International Journal of Advanced and Applied Sciences

Journal homepage : http://www.ijaas.in

Usability and security in online authentication systems

Randa Allafi, Abdulbasit A. Darem *

Department of Computer Science, College of Science, Northern Border University, Arar, Saudi Arabia

ARTICLE INFO

Article history:
Received 25 September 2024
Received in revised form
28 March 2025
Accepted 20 May 2025

Keywords:
Usability
Security
Multi-factor authentication
Biometric authentication
User experience

ABSTRACT

This study examines the balance between usability and security in electronic online services by comparing the effectiveness and user experience of different authentication methods, including password-only authentication, multi-factor authentication (MFA), and biometric authentication. A mixed-methods approach was used to collect both quantitative and qualitative data through usability tests, surveys, semi-structured interviews, and case studies. The findings reveal a clear trade-off between usability and security. While MFA offers stronger protection, it poses usability challenges, especially for novice users who face more errors and take longer to complete tasks. In contrast, password-only authentication was faster and easier, but was seen as inadequate for protecting sensitive data. Biometric authentication emerged as the most preferred option, receiving high satisfaction ratings from both novice and experienced users due to its balance between ease of use and security. These results emphasize the importance of designing user-centered security solutions, such as increasing the adoption of biometric methods and simplifying MFA to enhance the user experience without sacrificing security. The study offers practical recommendations for developers and security professionals to create more accessible and secure online services.

1. Introduction

Electronic online services refer to the broad spectrum of digital services that are delivered via the internet. These services include, but are not limited to, e-commerce, online banking, e-government, healthcare, and social networking platforms. The rapid advancement of internet technologies, combined with the widespread adoption of mobile devices, has drastically increased the accessibility and functionality of these services. This digital transformation has reshaped how individuals and businesses operate in modern economies, where information is exchanged almost instantaneously, and transactions can be conducted globally with ease (Mihu et al., 2023).

The scope of electronic services encompasses all areas of life, from communication to financial transactions. In today's digital economy, these services are a crucial driver of growth, contributing significantly to the overall productivity of economies. They enable businesses to reach broader markets, reduce operational costs, and enhance customer interaction through real-time communication and data-driven insights. Furthermore, electronic online services facilitate innovation by enabling new business models, such as the sharing economy, digital marketplaces, and fintech solutions, which further transform traditional sectors.

The importance of electronic online services in the digital economy cannot be overstated. They represent a critical component of the digital infrastructure that underpins global commerce. This infrastructure enables businesses to optimize their operations and offer enhanced convenience to consumers, leading to greater efficiency and economic value. As the global economy continues to evolve, electronic online services will remain central to promoting innovation, reducing transaction costs, and fostering greater inclusivity in digital access (Javaid et al., 2024).

Balancing usability and security in electronic online services is one of the most significant challenges in modern system design. Usability focuses on making systems intuitive, efficient, and easy to navigate, while security aims to protect users' data and the system from unauthorized access. However, these two objectives often conflict with each other. As security measures become more stringent, such as the use of multi-factor authentication, complex password policies, or CAPTCHAs, they can reduce usability by increasing friction in the user experience. Users might experience frustration, leading to disengagement or errors, which can, paradoxically, reduce security.

Research indicates that users often lack sufficient knowledge to fully understand the implications of security measures, causing them to make suboptimal decisions when faced with security prompts or settings (Ibrahim et al., 2010; Imbaquingo et al., 2024). Moreover, usability is critical in online services like e-government systems, where overly complex security procedures can limit accessibility and compliance with regulations (Monzón et al., 2020). This issue is not limited to specific sectors; social networking platforms, for example, face similar challenges, as privacy and security often conflict with users' expectations of ease of use and sociability (Zhang et al., 2010).

The result is a trade-off: systems with robust security measures might be more secure, but they risk alienating users if they become too complex to use. Conversely, overly simplified systems might offer a seamless user experience but leave critical security vulnerabilities. As such, striking a balance between these two factors is essential but difficult to achieve. Researchers argue that adaptive security models—where security measures dynamically adjust based on user behavior and risk—may offer a potential solution to this challenge (Furnell, 2016).

Balancing usability and security is critical for the success of electronic online services (Mujinga, 2024). When usability and security are not properly balanced, both the effectiveness of the system and user engagement can be negatively impacted. Poor usability often results in low user adoption, dissatisfaction, and a higher likelihood of errors. On the other hand, inadequate security can lead to serious consequences, including data breaches, financial losses, and damage to trust.

When online services prioritize security at the expense of usability, users may face complex authentication processes, intrusive security measures, or interfaces that are difficult to navigate (Oguta, 2024). This can deter users from adopting or continuing to use the service. For example, research in the e-government sector has shown that overly complex security measures reduce the accessibility and effectiveness of these services, leading to underutilization (Monzón et al., 2020). In contexts such as anonymity networks, bad usability has been shown to reduce the number of potential users, ultimately weakening the system's overall security by decreasing the pool of participants.

In contrast, systems that prioritize usability over security run the risk of exposing users to data breaches, fraud, and other malicious activities. This is especially critical in areas such as online banking, where the personal and financial data of users must be securely protected. Insufficient security in these contexts can lead to significant financial losses, legal repercussions, and damage to an organization's reputation (Feth, 2015). In e-commerce and mobile applications, if security features such as encryption and user authentication are not robust, users' personal information may be exposed to unauthorized access (Nimmi and Janet, 2018).

Therefore, achieving a balance between usability and security is essential to maintain user trust while ensuring that data remains protected. The integration of user-centric security features that enhance the user experience while maintaining robust security measures is crucial for fostering long-term adoption and trust in electronic services.

The primary purpose of this research is to explore the interaction between usability and security in electronic online services, aiming to understand how these two elements impact system design and user experience. This research will investigate the trade-offs that developers face when trying to create systems that are both user-friendly and secure. Specifically, it will identify common usability-security conflicts, analyze their impact on user engagement and security effectiveness, and propose potential solutions to address these challenges. The main objectives of this study include:

- Understanding how usability and security interact. The research will explore the interdependencies between usability and security, analyzing how enhancing one may negatively impact the other. For example, increasing security measures (e.g., complex password requirements) often reduces usability, leading to user frustration or system abandonment (Mihajlov et al., 2011).
- Identifying common trade-offs by reviewing various case studies and system implementations, this research will identify specific usability-security trade-offs. These insights will help pinpoint the design challenges that developers face (Monzón et al., 2020).

The findings of this study have significant implications across various sectors:

- E-commerce: Simplified authentication processes, such as biometric login and adaptive security measures, can reduce cart abandonment rates and improve customer retention. For example, integrating facial recognition for seamless checkout can enhance the shopping experience while ensuring transaction security.
- Online banking: Adaptive MFA systems can provide robust protection for high-risk transactions while maintaining ease of use for routine logins. Banks can implement push notifications or biometric verification for account access, offering both security and convenience.
- Healthcare: Patient portals can benefit from biometric authentication to secure sensitive medical information. Using fingerprints or facial recognition ensures secure access without burdening patients with complex passwords.
- Government services: E-government platforms can enhance citizen engagement by implementing

user-friendly security measures. For instance, biometric authentication can simplify processes such as tax filing and benefits applications while maintaining data security.

- Education: Online learning platforms can adopt biometric verification to ensure secure access to exams and coursework. This approach minimizes the risk of fraud and provides a seamless experience for students.

2. Literature review

Usability has long been a critical factor in the design of electronic online services, as it directly impacts user satisfaction, engagement, and adoption rates. Studies in the field of human-computer interaction (HCI) emphasize the importance of intuitive interfaces and minimal cognitive load to improve user experiences. For instance, research on e-commerce platforms highlights that simplified navigation and clear feedback mechanisms significantly enhance user satisfaction, particularly for novice users. Similarly, studies on online banking systems reveal that streamlined authentication processes are essential for retaining users in highly competitive markets. These findings underscore the necessity of prioritizing usability during system design to accommodate diverse user needs. Usability in electronic services refers to the ease with which users interact with digital platforms and is often studied within the field of Human-Computer Interaction (HCI). Historically, HCI has focused on creating systems that improve user experience by optimizing for efficiency, effectiveness, and satisfaction (Carroll, 1997). Over time, usability research has expanded to include emotional factors, such as how users feel about their interactions with technology. Aesthetics, satisfaction, and emotional engagement are now recognized as essential in understanding why users prefer some systems over others (Thüring and Mahlke, 2007). In the domain of electronic services, usability is essential for ensuring that systems are easy to use and promote continued engagement. However, usability and security are often at odds. Enhancing security measures can complicate the user experience by introducing additional steps or complex interfaces that may frustrate users and decrease system adoption (Kainda et al., 2010).

The interaction between user behavior and security in electronic services has been extensively studied. User behavior theories suggest that while users prioritize convenience and ease of use, they may not fully comprehend the importance of security, leading to poor decisions regarding their own safety in digital environments (Möller et al., 2011; Saeed, 2023). For example, users often opt for simpler authentication processes, such as weaker passwords, which compromise security. Models of user perception in electronic systems show that trust, security, and ease of use are critical for user engagement, particularly in areas like mobile banking and e-commerce. Studies have demonstrated that user perception of security directly influences their likelihood to adopt new technologies, especially when sensitive data is involved (Kindberg et al., 2004). Moreover, the perceived usability of security features, such as authentication methods, plays a crucial role in determining whether users continue to engage with these services (Mockel, 2011).

Incorporating robust security mechanisms into digital systems is not only a technical challenge but also an economic one. The Return on Security Investment (ROSI) framework is used to evaluate the financial impact of security measures. It balances the costs of implementing security features with the potential losses from security breaches. This model highlights the importance of cost-effective security solutions that do not compromise usability. Studies in e-commerce and banking have shown that while stricter security measures can mitigate risks, they must be implemented in a way that maintains usability to ensure customer retention. Research on behavioral economics also plays a role in understanding how users make decisions regarding security. For instance, users are more likely to invest in secure technologies if they perceive a direct personal benefit, such as protecting their own financial data. However, studies show that when security is seen as too complex or costly in terms of time and effort, users are more likely to abandon these safeguards (Dzidzah et al., 2020).

Security remains a paramount concern in electronic services due to the increasing prevalence of cyber threats. Multi-factor authentication (MFA) is widely regarded as a robust measure for enhancing security, but it often imposes additional steps on users, creating friction in the login process. Password complexity requirements, while effective against brute-force attacks, further exacerbate usability issues, particularly for novice users. Recent advancements in biometric authentication offer a promising alternative, combining enhanced security with user-friendly mechanisms such as fingerprint and facial recognition. These solutions minimize cognitive load and reduce the likelihood of user errors, making them a preferred option in modern systems.

While significant research has been conducted on the usability-security trade-off in online services, there remain critical gaps in the literature that need further exploration, like the lack of Comprehensive Frameworks. Several studies have noted that although security and usability are both essential for electronic services, there is no comprehensive framework that optimally balances these two aspects. Current frameworks tend to either focus on security or usability in isolation, rather than addressing them simultaneously in a manner that provides a holistic solution (Naqvi and Seffah, 2019). Researchers argue that there is a need for integrated models that can offer systematic approaches to managing these conflicting requirements in a unified way (Alsaleh et al., 2015). Antor exploration is the inadequate Real-World Application of Usability-

Security Models. Although theoretical models exist, many have not been validated in real-world contexts. For example, some usability-security models are overly complex, making them difficult to implement in everyday systems such as online banking or e-commerce platforms. Furthermore, these models are not always adaptable to rapidly evolving technologies like mobile and cloud computing environments, creating a gap in practical applicability (Katsini et al., 2016). One of the most significant shortcomings in existing research is the lack of emphasis on adaptive security mechanisms that adjust based on the user's behavior or context. Static security models, such as fixed authentication methods, do not consider user risk profiles or contextual changes in real-time, leading to a failure in optimizing both usability and security in varying situations (Alshamari, 2016).

Another gap identified is the inadequate integration of user-centric design principles into secure systems (Saltarella et al., 2024). Current systems often implement security features that are misaligned with how users behave or understand security protocols. This gap can lead to poor user experiences and decreased adoption of secure systems. The development of security frameworks that prioritize usability from the user's perspective is underexplored, despite evidence suggesting this would lead to better outcomes (Mohamed et al., 2017). Current evaluation metrics used to assess the balance between usability and security vary widely, and many fail to capture the complex relationship between these two aspects. Existing models lack standardized metrics for measuring how usability improvements impact security and vice versa. There is a need for a more consistent set of evaluation tools to better assess the trade-offs between these two areas (Alarifi et al., 2017).

These gaps highlight the need for continued research to develop practical, adaptive, and user-friendly frameworks that can be implemented across various online services while ensuring robust security without compromising user experience.

3. Research methodology

For this study on the usability and security of electronic online services, a mixed-methods research design is proposed in Fig. 1. The combination of both qualitative and quantitative methods will allow for a comprehensive understanding of the complex trade-offs between usability and security. A mixed-method approach is particularly valuable because it captures both the objective usability metrics from quantitative methods, such as surveys and usability tests, and the in-depth user insights from qualitative methods, such as interviews and case studies.

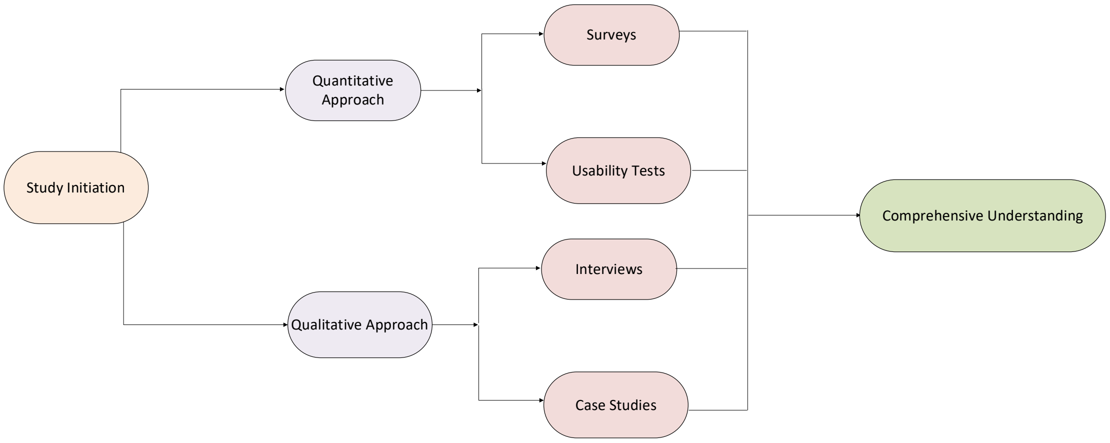

Fig. 1: Research methodology

3.1. Quantitative component

The quantitative portion will involve usability testing and surveys that assess how users interact with online services in terms of both security and ease of use. Metrics such as task completion times, error rates, and user satisfaction levels will be collected. Additionally, users will be asked to evaluate security features (e.g., multi-factor authentication) through standardized usability questionnaires (Luo and Botash, 2020).

3.2. Qualitative component

The qualitative component will involve semi-structured interviews and case studies with a subset of participants from the quantitative phase. These interviews will provide deeper insights into users' experiences, including their frustrations or perceptions of security features, allowing for a more nuanced understanding of the trade-offs users face (Alwashmi et al., 2019). Open-ended questions will be used to explore the decision-making process of users when encountering complex security protocols and how they balance security concerns with the desire for a smooth, user-friendly experience.

3.3. Iterative convergent mixed-methods design

This study will use an iterative convergent design, where both qualitative and quantitative data are collected and analyzed simultaneously, and the results of one phase will inform the next phase. This iterative approach ensures that any usability or security issues discovered in early phases can be further explored and resolved in subsequent rounds (Lesemann et al., 2007). This mixed-methods design provides a robust framework for exploring how usability and security interact in real-world contexts, enabling both breadth and depth in the analysis.

3.4. Sample size and demographics

For this study, the target participants will consist of users of online banking services and e-commerce platforms, as these sectors frequently face usability and security challenges. The sample will include users across different demographics such as age, gender, education level, and technical proficiency to ensure that the findings are generalizable and capture diverse user experiences.

The sample size will be determined based on prior research in usability testing, which suggests that observing between 15 and 20 participants can reveal most usability issues, especially when the likelihood of problem detection is high (Lewis, 1994). However, due to the complexity of balancing usability and security, a slightly larger sample will be utilized to ensure comprehensive coverage of usability problems and their interactions with security measures. Research has shown that increasing the sample size beyond 5 participants significantly increases the likelihood of detecting usability problems, with diminishing returns beyond 20 participants (Faulkner, 2003). Participants will range from young adults (18-35 years) to older adults (36+ years), as age can influence both usability perceptions and security concerns.The sample will include users with varying levels of familiarity with online services, ranging from novice users to advanced users. This will help capture how expertise impacts the trade-offs between usability and security. To ensure diverse perspectives, the sample will be balanced in terms of gender and will include participants from different professional backgrounds. Given these considerations, a sample size of 20-25 participants is planned to provide a robust analysis of both usability and security aspects of electronic online services. This size is sufficient to achieve high coverage of usability issues and ensure reliable data regarding security perceptions.

3.5. Data collection methods

To effectively study the usability-security trade-off in electronic online services, a combination of quantitative and qualitative data collection methods will be employed to ensure robust and comprehensive insights. Usability testing will be conducted to assess how users interact with online services, focusing on task completion, error rates, and user satisfaction. Participants will be observed performing common tasks such as logging into an online banking system or making purchases on an e-commerce platform. Tools such as SUS (System Usability Scale) will be used to measure usability perceptions quantitatively (Milosz and Chmielewska, 2020). Surveys will be given to participants before and after usability testing to understand their views on both usability and security. The pre-test surveys will collect background information about users' familiarity with the service, their security concerns, and expectations. The post-test surveys will evaluate users' experiences with specific security features, such as multi-factor authentication, and how these features affect their overall satisfaction and willingness to use the service. The surveys will be administered online, using tools like Google Forms.

In-depth interviews will be conducted using the think-aloud protocol, where participants will express their thoughts while completing tasks. This approach will help identify specific usability problems related to security features, such as difficulties with multi-factor authentication or password recovery. The qualitative data from these interviews will provide important context to the quantitative results from the usability tests and help identify how security features affect the user experience (Milosz and Chmielewska, 2020). By combining these methods, the study will provide a detailed understanding of how users interact with both usability and security features in online services.

3.6. Usability test for online services: Authentication and security features

The usability test aimed to assess the ease of use of various authentication methods, including password-only authentication, MFA, and biometric authentication. The primary objectives were to evaluate how users interacted with these methods, identify any usability issues such as login failures, user errors, or time delays, and gather feedback on user satisfaction with the security measures and their perceived effectiveness.

The test was conducted in a controlled environment where participants used either a standard desktop or a mobile device with internet access. Each participant was provided with a test account on an online banking or e-commerce platform, configured to support three authentication methods: Password-only, MFA, and biometric authentication (if available). Before beginning the tasks, participants received detailed written and verbal instructions to ensure they understood the process. Participants were asked to complete specific tasks, which included logging in using different authentication methods and performing a basic transaction. After completing each task, they were required to fill out a brief questionnaire to provide feedback on their experience, focusing on ease of use and their perception of the security features. This approach ensured that data on task performance, user satisfaction, and potential usability issues were systematically collected for analysis. Table 1 summarizes the tasks, objectives, instructions, metrics, and expected outcomes for each usability test.

Table 2 shows the post-task questionnaire information, and Fig. 2 shows the evaluation process.

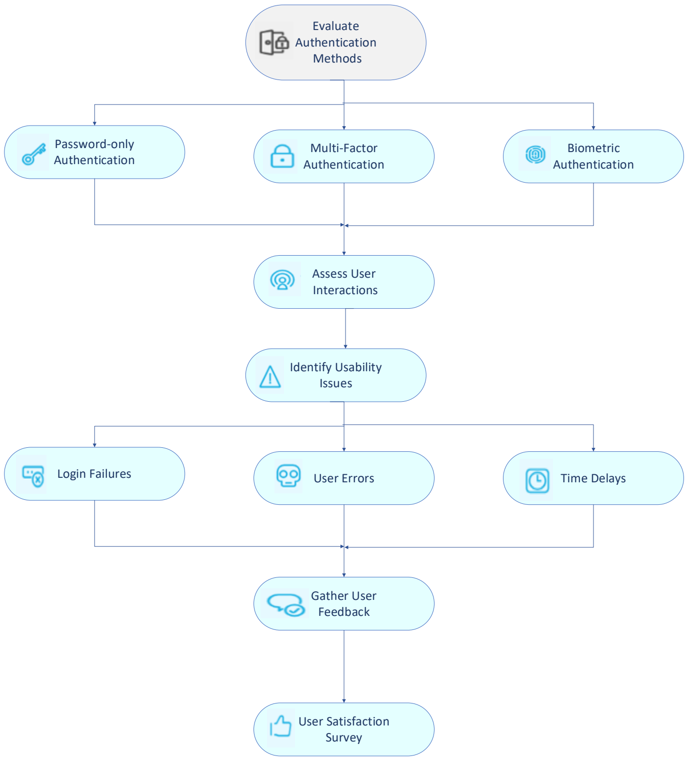

Fig. 2: Evaluation procedure

Table 1: Tasks of usability test

Task	Objective	Instructions for participants	Metrics to collect	Expected outcome
Task 1: Password-only login	Log in to the online service using a password-only authentication method.	Use your assigned username and password to log into the platform.	- Task completion time (start to login) - Error rate (incorrect attempts) - User feedback (difficulty rating: 1 = very difficult, 5 = very easy)	Successful login within 1–2 attempts.
Task 2: MFA login	Log in to the service using MFA.	Use your username, password, and the security code sent to your phone.	- Task completion time (including code receipt and entry) - Error rate (incorrect attempts) - User feedback (task difficulty rating)	Successful login after entering the correct security code.
Task 3: Biometric authentication	Log in to the platform using biometric authentication (e.g., fingerprint).	Log in using biometric authentication (e.g., scan your fingerprint).	- Task completion time (biometric scan duration) - Error rate (failed biometric scans) - User feedback (ease of use compared to other methods)	Immediate login with minimal biometric scan errors.
Task 4: Making a transaction	Complete a simple transaction (e.g., transfer or purchase) after logging in.	Make a $50 transfer or purchase an item using your test account.	- Task completion time (total time for transaction) - Error rate (transaction process errors) - User feedback (ease and perceived security rating)	Transaction completed with minimal errors.

Table 2: Post-task questionnaire

Question	Response options
1. How easy was the login process?	1 (Very difficult), 2 (Difficult), 3 (Neutral), 4 (Easy), and 5 (Very easy)
2. How secure did you feel using this method?	1 (Not secure at all), 2 (Not secure), 3 (Neutral), 4 (Secure), and 5 (Very secure)
3. Which login method do you prefer? Why?	Answer: ________________________
4. What frustrated you the most about the login process?	Answer: ________________________

4. Results and discussion

In this study, a combination of quantitative and qualitative analysis techniques was employed to process and interpret the data collected from usability testing, surveys, interviews, and security incident reports. Descriptive Statistics: The first step involves calculating basic descriptive statistics such as means, medians, and standard deviations to summarize the data from usability tests (e.g., task completion times, error rates, and satisfaction scores). This will provide an overview of the central tendencies and variability in the dataset (Taha et al., 2014). The scores will then be analyzed to assess the overall usability of the online services being tested (González et al., 2008). By using both statistical methods for the quantitative data and coding techniques for the qualitative data, this mixed-method approach will yield a comprehensive understanding of the usability-security trade-offs in electronic online services.

4.1. Quantitative analysis

4.1.1. Task completion time

The task completion times for each authentication method were recorded for all 25 participants. The average task completion times across the different authentication methods are presented in Table 3. Fig. 3 shows the usability testing of authentication methods and security features.

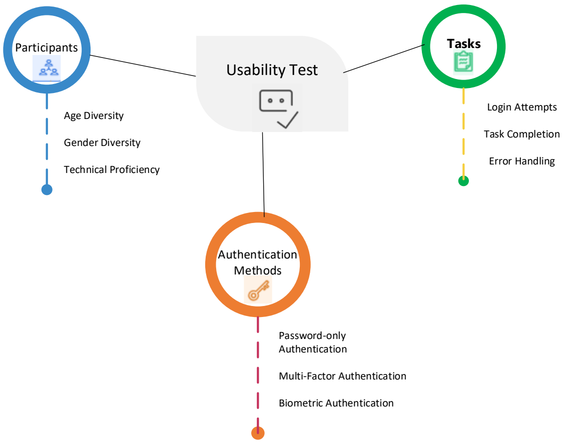

Fig. 3: Usability testing of authentication methods and security features

Table 3: Average task completion times

Authentication method	Mean completion time (seconds)	Standard deviation (seconds)
Password-only authentication	22.23	3.73
MFA	34.97	6.79
Biometric authentication	5%	1%
Transaction completion (post-login)	51.19	6.91

Table 3 shows that Password-Only Authentication had the fastest average completion time, with an average of 22.23 seconds, indicating that users find it relatively easy to use compared to more complex security measures. MFA increased the task completion time, with an average of 34.97 seconds, suggesting that additional security steps, such as receiving and entering verification codes, require more time and effort. Completing a transaction post-login had the longest completion time, with an average of 51.19 seconds, which is expected as the process involves multiple steps beyond authentication.

4.1.2. Error rates

The error rates for each authentication method were also tracked. Error rates were calculated as the percentage of failed attempts relative to the total number of attempts for each authentication method. Table 4 and Fig. 4 show that Password-Only Authentication had the lowest error rate, with an overall error rate of 7.5%. Novice users had a slightly higher error rate (10%) compared to experienced users (5%). MFA had a higher error rate, with 14% overall, highlighting the increased complexity of this method. Novice users struggled more with MFA, making errors in 20% of cases, while experienced users had an 8% error rate. During Transaction Completion, users encountered errors 8.5% of the time, with novice users (12%) struggling more than experienced users (5%).

4.1.3. User satisfaction

Satisfaction scores were collected using a Likert scale, with participants rating their experience. Participants were asked to rate their satisfaction with each authentication method on a scale of 1 to 5 (1=very dissatisfied, 5=very satisfied). Providing detailed interpretations of error rates and satisfaction scores, the data analysis highlights the critical differences in user experiences with various authentication methods, offering valuable insights for improving the design of electronic online services. The mean satisfaction scores are presented below.

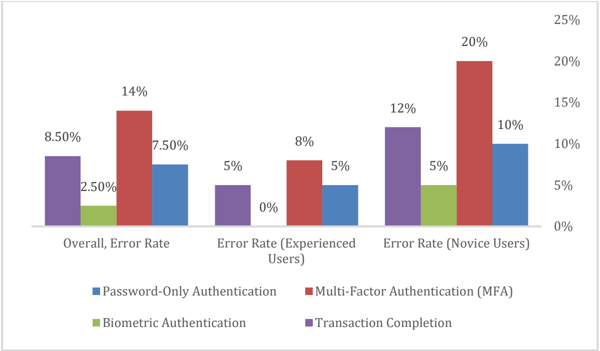

Fig. 4: Error rates of authentication methods

Table 5 shows that Password-Only Authentication was rated relatively well, with a mean satisfaction score of 4.2, indicating that users appreciated the simplicity of this method. MFA received a lower satisfaction score, with an average of 3.0, as participants found it more cumbersome due to the extra steps required. Biometric Authentication had the highest satisfaction score, with a mean score of 4.5, reflecting users' preference for this method due to its ease of use and perceived security.

4.1.4. Comparison of novice and experienced users

A deeper analysis of novice vs. experienced users highlighted that novice users had consistently higher error rates across all tasks, especially with MFA (20% error rate), compared to experienced users (8% error rate). Experienced users completed tasks more quickly and with fewer errors, particularly with Password-Only Authentication and Transaction Completion tasks. Both groups showed a clear preference for Biometric Authentication, with novice users reporting an average satisfaction score of 4.3 and experienced users 4.7.

Table 4: Error rates of authentication methods

Authentication method	Error rate (novice users)	Error rate (experienced users)	Overall, error rate
Password-only authentication	10%	5%	7.5%
MFA	20%	8%	14%
Biometric authentication	5%	0%	2.5%
Transaction completion	12%	5%	8.5%

Table 5: User satisfaction

Authentication method	Mean satisfaction score
Password-only authentication	4.2
MFA	3.0
Biometric authentication	4.5

4.1.5. Overall findings and practical implications

The analysis indicates that there is a clear usability-security trade-off. While Password-Only Authentication was faster and easier for users, it did not provide the same level of security as Multi-Factor Authentication or Biometric Authentication. However, Biometric Authentication stood out as the most user-friendly and secure method, offering a strong balance between ease of use and security. The error rates and satisfaction scores further highlight that Multi-Factor Authentication, while more secure, introduces usability challenges, especially for novice users.

This suggests a need for developers to streamline the MFA process and make it more user-friendly or consider adaptive security measures that tailor the level of authentication based on user behavior or risk. Incorporating Biometric Authentication more widely could be a practical solution for enhancing both usability and security, as it scored the highest in terms of user satisfaction and had minimal errors across both novice and experienced users.

4.2. Qualitative analysis (case studies)

The purpose of case studies is to gain deeper insights into real-world interactions with security features. Two participants (one novice and one experienced user) were selected for case studies. These case studies provided a more detailed examination of their interactions with the system, including usability challenges and their overall experience with security.

4.2.1. Case study 1: Novice user experience (participant A)

Participant A was a 32-year-old novice user with limited experience in online banking. They had an average completion time of 45 seconds for multi-factor authentication and made multiple errors during the login process. The key findings can be described as the struggles with MFA, password frustration, and preference for biometrics. In struggles with MFA, participant A found the MFA process frustrating, particularly the need to switch between devices to enter security codes. They noted that the process felt “tedious” and would prefer a simpler login method.

In the password frustration, the user reported feeling overwhelmed by password complexity requirements, often mistyping their password, which increased the number of login attempts. In preference for biometrics, participant A expressed a strong preference for biometric authentication, stating that “it’s quick, easy, and I don’t have to remember anything.” For novice users like Participant A, MFA and password complexity create significant usability challenges. Simplifying these processes or offering biometric authentication would improve the overall user experience.

4.2.2. Case study 2: Experienced user experience (participant B)

Participant B was a 45-year-old experienced user who regularly used online services, including online banking and shopping platforms. Their completion time for MFA was 28 seconds, with no errors, and they expressed confidence in using the system. The key findings are Efficiency with MFA, Strong Preference for Biometrics, and No Issues with Password Complexity. In efficiency with MFA, participant B did not experience major issues with MFA, stating that the additional security gave them peace of mind without feeling too burdensome. They completed the MFA process quickly and appreciated the added security. In strong preference for biometrics: Despite being comfortable with MFA, Participant B expressed a preference for biometric authentication due to its speed and simplicity, especially on mobile devices. In no issues with password complexity, participant B found password complexity requirements manageable, indicating that their familiarity with security measures made these tasks easier to complete. For experienced users like Participant B, MFA and password complexity were not significant barriers. However, biometric authentication was still preferred due to its convenience, suggesting that even experienced users value methods that reduce friction in the login process.

4.2.3. The main inference of case studies

- Usability challenges with MFA: Both novice and experienced users acknowledged that while MFA provides strong security, it creates friction in the user experience, particularly for less experienced users.
- Preference for biometrics: Across interviews and case studies, participants consistently preferred biometric authentication, noting its ease of use, speed, and perceived security.
- Cognitive load from passwords: Users expressed frustration with remembering and entering complex passwords, particularly when combined with MFA. Many suggested that simplifying or eliminating password requirements in favor of biometric authentication would improve usability without compromising security.
- Recommendations for future systems: Participants suggested that future systems should focus on reducing the cognitive load associated with security features, especially for novice users. Offering a seamless biometric login process or adaptive security measures based on user experience levels would help balance usability and security.

4.3. Qualitative analysis (semi-structured interviews)

The interviews revealed a clear difference between novice and experienced users regarding their experience with MFA. Table 6 shows that around 60% of novice users expressed frustration with MFA, citing the additional steps involved in receiving and entering security codes as overwhelming. One participant mentioned that "having to switch between devices to get the code felt tedious, especially when logging in multiple times a day. "Only 40% of experienced users reported frustration, with the majority finding MFA to be a manageable, albeit slightly inconvenient, extra layer of security.

Table 6: Frustration with MFA

User type	Frustrated with MFA
Novice users	60%
Experienced users	40%

Across both novice and experienced users, biometric authentication was universally praised for its ease of use and perceived security. Table 7 shows that all respondents, both novice and experienced, expressed trust in biometric authentication. This authentication method was described as "quick, easy, and more secure than passwords," especially for mobile devices. The consensus suggests that biometric methods strike a balance between convenience and security that is highly favored by all users.

Table 7: Trust in biometric authentication

User type	Trusting biometric authentication
Novice users	100%
Experienced users	100%

A significant number of novice users expressed frustration with remembering and managing complex passwords, while experienced users generally did not face the same challenges. Table 8 shows that 80% of novice users mentioned struggling with passwords, particularly when coupled with MFA. One novice participant stated that "having to remember complex passwords and then add MFA on top of that made the login process feel exhausting." Only 20% of experienced users expressed frustration with passwords, as most had developed strategies for managing complex password requirements (e.g., using password managers or creating memorable passphrases).

The qualitative findings revealed several key insights regarding user experiences with different authentication methods. Novice users found MFA to be a significant usability challenge, particularly when required to switch between devices to retrieve authentication codes, which aligns with the quantitative data showing higher error rates and longer task completion times for MFA among novice users. While experienced users generally accepted MFA as a necessary security measure, some noted minor inconveniences. Both novice and experienced users universally preferred biometric authentication due to its simplicity and security, which also corresponded with the quantitative results, where biometrics received the highest satisfaction scores. Users consistently praised biometric methods as faster and more secure alternatives to passwords and MFA. Additionally, password complexity requirements were a common source of frustration for novice users, who struggled to remember and correctly input complex passwords, especially when combined with MFA. In contrast, most experienced users did not face significant difficulties with passwords, often relying on tools like password managers to simplify the process.

Table 8: Frustrated with passwords

User type	Frustrated with passwords
Novice users	80%
Experienced users	20%

4.4. Practical implications for developers, security experts, and designers

The practical implications for developers, security experts, and designers highlight several strategies to enhance both usability and security. To improve the usability of MFA, particularly for novice users, developers should consider implementing adaptive MFA based on the user's risk profile or offering simplified verification methods, such as push notifications rather than manual code entry. Expanding the use of biometric authentication, which is universally trusted by users, could further enhance both satisfaction and security, with biometrics being prioritized in future systems, especially for mobile and frequently accessed services. Additionally, to address the frustration associated with password complexity, developers could integrate password managers into their platforms or implement passwordless authentication options, such as biometric login or single-use login links, reducing the cognitive load on users while maintaining security. Fig. 5 shows different issues with authentication methods.

5. Limitations of sample size and future directions

While this study provides valuable insights into the usability-security trade-off, the relatively small and homogeneous sample size poses certain limitations. The sample predominantly included users familiar with digital platforms, potentially overlooking the challenges faced by less technologically proficient individuals. Additionally, the sample did not fully account for diversity in demographics such as age, geographic location, or disability, which may influence user interaction with authentication systems.

Future studies should aim to include a broader and more representative sample to capture diverse user experiences. Expanding the sample size to include individuals from varying levels of digital literacy, as well as different cultural and socioeconomic backgrounds, will provide a more comprehensive understanding of usability and security challenges. Moreover, conducting longitudinal studies could offer insights into how user preferences and behaviors evolve over time with repeated exposure to authentication methods. Addressing these limitations will help refine and generalize the findings, enabling the development of more inclusive and user-centered security solutions.

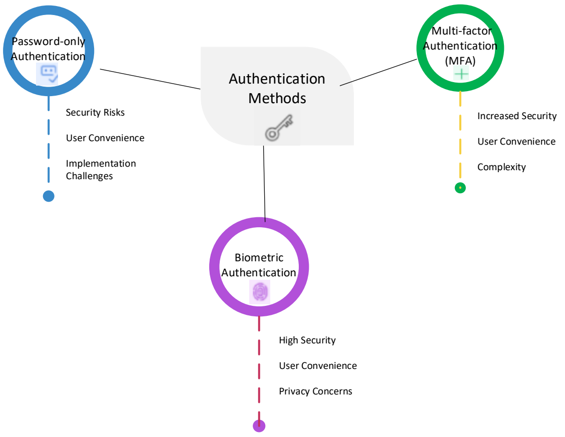

Fig. 5: Different issues with authentication methods

6. Emerging technologies: Future applications and challenges

The integration of advanced technologies such as continuous authentication and adaptive security measures presents significant opportunities and challenges for the future of electronic online services. Continuous authentication involves the ongoing verification of user identity through behavioral biometrics (e.g., typing patterns, mouse movements, or device usage). This approach enhances security by detecting anomalies in real-time, making it particularly valuable in high-security environments such as financial systems and government portals, where constant vigilance against unauthorized access is critical. However, implementing continuous authentication raises challenges related to privacy concerns and system performance, as it requires robust infrastructure and user consent for the collection and analysis of behavioral data.

Adaptive security measures dynamically adjust authentication requirements based on risk assessment. For instance, e-commerce platforms can simplify authentication for trusted users during low-risk transactions while imposing stricter measures for higher-risk activities. In healthcare, adaptive security can protect sensitive patient data by increasing authentication requirements during unusual access patterns. Despite their potential, these systems must be carefully calibrated to avoid overwhelming users or inadvertently compromising security. The success of these technologies hinges on achieving a balance between usability and security, ensuring seamless integration into existing systems without alienating users.

7. Future research directions

The findings of this study highlight several areas for further research to deepen the understanding of the usability-security trade-off in online services. Future studies could explore adaptive security models that adjust authentication requirements based on user behavior or risk profiles. This approach would help balance robust security with a seamless user experience, particularly for novice users who struggle with complex security measures like MFA.

Additionally, longitudinal studies tracking user engagement and satisfaction over extended periods would provide insights into how users adapt to security features over time, particularly whether initial frustrations diminish with repeated use. Investigating the integration of emerging technologies, such as voice recognition and continuous authentication, could offer alternative solutions for enhancing both usability and security.

Finally, future research should focus on developing comprehensive frameworks that optimize usability and security across various user groups and service types, ensuring that solutions are scalable and inclusive. These directions would contribute to the development of more user-friendly and secure online services, bridging the gap between theory and real-world application.

8. Conclusion

This study explored how to balance usability and security in online services by comparing different login methods: password-only, MFA, and biometric authentication. Using both quantitative and qualitative methods, the results showed a clear trade-off between usability and security. MFA offered stronger security but caused more difficulties for users, especially beginners, as shown by higher error rates, longer times to complete tasks, and lower satisfaction. In contrast, password-only login was easier to use but did not provide enough security for sensitive actions. Both new and experienced users preferred biometric authentication, rating it highly for both ease of use and security. This suggests that biometrics may provide the best balance between user-friendliness and strong protection. The findings highlight the need for system designers and security professionals to focus on using biometrics and to make MFA easier to use, especially for less experienced users. Improving password design or offering password management tools could also make systems easier to use, showing the importance of creating security solutions that are both effective and user-friendly.

Acknowledgment

The authors gratefully acknowledge the approval and the support of this research study by grant no.

SCIA-2023-12-2361 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Alarifi A, Alsaleh M, and Alomar N (2017). A model for evaluating the security and usability of e-banking platforms. Computing, 99: 519-535. https://doi.org/10.1007/s00607-017-0546-9

Alsaleh M, Alarifi A, Alshaikh Z, and Zarour M (2015). Online banking security and usability-towards an effective evaluation framework. In the Proceedings of 11th International Conference on Web Information Systems and Technologies (WEBIST-2015), SciTePress, Lisbon, Portugal: 141-149. https://doi.org/10.5220/0005493901410149

Alshamari M (2016). A review of gaps between usability and security/privacy. International Journal of Communications, Network and System Sciences, 9(10): 413-429. https://doi.org/10.4236/ijcns.2016.910034

Alwashmi MF, Hawboldt J, Davis E, and Fetters MD (2019). The iterative convergent design for mobile health usability testing: Mixed methods approach. JMIR mHealth and uHealth, 7(4): e11656. https://doi.org/10.2196/11656 **PMid:31025951 PMCid:PMC6658163**

Carroll JM (1997). Human–computer interaction: Psychology as a science of design. International Journal of Human-Computer Studies, 46(4): 501-522. https://doi.org/10.1006/ijhc.1996.0101

Dzidzah E, Kwateng KO, and Asante BK (2020). Security behaviour of mobile financial service users. Information and Computer Security, 28(5): 719–741. https://doi.org/10.1108/ICS-02-2020-0021

Faulkner L (2003). Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. Behavior Research Methods, Instruments, and Computers, 35: 379-383. https://doi.org/10.3758/BF03195514 **PMid:14587545**

Feth D (2015). User-centric security: Optimization of the security-usability trade-off. In the 10th Joint Meeting on Foundations of Software Engineering, Association for Computing Machinery, Bergamo, Italy: 1034-1037. https://doi.org/10.1145/2786805.2803195

Furnell S (2016). The usability of security–revisited. Computer Fraud and Security, 2016(9): 5-11. https://doi.org/10.1016/S1361-3723(16)30070-7

González MP, Lorés J, and Granollers A (2008). Enhancing usability testing through datamining techniques: A novel approach to detecting usability problem patterns for a context of use. Information and Software Technology, 50(6): 547-568. https://doi.org/10.1016/j.infsof.2007.06.001

Ibrahim T, Furnell SM, Papadaki M, and Clarke NL (2010). Assessing the usability of end-user security software. In: Katsikas S, Lopez J, and Soriano M (Eds.), International conference on trust, privacy and security in digital business: 177-189. Springer, Berlin, Germany. https://doi.org/10.1007/978-3-642-15152-1_16

Imbaquingo D, Díaz J, and Jácome J (2024). Quality and security as key factors in the development of computer audits in higher education institutions. Journal of Technology and Science Education, 14(4): 965-989. https://doi.org/10.3926/jotse.2275

Javaid M, Haleem A, Singh RP, and Sinha AK (2024). Digital economy to improve the culture of Industry 4.0: A study on features, implementation and challenges. Green Technologies and Sustainability, 2(2): 100083. https://doi.org/10.1016/j.grets.2024.100083

Kainda R, Flechais I, and Roscoe AW (2010). Security and usability: Analysis and evaluation. In the International Conference on Availability, Reliability and Security, IEEE, Krakow, Poland: 275-282. https://doi.org/10.1109/ARES.2010.77

Katsini C, Belk M, Fidas C, Avouris N, and Samaras G (2016). Security and usability in knowledge-based user authentication: A review. In the 20th Pan-Hellenic Conference on Informatics, Association for Computing Machinery, Patras, Greece: 1-6. https://doi.org/10.1145/3003733.3003764

Kindberg T, Sellen A, and Geelhoed E (2004). Security and trust in mobile interactions: A study of users' perceptions and reasoning. In: Davies N, Mynatt ED, and Siio I (Eds.), International Conference on Ubiquitous Computing: 196-213. Springer, Berlin, Germany. https://doi.org/10.1007/978-3-540-30119-6_12

Lesemann E, Woletz N, and Koerber S (2007). Combining methods to evaluate mobile usability. In the 9th International Conference on Human Computer Interaction with Mobile Devices and Services, Association for Computing Machinery, Singapore, Singapore: 444-447. https://doi.org/10.1145/1377999.1378051

Lewis JR (1994). Sample sizes for usability studies: Additional considerations. Human Factors, 36(2): 368-378. https://doi.org/10.1177/001872089403600215 **PMid:8070799**

Luo S and Botash AS (2020). Testing a mobile app for child abuse treatment: A mixed methods study. International Journal of Nursing Sciences, 7(3): 320-329. https://doi.org/10.1016/j.ijnss.2020.06.008 **PMid:32817855 PMCid:PMC7424146**

Mihajlov M, Blazic BJ, and Josimovski S (2011). Quantifying usability and security in authentication. In the IEEE 35th Annual Computer Software and Applications Conference, IEEE, Munich, Germany: 626-629. https://doi.org/10.1109/COMPSAC.2011.87

Mihu C, Pitic AG, and Bayraktar D (2023). Drivers of digital transformation and their impact on organizational management. Studies in Business and Economics, 18(1): 149-170. https://doi.org/10.2478/sbe-2023-0009

Milosz M and Chmielewska M (2020). Usability testing of e-government online services using different methods: A case study. In the 13th International Conference on Human System Interaction, IEEE, Tokyo, Japan: 142-146. https://doi.org/10.1109/HSI49210.2020.9142628

Mockel C (2011). Usability and security in EU e-banking systems-towards an integrated evaluation framework. In the IEEE/IPSJ International Symposium on Applications and the Internet, IEEE, Munich, Germany: 230-233. https://doi.org/10.1109/SAINT.2011.42

Mohamed MA, Chakraborty J, and Dehlinger J (2017). Trading off usability and security in user interface design through mental models. Behaviour and Information Technology, 36(5): 493-516. https://doi.org/10.1080/0144929X.2016.1262897

Möller S, Ben-Asher N, Engelbrecht KP, Englert R, and Meyer J (2011). Modeling the behavior of users who are confronted with security mechanisms. Computers and Security, 30(4): 242-256. https://doi.org/10.1016/j.cose.2011.01.001

Monzón FH, Tupia M, and Bruzza M (2020). Security versus usability in e-government: Insights from the literature. In: Rocha Á, Paredes-Calderón M, and Guarda T (Eds.), Developments and advances in defense and security. MICRADS 2020. Smart Innovation, Systems and Technologies, vol 181: 29-42. Springer, Singapore, Singapore. https://doi.org/10.1007/978-981-15-4875-8_3

Mujinga M (2024). Usable security of online banking authentication: An exploratory factor analysis. Journal of Information Systems and Informatics, 6(1): 409-420. https://doi.org/10.51519/journalisi.v6i1.673

Naqvi B and Seffah A (2019). Interdependencies, conflicts and trade-offs between security and usability: Why and how should we engineer them? In the 1st International Conference on HCI for Cybersecurity, Privacy and Trust, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, Springer International Publishing, Orlando, USA: 314-324. https://doi.org/10.1007/978-3-030-22351-9_21

Nimmi K and Janet B (2018). An analysis of the balance between security and utility of mobile applications. In the International Conference on Circuits and Systems in Digital Enterprise Technology, IEEE, Kottayam, India: 1-4. https://doi.org/10.1109/ICCSDET.2018.8821080

Oguta GC (2024). Securing the virtual marketplace: Navigating the landscape of security and privacy challenges in e-commerce. GSC Advanced Research and Reviews, 18(1): 084-117. https://doi.org/10.30574/gscarr.2024.18.1.0488

Saeed S (2023). A customer-centric view of e-commerce security and privacy. Applied Sciences, 13(2): 1020. https://doi.org/10.3390/app13021020

Saltarella M, Desolda G, Lanzilotti R, and Barletta VS (2024). Translating privacy design principles into human-centered Software Lifecycle: A literature review. International Journal of Human–Computer Interaction, 40(17): 4465-4483. https://doi.org/10.1080/10447318.2023.2219964

Taha A, Trapero R, Luna J, and Suri N (2014). AHP-based quantitative approach for assessing and comparing cloud security. In the IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, Beijing, China: 284-291. https://doi.org/10.1109/TrustCom.2014.39

Thüring M and Mahlke S (2007). Usability, aesthetics and emotions in human–technology interaction. International Journal of Psychology, 42(4): 253-264. https://doi.org/10.1080/00207590701396674

Zhang C, Sun J, Zhu X, and Fang Y (2010). Privacy and security for online social networks: Challenges and opportunities. IEEE Network, 24(4): 13-18. https://doi.org/10.1109/MNET.2010.5510913