

**ITWS Capstone Team 4**

Carter Ellis, Ketu Patel, Tianze (Robert) Zhu, Lu (Ryan) Zhou

*October 15th, 2023*

**Table of Contents**

[**1) Measurement Scale 3**](#_yy9xp5rbx6ac)

[**2) One Time Password (OTP) 4**](#_vbpqeexrvpkw)

[**3) Short Message (Text Message) Notification 7**](#_4tokp0qslc9f)

[**4) Email Notification 10**](#_3cpshrof6a4d)

[**5) QR Code 13**](#_xd593xg3sfh4)

[**6) Hardware Token 15**](#_qbvw4g3xewkt)

[**7) Fingerprint 17**](#_2zccelevdud0)

[**8) Face ID 20**](#_wqqsq7qo2n7h)

[**9) Location / Time-Based 23**](#_lodpws5fiseu)

[**10) Voice ID 24**](#_n74nktdex5w2)

[**11) Behavioral 26**](#_1lg0rpxlnozs)

[**12) Single Sign-On 28**](#_ibjog2t8e1ng)

[**13) Market Research Analysis 30**](#_j5t82xm5tj)

[**14) Works Cited 31**](#_oy5lb1padqkk)

# Measurement Scale

As a team, we have decided to grade different authentication methods on three other fronts on a scale of 1 through 10:

Security: The security metric encompasses the robustness of the authentication method in safeguarding sensitive information and preventing unauthorized access. The metric also includes evaluating the strength of encryption algorithms, resistance to cyber threats such as phishing or brute force attacks, and the effectiveness of intrusion detection systems. Additionally, the assessment of security measures extends to the protection of user credentials, secure transmission of data, and the overall resilience of the authentication process against emerging cyber threats. For the scale, the team has decided that one represents terrible security where the solution provides little to no security, and the system is still at risk of attacks. Then, a ten would mean a robust solution deterring all threats.

Usability: The usability metric goes beyond the mere functionality of an authentication method and delves into the user experience aspects. The metric involves evaluating the ease with which users can interact with the authentication system, considering factors such as user interface design, intuitiveness of the user journey, and accessibility features. Examining the user onboarding process, error handling, and providing adequate user guidance are integral to assessing usability. Seamless integration with existing workflows and compatibility with various devices and platforms are also essential considerations. For the scale, the team has decided that one represents terrible usability where the users hate utilizing the authentication system as they believe it to be a significant hindrance. Then, a ten would represent a solution that creates zero user friction.

Cost Value: Cost value analysis involves financial implications for implementing and maintaining the authentication method. This metric considers initial setup costs, such as software licensing, hardware acquisition, and deployment expenses. The ongoing operational costs include maintenance, updates, and support. Furthermore, the team considered other factors, such as potential scalability requirements and the long-term cost-effectiveness of the chosen authentication solution. For the scale, the team has decided that one represents terrible cost effectiveness where the solution is costly from an operational and setup perspective. Then, a ten would represent an inexpensive solution requiring minimal to no setup or operation costs.

# One Time Password (OTP)

## Overview

A One Time Password (OTP) is a password valid for only one login session or transaction on a computer system or other digital device. An OTP can be a string of characters or numbers automatically generated and sent to the user's device via SMS, Voice, or Push message (“What is a One Time Password?”).

The main advantages of OTPs are their security and convenience. They expire quickly and cannot be reused, which makes them more secure than traditional passwords. Since they are automatically generated and sent to the user's device, they also eliminate the need for users to remember complex passwords (Turney and Watson).

OTPs can be used in various scenarios, such as validating a new account, confirming a transaction, or resetting a lost password (“What is a One Time Password?”). They can also be used with other forms of authentication, such as biometrics or security questions, to provide multi-factor authentication.

## Cost Analysis

Implementing an OTP system involves several costs. First, there is the initial cost of setting up the OTP generation service on your application or connecting to an Authenticator app (May). This may involve purchasing hardware tokens, developing software, or subscribing to a third-party service.

There are also ongoing costs for sending OTPs to users. These costs can vary depending on the method used to send the OTPs (e.g., SMS, email, push notification), the volume of OTPs shipped, and the service provider's pricing structure (May).

Despite these costs, implementing an OTP system can be a cost-effective way to improve security. It can help prevent data breaches, resulting in significant financial losses and damage to a company's reputation (May). The OTP market was estimated at $1.5B in 2018 and is expected to reach $3.2B by 2024.

## Security Analysis

OTPs provide several security benefits. They are not vulnerable to replay attacks because they expire quickly and cannot be reused. They also help prevent unauthorized access if one system is breached, as the OTPs for other systems would still be safe (Abdullah).

However, OTPs are not immune to attacks. They can be intercepted or rerouted, and hard tokens can get lost, damaged, or stolen. Attackers can also use phishing attacks to impersonate the authorized user and obtain the OTP. Other common attacks include SMS code theft, SIM swap, and email hijacking.

## Usability Analysis

From a usability perspective, OTPs are generally easy for users to use. They are automatically generated and sent to the user's device, so the user does not need to remember them. The user must simply enter the OTP when prompted during the login or transaction process (“What is a One Time Password?”).

Implementing an OTP system can also be straightforward. It involves setting up an OTP generation service or connecting to an Authenticator app, creating a verification window, determining the OTP delivery channel, and setting up a system to match the entered OTPs to the authentication window (May).

While OTP systems are generally user-friendly, they have specific user challenges and requirements. For instance, in the case of Time-based One-Time Passwords (TOTPs), users must be able to receive their passwords before the time limit expires (Turney and Watson). This can be challenging in areas without high-speed broadband or reliable internet connections. Similarly, HMAC-based One-Time Passwords (HOTP) require users to actively request a new OTP for the previous one to become invalid (Turney and Watson).

To implement TOTP-based two-factor authentication, users need access to a phone application to generate an OTP. The user scans a QR code provided by the service, and the phone application generates a code using the user's secret key. The user then enters this code to enable two-factor authentication.

## Multi-factor Compliments

OTP systems can be used with various passwordless authentication methods to enhance security. For instance, OTPs can be used with magic links, security questions, security keys, and biometrics to provide multi-factor authentication (“A Developer's Guide to One-Time Passwords (OTPs) — WorkOS”).

There are several ways to use OTPs for authentication. For example, a service provider can send a one-time URL to an authenticated email address. When the user clicks the URL, the server authenticates the user. Alternatively, a service provider can send a personalized OTP to an authenticated email address. When the user enters the OTP on the website, the server authenticates the user.

## Summary

In summary, OTP systems offer a secure, cost-effective way to authenticate users. They provide several security benefits, such as protection against replay attacks, and are typically easy for users to use. However, they are not immune to attacks and can present challenges in specific scenarios, such as areas with unreliable internet connections.

When used with other forms of authentication, OTPs can provide a higher level of security. However, the implementation and user requirements can vary depending on the specific OTP method and the other forms of authentication used.

Considering the security, usability, and cost, I would rate OTP systems as follows:

* Security: 8/10. While OTPs provide several security benefits, they are not immune to all types of attacks.
* Usability: 7/10. OTPs are typically easy for users but can present challenges in specific scenarios.
* Cost: 7/10. Implementing an OTP system involves initial and ongoing costs, but it can be a cost-effective way to improve security.

These ratings are compared to other passwordless authentication methods, and the exact scores can vary depending on the specific OTP method and the different forms of authentication used.

# Short Message (Text Message) Notification

## Overview

SMS, or Short Message Service, is the protocol cellular phones use to send and receive text messages over a 2G, 3G, 4G, or 5G network. No data plan is required for SMS service. SMS allows for text messages of 160 characters (letters, numbers, and symbols). The maximum message size limit for other languages with a broader range of characters, such as Chinese or Arabic, is 70 characters (Triggs). If a message exceeds the 160 characters limit, it is broken up into multiple segments of 160 characters each, depending on its length (“What are SMS and MMS and How do They Differ?”). The short message usually contains a one-time password or a login web URL or requires the user’s reply to approve the login.

SMS outperforms traditional passwords in terms of ease of use and security. The user doesn’t need to memorize a password; they just need to look at the message and follow instructions. Also, this auth method requires users to bind their phones to their accounts, making it more secure than password-only auth. However, SMS is facing a security challenge. In recent years, SMS spam has become an issue, as has SMiShing, a security attack in which the user is tricked into downloading a Trojan horse, virus, or other malware onto a cellular phone or another mobile device. Distinguishing genuine and fake messages using the business as its sender name could be challenging for users.

The standard SMS use cases related to authentication include sending notifications from service centers to customers and sending codes as part of a multi-factor authentication platform.

## Cost Analysis

Not all SMS platforms offer the same features, service, or dependability, so not all services are priced the same. One SMS message costs between $0.01 to $0.05, while one international SMS costs $0.25 to $0.5. However, instead of charging per text, many providers will provide a certain number of message credits per plan with the option of purchasing additional monthly credits to lower the final total costs (“How Much Does SMS Marketing Cost?”).

In addition to purchasing an SMS service from a third-party platform, setting up a short message system by themselves is a better choice for large companies. All the business needs is to hire a group of employees in charge of building and maintaining a server that receives users’ requests, sends short messages, and gives login permissions.

## Security Analysis

Compared to a local OTP app, short messages sending an OTP generated from a server are more secure since it’s harder for attackers to decode the random OTP generator. However, message intervention is a significant security concern for this auth method.

As the Internet is a public network that everyone can access and view data on, sending data through it faces several problems, including security threats. Personal or confidential information can be stolen or hacked in various ways (Sameer)—for example, phishing and smishing attacks. Phishing is the practice of sending malicious emails to users. Smishing is a combined form of SMS and Phishing in which invaders send an SMS containing malicious content to the victim. This content sometimes includes links that redirect users to websites containing malicious applications, and user interfaces (Mishra, Sandhya, and Devpriya Soni). Detecting smishing attacks has been a problem for years, but no solution can accurately distinguish malicious messages from genuine messages.

Much research has been introducing new algorithms and techniques to text encryption. Still, they have yet to be widely implemented for multiple reasons such as costs, security evaluation, etc.

## Usability Analysis

Short messages could be combined with OTP, a one-time password generated on the server and sent to users via short messages. In this case, users must be able to receive their passwords and enter them into the login page before the time limit expires (Turney and Watson).

Also, the message could contain a URL that users must click on to approve login. This is a more convenient way, one step less than above, but potential message intervention from attackers may cause user information leaks. It is the same as when the message requires users to reply to authenticate login.

Setting up a business’s short message system is relatively easy. All it needs is to build and maintain a server running all weekdays, in charge of receiving users’ login requests, generating a random OTP (if necessary), sending short messages to users’ phones on file, receiving their feedback, and approving or denying the login.

Overall, the short message system is easy to use. When combined with OTP, it doesn’t require users to download any OTP app and open it for every login. Instead, it sends messages containing passwords that users can easily find and copy.

## Multi-factor Compliments

The most popular multi-factor complement for SMS is OTP, in which short messages send OTPs to users.

Besides, it may be combined with biometric auth like fingerprint and time / location-based auth when logging into a higher-security-level system, in which users need to provide their biometric features and can only log in within a specific time and location.

## Summary

Due to security concerns, short messages containing URLs or requiring user replies are not recommended due to security concerns since they are vulnerable to message interventions. Instead, short messages combined with OTP is a better choice. With OTP being sent via messages, users don’t need local OTP apps on their phones. While the password is generated from the server, it’s harder for attackers to decode the random password-generating algorithm. However, if the login information is sent via text, it’s vulnerable to message interventions. Attackers may be able to receive messages as well when users are trying to log in, making it insecure compared to local OTP apps.

The rating scores for short message authentication would be:

* Security: 7.5/10. While it’s hard to decode a password generator if it’s generated on the server, a message intervention could easily cause an information leak, so the security score is still slightly lower than OTP
* Usability: 8/10. Compared to OTP, users don’t need to install and open an OTP app for each login, but it still faces challenges in certain situations, such as a server crash or weak signal areas.
* Cost: 7/10. Third-party short message services are expensive for large volumes of logins, but they could be cost-effective in the long run if the business builds and maintains its short message server.

These rating scores are only for short messages with OTP combined. If it’s sending a URL or requiring users’ replies, the usability and cost scores may increase slightly (increase by less than 1) while the security score would be much lower (could be less than 5), so these two ways are not recommended.

# Email Notification

## Overview

Email notifications are used in passwordless authentication in two ways: email with an OTP (email OTP authentication) or email with a magic link.

The Email OTP method enables you to authenticate using the one-time password (OTP) sent to the registered email address. When you try to authenticate on any service, the server sends an OTP to the registered email address of the user (“Email OTP authentication | Authentication, authorization, and auditing application traffic”).

To use the Email OTP feature, you must first register your alternate email ID. An alternative email ID registration is needed so that the OTP can be sent to that mail ID since you would not be able to access the primary email ID if there was an account lockout or in the event of you forgetting the AD password. You can use Email OTP validation without email ID registration if you have already provided the alternate email ID as part of some AD attribute. You can refer to the same attribute in the email action instead of specifying the alternate email ID in the email address section (“Email OTP authentication | Authentication, authorization, and auditing application traffic”).

For the second method, magic link, the user just needs to enter an email address and follow the link sent by the authentication system. The link is unique, and authorization with its help is possible only for a specific user and only for a limited time. This approach dramatically simplifies registering new users, relieves them of the need to remember passwords, and provides reliable protection against several attacks related to password theft or brute-force attacks (Matiushin, I., and V. Korkhov).

## Cost Analysis

When combined with OTP, this auth method shares the exact costs as short messages with OTP since most OTP service providers can send OTP via emails. Different service providers offer different prices. For example, Twilio pricing for standard packages starts from USD 0.05 per successful verification plus standard charges per channel (Fathika). Instead of charging a price for every email, SendGrid provides four plans. The free plan allows you to send 100 emails each day indefinitely. The USD 14.95 per month Essentials package will enable you to send up to 100,000 emails monthly. The Pro plan costs between USD 89.95 and USD 749.00 a month and allows you to send up to 1.5 million emails monthly. The Premier plan is for higher volume requirements (Fathika). Like OTP, if the business has a large volume of logins daily, compared to relying on a third-party service, setting up its server could be more cost-effective.

When combined with magic links, the business can rely on an email hosting provider for email delivery, while the price per user and monthly minimum can vary a lot. Larger companies may want to build their server for magic link generation and email delivery based on server construction and maintenance costs analysis.

## Security Analysis

Besides the security concerns for serverside-generated OTP, email security is the main issue. If relying on an email service provider, missing emails will prevent users from logging in, and slow emails might lead to user abandonment or distraction (Specht).

Email security refers to safeguarding confidential information in email correspondence and account security from theft, loss, or compromise, employing misleading communications to persuade recipients to give sensitive information, download attachments, or click on links that lead to malware installation on the victim's device. Email is a common way for malware, spam, and phishing attempts in an enterprise network to increase and compromise sensitive company data (Akanksha, Kadam, et al.).

Researchers have introduced many techniques, such as new encoding algorithms, block-based algorithms, and steganography (Akanksha, Kadam, et al.). Research also focuses on email security threat detection, such as AI-based cyber security awareness systems against phishing attacks (Ansari, Farheen, et al.). However, most are still early in development and need more practical experiments. For now, email delivery is still vulnerable to cyber-attacks.

## Usability Analysis

The Email OTP method is not easy to use. When users try to log in, the OTP server sends a password to their emails. They need to open their emails, find and look at the email with an OTP, and enter the OTP into the login page. The usability is even worse than the OTP app and OTP with short messages since checking messages is more straightforward than checking emails.

In contrast, magic links are much easier to use. After checking their emails, users just need to click the magic link; they’re all set. While checking emails is still difficult, the number of steps is smaller than any OTP-based authentication.

## Multi-factor Compliments

Besides emails with OTP, magic links can also be used as a part of a multi-factor authentication (MFA) strategy and can assist users with trouble entering their password correctly (Specht). The most common auth method combined with it is OTP. Besides, some biometric auth such as face ID, voice ID, and other auth methods like location and time-based auth can also form a multifactor auth with email.

## Summary

Email OTP is very similar to OTP with short messages; the only difference is that checking emails is more challenging than messages, making its ease of use even worse. Rather than Email OTP, magic links could be another choice. Compared to email OTP, it has better usability, but as long as it relies on email delivery, email security could be a big concern. Overall, email has much lower usability compared to short messages, but it could be a better choice due to a higher security level.

The rating scores for email would be:

* Security: 8/10 for Email OTP. The security concerns mainly come from the process of email delivery.
* Usability: 6/10 for Email OTP and 6.5/10 for magic links. While magic links simplify authentication, checking emails still takes work.
* Cost: 7/10. Third-party email hosting services are expensive while holding their server could be cheaper for large businesses. The score could be higher, depending on the costs of building and maintaining the server and developing a magic link generator.

# QR Code

## Overview

A QR code is a type of barcode that can be scanned by a digital device and which stores information as a series of pixels in a square-shaped grid. QR codes are frequently used to track product information in a supply chain, and – because many smartphones have built-in QR readers – they are often used in marketing and advertising campaigns (Wang).

Technically, a QR code can be used as a magic link, sent to a phone or email when

the user has requested a login, or the user can simply scan the QR code. However, in most cases, the QR code is not used as an authentication method because of its deficient security level, especially on the client side.

## Cost Analysis

Many third-party QR code generator services provide several types of limited QR codes for free and more with unlimited dynamic links, projects, pixels, etc., while the most expensive plans are less than 100$. Therefore, QR code costs are relatively low even when used on a large scale. Also, the business can develop its own QR code-generating algorithm, which could be more cost-effective.

## Security Analysis

There is a plethora of recent research on QR code security, such as a new scanner framework that outperforms other scanners regarding security and privacy (Rafsanjani, Ahmad Sahban, et al.). However, the most significant security problem is the client-side QR code leak. Once the user receives a QR code image, anyone next to the user can scan the code. Also, it’s hard to prevent the user from intentionally leaking the code to others. Therefore, the QR code can technically be used as an authentication method, but it’s hardly used in practice because of its security concerns.

## Usability Analysis

QR code is highly user-friendly compared to most of the other authentication methods. All the user needs is to open their phone, open the scanner app, and scan the code. The number of clicks is smaller than most remote authentication methods, such as OTP, short messages, and email notifications.

## Multi-factor Compliments

A QR code can be combined with many other auth methods such as OTP, text or email notifications, or even biometric authentication methods like fingerprint or face ID. QR code could be the first authentication step, with the other authentication method as a second verification step. Or the QR code could be used as a magic link, sent to the user via a short message or email notification.

## Summary

Compared to other remote authentication methods, the QR code has a relatively lower cost and is more user-friendly. However, QR codes are hardly used as an authentication method because of their deficient security level, especially for client-side leaks. Therefore, a QR code could be a good choice if the business doesn’t require a high-security level. Otherwise, it’s not recommended as an auth method.

The rating scores for the QR code would be:

* Security: 3/10. Among all the auth methods, QR code has the lowest security level; this is also why it’s not recommended in most situations.
* Usability: 8.5/10. All the user needs is a phone with a QR code scanner to scan the code. Compared to other remote authentication methods, the QR code is more user-friendly.
* Cost: 8/10. Third-party QR code services are cheap or even free for a limited number of QR codes. Also, the business can develop its generator. QR code costs slightly less than OTP and text/email notifications.

# Hardware Token

## Overview

H[ardware token](https://www.cdw.com/search/Networking-Products/Network-Security/Tokens/?w=N35&ln=3)s allow you to access software and verify your identity with a physical device rather than relying on authentication codes or passwords. Still, it uses multiple factors in authorizing access to software. You may have heard of hardware tokens called key fobs, security tokens, or USB tokens, among other names. The key is that hardware is used instead of software to increase security (“Hard Tokens vs. Soft Tokens”). Examples of hardware tokens include smart cards, security keys, USB tokens, etc.

Hardware token has the highest security level compared to other auth methods since it relies on a physical device that avoids cyber attacks. However, the costs could be among the highest authentication methods since every employee allowed to log in requires a physical device. In the usability aspect, hard tokens are also not user-friendly since they don’t support remote authentication. The user has to come to the device they are logging into.

A hardware token combined with OTP, a hardware OTP token is also a popular authentication method. It’s a hardware token generating OTP or time-based OTP, which allows users to log in with the passcode. Compared to OTP-generating apps and OTPs sent by servers via text or emails, hardware OTP avoids the risks of potential cyber-attacks.

Therefore, hardware tokens could be the best choice if the business requires an extremely high level of security without considering the cost and usability.

## Cost Analysis

The costs of hardware tokens can vary a lot. The business can buy tokens such as smart cards (chip cards) from a third party, whose individual price varies from less than 10$ to hundreds of dollars, like security keys and USB tokens. Each type of hardware token has a bunch of providers. Leading smart card providers include Thales, IDEMIA, CardLogix, AT&T, etc. Primary security key providers include Yubico, CryptoTrust, Thetis, etc., and leading hardware OTP token providers include Yubico, Thales, One identity, RSA security, CDW, etc. All different hardware tokens have different prices; therefore, the cost depends on which token and which vendors the business chooses.

Besides the tokens, some tokens, such as security keys, require equipment to read and recognize the tokens. This is a source of cost as well, including equipment installation and maintenance.

## Security Analysis

Regarding security, hardware tokens could be the best choice among all other authentication methods. No matter whether a hardware token relies on embedded chips such as a smart card or information stored in a USB, it is immune to any kind of cyber attack. The only concern is hardware token theft. Besides, it could be costly to defend against potential attacks once a theft occurs. In the worst case, the business must update the auth system and transfer all the assets or information stored before installing a new auth system.

Although the outcome of a theft could be severe, this auth method is still ranked as the most secure method.

## Usability Analysis

Most hardware tokens require users to carry the tokens and physically appear in front of the system they are logging into. When combined with OTP, such as hardware OTP tokens, users can complete the authentication process remotely, but they still need to have the token. Therefore, the usability score would be lower than most passwordless authentication methods.

## Multi-factor Compliments

When a hardware token is used in remote auth, it’s combined with OTP, such as the hardware OTP token. When the token relies on a chip or embedded information, such as smart card, security key, or USB tokens, it could be combined with other biometric auth such as fingerprint, face ID, voice ID, and behavioral auth, which requires the user to be in front of the system.

## Summary

The hardware token is one of the most secure authentication methods, but token theft could be a big concern. In the aspect of cost and usability, it’s ranked lower than most of the other auth methods. Therefore, hardware token is only recommended when security requirements are extremely high.

The rating scores for hardware tokens would be:

* Security: 9/10. It’s immune to any cyber attacks, but token theft could be a big concern.
* Usability: 4/10. It requires users to carry the token in the auth process.
* Cost: 3/10. Everyone who can log in needs a token, while the equipment installation and maintenance could also be costly. Although different tokens have different prices, it’s still costly compared to other authentication methods.

# Fingerprint

## Overview

Fingerprint authentication verifies an individual's identity based on one or more of their fingerprints. The concept has been leveraged for decades across various efforts, including digital identity, criminal justice, financial services, and border protections (“How does Fingerprint Authentication work? | Security Encyclopedia”).

Fingerprint authentication or scanning is a form of biometric technology that enables users to access online services using images of their fingerprints. The biometric scan commonly relies on mobile and other devices' native sensing technology, as this has all but eclipsed software and third-party biometric algorithms. Some fingerprint scan solutions, such as FIDO, are architected in a decentralized model that ensures a user's fingerprint template is secured on the user’s device. Here, a user’s fingerprint scan is verified locally against itself, a token is sent to the service provider, and access is granted. The biometric authentication takes place locally, and the biometric data itself is not stored at the service provider (true secret). Other fingerprint scan solutions are architected in a legacy centralized scheme in which user templates are stored at the service provider, and matching is done against a library of all other users’ biometrics (shared secret). These systems are commonplace in criminal justice, border protection, and national security settings. Lastly, some fingerprint scan systems (e.g., in government) rely on specialized hardware at the point of care, access, or sale (“How does Fingerprint Authentication work? | Security Encyclopedia”).

Usually, fingerprint auths for business use follow the decentralized model; the fingerprint template is secured on local devices but not stored in the server for user privacy protection purposes. Fingerprints are high-security but could be very costly, depending on how you set up the system. Besides, the fingerprint is not suitable for small volumes of logins. Usually, the fingerprint has around 99% accuracy in recognizing a user successfully, but the fingerprint is not a good choice if the business has millions of daily logins.

## Cost Analysis

The cost of one fingerprint scanner can vary between less than a hundred $ (thermal line sensors) and several thousand $ (capacitive scanners) (“How Much Do Fingerprint Readers Typically Cost? | C&I Show Security”). When used in different situations, the fingerprint-scanning equipment also varies. If it’s used to unlock a door, a fingerprint padlock costs around 10$ to 100$, and it’s more expensive for advanced fingerprint-scanning electronic locks. A USB fingerprint reader is needed to open a computer, usually costing less than 100$ individually. If used for remote authentication, in which the user scans their fingerprint via smartphone and sends the results to the business server, it could be cheaper since many fingerprint scanning apps are free.

Fingerprint authentication can be used in various situations, and the costs differ. Among all the biometric authentication methods (face ID, voice ID, etc.), fingerprinting could be the cheapest (“Are biometric security solutions very expensive?”).

## Security Analysis

A fingerprint is one of the most secure authentication methods since it’s used in many high-security situations like criminal justice and border protection. However, fingerprint authentication usually has an accuracy of around 99% in recognizing fingerprints without giving a false acceptance or rejection. Fingerprint recognition uses machine learning and deep learning algorithms as part of its techniques, which cannot ensure an extremely high accuracy (more than 99.9%) in most cases (Chowdhury, AM Mahmud, et al.). This is why fingerprint authentication is usually combined with other auth methods (face ID, voice ID, or citizen identification information like SSN and passport).

Besides the accuracy problem, the fingerprint encryption process is also a security concern. To protect user privacy, after reading a fingerprint, it has to be encrypted before being stored in any business database. However, many chaotic image encryption schemes are vulnerable to chosen plaintext attack (CPA) (Li, Ruiping).

However, even though fingerprint auth has risks, it still has a high-security level since everyone has unique fingerprints, and attacking the fingerprint auth system could be costly.

## Usability Analysis

Fingerprint auth requires users to be physically in front of the scanner, and due to security and privacy concerns, fingerprinting is not a popular method for remote access. However, the user only needs to press the finger on the scanner during the entire auth process, and then the auth is complete. Unlike those OTP-based authentication methods, it doesn’t require the user to carry any device. Therefore, fingerprint authentication is easy to use from the user’s point of view but not from the business’s. Setting up the whole fingerprint system could be costly, including maintaining all the fingerprint-scanning devices.

## Multi-factor Compliments

In most cases, fingerprints are combined with other biometric auth such as face ID and voice ID, security questions, and maybe some other behavioral auth methods to form a complete biometric auth system in situations like unlocking a door, device, or in high-security level situations like border check in airports.

## Summary

Rather than supporting remote authentication, whose fingerprint could have more security concerns and a low level of usability, it’s more suitable for ‘in-person’ authentication situations, which require users to be physically next to the fingerprint scanning equipment. However, setting up the auth system could be costly for a business. Therefore, fingerprints cannot be used for a high volume of logins but only in security-sensitive conditions and are usually combined with other biometric authentication methods.

The rating scores for fingerprint would be:

* Security: 9/10. Unlike cyberattack concerns for OTP methods, hacking a fingerprint authentication system could be costly.
* Usability: 6/10. Users only need to press their fingers on the scanner, but users need to be next to the scanner, and recognizing the fingerprint could take a few seconds
* Cost: 3/10. Like hardware tokens, setting up a fingerprint scanning system could be costly, including physical equipment and fingerprint database maintenance.

# Face ID

## Overview

Face Authentication is a technology that enables people to access online services, physical settings, and other resources using images of their faces.

Face authentication, also called face/facial recognition, relies on mobile and other native sensing technology. Some third-party biometric algorithms, however, are deployed as software that leverages device cameras for this purpose. Liveness detection — with the user prompted to nod, smile, or move during authentication or continuously during the session — is often added as an additional security layer (“How does Face Authentication Work? | Security Encyclopedia”).

Some face authentication solutions are architected in a decentralized model using FIDO standards, ensuring a consumer or employee face template is secured on the user’s mobile device. Here, a user’s face scan is verified locally against itself, a token is sent to the service provider, and access is granted. The biometrics are not stored at the service provider (true secret).

Other face authentication solutions are architected in a legacy centralized scheme in which user templates are stored at the service provider, and matching is done against a library of all other users’ biometrics (shared secret). These systems are commonplace in criminal justice, international border crossings, and national security settings (“How does Face Authentication Work? | Security Encyclopedia”).

## Cost Analysis

If face recognition is used in a high-security level situation that requires users to physically appear (such as unlocking a door or accessing a protected device), the business would need to set up a whole facial recognition system, including all the required hardware for capturing face images (camera), a face image database, a face recognition software, and all other supporting hardware. If the security requirement is low, the cost could decrease. For example, users can scan their faces with their phones.

Instead of independently setting up a facial recognition system, many businesses choose a third-party facial recognition service such as Amazon Rekognition. In this case, a free trial allows a business to analyze 5000 face images and store 1000 faces per month, lasting 12 months. Compared to building a facial authentication system, this could be much cheaper.

## Security Analysis

The basic technique of facial auth is to recognize human identity from a static image, like the distance between eyes, using machine learning algorithms (Ali, Waqar, et al.). Unlike fingerprints, two people could have very similar human identities on their faces, which makes the recognition accuracy much lower than fingerprints.

Besides, like fingerprints, face images in a secured database must be encrypted to avoid spoofing attacks (Abusham, Eimad, et al.). This could be another source of security risk.

Overall, a fingerprint is more secure than face recognition. Therefore, it’s usually combined with other biometric auth.

## Usability Analysis

Face recognition is easier to use than fingerprints since scanning faces is easier for users. When face recognition is part of a high-security-level biometric authentication, users must be in front of the authentication equipment. If used for remote auth, a popular method among many businesses, users just need to open their phones and scan their faces. Therefore, the usability score for face recognition would be higher than a fingerprint.

## Multi-factor Compliments

In situations where security is highly prioritized over cost and usability, like border checks, face recognition could be combined with fingerprint, voice, and other human identities to form a multifactor biometric auth. Face recognition could be combined with OTP short message notifications if it is used for remote business access. If used for other ‘in-person’ auth such as unlocking doors computers, it could be combined with hardware tokens like smart cards, USB tokens, etc.

## Summary

Face recognition cannot come alone in most cases because of its low accuracy compared with other auth methods. Still, face recognition combined with other authentication methods like OTP has already become popular among many businesses due to its convenience. The cost could be low if the business relies on a third-party service instead of independently setting up the face recognition system. Face recognition has a lower security level and higher usability than fingerprint, while the cost could be lower, depending on the prices of hardware or third-party services.

The rating scores for face recognition would be:

* Security: 7/10. Unlike fingerprints, two people could have similar face identities, significantly decreasing face recognition accuracy.
* Usability: 8/10. Compared to pressing fingers on scanners, scanning a face is easier and quicker in most cases.
* Cost: 6/10. If used in high-security-required situations, setting up a biometric authentication system, including face recognition, is costly. Still, third-party services could be cheap if the business uses face recognition for everyday login.

# Location / Time-Based

## Overview

Basically, this method only allows users to log in at specific periods or locations, for example, 8 am to 9 am in the company for employee logins. ‘Time-based’ depends on the timeslot the user requests a login, and ‘location-based’ depends on the physical location of the device used for login, for example, the computer in the company. This method is only used as a second factor auth and can be used in various conditions. When combined with a remote access auth method like OTP, a time-based auth could be a second factor that only allows employees to log in between 8 and 9 am. When combined with biometric auth, time- and location-based can be used as a second factor, which restricts the auth time and locations.

## Cost Analysis

The cost is negligible since getting the current time and locations is easy, and no extra hardware equipment is needed.

## Security Analysis

The security level is low since this authentication step becomes useless once the attacker knows the login time slot.

## Usability Analysis

The usability score should be high since it doesn’t require users to do anything else. It just needs the login request time and location.

## Multi-factor Compliments

Time or location-based authentication is used as a secondary authentication factor. It could be combined with other authentication methods like OTP, hardware tokens, or biometric authentication.

## Summary

Adding this second authentication factor could block many attacks, but it cannot guarantee a high-security level auth system.

# Voice ID

## Overview

Biometric Voice Recognition uses the human voice to uniquely identify biological characteristics to authenticate an individual, unlike passwords or tokens that require physical input (“Biometric Voice Recognition - Everything You Should Know”).

Voice recognition (also called speaker recognition or voice authentication) applies analysis of a person’s voice to verify their identity. Airways, soft-tissue cavities, and the shape and movement of the mouth and jaw influence voice patterns to create a unique “voiceprint” (“Voice Authentication Software - Aware Biometrics Technology”). A voice recognition system first enrolls a known person by capturing their voice and sending that sample to a biometric engine. The biometric engine then creates a template from the sample. Finally, this engine identifies the distinguishing characteristics of a person’s speech and comes up with a “voiceprint” unique to that individual (“Voice Authentication Software - Aware Biometrics Technology”).

In recent years, massive advances in neural network technology have led to the development of voice biometrics that are faster and more accurate than other methods (“Biometric Voice Recognition - Everything You Should Know”). Therefore, voice recognition is expected to be as popular as other biometrics like fingerprint and face recognition in the near future. However, just like face recognition, voice recognition also has a low accuracy. Even if it could achieve a 99% recognition accuracy, like a fingerprint, it’s still not practical to appear independently as an auth method. It has to be combined with other auth methods to achieve a desirable accuracy in practice, just like other biometric auth.

Just like face recognition, its advantages include good usability with a low cost, but its low accuracy forces it to be combined with other auth methods in practical uses.

## Cost Analysis

Voice biometrics companies can charge less than $25K to well over $1M. The wide range in pricing among voice biometrics providers often aligns with a difference in product category (e.g., active vs passive) and complexity, but not necessarily in quality. A right-sized approach to voice biometrics software focuses on providing state-of-the-art capabilities in a platform that is easy to deploy for small to mid-sized organizations (“Illuma Answers Your Questions about Voice Biometrics”). It could be more costly than face recognition, but since voice biometrics has been a fast-growing market in recent years, it could cost less.

## Security Analysis

The voice template used for authentication isn’t a recording of a person’s voice but a proprietary representation of a person’s voice. During the authentication process, the voice authentication system uses this representation to match a person’s “live” voice. The authentication platform doesn’t store the original voice recording and isn’t at risk of being stolen. Even if a bad actor were to steal the voice template, they could not read or use it without the authentication provider’s proprietary decoding process (“Voice Authentication Software - Aware Biometrics Technology”).

However, the primary concern of voice recognition is its accuracy. The core technique used for recognizing human identities from a voice recording is deep learning algorithms such as CNN (Ariff, Noor Azwana Mat, et al.). However, the accuracy is not desirable, ranging from 90% to 99% (“Considering Voice Biometrics?”), For every 100 authentications, there could be up to 10 false accepts or rejects.

Therefore, due to accuracy concerns, voice recognition would be ranked lower than fingerprint and face recognition.

## Usability Analysis

Voice recognition is pretty easy to use since users don’t need to carry devices; just say something in front of the microphone to provide a voice recording. It also supports remote authentication since users can use their phones for voice recording. Therefore, the usability score for voice recognition would be high, approximately the same as face recognition.

## Multi-factor Compliments

Like face recognition, it could be combined with other biometrics like fingerprint and face to form a high-security-level biometric authentication system. Besides, it could be used in everyday logins, combined with other authentication methods like OTP and short message notifications.

## Summary

Voice biometric authentication technology still needs to be mature compared to fingerprint or face recognition, reflected in its low accuracy. However, machine learning technology has developed quickly in recent years, and the voice biometric market is also expanding rapidly. Voice recognition is expected to be at least as popular as face recognition shortly.

The rating scores for face recognition would be:

* Security: 6/10. Due to its low accuracy, the security score is lower than face recognition.
* Usability: 8/10. Users just need to say something to provide a voice recording; if used in remote authentication, they only need a phone.
* Cost: 5/10. Third-party service prices vary a lot, depending on the type of voice recognition. However, it’s still more costly than token-based authentication like OTP.

# Behavioral

## Overview

Behavioral biometrics analyzes a user’s digital physical and cognitive behavior to distinguish between cybercriminal activity and legitimate customers, identifying fraud and identity theft (Biger). Behavioral biometrics leverages machine learning to analyze patterns in human activity and detect whether someone is who they claim to be when interacting online and whether the activity is driven by a human or part of an automated attack (Biger).

There are two types of behavioral biometrics: passive and active. Passive behavioral biometrics include touchscreen (timestamp, finger pressure on the touchscreen, and the touch area covered by each finger, etc.), keystroke (typing patterns on a keypad, like pressure, finger size, hold time, keystroke latency, etc.), motion/gait (based on user actions while operating a smartphone, such as walking pattern, standing still or handling of the device), behavioral profiling (based on the usage of various digital services and apps in the smartphone). Active behavioral biometrics include handwaving, signature, and voice (Rayani, Praveen Kumar, et al.).

Behavioral biometrics can also be applied to risk-driven authentications, which continuously authenticate users after logging in with their behaviors. Once the user behaves differently from usual, the system forces them to log out (Buriro, Attaullah, et al.).

## Cost Analysis

The cost of behavioral authentication depends on the method. For example, walk patterns require detecting hardware, which could be costly, while touchscreen-based and keystroke-based only need software capturing users’ finger movement, which is much cheaper.

## Security Analysis

In the security aspect, like other biometrics auth, behavioral auth also uses machine learning to analyze users’ patterns, so the biggest issue is still accuracy. Compared to fingerprints and faces, behaviors contain much fewer details for user identification, so the accuracy is usually even lower.

## Usability Analysis

In the usability aspect, when behavioral auth is used in entry-point auth, users are required to do some actions (handwaving, signature, etc.). However, when used in continuous auth, users don’t need to do any extra movement.

## Multi-factor Compliments

For continuous auth, multiple behavioral biometrics are often combined together. For entry-point auth, it always acts as a secondary factor for entry-point auth, combined with a more accurate auth method like OTP or fingerprint.

## Summary

Behavioral auth is suitable for continuous auth, but for entry point auth, it’s always a second step auth.

# Single Sign-On

## Overview

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials. SSO works based on a trust relationship between an application, known as the service provider, and an identity provider, like OneLogin. This trust relationship is often based upon a certificate exchanged between the identity provider and the service provider. This certificate can be used to sign identity information sent from the identity provider to the service provider so that the service provider knows it is coming from a trusted source. In SSO, this identity data takes the form of tokens that contain identifying bits of information about the user, like a user’s email address or a username (“How Does Single Sign-On (SSO) Work?”).

If the business chooses a trusted third-party service for auth, the usability and security level depend on the trusted auth service, for example, OTP with short message notifications. However, there exist some benefits and drawbacks to using SSO instead of creating one auth method for each system.

For example, if users use one SSO certificate for logins on multiple accounts, they don’t need to repeat the process for all accounts once they want to change their profile. Besides, users can continue to authenticate to their accounts even during a temporary outage of a remote server providing an SSO service. And, when users register for a new account, they don’t need to create and memorize a new account, while users’ info won’t be stored in their accounts but only in the SSO database, which reduces the risk of user info leak (Alaca, Furkan, et al.).

However, there are also some drawbacks. Once the user’s SSO account is attacked, every service provider’s account bound with this SSO account will be affected. Also, users cannot change their account info for only one service provider. Once they make changes to their SSO accounts, the changes apply to all service provider accounts bound to their SSO accounts.

## Cost Analysis

In the cost aspect, there are plenty of SSO service providers, and the cost varies from less than $10 to over a hundred per user per month.

## Security Analysis

In the security aspect, it could be better to choose SSO if the trusted SSO service provider has a more sophisticated auth method.

## Usability Analysis

In the usability aspect, SSO could be a good choice since users don’t need a single auth process for each account.

## Multi-factor Compliments

NA

## Summary

SSO is not one of the authentication methods, but it’s a way to do authentication. If the SSO service provider (like Github) is trustworthy, the business can choose this authentication method. Overall, the scores will be 7/10 for cost, 7/10 for security, and 8.5/10 for usability.

# Market Research Analysis

The passwordless authentication market is growing rapidly, with several key factors driving its expansion. In 2023, the market was valued at approximately USD 14.4 billion [expertmarketresearch.com](https://www.expertmarketresearch.com/reports/passwordless-authentication-market). It is expected to grow at a Compound Annual Growth Rate (CAGR) of 15.20% between 2024 and 2032, reaching an estimated USD 33.66 billion by 2032 [expertmarketresearch.com](https://www.expertmarketresearch.com/reports/passwordless-authentication-market). Another source estimates a slightly higher CAGR of 15.3% from 2022 to 2032 (Saha).

This rapid growth is primarily driven by increasing data breaches, cyber threats, and rising demand for improved user experience [expertmarketresearch.com](https://www.expertmarketresearch.com/reports/passwordless-authentication-market). The adoption of biometric authentication and the affordable and user-friendly nature of multi-factor authentication are key trends fueling market growth (“Passwordless Authentication Market Size, Share 2024-2032”). The fingerprint authentication segment led the market in 2021, accounting for over 29% of global revenue (“Passwordless Authentication Market Size & Share Report, 2030”). This growth can be mainly attributed to the rise in identity threats, the widespread use of fingerprint sensors in consumer electronics, and the increasing use of biometric authentication in government offices. The face recognition segment is also expected to grow significantly in the coming years. This growth can be attributed to the increasing use of face recognition technology in the law enforcement sector and its widespread adoption in smartphones and some computers for activities like unlocking the phone, signing into mobile apps, and verifying payment (“Passwordless Authentication Market Size & Share Report, 2030”).

There is no central place where the passwordless authentication market exists, as it affects the global landscape, making a global market (“Passwordless Authentication Market Size, Share 2024-2032”).

In conclusion, the passwordless authentication market is growing rapidly and is expected to continue its growth trajectory. The increasing demand for improved user experience and the growing need for enhanced security measures amid rising cyber threats are the key factors fueling this growth.

# Works Cited

Abdullah, Iqbal. “All you need to know to implement a One Time Password (OTP) flow for your site – Part 1.” *GetOTP*, 9 August 2021, https://otp.dev/en/blog/124/all-you-need-to-know-to-implement-otp-for-your-site-part-1/. Accessed 17 December 2023.

“Are biometric security solutions very expensive?” *spectra-vision*, 2 October 2022, https://www.spectra-vision.com/resources/are-biometric-security-solutions-very-expensive/. Accessed 17 December 2023.

Biger, Ayelet. “What Is Behavioral Biometrics? featured image.” *BioCatch*, https://www.biocatch.com/blog/what-is-behavioral-biometrics. Accessed 17 December 2023.

“Biometric Voice Recognition - Everything You Should Know.” *Imageware*, https://imageware.io/biometric-voice-recognition/. Accessed 17 December 2023.

“Biometric Voice Recognition - Everything You Should Know.” *Imageware*, https://imageware.io/biometric-voice-recognition/. Accessed 17 December 2023.

“Considering Voice Biometrics?” *Voice Biometrics Group*, https://www.voicebiogroup.com/starting/considering-voice-biometrics.html. Accessed 17 December 2023.

“A Developer's Guide to One-Time Passwords (OTPs) — WorkOS.” *WorkOS*, 28 June 2021, https://workos.com/blog/guide-to-one-time-passwords-otps. Accessed 17 December 2023.

“Email OTP authentication | Authentication, authorization, and auditing application traffic.” *Citrix Product Documentation*, 31 July 2023, https://docs.netscaler.com/en-us/citrix-adc/current-release/aaa-tm/authentication-methods/email-otp. Accessed 17 December 2023.

Fathika, Rista. “Email OTP Price Update [2023] Best Price Guaranteed!” *fazpass*, 5 November 2023, https://fazpass.com/blog/authentication/email-otp-best-price-guaranteed/. Accessed 17 December 2023.

“Hard Tokens vs. Soft Tokens.” *CDW*, 11 August 2022, https://www.cdw.com/content/cdw/en/articles/security/hard-tokens-vs-soft-tokens.html. Accessed 17 December 2023.

“How does Face Authentication Work? | Security Encyclopedia.” *HYPR*, https://www.hypr.com/security-encyclopedia/face-authentication. Accessed 17 December 2023.

“How does Fingerprint Authentication work? | Security Encyclopedia.” *HYPR*, https://www.hypr.com/security-encyclopedia/fingerprint-authentication. Accessed 17 December 2023.

“How Does Single Sign-On (SSO) Work?” *OneLogin*, https://www.onelogin.com/learn/how-single-sign-on-works. Accessed 17 December 2023.

“How Much Does SMS Marketing Cost?” *EZ Texting*, https://www.eztexting.com/resources/sms-resources/how-much-does-sms-marketing-cost. Accessed 17 December 2023.

“How Much Do Fingerprint Readers Typically Cost? | C&I Show Security.” *C&I Show Hardware And Security Systems*, 28 March 2022, https://cishowhardware.com/fingerprint-readers-cost/. Accessed 17 December 2023.

“Illuma Answers Your Questions about Voice Biometrics.” *Illuma*, https://illuma.cx/answering-your-questions-about-voice-biometrics/. Accessed 17 December 2023.

May, Akyyoma. “A Developer’s Guide to One-Time Passwords (OTPs).” *bsg*, 2 October 2022, https://bsg.world/blog/a-developers-guide-to-one-time-passwords/. Accessed 17 December 2023.

“Passwordless Authentication Market Size, Share 2024-2032.” *Expert Market Research*, https://www.expertmarketresearch.com/reports/passwordless-authentication-market. Accessed 17 December 2023.

“Passwordless Authentication Market Size & Share Report, 2030.” *Grand View Research*, https://www.grandviewresearch.com/industry-analysis/passwordless-authentication-market-report. Accessed 17 December 2023.

Saha, Sudip. “Passwordless Authentication Market Size, Share & Trend | FMI.” *Future Market Insights*, https://www.futuremarketinsights.com/reports/passwordless-authentication-market. Accessed 17 December 2023.

Specht, Bettina. “The beginner's guide to magic links.” *Postmark*, 6 October 2022, https://postmarkapp.com/blog/magic-links. Accessed 17 December 2023.

Triggs, Robert. “What is SMS and how does it work?” *Android Authority*, 14 August 2023, https://www.androidauthority.com/what-is-sms-280988/. Accessed 17 December 2023.

Turney, Shasta, and Louise Watson. “The One-time Password (OTP) Ultimate Guide.” *Ping Identity*, 10 November 2023, https://www.pingidentity.com/en/resources/blog/post/one-time-password-ultimate-guide.html. Accessed 17 December 2023.

“Voice Authentication Software - Aware Biometrics Technology.” *Aware, Inc.*, 18 October 2023, https://www.aware.com/voice-authentication/. Accessed 17 December 2023.

Wang, Ynjiun. “What is a QR code and are they safe?” *Kaspersky*, https://usa.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan. Accessed 17 December 2023.

“What are SMS and MMS and How do They Differ?” *Twilio*, https://www.twilio.com/en-us/learn/messaging/what-are-sms-and-mms. Accessed 17 December 2023.

“What is a One Time Password?” *CM.com*, https://www.cm.com/glossary/what-is-one-time-password/. Accessed 17 December 2023.

Nooh, Sameer. "Combining encryption and preservation in information security to secure sending a message." *International Journal of Computer Science & Network Security* 22.4 (2022): 285-291.

Mishra, Sandhya, and Devpriya Soni. "Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis." *Future Generation Computer Systems* 108 (2020): 803-815.

Matiushin, I., and V. Korkhov. "Passwordless Authentication Using Magic Link Technology." *CEUR Workshop Proceedings*. Vol. 3041. 2021.

Akanksha, Kadam, et al. "Email Security." *Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN 2815-0953* 2.06 (2022): 23-31.

Ansari, Meraj Farheen, Pawan Kumar Sharma, and Bibhu Dash. "Prevention of phishing attacks using AI-based Cybersecurity Awareness Training." *Prevention* (2022).

Rafsanjani, Ahmad Sahban, et al. "QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework." *IEEE Access* (2023).

Chowdhury, AM Mahmud, and Masudul Haider Imtiaz. "Contactless fingerprint recognition using deep learning—a systematic review." *Journal of Cybersecurity and Privacy* 2.3 (2022): 714-730.

Li, Ruiping. "Fingerprint-related chaotic image encryption scheme based on blockchain framework." *Multimedia Tools and Applications* 80 (2021): 30583-30603.

Ali, Waqar, et al. "Classical and modern face recognition approaches: a complete review." *Multimedia tools and applications* 80 (2021): 4825-4880.

Abusham, Eimad, et al. "Facial image encryption for secure face recognition system." *Electronics* 12.3 (2023): 774.

Ariff, Noor Azwana Mat, and Amelia Ritahani Ismail. "Study of adam and adamax optimizers on alexnet architecture for voice biometric authentication system." *2023 17th International Conference on Ubiquitous Information Management and Communication (IMCOM)*. IEEE, 2023.

Rayani, Praveen Kumar, and Suvamoy Changder. "Continuous user authentication on smartphone via behavioral biometrics: a survey." *Multimedia Tools and Applications* 82.2 (2023): 1633-1667.

Buriro, Attaullah, et al. "Risk-driven behavioral biometric-based one-shot-cum-continuous user authentication scheme." *Journal of Signal Processing Systems* 93 (2021): 989-1006.

Alaca, Furkan, and Paul C. Van Oorschot. "Comparative analysis and framework evaluating web single sign-on systems." *ACM Computing Surveys (CSUR)* 53.5 (2020): 1-34.