IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Computer Science: Cybersecurity In Online Banking – Studying The Effectiveness Of Multi-Factor Authentication.

Devakinandan Sanapala

Student Researcher

Delhi

1 Introduction

1.1 Introduction

Banking institutions face growing challenges because advanced cyber threats keep advancing in their sector. Multi-factor authentication (MFA) is a critical security measure that prevents unauthorized access and fraud in online banking. MFA authentication method requires multiple authentication elements to verify a user, such as security tokens or biometric authentication combined with one-time passwords. Evidence shows MFA protects internet systems from cyber threats because it provides account security without compromising user convenience. The research investigates actual authentication practices during security breaches for demonstrated MFA's protective characteristics and vulnerabilities in security systems (Aburbeian, M, Fernández-Veiga, & M, 2024). Understanding how MFA functions enable better protection of online banking systems because the internet continues to grow. Financial institutions must establish an ongoing procedure to develop their user account security systems, since cyber threats grow, so they need progressive authentication methods. Modern authentication systems, which adjust their security methods to defend bank users against ongoing threats, yet maintain convenient banking web service access.

1.2 Background

The growth of digital banking has made it possible to ease the transplantation of financial transactions by utilizing convenience for users and leaving them vulnerable to increasing cyber threats. Cyber-attacks use phishing, malware, and credential theft to get past security precautions, rendering traditional password-based

and adequate. In response banks have introduced multi-factor authentication (MFA) to improve security. MFA wants clients to confirm their identification by different elements as knowledge (codes) holding (OTP, equipment tokens) and inherence (individual biometrics). As immigration increases, user reluctance, implementation expenses, and evolving cyber assaults remain (Venkatasubramanian, et al., 2024). This research article investigates the evolution of MFA, how it reduces fraud, and its shortcomings. Knowing these factors is part of the unsafe cyber guidelines in online banking and safe files of users' online transactions.

1.3 Research Objectives

- Determine the impact of MFA to prevent fraud and unauthorized banking.
- Assess the advantages and limitations of MFA systems with user interface quality, expenses, and protection weaknesses.
- Assess cyberattacks on the effectiveness of MFA in online banking security.

1.4 Research Questions

- How do multi-factor authentication methods help mitigate cyberattacks that include online banking?
- What effect has multi-factor authentication had on the security of online banking against criminals?
- What are the main benefits and drawbacks of the multi-factor authentication?

1.5 Relational

Multi-factor authentication (MFA) is a key to securing online banking with a multi-layered verification. Its connection to banking security is about minimizing the risk of unauthorized access, phishing attacks, and identity theft. As threats to the cyber world constantly evolve, the contemporary traditional password authentication model fails to secure the authentication feature, making MFA as an additional security necessity. Though, its process brings forth drawbacks about the consumer entitlement, cost, and potential vulnerabilities such as sim swapping & phishing resistant systems. Through previous cyber breaches, and authentication measures, this research paper considers how MFA contributes to improving banking security (Ogbanufe, M, Baham, & C, 2023). Understanding its efficiency and limitations will enable financial organizations to adjust their protective measures and maintain a balance between the comprehensiveness of protection and user-friendliness of access to banking systems.

1.6 Hypothesis

Null Hypothesis (H_0): Multi-factor authentication (MFA) is of little assistance in the fight against cyber threats against online banking.

Alternative Hypothesis (H_1): Multi-factor authentication (MFA) improves security, with a reduction of unauthorized access to online banking and cyber fraud.

1.7 Significance of the Study

The study evaluates the effect that MFA procedures have on improving the security of online banking systems. The rise of cyberattacks through phishing and stolen credentials for financial fraud makes password security an insufficient protection measure. MFA protects security, but organizations encounter three obstacles, including user resistance, expense costs, and evolving cyber threats. This study analyzes real bank security incidents to show how MFA acts as prevention with important MFA advantages and limitations. MFA is an educational protective cybersecurity defense system that studies its operations to guard online banking systems against threats for teaching purposes (Hassan & F, Boosting Ecommerce Security: Implementing Multi-Factor Authentication (MFA) and Advanced Cyber Forensics, 2021). Building banking frameworks for protection purposes requires service operators to understand these core elements to safeguard digital trust and information security for customers.

1.8 Limitations

Multi-factor authentication (MFA) shows effectiveness in online banking security, but it comes with various restrictions to its implementation. Users face the major drawback of inconvenience when MFA requires extra authentication measures, which leads to diminished adoption rates. User experience becomes inconvenient when they need to use authentication mechanisms such as biometrics with one-time passwords (OTPs), which cause security fatigue. The security provided by MFA remains vulnerable because cybercriminals use SIM swapping and phishing-resistant bypass approaches to bypass security measures and conduct man-in-the-middle attacks during online transactions (Hassan, A, Shukur, & Z, 2021). The integration of MFA by financial institutions faces expenses from two angles: financial costs related to system infrastructure development and security measures upgrades. Users who need mobile authentication will experience accessibility problems because of limited connectivity in certain regions. Security improvements through MFA do not solve every cyber threat in online banking systems, yet continuous development of complementary protections remains essential. Knowledge of these authentication system boundaries helps researchers create better security tools, maintain an equilibrium between safety comfort and universal banking access.

2 Literature Review

2.1 Evolution of Cybersecurity in Online Banking

According to (Ojo & S, 2024) Online banking growth enabled financial institutions to provide banking services across geographical locations. Online banking security emerged as an absolute necessity because the digital revolution created rising cyber security dangers for banking users. As online banking launched its first systems, they relied exclusively on username-password authentication for security purposes. The single-factor authentication security methods proved ineffective when cyber criminals developed complex methods

to break these approaches. Modern cyber attackers have updated phishing malware keyloggers and identity theft methods to steal financial information to unauthorized account access. Security solutions at financial institutions advance because social engineering attacks combined with credential stuffing methods to their systems to threats. Secure socket layer (SSL) protocols with encryption technologies and fraud detection systems operate at research institutions to guard data confidentiality. The implementation of multi-factor authentication (MFA) stands as the most critical security enhancement in the realm of online banking services. Users need to authenticate with three different authentication aspects when using MFA, which includes knowledge-based passwords with possession-based OTPs or security tokens and inherence-based biometric verifications. When data protection requires multiple authentication factors, it becomes one of the top security solutions that prevent cyber scams from unauthorized access (Ojo & S, 2024).

According to (Muir, et al., 2024) Security systems remain vulnerable against evolving cyberthreats; therefore, authentication strategies are needed to advance their capabilities. Security specialists working in information security have found distinct ways to bypass MFA systems using sophisticated phishing attacks and SIM swapping techniques, thus validating the need for upgraded security protocols. Safe digital finance transactions require advanced protective measures because opponents continue enhancing their cyber threats against banking systems. Online banking needs to make its security measures continuously adaptive against threats as financial technology continues to develop. Artificial intelligence working with machine learning enables cyber criminals to implement deepfake technology and automatic password stealing as combined fraudulent methods. When people use mobile banking applications, they have to contend with two security threats, their mobile operating system issues and the security concerns when connecting through public Wi-Fi networks. Participating financial institutions show continuous interest in blockchain technology because its transaction protective attributes help prevent fraudulent occurrences. Lack of international regulatory standards motivates banks to establish advanced security infrastructure systems. Research employees act as pivotal elements in shaping online banking security by identifying threats and creating upcoming security solutions.

2.2 Effectiveness of MFA in Preventing Cyber Threats

According to (Hossain, A, Raza, & A, 2023) MFA is an essential security system for online banking because it successfully decreases fraud risks and unapproved system entries. Financial institutions and banks continue implementing MFA to enhance their cyber security frameworks because the approach protects sensitive banking data from threats. Multiple research and field tests show MFA functions as an effective security tool because it implements various authentication methods to standard passwords for protection. MFA strengthens online banking security through authentication processes requiring multiple verification elements, which people can present as knowledge-based passwords/PINS and possession-based OTPs or security hardware or inherence-based biometric authentication such as fingerprint or face recognition. The layered security design minimizes unauthorized access because attackers must overcome multiple verification methods while

all attackers must submit to only one authentication. The adoption of MFA by banks leads to decreased successful cybersecurity breaches, when hackers use stolen passwords or brute force methods for attacks. Security breaches provide the most convincing evidence of Multi-Factor Authentication (MFA). Protected banking institutions confronted severe data breaches when they depended on passwords only, which resulted in substantial financial losses with numerous compromised user accounts. The integration of MFA authentication systems by banks decreased the occurrence of successful cyberattacks. Living proof comes from financial fraud investigations showing MFA successfully stops automated hacking attempts which operate through credential stuffing methods 99% of the time.

According to (Moepi, L, Mathonsi, & E, 2021)MFA systems encounter constant evolution from cybercriminals who aim to find ways around the security measures. The primary method attackers use to gain unauthorized access is social engineering, through which attackers deceive people into sharing account access. SIM swapping represents a threat that allows hackers to commandeer phone numbers related to MFA applications. Fraudulent hackers use deception to force mobile carriers into relocating targeted customers' phone numbers to their devices so they can break into financial accounts through intercepted OTPs. The current system weaknesses underline an essential requirement to regularly advance MFA protection approaches. Financial institutions enhance MFA security with user behavioral biometrics to help AI-based fraud detection systems. Behavior patterns through user activities that include typing speed, movement, and touchscreen gestures enable the detection of suspicious behavioral indicators of possible fraudulent activity. The automatic security risk assessment system triggers additional security procedures when it detects atypical user behavior. Continuous development of MFA technology and end user education remain essential to achieve its success as an anti-attack solution for online banking systems. Customer account protection requires banks to train people about fake message identification while emphasizing enhanced security for authentication details. MFA is a permanent defense system for online banking security because it advances in parallel with modern security technologies.

2.3 Challenges in MFA Implementation

According to (Sarower, et al., 2025) the deployment of MFA provides online banking protection, various implementation obstacles must be addressed to succeed in deployment. Multiple implementation obstacles affect financial institutions due to user resistance to change, high deployment expenses, plus the ongoing evolution of malicious cyberspace threats. The adoption of MFA depends on strategic updates which combine innovative approaches to prevent cyber fraud during its implementation phase. Users create the primary barrier to MFA implementation, as they resist new authentication procedures. At the same time, they resent the extra inconvenience. Several authentication steps create issues for users, which reduced acceptance because users become annoyed with the process. Fast banking transactions leave customers unimpressed with Multi-Factor Authentication since they need to deal with security tokens or mobile phone-based OTPs for second authentication. Biometric authentication poses issues to users because fingerprint recognition and

face recognition systems on the available hardware are unreliable. The difficulties of security authentication for guests will push them toward less secure systems that expose the organization to security dangers.

According to (Dahiya, P, Kant, & U, 2025) The implementation of MFA poses two main barriers to institutions, which include high implementation costs and complex technical requirements. To achieve smooth MFA implementation, financial institutions should budget funds for advanced authentication system development, secure databases, and fraud monitoring software implementations. High-level security measures come with financial requirements that prevent small banking institutions and their mid-sized counterparts from implementing advanced security applications, which results in elevated cyberattack vulnerability. The operation of MFA platforms requires continuous updates and platform maintenance support from IT experts at elevated costs. This support increases overall operational expenses. Network-based threats are evolving rapidly, which makes banking institutions increase their security efforts through constant process development. Cybercriminals develop subversive tactics that mix SIM swapping with phishing attacks and session hijacking to avoid MFA security protocols. SIM swapping represents phone number transfers by attackers on mobile carrier platforms to permit them access to OTPs, thus allowing them to take over banking accounts. Better and flexible authentication solutions must be created due to escalating digital threats.

3 Methodology

3.1 Introduction

The research outlines an evaluation method for understanding how multi-factor authentication (MFA) stands in online banking cybersecurity. User responses, security awareness, and fraud prevention abilities form the basis of the online questionnaire's research data. The research sample comprises 50 participants who belong to two groups that use online banking services and work as cybersecurity professionals. The study encompasses quantitative research design matched with sampling approach, data collection methods, and data analysis procedures (Morake & A, 2021). The research method gives an extensive analysis of MFA's security value in online banking and recommends improvements.

3.2 Research Design

The research employs quantitative analysis to understand multi-factor authentication (MFA) operation in online banking cyber security systems. The research implements a descriptive design method to collect numerical data about user security incidents with authentication reliability findings. The research use survey through online Google Form containing Likert scale questions to gather participant ratings about their perceptions. The investigation provide results in the form of pie chart with the percentage about participants feedback. Primary data collection for this study depends on structured questionnaires as the research instrument.

3.3 Sampling Strategy

The participants for this research are those who currently use online banking and have cybersecurity knowledge. Bank clients and cybersecurity experts form the peer group with their dual roles as financial analysts and bank clients. The study includes expert to determine how MFA protects users from unauthorized activity and fraudulent attempts (Aburbeian, M, Fernández-Veiga, & M, 2024). Data validity emerges from the sampling strategy, which collects diverse opinions from numerous prospects.

Sampling Technique

Purposive sampling method was used because the participants demonstrate an authoritative understanding of cyber protection in banking systems. People who joined the study have essential MFA understanding and practical experience, which bolsters validity

Sample Size

The analysis based on sample size with 50 individuals using online bank accounts together with security expertise. The study required 50 participants whose evaluations served multiple research purposes regarding MFA functionality. The sample design featuring identical representation of banking customers and security experts provides researchers with the capability to examine both system usability and protective security aspects properly (Obaidat, et al., 2020).

3.4 Data Collection Method

Primary Data Collection

It provides responses through an online Google Form containing closed-ended questions presented on Likert-scale format. The research questionnaire evaluates whether MFA security techniques effectively strengthen the overall security level of online banking.

Questionnaire Design

- The research gathers demographic data about participants regarding their age characteristics together with gender along with work and history of using online banking services for an understanding of their security awareness levels.
- Users' acceptance of authentication tools as well as reliability and usability are measured through examinations of MFA security methods including biometric methods and OTPs and security tokens.
- Banking users assess MFA systems for stopping fraud and unauthorized access and boosting security effectiveness through Perceived Effectiveness evaluations.

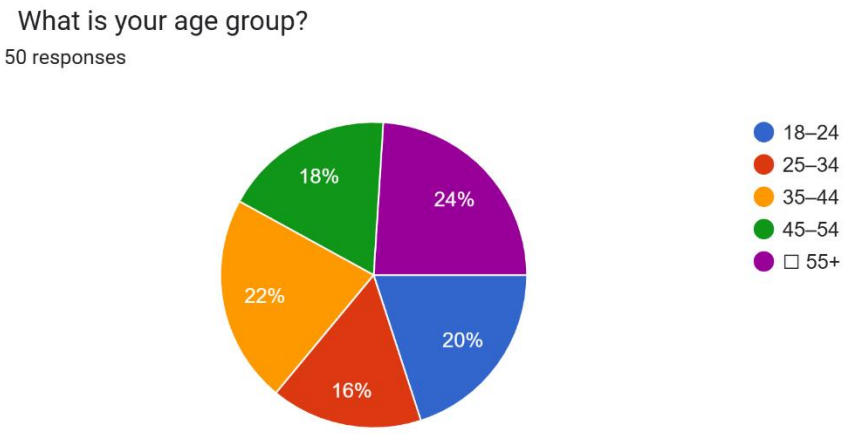
3.5 Ethical Considerations

Ethical standards need to be implemented in the study to maintain both findings' reliability and their accuracy. After receiving confirmation about response confidentiality participants are allowed to make their own decision about joining the research while becoming aware of its research purposes. Research data confidentiality protection maintains both information privacy of participants and the specific uses of study data within defined boundaries (Ali, et al., 2020). The researcher information inside Google Forms Likert-scale questionnaire to access the collected data.

3.6 Limitations

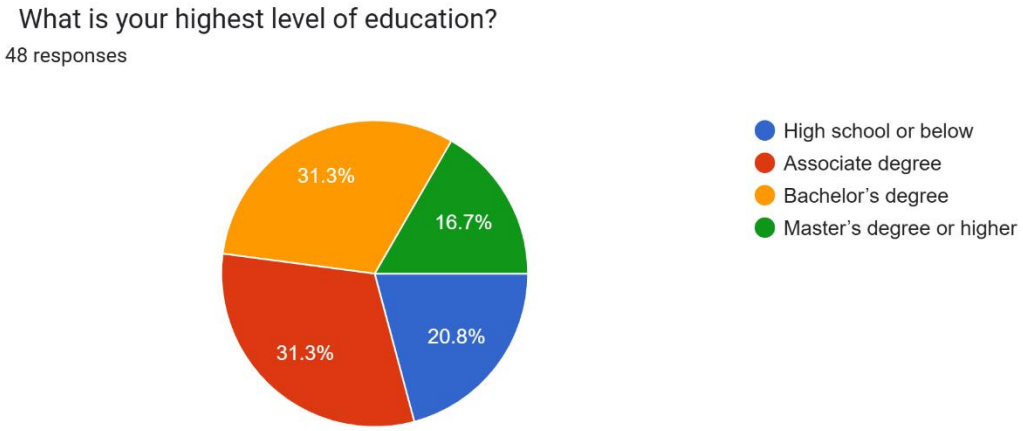
The research evaluation presents information related to MFA systems in online banking along with several restrictions. The study results probably contained biases because users based their input on opinions rather than technical evaluation. Unverified validity stands out in this research because it included a few participants who were surveyed. The implementation of an online information collection method introduced threats to participant engagement since users have different capabilities for accessing the internet and show varying degrees of interest. The research methodology generates thorough analytical results that recognize studying boundaries, but faces specific limitations from the participant diversity aspects (Hassan, A, Shukur, & Z, 2021)

4 Results and Discussion

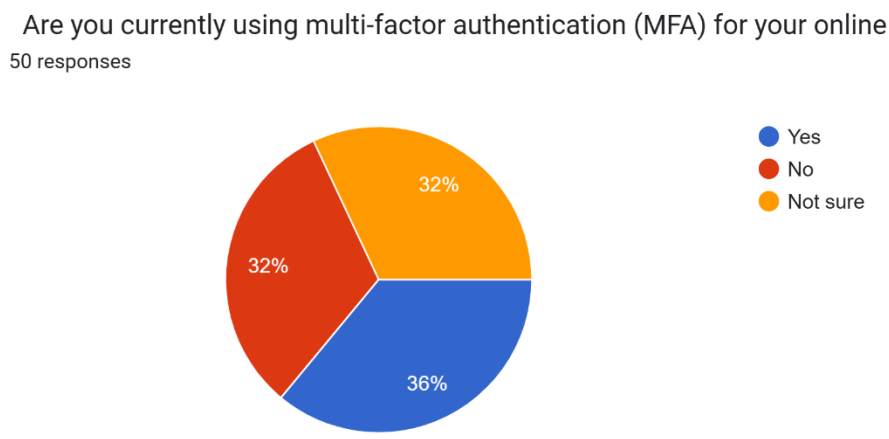


Each segment in the pie chart displays the proportion of different age ranges expressed as percentages. People aged 55 years and older make up the largest portion of 24% while older adults form a substantial segment in the population. The 35–44 age group demonstrates the second largest presence in the population at 22% according to the data. Data shows young adults between 18–24 years constitute twenty percent of the entire

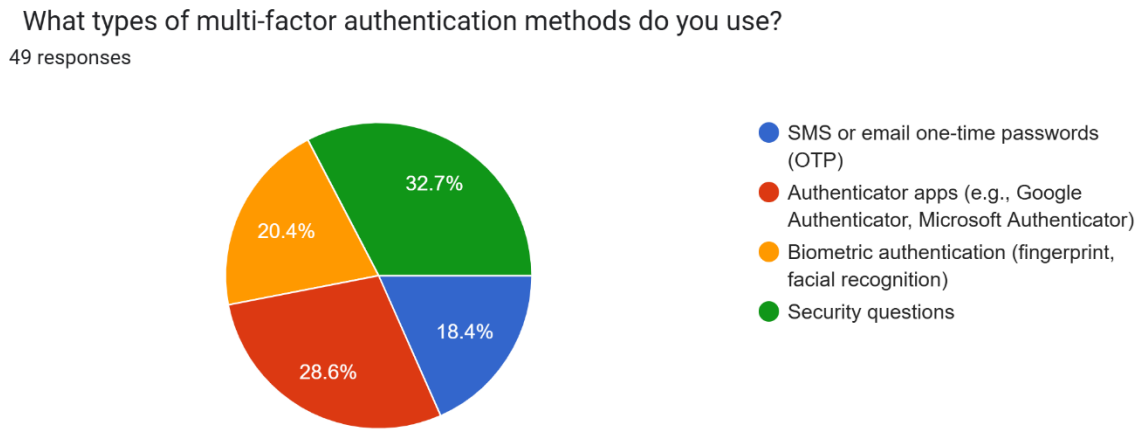
sample group. Nevertheless, the 45–54 age subsection represents 18% of the total population whereas the remaining age groups have slightly higher proportions. Our population survey shows that the age group category 25–34 contains 16% of participants while the remainder of the population segments prefer this early career stage. The dataset shows a balanced distribution among age groups with older people forming the largest portion among different adult demographics.



Research findings show that respondent education levels appear in the pie chart. Statistics show that more than thirty-one percent of respondents finished associate degree programs or bachelor degree coursework, making these levels the biggest individual groups. 20.8% of respondents stopped their education after completing high school. The population segment holding earned master's degrees or higher comprises 16.3% of the total. The survey results illustrate that the bulk of respondents reached higher educational attainment, obtaining associate and bachelor's degrees (Khadka & M, 2022). The composition shows extensive participation in higher education programs, yet the number of people having postgraduate degrees remains relatively small within the available data.

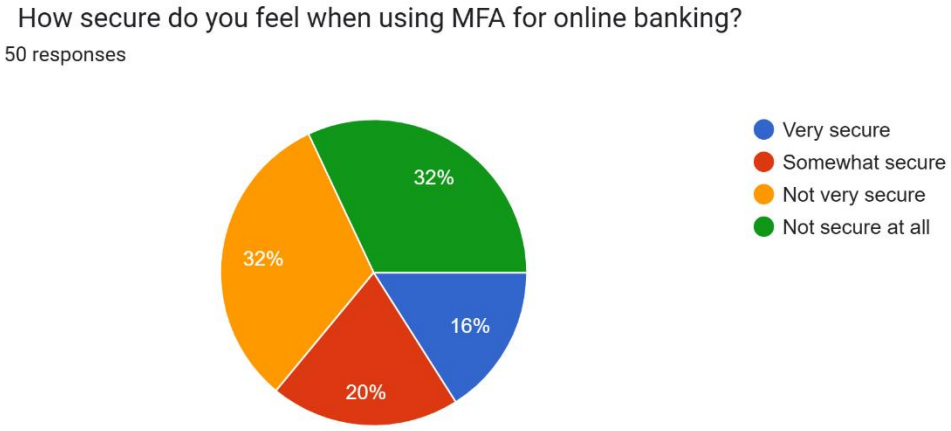


This visual display shows the MFA usage numbers for online bank security among 50 participant bank users. Out of the 50 respondents examined, 36% showed evidence of employing MFA safety protocols, which amounted to one-third of participants taking this extra security step. The results indicate that security risks from single-factor authentication affect 32% of participants because they do not utilize MFA. The survey revealed that 32 percent of respondents stated they were unsure about MFA, while 32 percent did not use it, which indicates insufficient knowledge about MFA security benefits. A total of 64% of respondents demonstrated a concerning level of ignorance regarding MFA status because they lack use or have no knowledge of MFA. The results reveal that financial organizations must increase educational efforts to demonstrate MFA advantages because these benefits currently prevent users from adopting this security method more frequently.

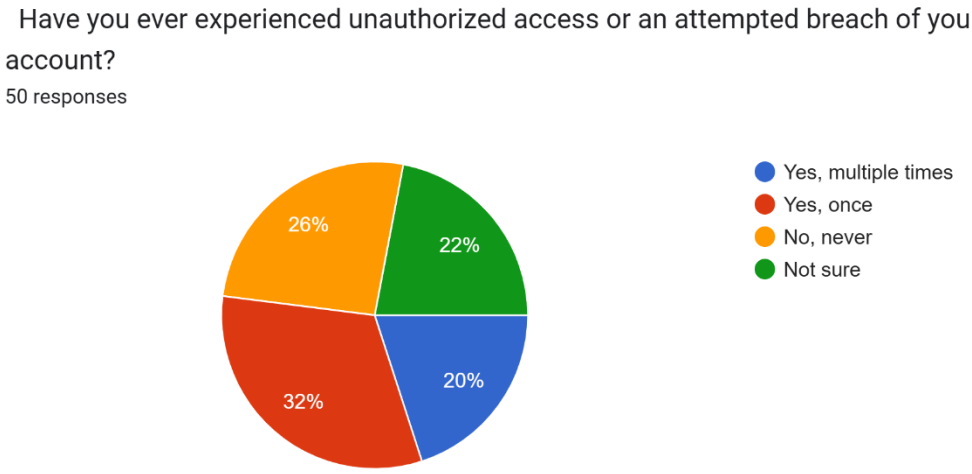


The collected 50 survey responses indicate how respondents implement multi-factor authentication (MFA) methods through this pie chart. The survey found security questions used as the basic authentication method by 32.7% of people even though their security risks are well-documented. Users find authenticator

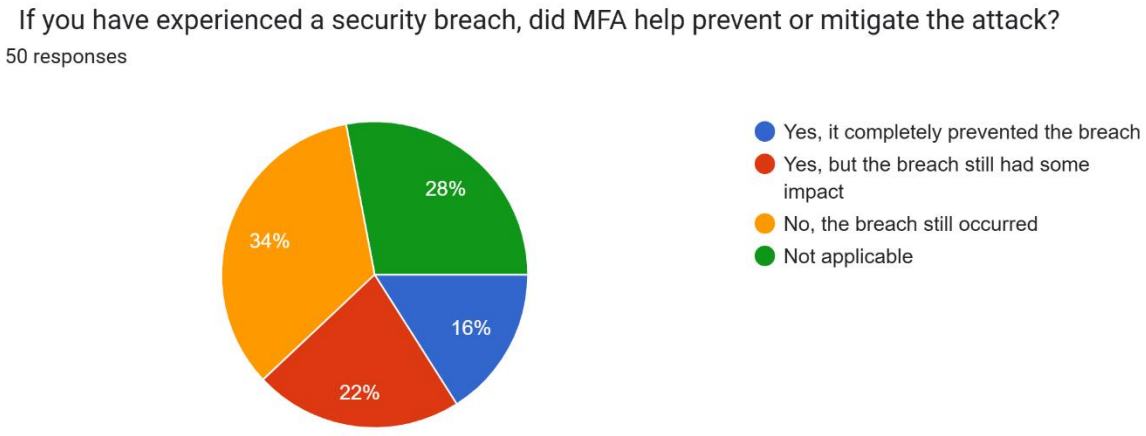
applications from Google and Microsoft the most secure MFA solution since they comprise 28.6% of chosen authentication methods. The integration of fingerprint alongside facial recognition authentication technologies within modern security protocols represents 20.4% of the field, thus demonstrating increasing popularity of modern security authentication measures (Sasikumar, K, Nagarajan, & S, 2025). Coherently 18.4% of respondents depend on SMS or email one-time passwords (OTPs) although many are worried about risks associated with SIM swapping attacks. The research demonstrates that organizations employ either historical or contemporary MFA strategies for authentication management. The usage of security questions and SMS OTPs requires immediate improvements to authentication security measures for protecting cyber systems better.



The graphical display presents how users view security levels during online banking transactions, which implement multi-factor authentication (MFA). The data shows that 16% of users consider their MFA-based online banking security very secure. Users who fall into the 32% category express security concerns about MFA, which may result from phishing attacks and attacks that involve SIM swapping or other cyber threats. The population survey shows another 32% of users express that they feel completely insecure with existing authentication systems. About 20% of employees express moderate trust in MFA, which indicates that they notice possible weak points (Suleski, et al., 2023). The survey results show that although MFA operates widely across banking platforms, its implementation does not establish complete assurance regarding user security. The reasons for users' lack of confidence stem from their knowledge of cyber threats and existing bad experiences with authentication methods. Users require financial institutions to both enhance MFA security measures and increase their understanding of authentication systems to build stronger trust in the process.

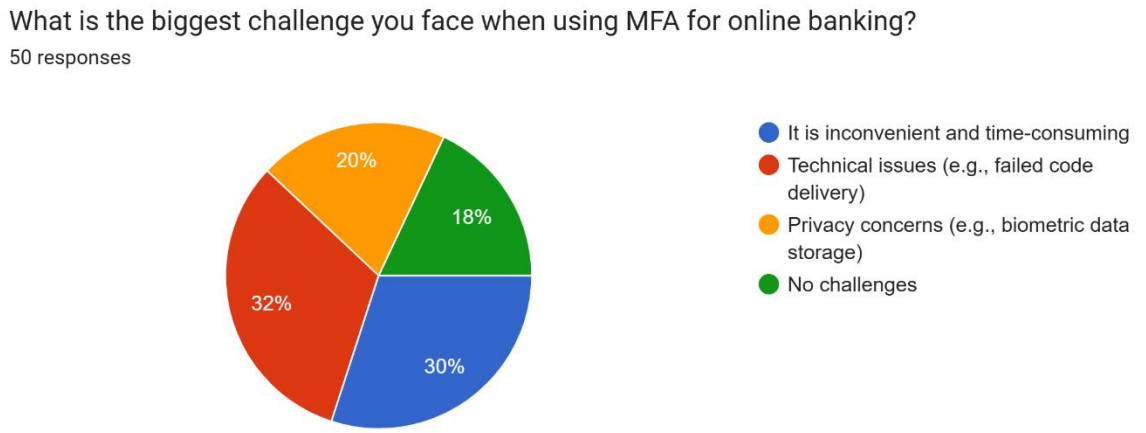


The illustrated chart displays information regarding the number of times individuals experienced unauthorized intruders accessing their online bank accounts. The data indicates that 52% of users encountered a minimum of one security incident, but multiple incidents were experienced by 20% of users and 32% suffered one security event. The figure demonstrates increasing security risks affecting online banking systems. Online banking accounts with complete security exist as only a minority of 26% among all respondents while the rest have experienced at least one security breach. Twenty-two percent of participants are not certain about their accounts' status regarding targeting by criminals, which demonstrates possible confusion about security breaches. Strong cybersecurity practices such as MFA and real-time fraud detection need immediate implementation due to the significant number of users who faced security threats. Financial institutions need to instruct their users better in regards to recognizing and blocking cyber security threats.

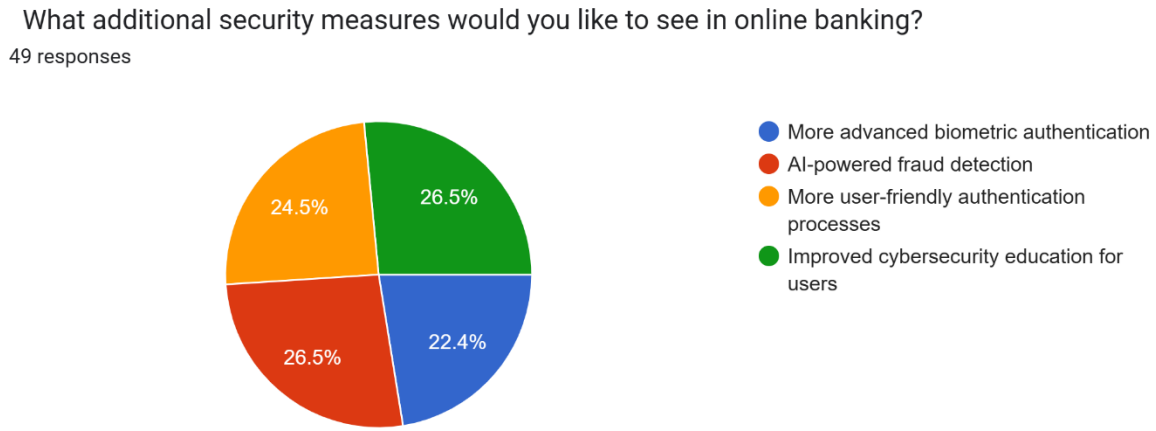


The security breaches from experienced attacks showed their impact on security through the pie-chart. The ability of MFA to stop breaches was rated complete by 16% of participants, although MFA proved effective at stopping attacks. When MFA did help stop breaches, it was partially effective for the 22% of users who reported this outcome. The statistics show alarming results that 34% of people still experienced breaches

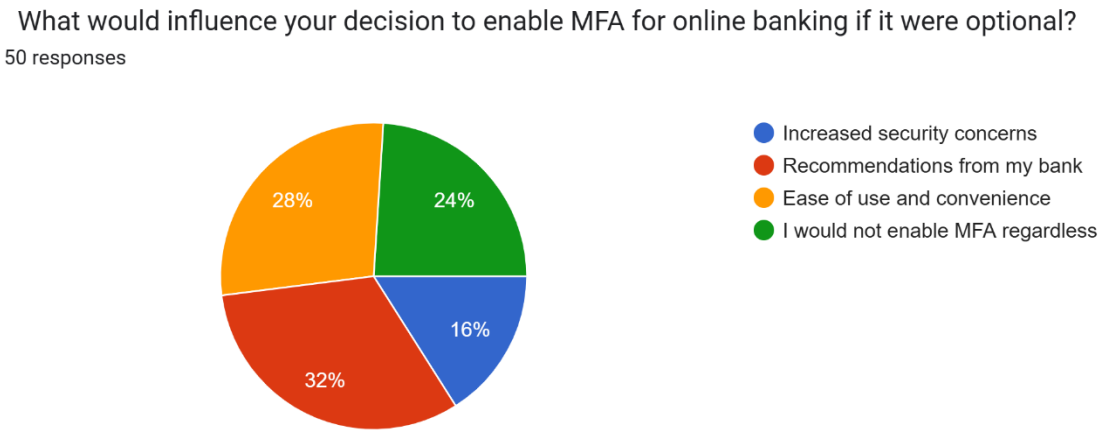
after implementing MFA, which demonstrates that MFA alone cannot stop cyber threats (Ogbanufe, M, Baham, & C, 2023). The group that checked "Not applicable" consisted of 28% of respondents, possibly due to their lack of experience with any security breaches. MFA improves security abilities, but it demonstrates limited effectiveness when it comes to preventing security breaches. Financial companies and their users must combine safe account tracking tools with powerful security codes and improved cyber threat systems to fight online threats better.



The graphic shows what problems most online banking users encounter with multi-factor authentication (MFA). Technical difficulties with code delivery, trouble one-third of customers who report this issue during MFA. The security of MFA gets strong support from 30% of users, but they want less time spent on procedures. The fear about biometric data protection made up 20% of the responses because users remain uneasy about how their personal information is processed. For MFA users, the results show that more than 80% meet challenges with their security feature. Banks and financial institutions need to solve technical and experience issues that make their current MFA systems hard to use. Banks need to make login processes faster and more secure while protecting personal data to get more users to use MFA. Though MFA defends data security from attacks, it needs improvement to make users find the process intuitive and helpful.



The illustration reveals security measures which digital banking users expect their banks to deploy beyond the current security measures in place. Twenty-six-point five percent of users chose a security solution that includes Artificial Intelligence for fraud protection and cybersecurity education for users. People realize technology-enhanced fraud detection requires combined efforts with elementary security education for users to succeed (Al-Sahli, et al., 2024). User-friendly authentication methods outperform strict security measures because they secured the choice of 24.5% of the users who emphasized safety and ease of access during login. Advanced biometric security methods including face and fingerprint scanning appeal to twenty percent of users because they want secure and effortless login processes. Customers desire stronger security safeguards while still choosing authentication procedures that have ease of use. The advent of Artificial Intelligence requires financial institutions to develop protective measures against AI attacks and safe security methods while providing customer education about banking safety to provide secure banking services easily accessible to clients.



Users' choice to opt for multi-factor authentication (MFA) in online banking depends on several factors according to this pie diagram, despite the option being voluntary. Recommendations from the respondent's bank prove to be the number one influence on MFA decisions according to 32% of respondents because users place their trust in banks regarding security guidance. The desire for both simple usage and convenient solutions stands as a strong secondary determinant for letting online banking enable MFA since 28% of users select this factor (Mostafa, et al., 2023). Doubts about security led users to disable MFA functions even though most other users (84%) could have used it. A significant portion of 24% expressed ardent resistance toward MFA despite indicating they would not enable it. This indicates a pervasive reluctance toward extra authentication protocols that stems from hassle or doubts about their security value. The research demonstrates banks need improved communication about MFA benefits because banks must make the technology both secure and easy to use to increase user acceptance.

Discussion

Consumers experience enhanced banking security because MFA implementation is an authentication strategy help in reducing financial losses. MFA provides protection against cyber threats by employing three different verification mechanisms: knowledge-based passwords, possession-based tokens and inherence-based biometrics. The research studied how MFA secures online banking and what protective capabilities it maintains to prevent cyberattacks and the challenges related to each. Security challenges for hackers rise when banks use MFA to authenticate users, which reduces cyberattack dangers effectively. The security benefits of MFA are available but organizations still struggle with its proper implementation. The problems of MFA spreading across systems come from user resistance and technical failures, plus large implementation costs and employee operational hurdles. Users avoid visiting MFA security checkpoints due to their opinion that approval periods run too long.

5 Conclusion

Banks pay for the authentication system care and future systems as they operate. Generally, it appears that increasing cybersecurity protection requires that organizations frequently upgrade the level of their authentications. The integration of AI in fraud detection with behavioral biometrics and the blockchain authentication for a conventional user service, will probably deliver the best security to the financial institutions. People have to know about cyber threats through training because this will help them to learn about which sectors they should protect themselves in their financial affairs. Online banking systems utilize MFA as their primary safeguarding method because various challenges have not diminished its position as an effective security measure. A perfect security system which cannot be compromised by any means does not exist. New banking security development relies on uniting MFA with advanced security solutions and user-friendly authentication procedures that serve as core defenses. Financial institutions must spend money on contemporary security systems that will generate improved digital trust and stronger fraud defense mechanisms, leading to superior security while users conduct online bank transactions.

Research conducted to deploy Multi-Factor Authentication (MFA) as an enhancement of security resilience for online banking against potential threats. Statistical data evaluation of user encounter surveys serves as the foundation to determine security effects in this study. Research protects integrity by implementing protection methods that ensure consent protection, and maintain user privacy, and secure private data. The research analyzed important MFA effectiveness data in preventing fraud, but it had two critical limitations that deteriorated the accuracy of user perception ratings. The author introduces alterations to enhance the internet banking system security evolution, with identifying successful MFA system variables.

Recommendations

To improve MFA performance in the banking sector, adopting AI-based fraud detection, behavioral biometrics, and blockchain-based authentication would be useful due to the increasing security threats such as SIM swapping, and phishing attacks. Further, it is possible to enhance the adoption of the various authentication systems through faithful identification through biometrics, making the system adaptive in the process it provides. Security updates should be regularized to parry new security risks and the environment in which the MFA security system (Kamaruddin, C, Zolkipli, & F, The Role of Multi-Factor Authentication in Mitigating Cyber Threats, 2024). Banks should also provide their customers with information on the safe use of banking services in preventing phishing and related problems. Therefore, stricter measures should be introduced to support the correct implementation of the MFA security policies among the banks. It is thus through such steps MFA can be optimally harnessed in banking to strike the optimum balance of ensuring consumer protection against cyber threats, while allowing customers the ease of access when they are accessing their banking services.

6 References

Aburbeian, M, A., Fernández-Veiga, &., & M. (2024). Secure Internet Financial Transactions. *A framework integrating multi-factor authentication and Machine Learning*, 177-194.

Ali, G, Dida, A., M, Sam, &. E., & A. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. *Future Internet*, 160.

Al-Sahli, A, R., Al-Mutairi, A, Nasr, &., & K. (2024). Secure Authentication System based on Multi-Factor Authentication. *Taibah University. doi*, 10.

Chennuri, & R, K. M. (2024). ADAPTIVE MULTI-FACTOR AUTHENTICATION SYSTEMS: A COMPREHENSIVE ANALYSIS OF MODERN SECURITY APPROACHES. *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET)*, 787-795.

Dahiya, P, Kant, &., & U. (2025). Multi-Factor Authentication Methods in Intelligent Systems. *In Intelligent Manufacturing and Industry*, 142-160.

Hassan, & F. (2021). *Boosting Ecommerce Security: Implementing Multi-Factor Authentication (MFA) and Advanced Cyber Forensics.*

Hassan, A, M., Shukur, &., & Z. (2021). A secure multi factor user authentication framework for electronic payment system. *In 2021 3rd International Cyber Resilience Conference (CRC)*, 1-6.

Hossain, A, M., Raza, &., & A, M. (2023). Exploring The Effectiveness Of Multifactor Authentication In Preventing Unauthorized Access To Online Banking Systems. *Multidisciplinary Science Journal*, 8-12.

Kamaruddin, C, N. H., Zolkipli, &., & F, M. (2024). The Role of Multi-Factor Authentication in Mitigating Cyber Threats. *Borneo International Journal eISSN 2636-9826*, 35-42.

Khadka, & M. (2022). A Systematic Appraisal of Multi-Factor Authentication Mechanisms for Cloud-Based E-Commerce Platforms and Their Effect on Data Protection. *Journal of Emerging Cloud Technologies and Cross-Platform Integration Paradigms*, 12-21.

Moepi, L, G., Mathonsi, &., & E, T. (2021). Multi-factor authentication method for online banking services in South Africa. *In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1-5.

Morake, & A, T. (2021). *A multi-factor authentication approach for e-banking.* South Africa: University of Johannesburg .

Mostafa, M, A., Ezz, M, Elbashir, K, M., . . . W. (2023). Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. *Applied Sciences*, 10871.

Muir, A, Brown, K, Girma, &., & A. (2024). Reviewing the Effectiveness of Multi-factor Authentication (MFA) Methods in Preventing Phishing Attacks. *In Proceedings of the Future Technologies Conference* , 597-607.

Obaidat, M, Brown, J, Obeidat, S, . . . M. (2020). A hybrid dynamic encryption scheme for multi-factor verification: a novel paradigm for remote authentication. *Sensors*, 4212.

Ogbanufe, M, O., Baham, &., & C. (2023). Using multi-factor authentication for online account security: Examining the influence of anticipated regret. *Information Systems Frontiers*, 897-916.

Ojo, & S, O. (2024). Development of a Three Factor Authentication System for Online Banking. *Ajayi Crowther Journal of Pure and Applied Sciences*.

Sarower, H, A., Bhuiyan, T, Hasan, M, M., . . . G. (2025). SMFA: Strengthening Multi-Factor Authentication with Steganography for Enhanced Security. *IEEE Access*.

Sasikumar, K, Nagarajan, &., & S. (2025). Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques. *IEEE Open Journal of the Computer Society*.

Suleski, T, Ahmed, M, Yang, W, . . . E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health*, 9.

Venkatasubramanian, D, Goyal, S, Ezhilarasan, G, . . . P. (2024). Evaluating the Effectiveness of Multi-Factor Authentication for Preventing Cyber Attacks. *In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1-6.