Modern Authentication Methods: A Study of Security and Usability

Sakshi Patil[1] Namrata Aher[2]
[1,2]Department of Information Technology
[1,2]Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

Abstract — Authentication is important for ensuring that digital accounts and services are protected from unauthorized access. Traditional passwords are commonly used, but they have vulnerabilities such as weak passwords, reusing passwords, phishing attacks, and the theft of credentials. Modern techniques like biometric authentication, Multi-Factor Authentication (MFA), One-Time Passwords (OTPs), authenticator apps, passkeys, passwordless authentication, and risk-based authentication offer stronger options. This study looks at these techniques in terms of security, usability, reliability, and how well they are accepted by users. A structured survey was conducted to understand users' awareness, usage patterns, concerns, and preferences. The study emphasizes the need to balance strong security with ease of use for these methods to be widely adopted.

Keywords: Authentication, Biometric Authentication, Multi-Factor Authentication, Passkeys, Password Security, Security-Usability Trade-off, Usability

I. Introduction

Digital authentication is the process used to verify a user's identity before allowing access to an account or service.

As more personal, financial, and business activities move online, secure authentication has become crucial for preventing unauthorized access and identity theft.

Traditional passwords are easy to use and inexpensive, but their effectiveness is limited by weak passwords, repeated use of the same password, forgotten credentials, phishing attacks, and credential-stuffing.

These shortcomings have prompted the adoption of more modern techniques such as biometrics, Multi-Factor Authentication (MFA), One-Time Passwords (OTPs), authenticator apps, passkeys, passwordless authentication, and risk-based authentication.

While these modern methods generally offer better security than traditional passwords, their acceptance largely depends on how user-friendly they are.

An authentication method that is very secure but hard to use, time-consuming, or inconvenient may not be accepted by users and may be bypassed, which can reduce its intended security benefits. On the other hand, methods that prioritize convenience at the expense of security can expose users to more risks. This creates a security–usability trade-off that needs to be carefully considered when choosing or evaluating an authentication method. Other factors such as reliability, resistance to phishing, and user acceptance further complicate this balance and are key to determining if a method is suitable for real-world use. Therefore, this study examines modern authentication methods in terms of their security, usability, reliability, resistance to phishing, and user acceptance.

The goal of this research is to explore modern authentication methods, understand their underlying principles and applications, and assess how well they provide secure, convenient, and reliable access to digital accounts while protecting users from unauthorized access and common security threats.

The study analyzes both the technical workings of these methods and the human factors that affect their effectiveness in real-world situations.

Traditional passwords are simple and inexpensive, but weak passwords, password reuse, forgotten credentials, phishing, and credential-stuffing attacks reduce their effectiveness. These limitations have encouraged the adoption of modern methods such as biometrics, Multi-Factor Authentication (MFA), One-Time Passwords (OTPs), authenticator applications, passkeys, passwordless authentication, and risk-based authentication.

While these methods generally offer improved security compared to traditional passwords, their adoption depends heavily on usability. An authentication method that is highly secure but difficult, slow, or inconvenient to use is likely to face user resistance or circumvention, which can undermine its intended security benefits. Conversely, methods optimized purely for convenience may expose users to greater risk. This creates an inherent security–usability trade-off that must be carefully balanced when evaluating or selecting an authentication approach. Additional factors such as reliability, resistance to phishing, and overall user acceptance further complicate this balance and are central to determining whether a given method is practical for real-world deployment. Accordingly, this study examines modern authentication methods in terms of security, usability, reliability, phishing resistance, and user acceptance.

The aim of this research is to study modern authentication methods, understand their underlying working principles and applications, and evaluate how effectively they provide secure, convenient, and reliable access to digital accounts while protecting users from unauthorized access and common security threats. The study examines both the technical mechanisms behind these methods and the human factors that influence their real-world effectiveness.

II. Literature Review

A. Authentication has been extensively studied as an important mechanism for protecting digital systems, online accounts, and sensitive data from unauthorized access.

Traditional authentication systems mainly rely on passwords and other knowledge-based credentials. However, password-based authentication has several drawbacks, including weak passwords, password reuse, credential theft, phishing attacks, and the difficulty of managing multiple passwords. These challenges have led researchers to look into modern authentication methods that can offer greater security without compromising user convenience.

Clarke and Furnell explored the development of usable authentication and discussed the shift from traditional passwords and tokens to biometrics and newer passwordless methods like passkeys.

Their work highlights the ongoing challenge of finding a suitable balance between authentication security and usability. The study also addresses issues related to accessibility, authentication across various devices and services, and the burden placed on users during the authentication process [1].

B. Passkeys have gained more attention as a passwordless authentication method.

Matzen et al. conducted a literature review focusing on challenges and potential improvements for passkey adoption from a user-centered perspective. Their study identifies usability, user understanding, compatibility, account recovery, and user acceptance as key factors affecting passkey adoption. While passkeys offer security and resistance to phishing, practical and user-related challenges remain to be addressed for their broader adoption [2].

C. Biometric authentication is another key area in modern authentication research.

Rui and Yan provided a survey of biometric authentication with a focus on secure and privacy-preserving identification. Their research discusses biometric characteristics such as fingerprints and facial features and their use in authentication systems. The study also points out security and privacy issues related to biometric information, indicating that secure implementation and protection of biometric data are essential for reliable biometric authentication [3].

D. Multi-Factor Authentication (MFA) adds an extra layer of protection by requiring two or more authentication factors.

Ometov et al. presented a survey of MFA approaches and analyzed various authentication factors and their combinations.

Their work shows that multi-factor authentication (MFA) can improve security by adding extra verification steps to prevent unauthorized access.

However, these additional steps may affect user convenience and ease of use, making the balance between security and usability a key factor [4].

E. The usability of two-factor authentication has also been studied from a user perspective.

De Cristofaro and their team conducted a comparison of different two-factor authentication methods and highlighted the importance of taking user effort and convenience into account when assessing authentication systems. Their findings support the idea that authentication methods should be judged not only by how secure they are but also by how easy they are for users to understand and use [5].

F. Risk-based authentication offers a flexible way to handle security.

Gunuganti explored this approach, which uses factors like device details, user location, and login behavior to assess the risk of an authentication attempt. If suspicious activity is detected, extra verification steps can be added. This method can offer stronger protection for high-risk logins while reducing unnecessary steps during regular access [6].

G. Accessibility has also become a major concern in designing authentication systems.

Di Campi and Luccio studied authentication methods for people with different cognitive abilities and stressed the importance of creating systems that can meet varying user needs. Their research suggests that authentication systems should take accessibility and inclusiveness into account alongside security and usability [7].

H. Recent studies have looked at how passwordless authentication works in Wi-Fi captive-portal settings.

Rivera-Dourado and their team compared passkeys and passwords in a study involving 50 participants. Their results showed that passkeys generally offered better usability, though the difference wasn't statistically significant. The study also found challenges related to platform compatibility and captive-portal environments, showing that the effectiveness of an authentication method depends on how it is implemented [8].

The relationship between security and usability has been explored by Braz, Seffah, and M'Raïhi using a metrics-based approach. Their work highlights the balance between strong security and user ease and suggests a model for considering both when assessing authentication systems. The study argues that authentication methods should offer sufficient security without causing undue inconvenience to valid users [9].

Overall, the reviewed studies highlight a common theme: the security benefits of modern authentication methods often come at the cost of usability.

The extent of this cost affects whether a particular method is used in real-world settings. Biometric and passkey-based methods [2], [3], [8] are generally favorable in terms of convenience and resistance to phishing but have their own issues, such as privacy concerns, device compatibility, and the challenge of recovering accounts. Ulti-Factor Authentication (MFA) and risk-based authentication [4], [6] enhance security by adding extra verification steps or contextual checks, but the extra effort may discourage regular use unless these steps are applied carefully. Studies focused on usability [1], [5], [7] show that ease of use, accessibility, and user comprehension are not secondary issues but key factors that determine whether stronger authentication is actually used instead of avoided. This observation leads to the current study's approach of assessing modern authentication methods across several dimensions at once — security, usability, reliability, phishing resistance, and user acceptance — rather than looking at them individually.

Clarke and Furnell studied the development of usable authentication and discussed the evolution from traditional passwords and tokens toward biometrics and newer passwordless approaches such as passkeys. Their work highlights the continuing challenge of achieving an appropriate balance between authentication security and usability. The study also considers issues related to accessibility, authentication across different devices and services, and the burden placed on users during authentication [1].

Passkeys have received increasing attention as a passwordless authentication approach. Matzen et al. conducted a literature review focusing on challenges and

potential improvements for passkey adoption from a user-centric perspective. Their study identifies usability, user understanding, compatibility, account recovery, and user acceptance as important factors influencing passkey adoption. Although passkeys provide security and phishing-resistance advantages, practical and user-related challenges need to be addressed for their wider adoption [2].

Biometric authentication is another important area of modern authentication research. Rui and Yan presented a survey of biometric authentication with emphasis on secure and privacy-preserving identification. Their research discusses biometric characteristics such as fingerprints and facial features and examines their applications in authentication systems. The study also highlights security and privacy concerns related to biometric information, indicating that secure implementation and protection of biometric data are important for reliable biometric authentication [3].

Multi-Factor Authentication (MFA) provides an additional layer of protection by combining two or more authentication factors. Ometov et al. presented a survey of MFA approaches and examined different authentication factors and their combinations. Their work demonstrates that MFA can strengthen protection against unauthorized access by requiring additional verification. However, the additional steps involved in MFA can influence user convenience and usability, making the security-usability balance an important consideration [4].

The usability of two-factor authentication has also been examined through user-focused research. De Cristofaro et al. conducted a comparative usability study of two-factor authentication methods and demonstrated the importance of considering user effort and convenience when evaluating authentication systems. Their research supports the view that authentication methods should be evaluated not only based on their security capabilities but also on how easily users can understand and use them [5].

Risk-based authentication provides an adaptive approach to authentication security. Gunuganti discussed risk-based authentication, in which information such as device characteristics, location, and login behavior can be considered when evaluating the risk associated with an authentication attempt. When suspicious activity is detected, additional verification can be requested. This approach can provide stronger protection for higher-risk login attempts while reducing unnecessary authentication requirements during normal access [6].

Accessibility has also become an important consideration in authentication system design. Di Campi and Luccio investigated authentication methods for persons with diverse cognitive abilities and emphasized the importance of designing authentication systems that accommodate different user needs. Their research indicates that authentication systems should consider accessibility and inclusiveness in addition to security and usability requirements [7].

Recent research has examined the practical usability of passwordless authentication in Wi-Fi captive-portal environments. Rivera-Dourado et al. compared passkeys and passwords in a controlled study involving 50 participants. Their findings indicated that passkeys tended to provide better usability, although the differences were not statistically significant. The study also identified practical challenges related to platform compatibility and captive-portal environments, demonstrating that the effectiveness of authentication methods can depend on their implementation context [8].

The relationship between security and usability has been studied by Braz, Seffah, and M'Raïhi through a metrics-based approach. Their research emphasizes the trade-off between security strength and user convenience and proposes a model for considering both aspects when evaluating authentication systems. The study supports the idea that authentication systems should provide adequate security without creating unnecessary difficulties for legitimate users [9].

Taken together, the reviewed studies point to a recurring theme: security gains from modern authentication are rarely free of a usability cost, and the size of that cost determines whether a method is actually adopted in practice. Biometric and passkey-based approaches [2], [3], [8] consistently score well on convenience and phishing resistance but raise separate concerns around privacy, device compatibility, and account recovery. MFA and risk-based authentication [4], [6] strengthen protection by adding verification steps or contextual checks, but the added friction can discourage routine use unless it is applied selectively. Usability-focused studies [1], [5], [7] further show that ease of use, accessibility, and user understanding are not secondary concerns but direct predictors of whether stronger authentication is actually used rather than bypassed. This pattern motivates the present study's decision to evaluate modern authentication methods along multiple dimensions at once — security, usability, reliability, phishing resistance, and user acceptance — rather than in isolation.

III. Research Gap

The reviewed literature addresses various important areas related to modern authentication, such as biometric authentication, Multi-Factor Authentication, passkeys, passwordless authentication, risk-based authentication, accessibility, security, usability, and user acceptance [1]–[9].

However, many of these studies focus on a single authentication technology or a specific aspect like technical security, usability, accessibility, or adoption. To address this, the present study takes a broader, user-centered approach by examining multiple modern authentication methods together. It considers security, usability, reliability, phishing resistance, and user acceptance, while also investigating users' awareness, usage practices, security concerns, preferences, and willingness to adopt modern authentication methods through a structured questionnaire. This offers a comprehensive view of the security and usability of modern authentication methods in everyday digital services.

IV. Modern Authentication Methods

Authentication is the process of confirming a user's identity before allowing access to a digital system, application, or account.

Traditional password-based authentication is increasingly being supplemented or replaced by modern methods that aim to offer stronger security, better convenience, and improved protection against common cyber

threats. The main modern authentication methods considered in this study are described below.

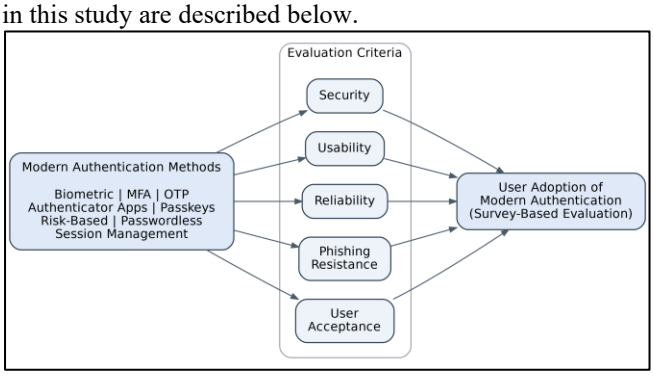

Fig. 1: Conceptual framework linking modern authentication methods, evaluation criteria, and user adoption, as examined in this study.

Fig. 1 shows the conceptual framework that guides this study. Each authentication method (Section III) is assessed against five criteria — security, usability, reliability, phishing resistance, and user acceptance (Section IV) — and these criteria together influence practical user adoption, which is explored through the survey presented in Sections V and VI.

A. Biometric Authentication

Biometric authentication confirms a user's identity using unique physical or behavioral traits.

Examples include fingerprint, facial, and iris recognition. This method reduces the need for users to remember passwords and offers a convenient way to verify identity. It is widely used in smartphones, banking apps, and other digital services. However, the secure storage and protection of biometric data are crucial because biometric features are closely tied to an individual and cannot be easily changed if compromised [3].

B. Multi-Factor Authentication

Multi-Factor Authentication (MFA) requires users to provide two or more authentication factors before access is granted.

These factors typically include something the user knows (like a password), something the user has (such as a mobile device or security token), and something the user is (like a fingerprint or facial recognition). Using multiple factors adds an extra layer of security if one factor is compromised [4].

C. One-Time Password

A One-Time Password (OTP) is a temporary code that can be used only once or for a limited time.

OTPs are commonly used as an additional factor for online banking, account login, and transaction verification. They help reduce the risk of reusing static passwords. However, the security of an OTP system depends on how the code is delivered and protected.

D. Authenticator Applications

Authenticator applications create temporary verification codes that users input during the authentication process.

These applications are often used as an extra layer of security in multi-factor authentication (MFA) and can serve as an alternative to receiving verification codes via SMS. By requiring access to a registered device alongside the main authentication credential, authenticator applications can enhance account security.

E. Passkeys

Passkeys are a method of authentication that does not rely on traditional passwords.

They use public-key cryptography and enable users to authenticate using a device through methods like fingerprint scanning, facial recognition, a PIN, or device unlock. Passkeys are designed to be more secure against phishing attacks and help lower the risk of password-related breaches. However, the adoption of passkeys can be influenced by user awareness, device compatibility, account recovery options, and platform support [2].

F. Risk-Based Authentication

Risk-Based Authentication assesses the risk level of a login attempt by analyzing various contextual details such as the device being used, the user's location, the IP address, and their behavior patterns.

If an authentication attempt is flagged as suspicious or unusual, the system may ask for further verification. This flexible method can offer stronger protection for potentially harmful login attempts while minimizing the need for extra verification during regular, safe access [6].

G. Passwordless Authentication

Passwordless authentication enables users to access systems without needing to enter a conventional password.

Instead, they can authenticate using biometric data, security keys, passkeys, device-based verification, or other secure alternatives. The goal of these methods is to address common issues with passwords, such as the difficulty of creating them, their tendency to be reused, and the risk of being stolen. However, the success of passwordless authentication depends on how securely it is implemented, the availability of devices, compatibility with different systems, and the presence of effective account recovery options [1], [2].

H. Secure Session Management

Secure session management is a crucial part of the authentication process.

Once a user has successfully authenticated, the system generates and controls a session that keeps the user logged in. Proper session management helps prevent unauthorized access that could result from stolen or altered session information. Secure handling of sessions should include appropriate expiration policies and security measures to protect the authenticated user's session.

Overall, modern authentication methods offer various ways to enhance digital security and reduce the likelihood of unauthorized access.

V. SECURITY AND USABILITY

The effectiveness of an authentication system depends not only on its ability to prevent unauthorized access but also on how easily and reliably legitimate users can complete the authentication process. Modern authentication methods are therefore evaluated using multiple factors, including security,

usability, reliability, resistance to phishing, and user acceptance. A suitable authentication method should provide adequate protection without creating unnecessary difficulties for users.

A. Security

Security is one of the primary objectives of an authentication system. Traditional password-based authentication can be affected by weak passwords, password reuse, credential theft, and phishing attacks. Modern authentication methods can provide additional protection by using multiple verification factors, biometric characteristics, device-based credentials, or cryptographic mechanisms. Multi-Factor Authentication (MFA), for example, provides an additional verification layer when a password is compromised, while passkeys are designed to reduce the risks associated with password theft and phishing [2], [4].

B. Usability

Usability refers to how easily and conveniently users can understand and operate an authentication system. Authentication procedures that are complicated, time-consuming, or difficult to remember may cause user frustration and can discourage users from adopting stronger security practices. Biometric authentication and passkeys can improve convenience by allowing users to authenticate through a fingerprint, facial recognition, PIN, or device unlock mechanism. Previous research has highlighted the importance of considering user effort and convenience when evaluating authentication systems [1], [5].

C. Reliability

Reliability refers to the ability of an authentication system to function consistently and provide legitimate users with access when required. Authentication failures can occur because of device compatibility problems, network availability, biometric recognition errors, or problems with account recovery. Therefore, a reliable authentication system should provide consistent authentication while also offering suitable recovery mechanisms when the primary authentication method is unavailable [2].

D. Phishing Resistance

Phishing is a common security threat in which attackers attempt to obtain sensitive information by pretending to be a legitimate service or organization. Authentication methods that rely heavily on passwords or codes entered into websites can be vulnerable to phishing attacks. Passkeys are designed to provide stronger resistance to phishing by using public-key cryptography and binding authentication to the legitimate website or service. This makes phishing-based credential theft more difficult compared with traditional password authentication [2].

E. User Acceptance

User acceptance is an important factor in the practical adoption of modern authentication technologies. Users are more likely to adopt an authentication method when it provides clear security benefits without creating excessive effort or inconvenience. Factors such as ease of use, privacy, accessibility, device compatibility, and understanding of the authentication process can influence acceptance. Research on authentication usability and accessibility shows that authentication systems should consider the diverse needs and capabilities of users [1], [5], [7].

F. Balance Between Security and Convenience

There is an important relationship between authentication security and user convenience. Increasing security requirements may sometimes introduce additional steps or complexity, while highly convenient methods may not always provide sufficient protection against advanced threats. Therefore, authentication systems should aim to achieve an appropriate balance between security and usability. Previous research has emphasized the importance of evaluating these two factors together rather than considering security or usability independently [4], [9].

G. Overall Evaluation

Modern authentication methods differ in their security capabilities, usability, reliability, phishing resistance, and user acceptance. No single authentication method is suitable for every application or user. The appropriate method depends on factors such as the sensitivity of the account, potential security risks, available technology, and user requirements. Therefore, organizations should evaluate authentication methods using multiple criteria and select an approach that provides adequate security while maintaining a practical and convenient user experience.

VI. Research Methodology

A. Research Design

This study uses a quantitative research approach with a descriptive research design. The study focuses on understanding users' awareness, usage, security concerns, preferences, and acceptance of modern authentication methods. Primary data was collected through a structured online questionnaire, and the responses were analyzed using frequencies and percentages.

B. Survey and Data Collection

Primary data was collected through a structured online questionnaire created using Google Forms. The survey was conducted to understand users' awareness, usage, security concerns, preferences, and acceptance of modern authentication methods. The survey was conducted anonymously, and respondents' names and email addresses were not collected. A total of 77 valid responses were received (75 for the awareness-of-threats question, which two respondents left unanswered).

C. Questionnaire

A structured questionnaire consisting of 16 questions was prepared to collect primary data regarding modern authentication methods. The questions covered: (1) age group, (2) current status, (3) comfort with new digital technologies, (4) awareness of online security threats, (5) familiarity with authentication methods, (6) frequency of use of modern authentication methods, (7) modern authentication methods used, (8) difficulties faced with traditional passwords, (9) authentication methods used in daily life, (10) perceived main security advantage of modern authentication, (11) main concern when using modern authentication, (12)

preference between traditional and modern authentication, (13) importance of security when choosing an authentication method, (14) factors that would encourage greater use of modern authentication, (15) comfort using modern authentication for most online accounts, and (16) preference for modern authentication over traditional passwords in the future.

VII. Results and Discussion

A. Respondent Age:

The results show that the majority of respondents (N = 77) belong to the 18–24 age group (68.8%), followed by the 25–34 age group (22.1%). A smaller proportion belongs to the 35–44 age group (6.5%) and the more than 45 age group (2.6%).

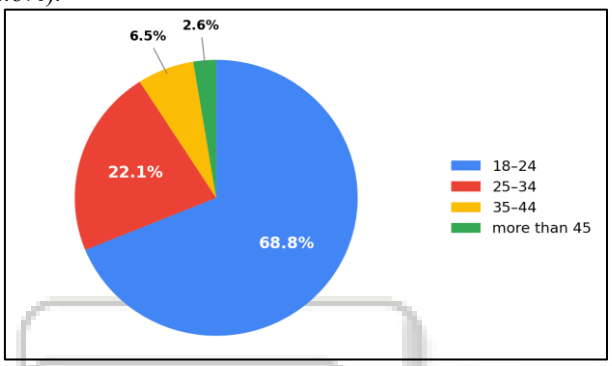

Fig. 2: Age group of respondents.

B. Current Status:

The results show that students form the largest group of respondents (51.9%), followed by employed respondents (24.7%). Unemployed respondents account for 16.9%, while self-employed/business respondents represent 5.2% and other respondents account for 1.3%.

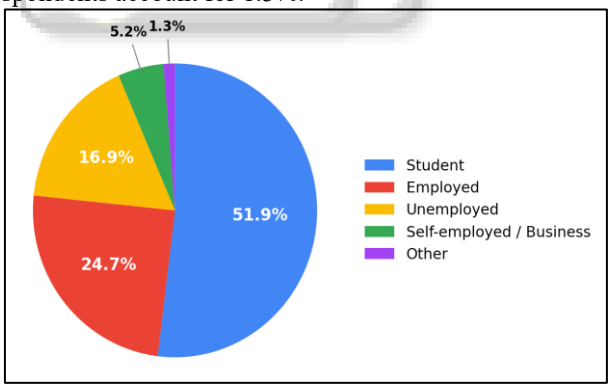

Fig. 3: Current status of respondents.

C. Comfort with Digital Technologies:

Among the 75 respondents who selected a labeled option, 61.3% reported being very comfortable with using new digital technologies, 33.3% comfortable, and 5.3% neutral, indicating that most respondents are comfortable with adopting new digital technologies. Two of the 77 raw responses to this question were recorded as the numeral "1" rather than a labeled option; since it is not confirmed what this value corresponds to on the original form, these two responses are excluded from the percentages above rather than assumed to mean any particular option.

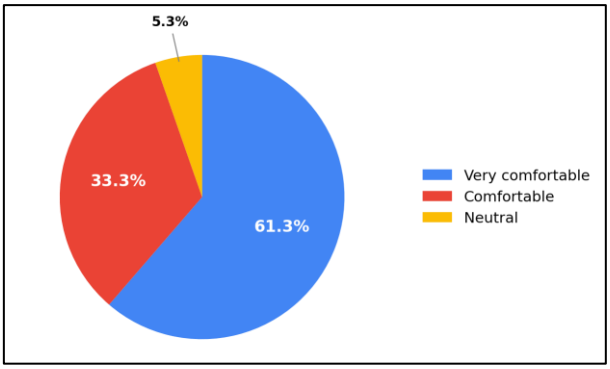

Fig. 4: Comfort level with using new digital technologies.

D. Awareness of Online Security Threats:

The results indicate a high level of awareness of online security threats among the respondents (N = 75; 2 respondents did not answer this question). A majority of respondents reported being very aware of threats such as phishing, hacking, and identity theft, while others reported being somewhat or slightly aware. Only a small proportion indicated that they were not aware of such threats. This suggests that respondents generally have a good understanding of common online security risks.

E. Familiarity with Authentication Methods:

The results show that respondents generally have a good level of familiarity with authentication methods used to protect online accounts. A majority of respondents reported being very familiar with these methods, while others indicated that they were somewhat or slightly familiar. Only a small proportion were unsure about authentication methods. This indicates that modern authentication concepts are generally known among the respondents.

Aspect	Result
Awareness of online security threats (n=75)	Very aware – 69.3%; Somewhat aware – 20.0%; Slightly aware – 9.3%; Not aware – 1.3%
Familiarity with authentication methods (n=77)	Very familiar – 62.3%; Somewhat familiar – 19.5%; Slightly familiar – 15.6%; Not sure – 2.6%
Frequency of modern authentication use (n=77)	Daily – 64.9%; Several times/week – 18.2%; Once/week – 9.1%; A few times/month – 5.2%; Rarely – 2.6%

Table I: Awareness And Usage of Modern Authentication

F. Usage of Modern Authentication Methods:

Fig. 5 shows the modern authentication methods used by respondents (N = 77; multiple selections allowed). Fingerprint authentication was the most commonly used method (76.6%), followed by OTP (57.1%), face recognition (49.4%), and passkeys (46.8%). Microsoft SSO had comparatively limited usage (1.3%). The results indicate that biometric authentication and OTP-based methods are more familiar and commonly adopted among respondents.

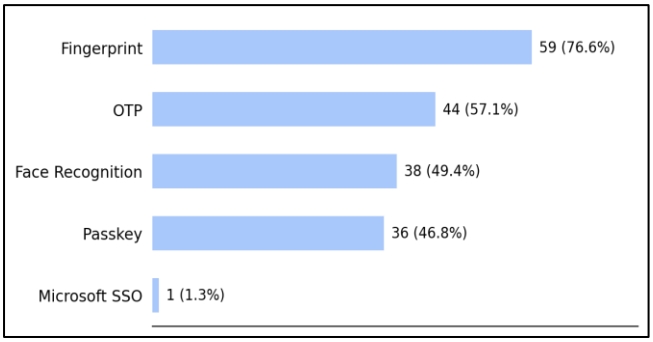

Fig. 5: Modern authentication methods used by respondents.

G. Difficulties with Traditional Passwords:

The results show that traditional password authentication creates several difficulties for users. Forgetting passwords was the most common individual difficulty, closely followed by respondents who selected all of the listed difficulties, and remembering multiple passwords. Password-reset requirements and security concerns were reported less frequently. These findings indicate that password management can reduce convenience and contribute to a less satisfactory authentication experience.

Difficulty	Percentage
Forgetting passwords	35.1%
All of the above	33.8%
Remembering many passwords	18.2%
Password reset	7.8%
Security concerns	5.2%

Table II: Difficulties Faced with Traditional Passwords (N = 77)

H. Authentication Methods Used in Daily Life:

Fig. 6 shows the authentication methods commonly used by respondents in their daily lives (N = 77; multiple selections allowed). Fingerprint authentication is the most frequently used method (72.7%), followed by traditional passwords (64.9%) and face recognition (42.9%). Pattern locks are also used by a considerable proportion of respondents (31.2%), while passkeys show comparatively lower daily usage (24.7%). The results indicate that biometric authentication is widely integrated into users' everyday digital activities, and that traditional passwords remain in common parallel use despite their known drawbacks.

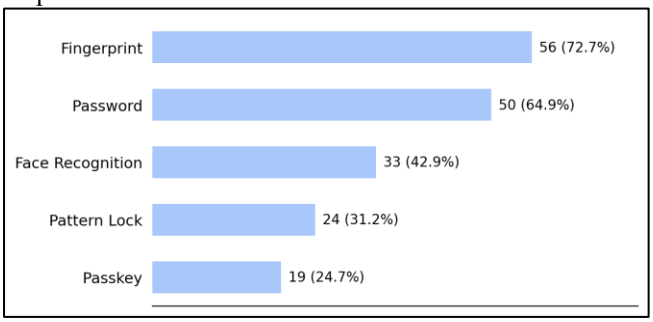

Fig. 6: Authentication methods used by respondents in daily life.

I. Perceived Security Advantages:

Table III shows that respondents consider modern authentication methods more secure than traditional passwords. The most common response was that all of the listed advantages apply, closely followed by reduced risk of password theft, indicating that users primarily value protection against credential theft, followed by phishing resistance and reduced reliance on memorized passwords.

Advantage	Percentage
All of the above	40.3%
Less risk of password theft	39.0%
Better protection from phishing	16.9%
No need to remember passwords	3.9%

Table III: Perceived Main Security Advantage of Modern Authentication

J. Main Concerns:

Privacy is the main concern among respondents when using modern authentication methods. Other concerns include losing the authentication device, technical issues, and limited website support.

Concern	Percentage
Privacy	46.8%
All of the above	31.2%
Losing device	11.7%
Technical issues	6.5%
Website support	3.9%

Table IV: Main Concerns with Modern Authentication

K. Authentication Preference:

Most respondents (55.8%) prefer modern authentication methods when given a choice between traditional passwords and modern alternatives. A further 32.5% prefer using both methods depending on the situation, while only 9.1% prefer traditional passwords and 2.6% were not sure.

Fig. 7: Respondents' preference for traditional and modern authentication methods.

L. Security Importance and Adoption Factors:

The results show that security is considered highly important when choosing an authentication method (72.7% rated it "very important"). Better security was the main factor that could encourage respondents to use modern authentication methods more often (40.3%), followed by respondents selecting all of the listed factors (36.4%) and faster, easier login (16.9%). This indicates that both security and usability influence the adoption of modern authentication.

M. Willingness and Future Preference:

Table V shows strong acceptance of modern authentication methods. Most respondents indicated that they would be comfortable using these methods for most online accounts (74.0% definitely yes) and would prefer them over traditional passwords in the future (71.4% definitely yes).

Response	Comfortable Using Modern Authentication	Prefer Modern Authentication in Future
Definitely Yes	74.0%	71.4%
Probably Yes	20.8%	22.1%
Probably No	5.2%	3.9%
Definitely No	0.0%	2.6%

Table V: Willingness And Future Preference for Modern Authentication (N = 77)

N. Hypothesis Testing

Hypothesis testing is a statistical method used to determine whether the observed survey responses provide sufficient evidence to support a particular assumption about the population.

- H_0 (Null Hypothesis): The responses to Q16 (future preference for modern authentication over traditional passwords) are equally distributed across the four response categories (Definitely Yes, Probably Yes, Probably No, Definitely No).
- H_1 (Alternative Hypothesis): The responses to Q16 are not equally distributed across the four response categories.
- Test (Statistic): To test the above hypotheses, the Pearson Chi-Square Goodness-of-Fit Test is used. This test determines whether the observed frequencies across the response categories differ significantly from the frequencies expected under an equal (uniform) distribution. The variable considered is Q16 — future preference for modern authentication methods instead of traditional passwords.
- Level of Significance: $\alpha = 0.05$ (5%). A result is considered statistically significant when the p-value is less than 0.05.
- Confidence Level: 95%.
- Chi-Square Formula: $\chi^2 = \Sigma (O - E)^2 / E$, where O = observed frequency, E = expected frequency, χ^2 = chi-square test statistic.
- Step 1 – Observed Frequencies: Definitely Yes = 55, Probably Yes = 17, Probably No = 3, Definitely No = 2, Total = 77. These values represent the actual responses obtained from the survey.
- Step 2 – Expected Frequencies: There are 4 response categories. Assuming an equal expected distribution, Expected Frequency = Total responses / Number of categories = 77 / 4 = 19.25 for each category.

Response	Observed (O)	Expected (E)
Definitely Yes	55	19.25
Probably Yes	17	19.25
Probably No	3	19.25
Definitely No	2	19.25

Table VI: Observed And Expected Frequencies (Q16)

- Step 3 – Chi-Square Calculation: Definitely Yes: $(55 - 19.25)^2 / 19.25 = 66.39$. Probably Yes: $(17 - 19.25)^2 / 19.25 = 0.26$. Probably No: $(3 - 19.25)^2 / 19.25 = 13.72$. Definitely No: $(2 - 19.25)^2 / 19.25 = 15.46$. Therefore, $\chi^2 = 66.39 + 0.26 + 13.72 + 15.46 = 95.83$.
- Step 4 – Degrees of Freedom: For a goodness-of-fit test, $df = k - 1$, where k = number of categories = 4. Therefore, $df = 4 - 1 = 3$.
- Step 5 – P-Value: The calculated values are $\chi^2 = 95.83$ and $df = 3$. The corresponding p-value is $p \approx 1.22 \times 10^{-20}$, which is far below the $\alpha = 0.05$ threshold ($p < 0.001$).
- Step 6 – Decision: The decision rule is: if $p < 0.05$, reject H0; if $p > 0.05$, fail to reject H0. Here, $p < 0.001 < 0.05$. Therefore, we reject the Null Hypothesis (H0).

O. Conclusion:

We reject the Null Hypothesis (H0). The observed distribution of responses to Q16 differs significantly from an equal distribution across the four categories — that is, respondents did not select the four options with equal likelihood. The largest category by far was "Definitely Yes" (55 of 77 responses), so the direction of this departure is toward strong future acceptance of modern authentication; however, the test itself establishes only that the distribution is non-uniform, not that any single respondent's preference is free of chance influence.

P. Discussion

The survey results are broadly consistent with the patterns identified in the literature review. Respondents reported high awareness of online security threats (69.3% very aware) and strong familiarity with authentication methods (62.3% very familiar), which supports Clarke and Furnell's observation that usable authentication is increasingly embedded in everyday digital experience rather than treated as a specialist concern [1]. Fingerprint authentication was the most-used method both in general (76.6%) and in daily life (72.7%), reinforcing the survey and privacy findings of Rui and Yan regarding the practical dominance of biometric authentication in consumer settings [3].

The difficulties most commonly reported with traditional passwords — forgetting passwords (35.1%) and remembering multiple passwords (18.2%) — directly mirror the usability burden documented by De Cristofaro et al. in their comparative usability study of authentication methods [5], and help explain why 55.8% of respondents preferred modern authentication outright and a further 32.5% preferred a mixed approach depending on the situation. At the same time, privacy emerged as the leading concern with modern methods (46.8%), echoing the privacy and secure-storage issues raised around biometric data by Rui and Yan [3] and the adoption barriers identified by Matzen et al. for passkeys specifically [2]. This survey cannot establish a broader shift in concern over time, but the fact that privacy — rather than password-management burden — was the top concern reported for modern methods is consistent with the literature's expectation that biometric and device-bound credentials introduce a different category of concern than passwords do.

The chi-square goodness-of-fit test result ($\chi^2 = 95.83$, $df = 3$, $p \approx 1.22 \times 10^{-20}$) indicates that responses to the future-preference question (Q16) are not evenly spread across the four categories — the observed distribution departs significantly from the equal distribution assumed under H0. Combined with the finding that security was rated "very important" by 72.7% of respondents and that better security was the top factor that would encourage greater use (40.3%), this pattern is consistent with the security-usability trade-off model proposed by Braz, Seffah, and M'Raïhi [9]: respondents appear to be favoring methods perceived to

deliver both security and convenience, rather than trading one for the other. This is also consistent with the practical usability findings of Rivera-Dourado et al., who found passkeys performed at least as well as passwords on usability while offering stronger phishing resistance [8].

VIII. Conclusion

This study examined modern authentication methods with a focus on security, usability, reliability, phishing resistance, and user acceptance, using a structured survey of 77 respondents. The findings show that users are generally aware of online security threats (69.3% very aware) and familiar with authentication methods (62.3% very familiar), and that biometric authentication — particularly fingerprint recognition — is already the dominant method in both general use (76.6%) and daily life (72.7%).

Forgetting and managing multiple passwords remain important problems with traditional authentication. The results also show a preference for modern authentication methods: 55.8% of respondents preferred modern authentication outright, while a further 32.5% preferred using both modern and traditional methods depending on the situation, compared with 9.1% who preferred traditional passwords alone. Security was considered very important by 72.7% of respondents. The chi-square goodness-of-fit test showed that responses to the future-preference question are not evenly distributed across the four response categories ($\chi^2 = 95.83$, $df = 3$, $p < 0.001$) — the sample's preference is skewed toward modern authentication rather than occurring by chance.

At the same time, privacy (46.8%) and, to a lesser extent, device loss and technical reliability remain genuine barriers that modern authentication providers need to address. Overall, the results support the view that modern authentication methods can offer a practical and well-accepted alternative to traditional passwords, provided that security gains are not achieved at the expense of usability, and that privacy-related concerns are addressed transparently.

IX. Future scope

This study is based on a single institution-linked sample skewed toward the 18–24 age group (68.8%) and students (51.9%), so future research should replicate the survey across larger, more age- and occupation-diverse populations to test whether the strength of preference for modern authentication holds across demographics.

Future work can also move beyond self-reported preference toward observed behavior — for example, measuring actual authentication success and abandonment rates for passkeys, biometric methods, and risk-based authentication in real deployment settings, rather than relying solely on survey responses. Given that privacy was the leading concern in this study, targeted research into how modern authentication providers communicate and control biometric and device data could help close the gap between perceived and actual privacy risk identified here and in prior work [2], [3].

Finally, longitudinal studies that track the same users' authentication behavior as passkeys and passwordless systems become more widely supported by websites and apps would help determine whether the strong stated intent to adopt modern authentication (Section VI) translates into sustained real-world use, and whether integrating multiple methods (e.g., biometrics combined with risk-based triggers) can further reduce the security-usability trade-off documented in this and prior studies [4], [6], [9].

References

[1] N. Clarke and S. Furnell, "Usable authentication: Are we there yet?," *Computers & Security*, vol. 162, Art. no. 104823, 2026. DOI: 10.1016/j.cose.2025.104823

[2] A. Matzen, A. Rüffer, M. Byllemos, O. Heine, M. Papaioannou, G. Choudhary, and N. Dragoni, "Challenges and potential improvements for passkey adoption—A literature review with a user-centric perspective," *Applied Sciences*, vol. 15, no. 8, Art. no. 4414, 2025. DOI: 10.3390/app15084414

[3] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019. DOI: 10.1109/ACCESS.2018.2889996

[4] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, Art. no. 1, 2018. DOI: 10.3390/cryptography2010001

[5] E. De Cristofaro, H. Du, J. Freudiger, and G. Norcie, "A comparative usability study of two-factor authentication," *arXiv preprint arXiv:1309.5344*, 2013. DOI: 10.48550/arXiv.1309.5344

[6] A. Gunuganti, "Risk based authentication," *Journal of Artificial Intelligence & Cloud Computing*, vol. 1, no. 1, pp. 1–6, 2022. DOI: 10.47363/JAICC/2022(1)305

[7] A. M. Di Campi and F. L. Luccio, "Accessible authentication methods for persons with diverse cognitive abilities," *Universal Access in the Information Society*, vol. 24, pp. 2195–2217, 2025. DOI: 10.1007/s10209-025-01189-4

[8] M. Rivera-Dourado, R. Pérez-Jove, A. Pazos, and J. Vázquez-Naya, "Usability of passwordless authentication in Wi-Fi networks: A comparative study of passkeys and passwords in captive portals," *arXiv preprint arXiv:2603.25290*, 2026. DOI: 10.48550/arXiv.2603.25290

[9] C. Braz, A. Seffah, and D. M'Raïhi, "Designing a trade-off between usability and security: A metrics based-model," in *INTERACT 2007: 11th IFIP TC 13 International Conference on Human-Computer Interaction*, pp. 114–126, 2007. DOI: 10.1007/978-3-540-74800-7_9

