Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Choosing the right MFA method for online systems: A comparative analysis

Nader Abdel Karim[a*], Hasan Kanaker[b], Waleed K. Abdulraheem[c], Majdi Ali Ghaith[d], Essam Alhroob[b] and Abdulla Mousa Falah Alali[e]

[a]*Department of Intelligent Systems, Faculty of Artificial Intelligence, Al-Balqa Applied University, Al-Salt, Jordan*
[b]*Department of Cyber Security, Isra University, Amman, Jordan*
[c]*The World Islamic Sciences and Education University Amman, Jordan*
[d]*Department of Islamic Banking, The University of Jordan, Amman, Jordan*
[e]*Department of Computer Science, Isra University, Amman, Jordan*

C H R O N I C L E

Article history:
Received: July 18, 2023
Received in revised format: September 3, 2023
Accepted: October 4, 2023
Available online: October 4, 2023

Keywords:
Online systems
Online accounts
Authentication methods
MFA
User authentication
User verification

A B S T R A C T

A robust authentication method is needed to protect online user accounts and data from cyber-attacks. Using only passwords is insufficient because they can be easily stolen or cracked. Multi-factor authentication (MFA) increases security by requiring two or more verification factors from the user before granting access to a resource such as an online account or an application. MFA is essential to a strong identity and access management (IAM) policy. This study evaluates and contrasts several MFA methods for online systems, including Microsoft Authenticator, FIDO2 security keys, SMS, voice calls, and biometrics. We assess these methods based on four criteria: security, usability, cost, and compatibility. We discover that only some MFA methods excel across the board. The best MFA method will depend on the organization's and users' specific needs and preferences. Each MFA method has benefits and drawbacks on its own. Based on our analysis, we do, however, make some general observations and recommendations, such as preferring FIDO2 security keys and certificate-based authentication for high-security scenarios, choosing Microsoft Authenticator and biometrics for high-usability scenarios, and avoiding SMS and voice calls for low-security and low-usability scenarios.

1. Introduction

Online systems, such as online banking, emails, social networks, and e-learning systems are more frequent targets of cyberattacks that aim to hack user accounts and access confidential data or resources. For user authentication in the online environment, both traditional and modern methods like passwords, PINs, and OTPs (i.e., tokens) are frequently utilized. Due to their widespread usage, these approaches are known to most users. However, passwords and PINs can also be exploited by guessing, dictionary, brute-force, and shoulder-surfing attacks. Furthermore, passwords can be bypassed by various techniques, such as social engineering, phishing, or channel-jacking, that trick users into disclosing their credentials or intercepting their communication. Smart cards and other tokens that require the OTP, such as smartphones, are susceptible to theft, duplication, and loss (Karim & Shukur, 2015; Karim et al., 2021). Furthermore, Biometric based authentication (BBA) is a common authentication strategy used with online systems. Biometric authentication uses unique physiological or behavioral characteristics to identify users (Karim et al., 2021; Lee & Jeong, 2021). Since they are based on everyone's unique features, physiological biometrics like facial, fingerprint, and iris recognition are reliable and accurate. However, potential issues like alterations in lighting, facial hair, or physical injuries could impact how accurate these biometric readings are. Additionally, several privacy issues and erroneous uses of biometric data are being raised (Karim et al., 2020; Rui & Yan, 2019). With the online system, fingerprint recognition is the physiological biometric method that is most frequently used. This method looks at the ridges and valleys on a person's fingertips. Due to its simplicity and non-intrusiveness, behavioral biometrics such as voice

* Corresponding author.
E-mail address: nader.salame@bau.edu.jo (N. A. Karim)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2023.10.003

recognition, keyboard dynamics, and touchscreen interactions can offer a potential solution for user identification in online systems (Zhang et al., 2020). However, environmental factors such as noise, illness, or emotional state make them less accurate than physiological biometrics (Karim et al., 2020; Rui & Yan, 2019; Zhang et al., 2020). For the privacy and security of biometric authentication, it's crucial to ensure the storage and transfer of biometric data and individual training and awareness.

According to a report by Microsoft (Maynes, 2019), more than three hundred million fraudulent sign-in attempts are identified across its cloud services daily. Single-factor authentication (e.g., passwords) is one of the leading causes of this vulnerability. Online systems should employ more robust authentication measures than single-factor authentication. Multi-factor authentication (MFA), sometimes known as two-factor authentication (2FA) or 2-step verification (2SV), is the most common authentication technique that goes “beyond single-factor authentication” (Sinigaglia et al., 2020). Any MFA account requires the user to provide a second factor to verify their identity (Ometov et al., 2018). This second factor can be based on one of the following categories:

- Knowledge-based authentication (KBA): Something the user knows, typically a password, Personal Identification Number (PIN), and security question.
- Possession-based authentication (PBA): Something the user has (i.e., Token), such as a trusted device that is not easily duplicated, like a magnetic card, a phone, a dongle, or a hardware key.
- Biometric-based authentication (BBA): Something the user is - biometrics like a fingerprint or face scan.

By requiring two or more factors from different categories, MFA can significantly reduce the risk of unauthorized access, as an attacker must compromise both factors to succeed (Ometov et al., 2018). For example, even if the attacker obtains the user's password through phishing, they will still need access to the user's device to complete the authentication process. However, not all MFA methods are safe, usable, cost-effective, or compatible with various online platforms. Therefore, selecting the appropriate MFA method for a given scenario requires careful consideration of various factors and trade-offs. This paper aims to provide a comprehensive review and comparative analysis of some of the most popular and widely used MFA approaches for online systems. We focus on the following methods:

- Microsoft Authenticator: A mobile application that uses push notifications, biometrics, or one-time passcodes (OTPs) as an authentication agent (Meyer et al., 2023).
- FIDO2 security keys: Devices that use cryptographic protocols to verify users without asking for passwords(Huseynov, 2022).
- Certificate-based authentication: in this method, we use a digital certificate saved on smart cards or USB tokens as an authentication agent (Gupta & Varshney, 2023).
- OATH Device Tokens: A hardware device that generates OTPs based on the time or synchronization of the event(Bae et al., 2022).
- OATH Software Tokens: Its software application generates OTPs based on the time or synchronization of the event (Khan & Miah, 2022).
- SMS: Using text messages to receive OTPs on the user's phone number (Karim et al., 2020).
- Voice Call: A method of calling the user's phone number and asking him/her to enter the OTP using the keypad (Smallman, 2020).
- Biometrics: A method that relies on the physiological or behavioral characteristics of the user as authentication factors (Karim et al., 2020).

The contribution that this research is supposed to make in the field of MFA is as follows:

- Increased MFA awareness: The paper is anticipated to increase MFA awareness among organizations and users. This will encourage more businesses to use MFA and more users to use it.
- A better comprehension of MFA techniques: The paper is anticipated to offer an understanding of MFA techniques and their advantages and disadvantages. This will enable businesses to select the best MFA technique for their requirements.
- Increased MFA acceptance: The paper is anticipated to increase MFA adoption across organizations and users. This will decrease the possibility of data breaches and aid in improving security.

The rest of the article is organized as follows: Section 2 explores related works, Section 3 describes the methodology, Section 4 presents the results, Section 5 discusses the implications, and Section 6 concludes the article.

2. Related Works

Previous studies have investigated various aspects of online systems' multifactor authentication (MFA) methods, such as usability, security, reliability, and user preferences. For example, Drager (2021) compared the user experience of different MFA methods, such as SMS, voice calls, email, and authentication applications, and the results showed that authentication applications were the preferred choice by users.

Subbarao et al. (2023) evaluated the security and usability of FIDO2 security keys and found that they were more secure than passwords. Witts (2023) surveyed on MFA adoption and use among 1,525 online users and found that only 28% had used MFA for at least one online account. The main barriers to adopting the MFA approach were a need for more awareness and perceived complexity and inconvenience. (Mohanakrishnan, 2021) Comparing the performance and user satisfaction of different types of OTPs, such as SMS, voice calls, email, and software tokens, it was found that software tokens had the highest accuracy and satisfaction rates.

Analyze biometric authentication's security risks and benefits and propose a framework for evaluating MFA biometric methods based on various criteria. (Velásquez et al., 2017) conducted a systematic literature review of 515 single-factor authentication techniques and 442 multi-factor authentication techniques proposed in the literature. They also discussed seventeen articles on comparison and selection criteria for authentication technologies and eight frameworks that help in such a task. They found that smart card-based authentication was the most-searched single-factor technology while combining text passwords and smart cards was the most-searched multi-factor method. They also noted that usability, security, and costs were the most frequently used criteria for comparing and selecting authentication systems.

Authors (Ometov et al., 2018) comprehensively surveyed different MFA styles based on knowledge, possession, and heredity factors. They also discussed challenges and future directions for MFA research. They classified MFA approaches into four categories: static, dynamic, adaptive, and risk-based. They highlight each category's advantages and disadvantages and suggest recommendations to improve MFA security and usability. However, most previous research either concentrated on a few MFA approaches or did not offer a thorough comparative analysis of their advantages and disadvantages. Additionally, some MFA techniques have improved or added new features over time, which may impact on their efficiency and user satisfaction. Therefore, a current and thorough analysis of the most common and widely employed MFA techniques for online systems is required. We also review each method's benefits and drawbacks and provide recommendations for users and online service providers.

Based on (Covavisaruch, 2006; Elshamy et al., 2021; Tarannum & Rahman, 2019) other biometric modalities are being investigated for use as MFA in biometric systems, in addition to fingerprint and facial identification, including iris and retina scanning and voice recognition. The biometric modalities of iris and retina scanning are considered remarkably accurate and less prone to spoofing attacks than other modalities like fingerprints. Another interesting biometric technology is voice recognition (i.e., behavioral biometric), which can recognize persons even when they are not looking at the camera or wearing a mask. Behavioral biometrics can identify users even if they use a different device or if their appearance has changed (Furnell et al., 2018; Saevanee et al., 2012; Silva, 2021). But to guarantee the security of biometric systems, several issues also need to be resolved. A difficulty is preventing unauthorized access to biometric data. The sensitivity of biometric data is frequently seen as being higher than that of other categories of personal information, such as passwords and credit card numbers. The authentic user could be impersonated if biometric data is compromised (Hublikar et al., 2023; Karim et al., 2020).

3. Evaluation Method

Based on four main factors—security, usability, cost, and compatibility— which are considered the main factors in evaluating user authentication methods (Elshenaway & Guirguis, 2021; Ghorbani Lyastani et al., 2020; Gunson et al., 2011; Kim et al., 2022; Ogbanufe & Kim, 2018; Sadhu et al., 2022), this study assesses the MFA methods that are most widely used. Based on our evaluation of the literature and our own experiences, we rate each criterion from 1 (lowest) to 5 (highest). Our evaluation depends on previous literature that studies each authentication method's features. Also, expert evaluation is essential in this research. Four authors of this manuscript are cyber security specialists in user authentication, malware, and cryptography.

The paper summarizes our findings in a table and recommends the most appropriate MFA method for several scenarios.

3.1 Security

Security is the core criterion for evaluating MFA methods, as it indicates how well they can defend against common identity attacks. Based on the literature review, this study considers the following security aspects:

- Phishing resistance: Phishing is a form of social engineering in which online attackers use email or malicious websites to obtain user information or credentials (Kanaker et al., 2022). Some MFA methods are vulnerable to phishing because they rely on user input or interaction that attackers can intercept or manipulate. For example, an attacker could create a fake website that simulates a legitimate login portal and requires the user to enter a username, password, and OTP. Alternatively, the attacker could bombard the user with push notifications until they hit the "Accept" button, thus granting the attacker access to the Network (Hall et al., 2023). Phishing-resistant MFA methods are immune from attempts to compromise or subvert the authentication process, commonly achieved through phishing attacks. Phishing-resistant MFA methods are immune to attempts to hack or sabotage the authentication process, mostly achieved through phishing attacks. Anti-phishing MFA methods use cryptographic protocols that bind authentication to the domain and prevent authentication secrets or output from being revealed to a website or application masquerading as a legitimate system (Ciolino et al., 2019). Examples of phishing-proof MFA methods are FIDO2 security keys and certificate-based authentication.

- Resistance to other attacks: Besides phishing, different types of attacks can target MFA methods, such as brute force attacks, man-in-the-middle attacks (Wang et al., 2021) replay attacks, credential stuffing, SIM swap attacks, and exploitation of SS7 protocol vulnerabilities. These attacks aim to bypass, intercept, or compromise MFA methods' verification agents or channels. For example, an attacker can use a brute force attack to guess the OTP generated by a hardware or software token. Alternatively, the attacker could use a SIM swap attack to transfer the user's phone number to a new SIM card and receive verification codes from SMS or voice calls(Ciolino et al., 2019; Karim et al., 2021). Another attack resistance depends on each MFA method's security features and mechanisms, such as encryption, hashing, salting, nonce generation, challenge-response protocols, and device verification. Based on these aspects of security.

The results in Table 1 are based on a literature review(Alhakami, 2020; Ghorbani Lyastani et al., 2020; Komarova et al., 2018; Org et al., 2017; Rajeswari & Seenivasagam, 2016; Velásquez et al., 2019) that discusses the security aspects of each authentication method and compares each user authentication method with other authentication methods. Also, breaches or vulnerabilities reported by Authorities specialized in the field, such as Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD) (Dong et al., 2019; MITRE, 2023; NIST, 2023), are also taken into consideration.

Table 1
MFA methods scores in terms of security

MFA Method	Security Score	Explanation
Microsoft Authenticator	4	Microsoft Authenticator uses push notifications, biometrics, or OTP as authentication factors. Push notifications and biometrics are more secure than OTPs because they do not depend on user interaction or input that an attacker could intercept or modify. Nonetheless, push notifications can still be vulnerable to blasting attacks if the user is not careful. OTPs can also be hacked by phishing or other attacks if users enter them on a fake website or app (Meyer et al., 2023).
FIDO2 security keys	5	FIDO2 security keys use cryptographic protocols that bind authentication to the domain and prevent authentication secrets or output from being disclosed to a website or application masquerading as a genuine system. FIDO2 security keys are considered the gold standard for MFA by CISA because they are immune to phishing and other common identity attacks (Huseynov, 2022).
Certificate-based authentication	5	Smart cards or USB tokens that store digital certificates are used as authentication elements in certificate-based authentication. Additionally, certificate-based authentication uses cryptographic protocols to bind the authentication to the domain and prohibit the disclosure of authentication secrets or output to a website or application pretending to be a legitimate system. Phishing and other typical identity attacks cannot be used against certificate-based authentication (Ometov et al., 2018).
OATH hardware tokens	3	OATH hardware tokens produce OTPs depending on synchronized events or time. Users who input their OTP on a fake website or application are susceptible to phishing and other assaults. Hardware tokens can also be damaged, stolen, or misplaced, which might limit their usability and availability (Khan & Miah, 2022).
OATH software tokens	3	OATH software tokens provide OTPs based on the synchronization of events or time. Users who input their OTP on a fake website or application are susceptible to phishing and other assaults. Additionally, software tokens depend on the functionality and security of the device on which they are installed, which might be compromised by malware or other threats(Bae et al., 2022).
SMS	2	SMS uses the user's phone number to text OTPs to the user. Users who input their SMS on a fake website or application are susceptible to phishing and other attacks. Furthermore, SIM swap attacks could intercept or corrupt SMS(Jover, 2020).
Voice call	2	When a user receives a voice call, they are prompted to enter an OTP using the keypad. Users who input their phone numbers on a fake website or application are susceptible to phishing and other attacks. Additionally, SIM swap attacks and the use of SS7 protocol vulnerabilities can lead to voice call interception or compromise (Elshamy et al., 2021).
Biometrics	4	Biometrics utilizes the user's behavioral or physiological characteristics as verification factors, such as voice, face, iris, or fingerprint identification. Because they do not rely on user interaction or input that can be intercepted or manipulated by attackers, biometrics are more secure than OTPs. However, sophisticated attacks that exploit fake biometric samples or devices can still spoof or circumvent biometrics (Heidari & Chalechale, 2022; Rui & Yan, 2019).

3.2 Usability

Usability is another crucial factor when assessing MFA techniques because it shows how easy and convenient, they are for users to learn and apply. We consider the following elements of usability:

- User experience: User satisfaction level and comfort with an MFA approach is called user experience. The ease of enrollment, ease of use, verification speed, error rate, and user feedback can all impact the user experience. For instance, a long OTP that users must input each time they sign in may result in a poor user experience compared to an MFA technique that only requires users to tap a hardware key or scan their fingerprint.
- Availability: This indicates how accessible and reliable an MFA approach is. Device dependence, network dependence, battery life, and durability are some factors that can affect availability. For instance, if a mobile phone is lost, stolen, destroyed, or runs out of battery, an MFA technique that relies on it may not be as available. If the network is slow, unstable, or unavailable, an MFA technique that relies on a network connection may have limited availability.

In this comparison criterion, we based our analysis on literature (Ghorbani Lyastani et al., 2020; Karim et al., 2020; Komarova et al., 2018; Ogbanufe & Kim, 2018; Oren & Arad, 2022; Org et al., 2017; Rajeswari & Seenivasagam, 2016), which discusses the user satisfaction and usability aspects of each authentication method. We also referred to the usability features provided by vendors (Akar & Mardiyan, 2016; Alex, 2022; *FIDO2 Passwordless Authentication | YubiKey |*, 2023). Table 2 displays the scores for each MFA method based on the above usability criteria.

Table 2
MFA methods scores in terms of usability

MFA Method	Usability Score	Explanation
Microsoft Authenticator	4	The user interface of Microsoft Authenticator is good, and it allows users to verify their identities using push notifications, biometrics, or OTPs. Compared to OTPs, push notifications and biometrics are easier to use and faster because they do not need user input or interaction. If biometrics or push notifications fail or are not accessible, OTPs can still be utilized as a backup option. Due to its reliance on a mobile device that may be lost, stolen, broken, or run out of battery, Microsoft Authenticator has a moderate degree of availability. Push notifications and OTPs require a network connection as well. To help customers recover their accounts on a new device, Microsoft Authenticator enables encrypted cloud backup and recovery (Meyer et al., 2023).
FIDO2 security keys	5	Users of FIDO2 security keys have outstanding user experience since they can easily authenticate themselves by tapping a hardware device attached to their computer or connected to it via Bluetooth or NFC. FIDO2 security keys do not need user input or activity that an attacker could intercept or modify. Due to their independence from a network or power source, FIDO2 security keys are highly available. They are also strong, lightweight, and convenient tools that work with many PCs (Huseynov, 2022).
Certificate-based authentication	4	Certificate-based authentication has a good user experience, enabling users to verify themselves by inserting a smart card or USB token into their computer or connecting via Bluetooth or NFC. Certificate-based authentication does not need user input or interaction that attackers could intercept or tamper with. Certificate-based authentication has moderate availability because it relies on a smart card or USB token that can be lost, stolen, damaged, or incompatible with some computers. It also depends on the network connection for certificate validation and revocation check (Bae et al., 2022).
OATH hardware tokens	3	OATH hardware tokens have a bland user experience, requiring users to enter a device-generated OTP each time they log in. This could be time-consuming and error-prone, particularly if the OTP is lengthy or frequently changes. Because they are independent of a network or battery, OATH hardware tokens have a moderate level of availability. However, the availability and usability of these items can be impacted if they are lost, stolen, or damaged (Khan & Miah, 2022).
OATH software tokens	3	OATH software tokens have a mediocre user experience since each time a user signs in; they must enter an OTP generated by a software program. If the OTP is long or regularly changes, this can be exhausting and error-prone. OATH software tokens have limited availability due to their reliance on mobile devices, which can be damaged, lost, stolen, broken, or run out of battery. Additionally, they require a network connection to synchronize their time (Khan & Miah, 2022).
SMS	2	SMS provides a poor user experience since each time users sign in, they must input an OTP that was supplied to them via text message. This can be tedious and error-prone, especially if the OTP is long or changes frequently. Because SMS relies on a mobile phone, which can be damaged, lost, stolen, or run out of battery, it is not always available. Additionally, it depends on cellular service, which can be slow, unreliable, or unavailable, as well as a network connection (Jover, 2020; Salameh et al., 2016).
Voice call	2	Voice call has a poor user experience since every time a user signs in; they must input an OTP using the keyboard after receiving a phone call. If the OTP is long or frequently changes, this can be tedious and error-prone. Voice calls are only sometimes available since they rely on mobile devices, which can be damaged, lost, stolen, broken, or run out of battery. Additionally, it depends on cellphone service, which may be slow, unreliable, or unavailable (Elshamy et al., 2021).
Biometrics	4	Biometrics has good user experience, allowing users to verify themselves using their fingerprint, face, iris, or voice recognition. Biometrics are more accessible and faster than OTPs, as they do not require user input or interaction. However, biometrics can still fail or be unavailable due to environmental factors like lighting, noise, or dirt. Biometrics have moderate availability, as they depend on a biometric sensor that can be damaged or incompatible with some devices. They depend on a network connection for biometric validation and revocation checking (Heidari & Chalechale, 2022; Rui & Yan, 2019).

3.3 Cost

Cost is another important criterion for evaluating MFA methods, as it reflects how much they require in terms of initial investment and ongoing maintenance. We consider the following elements of cost:

- Hardware cost: Hardware cost refers to acquiring and maintaining the hardware devices needed for an MFA method. For example, hardware costs include buying and replacing FIDO2 security keys, smart cards, USB tokens, or OATH hardware tokens.
- Software cost: Software cost refers to acquiring and maintaining the software applications needed for an MFA method. For example, software cost includes the cost of buying and updating OATH software tokens or biometric software.
- Service cost: Service cost refers to using and managing the services needed for an MFA method. For example, service cost includes subscribing to Azure AD Premium plans that enable certain MFA features or sending SMS or voice call verification codes.

Table 3 displays the scores for each MFA method based on the above cost criteria.

Table 3
MFA methods scores in terms of cost

MFA Method	Cost Score	Explanation
Microsoft Authenticator	4	Since it only requires a mobile phone as hardware, Microsoft Authenticator has a cheap hardware cost. It has a low software cost as a free program that can be downloaded from the app store. Since specific MFA capabilities and policies can only be enabled with an Azure AD Premium plan, it has a moderate service cost (Cherry, 2022).
FIDO2 security keys	3	FIDO2 security keys have a moderate hardware cost, requiring users to purchase and maintain devices ranging from $10 to $100 per unit. They have a low software cost, as they do not require any additional software applications besides a compatible browser. They have a low service cost and do not need other services besides Azure AD (Würsching et al., 2023).
Certificate-based authentication	3	Certificate-based authentication has a moderate hardware cost because it requires users to buy and maintain USB tokens or smart cards, costing between $10 to $50 each. The software is inexpensive because it only needs a compatible browser and does not require any other applications. It has a low service cost and does not require additional services besides Azure AD (Microsoft, 2023).
OATH hardware tokens	2	OATH hardware tokens have a high cost, as they require users to purchase and maintain hardware devices ranging from $20 to $100 per unit. They have a low software cost, as they do not require any additional software applications besides a compatible browser. They have a low service cost and do not need other services besides Azure AD (Hall, 2023; Microcosm, 2023).
OATH software tokens	3	OATH software tokens have a low hardware cost because they only need a mobile phone as a necessary piece of hardware. They require users to buy and update applications, which can cost anywhere between $1 and $10 per device. Hence, they have a moderate software cost. Since they only need Azure AD, they have a cheap service cost (J. F. J. ,msft, luc, M. S. H. Y. Hall, 2023; Microcosm, 2023).
SMS	2	Because SMS needs a mobile phone as its primary hardware device, it has a low hardware cost. Since it only needs a compatible browser, it has a cheap software cost. It has a high service cost, requiring users to pay for text messages and cellular service that can vary depending on the provider and location (Jr. et al., 2021).
Voice call	2	Because voice calls only need a mobile phone and no other hardware, they have a minimal hardware cost. The software is inexpensive because it only requires a compliant web browser as an additional piece of software. Since customers must pay for phone calls and cellular service, which might vary depending on the provider and area, it has a high cost of service (Elshamy et al., 2021; Jr. et al., 2021).
Biometrics	4	The cost of biometric multi-factor authentication methods can vary depending on the type of authentication used. Regarding fingerprint authentication, most mobile phones and laptops nowadays come with Touch ID fingerprint readers, which leads to lower hardware costs, as well as the face and voice print, as the microphone and camera inside the devices can be used. Biometrics does not need additional software programs besides those supporting biometric authentication (e.g., Windows Hello), so they have a low software cost. Since they only need Azure AD, they have a low service cost (Alsunaidi et al., 2020; Bello & Olanrewaju, 2022; Ogbanufe & Kim, 2018; Rui & Yan, 2019)

Note: The lowest score means the highest cost

3.4 Compatibility

Compatibility is crucial when assessing MFA techniques because it shows how well-suited they are to various devices and applications. We consider the following compatibility factors:

- Application compatibility: Application compatibility describes an MFA method's ability to integrate with various application types, including web, mobile, desktop, and legacy applications. Application compatibility can be affected by factors such as authentication protocols, standards, and APIs. For instance, whereas an MFA method that supports RADIUS or LDAP protocols can integrate with legacy applications, an MFA method that supports OpenID Connect or SAML protocols can be used with modern web applications.
- Device compatibility: Device compatibility is the ability of an MFA technique to function with various device types, including computers, tablets, smartphones, and wearable technology. Operating systems, browsers, drivers, and hardware requirements are just a few examples of the variables that can affect device compatibility. For instance, a method of MFA that needs a USB port or a biometric sensor might not function with some devices that do not have these features.

MFA Vendors' Technical Specification/Documentation and previous literature were the primary sources for the evaluation process (Alex, 2022; *FIDO2 Passwordless Authentication | YubiKey |*, 2023; *User Authentication Specifications Overview*, 2023; Ghorbani Lyastani et al., 2020; J. F. J. ,msft, luc, M. S. H. Y. Hall, 2023). Table 4 displays the scores for each MFA method based on the above compatibility criteria.

Table 4
MFA methods scores in terms of compatibility

MFA Method	Compatibility Score	Explanation
Microsoft Authenticator	4	Microsoft Authenticator has a high degree of application compatibility because it supports the Open ID Connect, SAML, RADIUS, and LDAP protocols. Additionally, using Azure AD Conditional Access policies, MFA can be imposed for particular applications or scenarios. As it functions with iOS and Android devices that have a network connection and a camera, Microsoft Authenticator has a mediocre level of device compatibility. It does not, however, function with Windows phones or camera-less devices (Meyer et al., 2023).
FIDO2 security keys	4	Since FIDO2 security keys support the widely used WebAuthn and FIDO2 standards, they have an elevated level of application compatibility. They additionally support Azure AD Conditional Access policies, which can impose MFA for particular applications or scenarios. A USB port, Bluetooth, or NFC connection is required for FIDO2 security keys to function with Windows 10 and macOS devices. These features, however, are not compatible with iOS devices or other devices (Owens et al., 2021; Owens & Anise, 2020).
Certificate-based authentication	4	Certificate-based authentication has high application compatibility, as it supports OpenID Connect, SAML, RADIUS, and LDAP protocols. It also supports Azure AD Conditional Access policies that can enforce MFA for specific applications or scenarios. Certificate-based authentication has moderate device compatibility, as it works with Windows and macOS devices with a smart card reader or a USB port. However, it does not work with iOS or Android devices or devices that do not have these features (O'Neill et al., 2017).
OATH hardware tokens	3	OATH hardware tokens support RADIUS and LDAP protocols, giving them a moderate level of application compatibility. Additionally, they support Azure AD Conditional Access policies that can impose MFA for particular scenarios or applications. They do not, however, support the widely used SAML or OpenID Connect protocols for modern web applications. OATH hardware tokens are moderately compatible with most devices because they operate on anyone with a web browser. However, they demand that users carry and care for additional hardware that may get damaged, lost, or stolen. (Erdem & Sandikkaya, 2018).
OATH software tokens	3	OATH software tokens support RADIUS and LDAP protocols, giving them a moderate level of application compatibility. Additionally, they support Azure AD Conditional Access policies that can impose MFA for scenarios or applications. They do not, however, support the widely used SAML or OpenID Connect protocols for modern web applications. OATH software tokens can be used with various iOS and Android devices if they have a network connection and a camera. However, they are incompatible with Windows Phone models or devices without cameras(Erdem & Sandikkaya, 2018).
SMS	3	SMS supports the LDAP and RADIUS protocols, giving it a moderate level of application compatibility. Additionally, it supports Azure AD Conditional Access policies that can impose MFA for scenarios or applications. OpenID Connect and SAML, which are frequently used by modern web applications, are not supported. SMS is compatible with various devices if they have a mobile phone number and can send and receive text messages. However, depending on the provider and location, users must pay for text messages and cellular service (Jover, 2020).
Voice call	3	Due to its support for the LDAP and RADIUS protocols, voice calls have poor application compatibility. Additionally, it supports Azure AD Conditional Access policies that can impose MFA for scenarios or applications. OpenID Connect and SAML, which are frequently used by modern web applications, are not supported. Voice calls work with any device with a mobile phone number and can make or receive phone calls, indicating a moderate level of device compatibility. The cost of calls and cellular service, which varies depending on the provider and location, must be paid for by users. However, it requires users to pay for phone calls and cellular service that can vary depending on the provider and location (Elshamy et al., 2021; Vibar, 2021).
Biometrics	4	Because the OpenID Connect and SAML protocols are supported, biometrics has an elevated level of application compatibility. Additionally, it supports Azure AD Conditional Access policies, which can make MFA mandatory for applications or scenarios. When using an iOS or Android device with a biometric sensor and a network connection, biometrics has moderate device compatibility. Nevertheless, it does not work with Windows or macOS devices or devices that do not have a biometric sensor (Alsunaidi et al., 2020; Bello & Olanrewaju, 2022; Ogbanufe & Kim, 2018; Rui & Yan, 2019).

4. Discussion

Based on the scores we assigned to each MFA method based on security, usability, cost, and compatibility, we can see that no single MFA method is the best in all criteria (see Table 5 and Fig. 1).

Table 5
Overall scores for MFA methods

MFA Method	Security Score	Usability Score	Cost Score	Compatibility Score
Microsoft Authenticator	4	4	4	4
FIDO2 security keys	5	5	3	4
Certificate-based authentication	5	4	3	4
OATH hardware tokens	3	3	2	3
OATH software tokens	3	3	3	3
SMS	2	2	2	3
Voice call	2	2	2	3
Biometrics	4	4	4	4

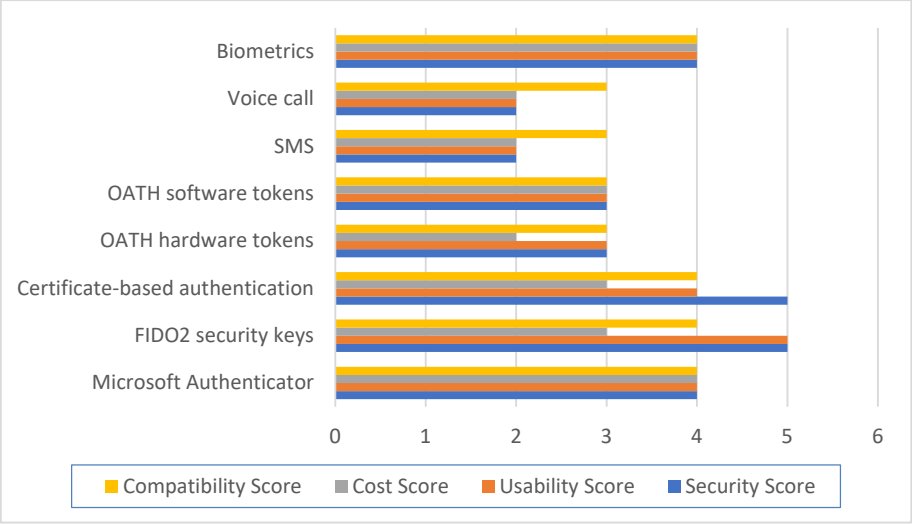

Fig. 1. Performance scores of MFA methods

As shown in Table 5 and Fig. 1, The MFA methods have advantages and disadvantages of their own, and the best option will depend on the requirements and preferences of the organization and the users. Based on our evaluation, we can make the following broad observations and suggestions:

- The most secure and phishing-resistant MFA techniques use FIDO2 security keys and certificate-based authentication; however, these techniques come with a moderate to high hardware cost and limited device compatibility. They are appropriate for organizations with high-security demands who can afford to spend money on user hardware. They are also appropriate for users of Windows or macOS computers with USB ports or smart card readers.
- The most user-friendly MFA techniques are Microsoft Authenticator and biometrics, but they also rely on mobile devices and networks that may be unavailable or compromised. They are appropriate for organizations that prioritize convenience and user experience over cost and security. They are also appropriate for users of iOS or Android devices with cameras or biometric sensors.
- SMS and voice calls are the least secure and least easy to use MFA methods, as they are susceptible to phishing and other attacks and require users to pay for text messages and phone calls. They are not advised for organizations with limited resources or high-security requirements. Additionally, they are not advised for users without a reliable mobile phone number or cellular service.
- Although OATH hardware tokens and OATH software tokens are moderately secure and user-friendly MFA methods, they also require users to enter an OTP each time they sign in, which can be time-consuming and prone to error. They are appropriate for organizations looking for a balance between security and usability and do not want to depend on mobile devices or network connections. They are also appropriate for users of any web-enabled device.
- Biometrics has a perfect security and usability score, the same as Microsoft Authenticator. This means that biometric authentication is an excellent choice for those who want a balance between security and usability and its reasonable cost. However, the privacy issue could be one of the fundamental issues of biometric authentication. If biometric data is compromised or falls into the wrong hands, it can be used for identity theft, fraud, or other malicious purposes.

Therefore, your organization's specific security, usability, cost, and compatibility requirements will determine which MFA method is best for you. Organizations should consider the trade-offs between these criteria and choose the MFA method that best suits their needs. Organizations can also use a combination of different MFA methods to provide more flexibility and options for their users. For instance, you can use FIDO2 security keys as the primary MFA method for high-risk scenarios or users and Microsoft Authenticator or biometrics as the secondary or backup MFA method for low-risk scenarios or users. You can also use Azure AD Conditional Access policies to enforce different MFA methods based on numerous factors, such as user group, device state, location, or sign-in risk.

5. Conclusion

This article has compared six MFA methods—namely, Microsoft Authenticator, FIDO2 security keys, SMS, voice calls, and biometrics—based on four criteria: security, usability, cost, and compatibility. Based on these criteria, we have scored each MFA method and specified the benefits and drawbacks of each method. The results show that no single MFA method excels across the board. The best MFA method will depend on the organization's and users' specific needs and preferences. Each MFA method has benefits and drawbacks on its own. Based on our analysis, we do, however, make some general observations and recommendations, such as preferring FIDO2 security keys and certificate-based authentication for high-security scenarios,

preferring Microsoft Authenticator and biometrics for high-usability scenarios, and avoiding SMS and voice calls for low-security and low-usability scenarios. We hope this article can help you make an informed decision about implementing MFA in your environment. However, this article does not cover all existing MFA methods. Also, other factors or evaluation criteria are relevant to your specific situation or needs. There may also be new developments or innovations in the field of MFA that can change the landscape or introduce new options. Therefore, further research needs to comprehensively review available MFA methods with other ways to measure or quantify the performance or quality of the MFA methods based on different metrics or weights.

***Funding Statement*:** The authors received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

Karim, N. A., & Shukur, Z. (2015). Review of user authentication methods in online examination. *Asian Journal of Information Technology*, *14*(5), 166-175. https://doi.org/10.3923/ajit.2015.166-175

Alhakami, H. (2020). Knowledge based authentication techniques and challenges. *International Journal of Advanced Computer Science and Applications*, *11*(2).

Alex, W. (2022). *Advanced Microsoft Authenticator security features are now generally available! - Microsoft Community Hub*. Microsoft . https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/advanced-microsoft-authenticator-security-features-are-now/ba-p/2365673

Akar, E., & Mardiyan, S. (2016). Analyzing factors affecting the adoption of cloud computing: A case of Turkey. *KSII Transactions on Internet and Information Systems*, *10*(1). https://doi.org/10.3837/tiis.2016.01.002

Alsunaidi, S. J., Saqib, N. A., & Alissa, K. A. (2020). A comparison of human brainwaves-based biometric authentication systems. *International Journal of Biometrics*, *12*(4), 411–429. https://doi.org/10.1504/IJBM.2020.110814

Microsoft. (2023). *Azure Active Directory Pricing*. Microsoft Security. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing

Bae, Y., Banerjee, S., Lee, S., & Peinado, M. (2022). Spacelord: Private and Secure Smart Space Sharing. *ACM International Conference Proceeding Series*, 427–439. https://doi.org/10.1145/3564625.3564637

Bello, O., & Olanrewaju, O. (2022). Factors influencing biometric technology adoption: Empirical evidence from Nigeria. *African Journal of Science, Technology, Innovation and Development*, *14*(2), 392–404. https://doi.org/10.1080/20421338.2020.1837415

Cherry, D. (2022). Multi-Factor Authentication. *Enterprise-Grade IT Security for Small and Medium Businesses*, 83–96. https://doi.org/10.1007/978-1-4842-8628-9_7

Ciolino, S., Parkin, S., & Dunphy, P. (2019). Of two minds about two-factor: Understanding everyday FIDO U2F usability through device comparison and experience sampling. *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019*.

Covavisaruch, N. (2006). Personal identification system using hand geometry and iris pattern fusion. *IEEE International Conference on Electro/Information Technology*, 597–602. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4017768

Dong, Y., Guo, W., Chen, Y., Xing, X., Zhang, Y., & Wang, G. (2019). Towards the detection of inconsistencies in public security vulnerability reports. *Proceedings of the 28th USENIX Security Symposium*.

Drager, N. (2021). *Which Method of Multi-Factor Authentication is Most Secure? (and Other MFA Considerations)*. QUANTUM TECHNOLOGIES. https://quantumpc.com/mfa-most-secure/

Elshamy, E. M., Hussein, A. I., Hamed, H. F. A., Abdelghany, M. A., & Kelash, H. M. (2021). Voice over internet protocol voicemail security system using two factor authentication and biometric prints with new efficient hybrid cryptosystem. *Multimedia Tools and Applications*, *80*(7), 9877–9893. https://doi.org/10.1007/S11042-020-09986-0

Elshenaway, A. R., & Guirguis, S. K. (2021). Adaptive Thresholds of EEG Brain Signals for IoT Devices Authentication. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3093391

Erdem, E., & Sandikkaya, M. T. (2018). OTPaaS-One time password as a service. *IEEE Transactions on Information Forensics and Security*, *14*(3). https://doi.org/10.1109/TIFS.2018.2866025

FIDO2 Passwordless Authentication | YubiKey |. (2023). Yubico. https://www.yubico.com/authentication-standards/fido2/

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers and Security*, *75*, 1–9. https://doi.org/10.1016/j.cose.2018.01.016

Ghorbani Lyastani, S., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is FIDO2 the kingslayer of user authentication? a comparative usability study of FIDO2 passwordless authentication. *Proceedings - IEEE Symposium on Security and Privacy*, *2020-May*. https://doi.org/10.1109/SP40000.2020.00047

Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers and Security*, *30*(4). https://doi.org/10.1016/j.cose.2010.12.001

Gupta, C., & Varshney, G. (2023). An improved authentication scheme for BLE devices with no I/O capabilities. *Computer Communications*, *200*. https://doi.org/10.1016/j.comcom.2023.01.001

Hall, J., Khader, Tamara, F. (2023). *Azure AD Multi-Factor Authentication Overview*. Microsoft Entra | Microsoft Learn. https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Hall, J. F. J. (2023). *OATH tokens authentication method*. Microsoft Entra | Microsoft Learn. https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-oath-tokens

Heidari, H., & Chalechale, A. (2022). Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail. *Expert Systems with Applications*, *191*. https://doi.org/10.1016/j.eswa.2021.116278

Hublikar, S., Pattanashetty, V. B., Mane, V., Pillai, P. S., Lakkannavar, M., & Shet, N. S. V. (2023). Biometric-Based Authentication in Online Banking. *Lecture Notes in Networks and Systems*, *400*, 249–259. https://doi.org/10.1007/978-981-19-0095-2_26/COVER

Huseynov, E. (2022). Passwordless VPN using FIDO2 Security Keys: Modern authentication security for legacy VPN systems. *Proceedings - 2022 4th International Conference on Data Intelligence and Security, ICDIS 2022*. https://doi.org/10.1109/ICDIS55630.2022.00075

Jover, R. P. (2020). Security analysis of SMS as a second factor of authentication. *Communications of the ACM*, *63*(12), 46–52. https://doi.org/10.1145/3424260

Kanaker, H., Karim, N. A., Awwad, S. A. B., Ismail, N. H. A., Zraqou, J., & Al ali, A. M. F. (2022). Trojan Horse Infection Detection in Cloud Based Environment Using Machine Learning. *International Journal of Interactive Mobile Technologies*, *16*(24). https://doi.org/10.3991/ijim.v16i24.35763

Karim, N. A., Kanaker, H., Almasadeh, S., & Zarqou, J. (2021). A Robust User Authentication Technique in Online Examination. *International Journal of Computing*, *20*(4), 535–542. https://doi.org/10.47839/ijc.20.4.2441

Karim, N. A., Shukur, Z., & AL-banna, A. E. M. (2020). UIPA: User authentication method based on user interface preferences for account recovery process. *Journal of Information Security and Applications*, *52*. https://doi.org/10.1016/j.jisa.2020.102466

Khan, R. H., & Miah, J. (2022). Performance Evaluation of a new one-Time password (OTP) scheme using stochastic petri net (SPN). *2022 IEEE World AI IoT Congress, AIIoT 2022*, 407–412. https://doi.org/10.1109/AIIOT54504.2022.9817203

Kim, S., Mun, H. J., & Hong, S. (2022). Multi-Factor Authentication with Randomly Selected Authentication Methods with DID on a Random Terminal. *Applied Sciences (Switzerland)*, *12*(5). https://doi.org/10.3390/app12052301

Komarova, A., Menshchikov, A., Negols, A., Korobeynikov, A., Gatchin, Y., & Tishukova, N. (2018). Comparison of authentication methods on web resources. *Advances in Intelligent Systems and Computing*, *679*, 104–113. https://doi.org/10.1007/978-3-319-68321-8_11

Lee, Y. K., & Jeong, J. (2021). Securing biometric authentication system using blockchain. *ICT Express*, *7*(3). https://doi.org/10.1016/j.icte.2021.08.003

Maynes, M. (2019). *One simple action you can take to prevent 99.9 percent of attacks on your accounts*. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. L. (2023). How effective is multifactor authentication at deterring cyberattacks?. *Arxiv.Org*. https://arxiv.org/abs/2305.00945

MITRE. (2023). *CVE security vulnerability database. Security vulnerabilities, exploits, references and more*. Https://Www.Cvedetails.Com/.

Mohanakrishnan, R. (2021). *Top 10 Multi-Factor Authentication Software Solutions for 2021 - Spiceworks*. https://www.spiceworks.com/it-security/identity-access-management/articles/top-10-multi-factor-authentication-software-solutions/

NIST. (2023). *NVD - Home*. https://nvd.nist.gov/

Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems*, *106*, 1–14. https://doi.org/10.1016/j.dss.2017.11.003

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1). https://doi.org/10.3390/cryptography2010001

O'Neill, M., Heidbrink, S., Ruoti, S., Whitehead, J., Bunker, D., Dickinson, L., Hendershot, T., Reynolds, J., Seamons, K., & Zappala, D. (2017). TrustBase: An architecture to repair and strengthen certificate-based authentication. *Proceedings of the 26th USENIX Security Symposium*.

Microcosm. (2023). *One-Time Password (OTP) Tokens | OATH-compliant Authentication Tokens, Keypads and Cards*. https://www.microcosm.com/it-security-hardware/oath-otp-authentication-tokens

Oren, Y., & Arad, D. (2022). Toward Usable and Accessible Two-Factor Authentication Based on the Piezo-Gyro Channel. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3150519

Org, W. C., Sharmila, K., Janaki, V., & Nagaraju, A. (2017). A survey on user authentication techniques. *Pdfs.Semanticscholar.Org*, *10*(2). https://doi.org/10.13005/ojcst/10.02.37

Owens, K., Anise, O., Krauss, A., & Ur, B. (2021). User perceptions of the usability and security of smartphones as FIDO2 roaming authenticators. *Proceedings of the 17th Symposium on Usable Privacy and Security, SOUPS 2021*.

Owens, K., Ur, B., & Anise, O. (2020). A Framework for Evaluating the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. *Who Are You?! Adventures in Authentication Workshop*.

Rajeswari, S. R., & Seenivasagam, V. (2016). Comparative Study on Various Authentication Protocols in Wireless Sensor Networks. In *Scientific World Journal* (Vol. 2016). https://doi.org/10.1155/2016/6854303

Rui, Z., & Yan, Z. (2019). A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. In *IEEE Access* (Vol. 7). https://doi.org/10.1109/ACCESS.2018.2889996

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. *Sensors 2022, Vol. 22, Page 7433*, *22*(19), 7433. https://doi.org/10.3390/S22197433

Saevanee, H., Clarke, N. L., & Furnell, S. M. (2012). Multi-modal behavioural biometric authentication for mobile devices. *IFIP Advances in Information and Communication Technology*, *376 AICT*, 465–474. https://doi.org/10.1007/978-3-642-30436-1_38

Salameh, A., Elias, nur fazidah, & Karim, nader abdel. (2016). Proposed Model for Measuring Acceptance of Online Ads. *Journal of Engineering and Applied Sciences*. http://docsdrive.com/pdfs/medwelljournals/jeasci/2016/2181-2185.pdf

Silva, R. da. (2021). Calls for behavioural biometrics as bank fraud soars. *Biometric Technology Today*, *2021*(9), 7–9. https://doi.org/10.1016/S0969-4765(21)00095-3

Sinigaglia, F., Carbone, R., Costa, G., & Zannone, N. (2020). A survey on multi-factor authentication for online banking in the wild. *Computers & Security*, *95*, 101745. https://doi.org/10.1016/J.COSE.2020.101745

Smallman, M. (2020). Good call: the hybrid answer to voice authentication. *Biometric Technology Today*, *2020*(4). https://doi.org/10.1016/S0969-4765(20)30051-5

Subbarao, D., Raju, B., Anjum, F., Rao, C. venkateswara, & Reddy, B. M. (2023). Microsoft Azure active directory for next level authentication to provide a seamless single sign-on experience. *Applied Nanoscience (Switzerland)*, *13*(2). https://doi.org/10.1007/s13204-021-02021-0

Tarannum, A., & Rahman, M. Z. U. (2019). Multi-modal biometric system using Iris, Face and fingerprint images for high-security application. *International Journal of Recent Technology and Engineering*, *7*(6).

User Authentication Specifications Overview. (2023). FIDO Alliance. https://fidoalliance.org/specifications/

Velásquez, I., Caro, A., Caro, A., & Rodríguez, A. (2017). Authentication Schemes and Methods: a Systematic Literature Review. *Elsevier*. https://doi.org/10.1016/j.infsof.2017.09.012

Velásquez, I., Caro, A., Rodríguez, A., Velásquez, I., Caro, A., & Rodríguez, A. (2019). Multifactor Authentication Methods: A Framework for Their Comparison and Selection. *Computer and Network Security*. https://doi.org/10.5772/INTECHOPEN.89876

Vibar, J. C. N. (2021). Authentication key-exchange using SMS for web-based platforms. *Journal of Computer and Communications*, *9*(08), 1-12. https://doi.org/10.4236/JCC.2021.98001

Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications*, *188*, 103080. https://doi.org/10.1016/J.JNCA.2021.103080

Witts, J. (2023). *Top 11 Multi-Factor Authentication (MFA) Solutions for Business In 2023*. Expertinsights. https://expertinsights.com/insights/the-top-multi-factor-authentication-mfa-solutions-for-business/

Würsching, L., Putz, F., Haesler, S., & Hollick, M. (2023). *FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones*. https://doi.org/10.1145/3544548.3580993

Zhang, X., Cheng, D., Jia, P., Dai, Y., & Xu, X. (2020). An Efficient Android-Based Multimodal Biometric Authentication System with Face and Voice. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2999115