile data from numerous cybersecurity research projects for synchronization, the second author of this paper conducted an extensive and in-depth analysis of the suggested study on 4digital libraries.

Phase 1: Four digital libraries are methodically searched in order to locate papers pertinent to the suggested topic. The results of the search were classified as perspective studies.

Phase 2: Articles based on keyword strings are retrieved from these libraries.

Phase 3: The internet digital libraries are mined for pertinent studies. For this SLR process, the top four pre reviewed online repositories have been selected.

IV. THE PROPOSED PIN ENTRY METHOD

Through the use of the challenge-response mechanism, the PIN is entered indirectly in the suggested PIN-entry method. The challenge response method generates an OTP that hides the original PIN by using a mini challenge keypad and the addition mod 10 algorithm. In order to prevent shoulder-surfing and recording assaults, the addition mod 10 is employed to generate equally likely OTP digits, hence eliminating any association between authentication sessions. The challenge keypad is used to send the challenge to the user.

$$OTP = (P + R) \bmod 10$$

A. CHALLENGE KEYPAD

To find the challenge digits, utilize the small random digit keypad called the challenge keypad. It is compatible with a key location as indicated in Figure 1 within the standard keypad.

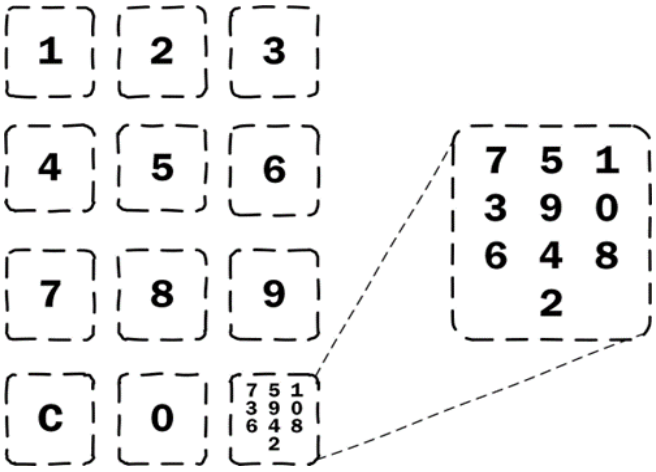


Figure 1. Challenge keypad incorporated within regular keypad

The challenge number, R, has the same amount of digits as the original PIN, but it is generated at random. The user rearranges the R digits during every authentication session. The user must map the PIN key locations on the challenge keypad in order to derive R. As an example, let's say that the user's PIN is 1234 and that the challenge keypad that the server sent is shown in Figure 1.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

To generate R digits (i.e., 7, 5, 1, 3), the user must map his PIN key locations (i.e., 1234) on the challenge keypad (shown in Figure 1). R digits should be arranged in the same sequence as the PIN digits on a standard keypad layout, that is, 1, 2, 3,..., 9, 0; this will prevent sessions from correlating and make it more difficult for an attacker to deduce the initial PIN. Let's say the user sets the PIN to 1472, for instance. The R digits are 7, 3, 6, and 5, same like in Fig 1. It is evident that the mapping of the PIN's second (fourth) digit with its key placement on the challenge keypad yields the fifth digit of the R digits.

To stop the correlation between the authentication sessions, the R digit sequence needs to be reorganized in ascending order depending on the key placements of the PIN digits on the conventional keypad layout (i.e., 1, 2, 3,..., 9, 0). Because digit 2 comes before digits 4 and 7 of the PIN on the standard keypad layout, the fifth digit of the R must be positioned before the third and sixth digits. R is therefore 7536. We note that all users have to do to solve the challenge is to recall their initial PIN. The suggested PIN-entry method's ability to preserve regular PIN compatibility is one of its strong points.

B. HOW THE PROPOSED PIN-ENTRY METHOD WORKS?

1. REGISTRATION PHASE

The user establishes a four-digit PIN password and registers a username during this phase. We stick with a 4-digit PIN in order to simplify our process. It is believed that the registration procedure is secure.

2. LOGIN PHASE

At this phase, the user has to provide their username (i.e., ID) and the OTP to login into the system. Fig 2 shows how the user logs in to the database. The user inputs their username first.

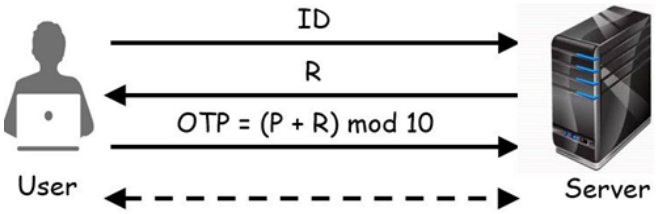


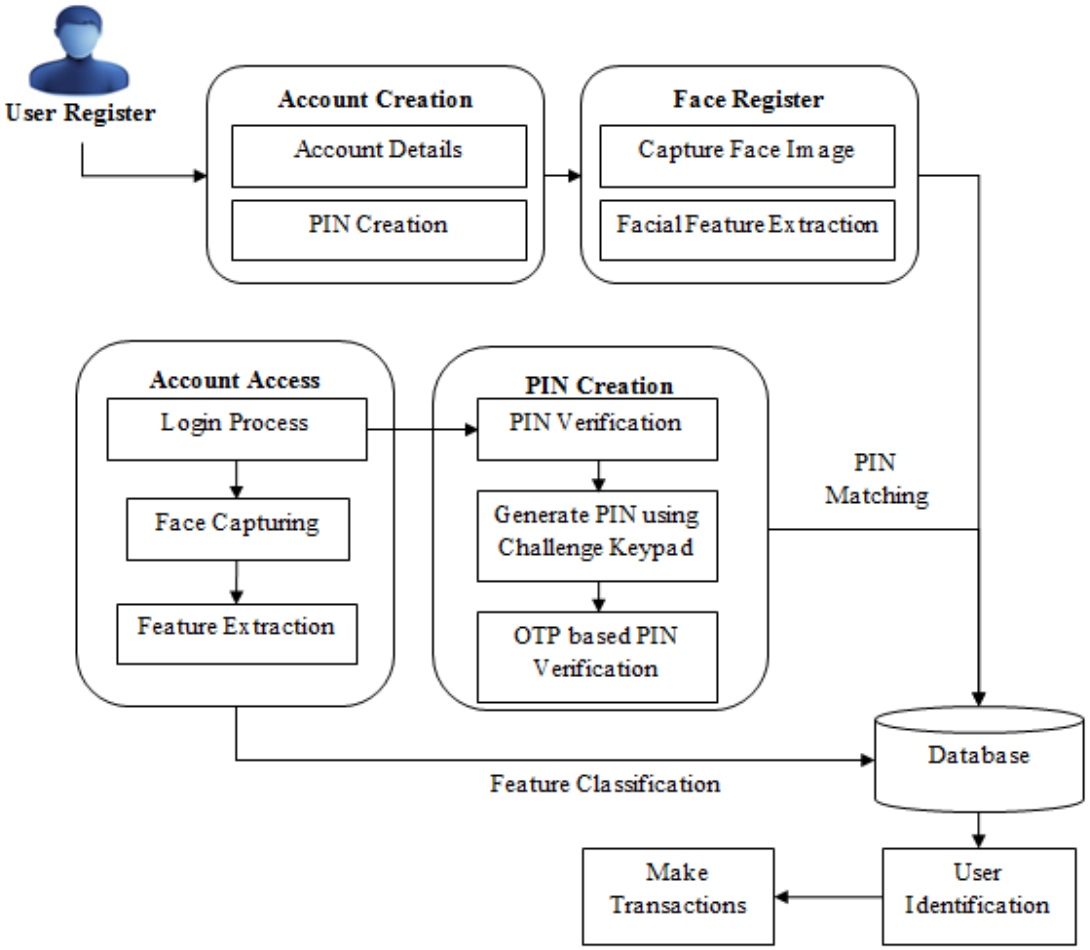
Figure 2. Login phase

The challenge keypad is then sent by the server together with R. Ultimately, the OTP needs to be calculated by the user and sent to the server. Let's take an example where the keypad supplied by the server for authentication is represented by Fig 1. Assuming P = 1472, OTP = 8908 and R = 7536. For example, the first OTP digit is the product of the first P and first R digits added using mod 10, or 1 + 7 mod 10 = 8. To generate the remaining OTP numbers, the user must repeat this step.

When a person commits the PIN digit key locations to memory, figuring out the challenge digits becomes simple. As can be seen in Fig 3a, the challenge keypad's equivalent numbers for the user's PIN of 1472 are 7365. The user must rearrange the PIN numbers (1, 2, 3,..., 9, 0) in consecutive order as shown in Fig. 3b in order to obtain the challenge digits. By now, the user should have no trouble remembering the PIN's digit order. Therefore, 1247 is the new order of the 1472 PIN digits, and 7536 are the equivalent challenge digits.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

ARCHITECTURE



V. EVALUATION AND ANALYSIS

This section outlines the threat model and the user study that was carried out to assess the usability and security of the suggested PIN entry technique. In addition, we present the suggested PIN-entry method's security and usability study and contrast it with alternative PIN-entry techniques.

1. SHOULDER-SURFING ATTACK

The attacker in this kind of attack gathers the authentication session data with his unaided eyes. PINs may be threatened by shoulder surfing in crowded, public areas like trains, airports, and marketplaces. User PINs are entered in a semipublic setting in order to assess the effectiveness of the suggested PIN entry technique against this attack. The attacker is able to watch the authentication session repeatedly since they are close to the user.

2. VIDEO RECORDING ATTACK

We recorded the user's authentication session more than once in this attack by using a camera device. Once these videos have been viewed, the attacker copies the original PIN.

3. SPYWARE ATTACK

The attacker can examine the suggested PIN-entry technique against this attack by having access to all data transmitted during the authentication session, including screen content and user input.

4. GUESSING ATTACK

An attempt to log in using all potential PIN combinations (brute-force attack) or the most popular PINs (dictionary attack) is known as a guessing assault. Analyzing the guessing attack serves the objective of determining how secure the suggested PIN-entry method is against an uninformed attacker. Assuming the attacker has physical access to the device, we can use both approaches to manually guess the 4-digit PIN.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

VI. RESULT AND DISCUSSION

The suggested multi-layer authentication system, which combines face biometric verification, account number verification, and OTP (one-time PIN) verification, is a major step forward in fortifying online banking systems' security protocols.

The online banking system's security is greatly improved by the integration of various authentication layers. The possibility of unwanted access is significantly decreased by requiring users to go through account number verification, face biometric verification, and OTP verification. Potential attackers face more obstacles with every layer added, increasing the difficulty of their attempt to compromise the system.

Text passwords and other traditional authentication techniques are vulnerable to phishing and password cracking, among other issues. The suggested method successfully overcomes these issues by combining face biometric verification and OTP-based PIN generation. OTP-based PIN generation adds an additional layer of security against password related assaults, while face biometric verification offers a more reliable and challenging-to-spoof authentication approach.

The suggested solution strives to provide a smooth and user-friendly experience in spite of the additional security precautions. Face biometrics streamlines the authentication process by removing the need for users to memorize complicated passwords. Furthermore, the original PIN is kept secret thanks to the challenge-response method utilized for OTP generation, which minimizes user irritation while maximizing security.

The system's security posture is further strengthened by the proactive notification implementation. The solution enables customers to take rapid action in response to suspicious activity by promptly notifying them of any access to their banking interface or big transactions. This feature of real-time notifications is very helpful in identifying and reducing fraudulent transactions.

Both admin and user interfaces must be created as part of the online banking system's foundation development. The admin interface gives administrators the resources they need to efficiently handle user accounts and keep an eye on transactions. In the meantime, the user interface provides a smooth and safe platform for users to carry out a range of banking transactions.

Despite the robustness of the proposed system, several challenges and areas for future improvement exist. These may include refining the accuracy and efficiency of face biometric verification algorithms, optimizing the challenge-response approach for OTP generation, and continually updating the system to address emerging security threats. All things considered, the introduction of the multilayer authentication system featuring face biometric verification and OTP-based PIN generation shows a notable improvement in the security of online banking. The solution lowers the possibility of fraudulent activity and illegal access while increasing user confidence in the security of their financial transactions by including these cutting-edge authentication techniques and proactive notification systems

VII. CONCLUSION

To sum up, the suggested multi-layer authentication method, which combines face biometric verification, account number verification, and OTP-based PIN generation, provides a strong answer to the ongoing problems with online banking security. The system greatly improves security measures by utilizing these sophisticated authentication techniques, which lowers the possibility of unwanted access and lessens the dangers related to fraudulent transactions. The integration of face biometric verification provides a cost-effective and reliable means of authenticating users, leveraging the Grassmann algorithm for efficient facial feature recognition. This approach not only strengthens security but also enhances user experience by offering a seamless and intuitive authentication process. Moreover, the innovative OTP-based PIN generation method, employing a challenge-response approach, adds an additional layer of security to the authentication process. By obscuring the original PIN and generating unique OTPs for each transaction, the system effectively guards against interception and unauthorized use of login credentials. Furthermore, the proactive notification system ensures that users are promptly alerted to any suspicious activity, empowering them to take immediate action and safeguard their accounts against potential threats. Overall, the proposed framework presents a comprehensive solution to the complex security challenges facing online banking systems. By implementing multi-layer authentication

methods and proactive security measures, the system not only enhances security but also instills confidence and trust among users, ensuring a safer and more secure online banking experience for all stakeholders.

VIII. REFERENCES

[1] A. T. S. Carneiro, C. E. L. Elmadjian, C. Gonzales, F. L. Coutinho, and C. H. Morimoto, ‘‘PursuitPass: A visual pursuit-based user authentication system,’’ in Proc. 32nd SIBGRAPI Conf. Graph., Patterns Images (SIBGRAPI), Oct. 2019, pp. 226–233.

[2] D. M. Ibrahim and S. Ambreen, ‘‘Gaze touch cross PIN: Secure multimodal authentication using gaze and touch PIN,’’ Int. J. Eng. Adv. Technol., vol. 9, no. 1, pp. 777–781, Oct. 2019.

[3] C. Kumar, D. Akbari, R. Menges, S. MacKenzie, and S. Staab, ‘‘TouchGazePath: Multimodal interaction with touch and gaze path for secure yet efficient PIN entry,’’ in Proc. Int. Conf. Multimodal Interact., Oct. 2019, pp. 329–338.

[4] S. M. H. Krishna, G. Pradyumna, B. Aishwarya, and C. Gayathri, ‘‘Development of personal identification number authorization algorithm using real-time eye tracking & dynamic keypad generation,’’ in Proc. 6th Int. Conf. for Converg. Technol. (I2CT), Apr. 2021, pp. 1–6.

[5] J. D. Still and J. Bell, ‘‘Incognito: Shoulder surfing resistant selection method,’’ J. Inf. Secur. Appl., vol. 40, pp. 1–8, Jun. 2018.

[6] V. Sugumar and P. Soundararajan, ‘‘Cursor masquerade: Masking of authentic cursor using random numeric keypad and spurious cursors,’’ in Proc. 3rd Int. Conf. Adv. Electr., Electron., Inf., Commun. Bio-Informat. (AEEICB), Feb. 2017, pp. 80–84.

[7] M. M. Kabir, N. Hasan, M. K. H. Tahmid, T. A. Ovi, and V. S. Rozario, ‘‘Enhancing smartphone lock security using vibration enabled randomly positioned numbers,’’ in Proc. Int. Conf. Comput. Adv., Jan. 2020, pp. 1–7.

[8] G. Nandhini and S. Jayanthy, ‘‘Mobile communication based security for ATM PIN entry,’’ in Proc. Int. Conf. Comput. Netw. Commun. Technol. Singapore: Springer, 2019, pp. 453–467.

[9] M. Guerar, M. Migliardi, F. Palmieri, L. Verderame, and A. Merlo, ‘‘Securing PIN-based authentication in smartwatches with just two gestures,’’ Concurrency Comput., Pract. Exp., vol. 32, no. 18, Sep. 2020, Art. no. e5549.

[10] K. Krombholz, T. Hupperich, and T. Holz, ‘‘Use the force: Evaluating force-sensitive authentication for mobile devices,’’ in Proc. 12th Symp. Usable Privacy Secur. (SOUPS), 2016, pp. 207–219.

[11] S. Rajarajan, R. Kalita, T. Gayatri, and P. Priyadarsini, ‘‘SpinPad: A secured PIN number based user authentication scheme,’’ in Proc. Int. Conf. Recent Trends Adv. Comput. (ICRTAC), Sep. 2018, pp. 53–59.

[12] Y.-X. Dan and W.-C. Ku, ‘‘A simple observation attacks resistant PIN-entry scheme employing audios,’’ in Proc. IEEE 9th Int. Conf. Commun. Softw. Netw. (ICCSN), May 2017, pp. 1410–1413.

[13] G. Dhandapani, J. Ferguson, and E. Freeman, ‘‘HapticLock: Eyes-free authentication for mobile devices,’’ in Proc. Int. Conf. Multimodal Interact., Oct. 2021, pp. 195–202.

[14] N. Chakraborty, S. V. Anand, G. S. Randhawa, and S. Mondal, ‘‘On designing leakage-resilient vibration based authentication techniques,’’ in Proc. IEEE Trustcom/BigDataSE/ISPA, Aug. 2016, pp. 1875–1881.

[15] M.-K. Lee, H. Nam, and D. K. Kim, ‘‘Secure bimodal PIN-entry method using audio signals,’’ Comput. Secur., vol. 56, pp. 140–150, Feb. 2016.

[16] O. K. Kasat and U. S. Bhadade, ‘‘Revolving flywheel PIN entry method to prevent shoulder surfing attacks,’’ in Proc. 3rd Int. Conf. Converg. Technol. (I2CT), Apr. 2018, pp. 1–5.

[17] E. von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, ‘‘SwiPIN: Fast and secure PIN-entry on smartphones,’’ in Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst., Apr. 2015, pp. 1403–1406.

[18] V. Roth, K. Richter, and R. Freidinger, ‘‘A PINentry method resilient against shoulder surfing,’’ in Proc. 11th ACM Conf. Comput. Commun. Secur., Oct. 2004, pp. 236–245.