International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study on Awareness of Cryptographic PINs as an Authentication Method in Banking Apps

Bindhushree S [1] ***, Dr. Vidhya S*** [2]

[1] PG Student, Department of Commerce (PG), Kristu Jayanti College (Autonomous), Bengaluru
[2] Associate Professor, Department of Commerce (PG), Kristu Jayanti College (Autonomous), Bengaluru
bindhushree.sriram@gmail.com

ABSTRACT:

There is a greater need for safe and convenient authentication techniques as a result of the growing dependence on mobile banking apps. As a possible substitute for conventional authentication methods, cryptographic PINs (personal identification numbers) provide increased security without sacrificing usability. This study investigates how users of banking apps are aware of and use encrypted PINs. We measure user knowledge of cryptographic PINs, perceived security, and willingness to switch from traditional PIN-based authentication to this approach through surveys and interviews. The results show user awareness gaps and point to elements that affect acceptability, such as security worries, usability, and financial institution confidence. The significance of user education and usability enhancements in advancing cryptographic PINs as a workable authentication option in online banking is highlighted by our study.

Keywords : Cryptographic PINs , Banking Apps , User Awareness , Digital Banking , PINs based Authentication , User Perception , Financial Technology

Introduction :

Digital banking's explosive expansion has revolutionized financial transactions by increasing their accessibility and convenience. Significant security issues have been brought about by this change, nevertheless, especially with regard to the authentication techniques used to safeguard user accounts. Although traditional PIN-based authentication is still often used in banking applications, it is susceptible to brute-force assaults, shoulder surfing, and phishing. Cryptographic PINs have become a more secure option in response to these worries, utilizing encryption methods to improve security without sacrificing usability. The degree to which users of banking apps are aware of and comprehend encrypted PINs is yet unknown, despite the potential advantages. Adoption may be hesitant since many users would not be able to tell the difference between cryptography and regular PINs. The use of online banking has become very common as a means of access to accounts and to make various transactions. However, providing online banking access to untrusted devices without user authentication can be exploited by malicious applications on these platforms. The use of two-factor authentication can mitigate this problem. Mobile authentication software tokens are usually used to send one-time passwords but can be subject to the same threat as online mobile banking. The use of a cryptographic personal identification number, which is created in the mobile device, is a more secure approach. The use of Android-based applications was studied together with participants to assess these means of authorizing transactions.

2 REVIEW OF LITREATURE :

A report by Dashlane (2024) indicates a 400% increase in passkey adoption, with one in five active users incorporating at least one passkey into their security measures. This surge reflects a growing awareness and acceptance of passwordless authentication methods among users. Similarly, major tech companies such as Apple, Google, and Microsoft have integrated passkey support, facilitating a broader transition away from traditional PINs and passwords (AP News, 2024).

The European Payments Council's 2024 report emphasizes the importance of implementing two-factor authentication (2FA) in a user-friendly manner to enhance security in mobile payment applications. The report suggests that while traditional PINs are still in use, they are increasingly being supplemented or replaced by more robust authentication methods to mitigate security threats (European Payments Council, 2024).

Despite these advancements, challenges persist. The Guardian (2024) highlights that while new authentication systems offer improved security, they are not impervious to threats such as device theft and sophisticated malware. This underscores the necessity for continuous user education and the implementation of comprehensive security measures beyond reliance on a single authentication method , the trend in 2024 indicates a significant shift towards the adoption of passkeys and biometric authentication in banking applications. This transition is driven by the dual objectives of enhancing security and improving user convenience. However, maintaining user awareness and implementing multi-layered security strategies remain critical components in safeguarding against emerging threats.

Wang et al. (2024) emphasize that traditional, one-size-fits-all cybersecurity education programs are often insufficient due to varying levels of digital literacy and security awareness across user demographics. To address this, the study implemented continuous education campaigns that provided personalized advice and frequent security alerts. This adaptive approach proved effective in increasing users' understanding of cryptographic PINs and their importance in safeguarding sensitive information. The study also revealed that consistent interactions significantly impacted user behaviours, leading to improved security practices across diverse user communities. By tailoring educational content to specific demographic needs, the campaigns successfully bridged the knowledge gap, encouraging users to adopt more secure authentication methods. This aligns with existing literature that suggests targeted educational interventions are more effective than generic awareness programs

Chen et al. (2023) conclude that the success of MFA largely depends on its implementation design. Streamlining the MFA procedure by integrating cryptographic PINs with biometric authentication not only enhances security but also improves user acceptance and compliance. This approach supports the development of more secure and user-centric authentication systems. By leveraging biometrics such as facial recognition or fingerprint scanning, the authentication process becomes more seamless and user-friendly. This aligns with existing research that emphasizes the importance of balancing security with usability to encourage better compliance with security practices.

RESEARCH GAP

Users' awareness and comprehension of cryptographic PINs are still lacking, despite the growing significance of secure authentication in digital banking. Although both biometric and traditional PINs are frequently used, customers frequently don't know about cryptographic PINs, their security advantages, or how they vary from previous authentication methods. The majority of current research focuses on biometric security, two-factor authentication , and password less authentication; however, it does not examine user perception or adoption hurdles unique to cryptographic PINs. In order to increase acceptance and trust in cryptographic PINs as a workable authentication technique, targeted education and usability improvements are necessary, as evidenced by the disconnect between user awareness and technology progress.

STATEMENT OF PROBLEM :

As digital banking grows rapidly, secure authentication methods like cryptographic PINs have become more common. This lack of knowledge increases the chance of unauthorized access and fraud in banking apps. The issue lies in the gap between the security potential of the technology and users' understanding of its strengths and weaknesses. This research aims to explore how much users know about cryptographic PINs in banking apps, their understanding of security features, and how this influences their behaviour. The results will help improve user education and the design of safer authentication systems, ultimately strengthening the security of banking apps and reducing risks related to user mistakes.

SCOPE OF STUDY :

This study's scope includes a thorough investigation of users' knowledge and opinions about the usage of cryptographic Personal Identification Numbers (PINs) for banking application authentication. It examines a wide range of banking app users, looking at things like technology aptitude, banking habits, and demographic traits. The study's objectives are to evaluate user behaviours pertaining to cryptographic PIN usage and maintenance in addition to the degree of awareness regarding these codes

OBJECTIVE :

To evaluate the perceived effectiveness and security of cryptographic PINs compared to other authentication methods.

HYPOTHESIS OF THE STUDY

1. **H_0 (Null Hypothesis):** There is no significant difference in the perceived effectiveness and security of cryptographic PINs compared to other authentication methods in banking apps.
2. **H_1 (Alternative Hypothesis):** Cryptographic PINs are perceived as more effective and secure than other authentication methods in banking apps.

RESEARCH METHODOLOGY :

Primary data for this study was collected using a structured questionnaire distributed via Google Forms to students, employees, and unemployed individuals to assess their awareness and perception of cryptographic PINs in banking applications. A cross-sectional research design was employed, utilizing a non-probability convenience sampling method to ensure a diverse representation of banking app users. The questionnaire covered demographic details, awareness levels, perceived security, and willingness to adopt cryptographic PINs. Data analysis was conducted using SPSS software, with descriptive statistics summarizing responses and ANOVA used to test the hypothesis regarding the perceived security and effectiveness of cryptographic PINs compared to traditional authentication methods. A pilot test was conducted to ensure reliability, while content validity was established through expert consultation. Ethical considerations, including informed consent, confidentiality, and voluntary participation, were upheld to protect respondents' rights. Despite potential limitations such as sampling bias and reliance on self-reported data, the study provides valuable insights into user perceptions of cryptographic PINs and their potential adoption in banking application.

RESULTS AND DISCUSSION :

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Do you think cryptographic PINs are necessary for ensuring the safety of your banking apps?	Between Groups	13.864	3	4.621	6.450	.000
	Within Groups	72.365	101	.716		
	Total	86.229	104			
How secure do you think Cryptographic PINs are compared to regular PINS?	Between Groups	46.567	3	15.522	16.684	.000
	Within Groups	93.966	101	.930		
	Total	140.533	104			
Do you think cryptographic PINs are more secure than other authentication methods, such as passwords or biometrics (fingerprint, face recognition)?	Between Groups	28.254	3	9.418	15.148	.000
	Within Groups	62.794	101	.622		
	Total	91.048	104			
Do you prefer using Cryptographic PINs for authentication in banking apps over traditional methods like regular PINs or passwords ?	Between Groups	30.471	3	10.157	21.785	.000
	Within Groups	47.091	101	.466		
	Total	77.562	104			

INFERENCE

The second objective of this study was to evaluate the perceived effectiveness and security of cryptographic PINs compared to other authentication methods in banking applications. ANOVA analysis was conducted to determine whether users perceive cryptographic PINs as more secure and effective than traditional authentication methods, such as regular PINs, passwords, and biometric authentication. The results showed statistically significant differences in user perceptions across all evaluated aspects, with p-values of 0.000 in multiple comparisons. Specifically, users believe that cryptographic PINs offer greater security than traditional PINs (F = 16.684, p = 0.000) and are a preferable authentication method compared to passwords and biometrics (F = 15.148, p = 0.000). Additionally, a strong preference for cryptographic PINs over traditional methods was observed (F = 21.785, p = 0.000).

Since all p-values are below the significance threshold of 0.05, the null hypothesis (H_0), which states that there is no significant difference in the perceived effectiveness and security of cryptographic PINs compared to other authentication methods, is rejected. The alternative hypothesis (H_1), which states that cryptographic PINs are perceived as more effective and secure than other authentication methods, is accepted. These findings indicate that users generally recognize cryptographic PINs as a superior security feature. However, despite this positive perception, some users may still prefer traditional methods due to familiarity or convenience. To further enhance adoption, banks should emphasize the advantages of cryptographic PINs through security awareness campaigns and ensure that their implementation remains user-friendly. By addressing user concerns and promoting ease of use, financial institutions can encourage broader acceptance and trust in cryptographic PINs as a secure authentication method.

FINDING:

- **Awareness Disparity** – The study reveals a lack of widespread awareness regarding cryptographic PINs, particularly among users with lower digital literacy.
- **Perceived Security** – Users who are aware of cryptographic PINs generally perceive them as more secure than traditional PINs and passwords. Statistical analysis (ANOVA) confirms a significant preference for cryptographic PINs over conventional authentication methods.
- **Adoption Barriers** – Despite the security advantages, some users hesitate to adopt cryptographic PINs due to usability concerns, lack of familiarity, and reluctance to shift from traditional methods.
- **Demographic Influence** – Factors such as age, education level, and occupation significantly impact awareness and acceptance of cryptographic PINs. Younger and tech-savvy users are more inclined to adopt them.
- **Security vs. Convenience** – While security is a top priority for users, they also seek ease of use. The study highlights the need for a balance between security and usability to encourage broader adoption.

SUGGESTION:

- **User Education Campaigns** – Banks and financial institutions should implement awareness programs to educate users about cryptographic PINs and their benefits.
- **Improved UI/UX Design** – Banking apps should enhance user-friendly interfaces to make cryptographic PIN authentication more intuitive and accessible.
- **Integration with Biometric Authentication** – A multi-layered security approach, combining cryptographic PINs with biometrics, can enhance both security and user convenience.
- **Personalized Security Recommendations** – Providing users with customized security tips based on their behaviour and preferences can encourage adoption.
- **Regulatory Support & Standardization** – Financial regulators should encourage the adoption of cryptographic PINs through policy guidelines and security standards.

CONCULSION:

The study on the awareness and adoption of cryptographic PINs as an authentication method in banking applications highlights several key findings that underscore the importance of security, education, and user perception in digital banking. As financial institutions continue to embrace digital transformation, the implementation of robust authentication mechanisms such as cryptographic PINs has become critical in ensuring secure transactions and protecting user data from cyber threats.

The research establishes that user awareness regarding cryptographic PINs is not uniform across different demographics. Findings indicate that factors such as age, education level, and occupation significantly influence knowledge and understanding of cryptographic PINs. While some users exhibit strong familiarity and trust in cryptographic authentication, others lack sufficient exposure, thereby highlighting an awareness gap that needs to be addressed through targeted educational initiatives.

SCOPE FOR FUTURE STUDY:

Future research can explore the long-term adoption trends of cryptographic PINs and their impact on digital banking security. Studies should assess the effectiveness of targeted user education programs in improving awareness and trust in these authentication methods. Comparative usability research can examine how cryptographic PINs perform against biometric authentication and traditional PINs in terms of security and convenience. Additionally, investigating the integration of cryptographic PINs with emerging technologies, such as AI-driven security systems and multi-factor authentication, can offer valuable insights. Research can also focus on demographic and cultural influences on adoption, ensuring that security solutions are inclusive and user-friendly. Regulatory implications and industry policies affecting the widespread implementation of cryptographic PINs should also be explored. Lastly, future studies can analyze their effectiveness in reducing fraud and cyber threats, extending their application beyond banking to sectors like e-commerce, healthcare, and government services.

REFERENCE :

1. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
2. Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *NDSS Symposium 2014*, 23(1), 1–15.
3. Guri, M. (2019). Air-gap security and cryptographic PINs: An analysis of banking authentication vulnerabilities. Journal of Cybersecurity Research, 7(2), 121–137.
4. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). Wiley.
5. Federal Financial Institutions Examination Council (FFIEC). (2021). Authentication and access to financial institution services and systems.