Breaking Barriers: Passwordless Authentication as the Future of Security

Abhishek Prasad
University of Southern California
Los Angeles, California, USA

ABSTRACT
In today's scenario, software applications are facing new challenges while using password authentication for providing access to accounts. It can be easily understood and appreciated that while passwords have been existing for decades, they have become highly vulnerable to security attacks leading to data breaches. With the huge advancement in Artificial Intelligence, there has been a tremendous increase in sophisticated tools used by cybercriminals to gain unauthorized access. Therefore, there is a growing demand for passwordless technologies that can provide a highly secure and efficient way for authentication. This study explores detailed information on various passwordless authentication technologies and analyzes their benefits and drawbacks. Additionally, it attempts to make a comparison between these technologies based on different criteria. Passwordless authentication is commonly based on public-key cryptography, which uses a cryptographic key pair with a public and private key. The public key is used by authenticating services to authenticate users using the private key stored on the user's device secured behind a non-knowledge based authentication factor.

Keywords
Passwordless Authentication, Biometrics, Fido, Fingerprint, Decentralized, Certificate, Comparison, Security, Cost, Usability, Passwordless, Behavior, Future

1. INTRODUCTION

1.1 What is Passwordless Authentication?
In recent years, there has been a growing debate and interest surrounding the obsolescence of passwords as a security measure. We have been exploring different methods including end user authentication for substituting passwords, but none of them have been consistently reliable. Authentication is based on three factors which can be grouped into these categories:

- **Knowledge factors**: Something the user knows which includes passwords, passphrases, and security questions.
- **Possession factors**: Something the user has which includes devices such as cellular phones, smart cards, one-time password (OTP) tokens and hardware tokens.
- **Inherence factors**: Something the user is which includes face recognition, voice recognition, fingerprints, retinal scans, and other biometric identifiers.

Passwordless authentication allows users to authenticate using possession or inheritance factors instead of knowledge factors [10]. It typically utilizes a public-key cryptography infrastructure, where the authenticating service (remote server, application, or website) receives the public key during registration, while the private key remains on the user's device (smartphone, personal computer or an external security token). Access to the private key is restricted and requires providing a biometric signature or another non-knowledge based authentication factor.

1.2 Problems with Password Authentication
The traditional method of using passwords to protect digital accounts has come under scrutiny due to several factors. One of the main reasons is the large volume of passwords that an average person needs to remember. With the proliferation of online accounts, users often have to juggle dozens or even hundreds of different passwords, which makes it challenging to create and maintain strong and unique passwords for each account. This reliance on a large number of passwords often leads to password reuse, making users more susceptible to credential stuffing attacks. Another contributing factor is the increasing sophistication of cybercriminals. Password cracking tools and techniques have become more advanced, allowing attackers to easily brute-force or guess weak passwords. Phishing scams, keyloggers and social engineering attacks also exploit human vulnerabilities to trick users into revealing their passwords or other sensitive information. The growing prevalence of data breaches has further compromised the security of passwords, as stolen password databases are often sold on the dark web for criminals to exploit. Passwords are susceptible to man-in-the-middle attacks by intercepting communications streams such as public Wi-Fi and replaying credentials to gain access to accounts.

1.3 Why use Passwordless Authentication?
Due to frequent reuse, sharing, and susceptibility to hacking, passwords represent a vulnerable point in computer networks, utilized as a primary attack vector responsible for a significantly high proportion of security breaches. Passwordless authentication provides improved security by eliminating passwords as a potential vulnerability, thus reducing the risk of password-related security incidents. It is resistant to brute-force attack, credential stuffing, keyloggers, man-in-the-middle attacks and replay attacks. Organizations can mitigate the occurrence and potential severity of cyberattacks, leading to lower long-term costs. Passwordless authentication offers improved scalability compared to traditional password-based authentication. By eliminating the need for storing and managing user credentials, organizations can streamline the authentication process and contain costs effectively, even as they grow and the number of users rise. Reducing the number of support requests related to password resets, compliance with password storage rules and troubleshooting can significantly decrease the workload of support teams, leading to reduced operational expenses. It also improves user experience by simplifying the user onboarding process and login experience leading to increased conversion rate.

2. PASSWORDLESS AUTHENTICATION TECHNOLOGIES

2.1 Email-Based One-Time Code Authentication

The user initiates the authentication process by providing their registered email address to the application. This email address serves as a unique identifier associated with the user's account. Upon submitting, the system promptly dispatches a unique one-time code to the email address. This code serves as a temporary and time-sensitive code designed to provide additional security. The user is then prompted to enter the code sent to their email into the application. The code is matched with the system generated OTP. If the comparison is successful, the authentication process is deemed successful. The user is granted access to their account and a new session is initiated. [5]

Advantages: Convenient and easy to use as users have email access on multiple devices including mobile and desktop. Offers a cost-effective solution by utilizing the users existing email accounts and eliminating the need for additional user-side requirements. Provides an additional layer of security by requiring users to verify their identity beyond just their password or security questions for Multi-factor Authentication(MFA).

Disadvantages: Susceptible to phishing attacks, where malicious actors attempt to deceive users into divulging their one-time password. Email delivery may fail due to lost internet connectivity, mail being labeled as spam, mail bounced back by server and delivery queue becoming congested. The primary target of malicious actors is email accounts, and most cyberattacks enter an organization through email. It is easy to infiltrate many other accounts connected to email when an email address gets compromised.

2.2 SMS-Based One-Time Code Authentication

The user initiates the login process by providing their registered valid phone number to the application. Upon submitting, the system promptly dispatches a SMS with a unique one-time code to the phone number. This code serves as a temporary and time-sensitive code designed to provide additional security. The user is then prompted to enter the code sent to their phone number into the application. The code is matched with the system generated code. If the comparison is successful, the authentication process is deemed successful. The user is granted access to their account and a new session is initiated. Some applications also offer receiving code through voice call as an alternative. [5]

Advantages: User-friendly and inexpensive as it doesn't require configuring hardware or installing applications. Provides an additional layer of security by requiring users to verify their identity beyond just their password or security questions for Multi-factor Authentication(MFA).

Disadvantages: It is susceptible to security risks such as phishing attacks and SIM cloning. SMS delivery may fail without mobile connection. Mobile can get lost or stolen. It is easy to infiltrate many other accounts connected to a mobile when a mobile gets compromised using techniques such as password reset.

2.3 Magic Links Authentication

The authentication technique requests users to provide their email addresses. After submitting the email address, the framework generates and stores an identification key for future reference. An email containing a unique URL is sent to the user as a token. The magic link has a predetermined lifespan for the user before it becomes invalid. Similar to one-time passwords, the link is no longer valid after being used. When the user clicks on the link, the server authenticates the token and creates a long-term token stored in the server database. Users can access the application using that long-term token without a password. [7]

Advantages: Convenient and easy to use as users can easily access email on multiple devices including mobile and desktop. Offers a cost-effective solution by utilizing the users existing email accounts, eliminating the need for additional user-side requirements. The links are time sensitive and generated on-demand that enhances the security by reducing risk of unauthorized access.

Disadvantages: As users become accustomed to clicking links in emails, they may mistakenly perceive phishing attempts as legitimate authentication emails, making them more susceptible to phishing attacks. Email delivery may fail due to lost internet connectivity, mail being labeled as spam, mail bounced back by server and delivery queue becoming congested. If a user is on an unencrypted network, magic links are susceptible to man-in-the-middle attacks, potentially resulting in a hacker intercepting the token.

2.4 Time-Based One-Time Password (TOTP)

When a user registers with the One-Time Password (OTP) platform, a shared secret, known as a seed, is created and stored on the server. Subsequent login attempts will utilize OTPs generated from the same seed, ensuring user validation remains consistent despite variations in the code. During a login attempt, the app or website generates an OTP based on the seed and a moving factor that is dependent on Unix time. This ensures the OTP expires if the user does not enter it within a specified interval, typically between 30 and 90 seconds. The user views this code on their authenticator app and enters it in the designated field. Concurrently, the server generates its own OTP using the same seed and moving factor. If the OTP entered by the user matches that generated by the server, the user is successfully logged in.

Advantages: It can be embedded in hardware tokens and third-party trusted software such as Google Authenticator and Microsoft Authenticator. Easy to implement that makes it cost efficient. The Authenticator app automatically generates codes so a user has a backup even if their device doesn't have connectivity.

Disadvantages: Synchronized time between server and client is required. TOTP values can be generated using stolen shared secrets by the attackers to authenticate the system.

2.5 HMAC-Based One-Time Password (HOTP)

HOTP functions similar to TOTP with small variation. The moving factor is not the ticking of the clock's hands but a counter that moves upon request validation. [4]

Advantages: The one-time password generated through HOTP lasts longer compared to TOTP. This extended validity period provides a buffer against potential delivery issues or logistical challenges that could make TOTPs impractical or ineffective.

Disadvantages: Due to the longer validity period, it is vulnerable to brute-force attack. In the HOTP algorithm, the

event counter discrepancy might lead to a possible desynchronization issue between the server and the OTP token.

2.6 Push Notification Authentication

Authenticates users by sending notifications directly to a secure application on their device, alerting them of an authentication attempt. With a simple press of a button, users can review authentication details and approve or deny access [5]. Push notifications can be sent in-band or out-of-band, utilizing various communication channels. This method enhances security by sending authentication requests directly to the user's device, reducing the risk of unauthorized access. Push notifications serve as a method of authenticating users by verifying that the registered device, often a mobile device, is in their possession and matches the authentication system's records. Sometimes, push notification might require users to select or type the number matching on the approval request for enhanced security.

Advantages: Users can instantly validate their login by receiving the authentication request directly. Validating an authentication request is often quicker than entering a complex password or authentication code. Users can obtain information about the person trying to log in, including the device type, IP address, and approximate location. This alerts users about any potentially malicious login attempts if they occur.

Disadvantages: To authenticate push notifications on device, internet connection is necessary. Without an active data connection or Wi-Fi, the login prompt will not appear. It's also important to note that push notifications have the potential to bypass the review process and be automatically approved. This means that if not careful, one could unintentionally grant access to individuals who should not have it.

2.7 Third-Party Identity Provider

Allows users to login to a website or application using their existing account credentials from a third-party identity provider, such as Google, Facebook, or Twitter. Eliminates the need for users to create and remember multiple usernames and passwords for different websites and applications. 3rd party IDP authentication involves redirecting users to the IDP sign-in page to enter credentials and authenticate. Upon successful authentication, the IDP redirects the user back to the website or application.

Advantages: Using third-party IDPs offers convenience, security, and scalability benefits for user authentication. Single-click sign-in eliminates the need for separate account creation, while strong security measures and scalability ensure smooth handling of high authentication volumes.

Disadvantages: Less control over storage and usage of user's data. Users will not be able to access the main application if IDP experiences downtime. There can be high costs associated with using services. Limited set of features and customization options can make it difficult to tailor the authentication process to company specific needs. It could be vulnerable to attack if the IDP is not properly secured.

2.8 Fingerprint Authentication

The human fingerprint, composed of unique ridges and lines, serves as a remarkable identifier [6]. During onboarding, users engage with a fingerprint scanner to provide their fingerprint information. The scanner repeatedly scans the finger to capture accurate patterns. This fingerprint information is then encoded into a biometric schema, a data representation used as a comparison point in future authentication sessions [3]. A database securely stores this template, ensuring its availability for future reference. When users attempt to access a system using a fingerprint authentication-enabled device, they place their finger on the fingerprint scanner. Optical, capacitive, thermal, and ultrasonic scanners are the four primary types of scanners used. Once scanned, the fingerprint is converted into a biometric schema, encrypted, and transmitted to the authentication service, where it is compared to the user's original schema. A successful match results in authentication. There is some flexibility in the comparison process. The authentication mechanism compares and approves fingerprint schemas within an acceptable failure rate, allowing for minor variations. Biometric authentication is becoming more prevalent in the electronics industry, with a focus on devices such as computers and smartphones. Governments and private organizations are also implementing biometric identification systems in sensitive areas like military bases, airports, and border crossings to enhance security and access control. [8]

Advantages: Provides additional security for securing devices. Simple to deploy devices with fingerprint authentication and cost effective compared to another biometric authentication.[9]

Disadvantages: Fingerprints may deteriorate and degrade over time, which can lead to performance and access issues. Hackers can access and steal biometric schemas from security databases, which can be used to deceive authentication systems.[9]

2.9 Eye Recognition

Retina scanner and Iris scanner are the most commonly used eye biometric authentication. Retina scanners employ a low-power infrared light beam directed into the eye. This light is differentially absorbed by the retinal blood vessels compared to surrounding tissues, resulting in a distinctive pattern. A sensor captures this pattern, transforming it into a digital image and matches to the accepted data stored in the database. Similar to the retina, the iris scanner captures detailed images of the iris, the colored ring around the pupil. This method is effective because the iris possesses intricate and distinct patterns like striations, freckles, and crypts, making it valuable for individual identification and verification. These patterns are formed before birth and remain consistent throughout one's life. Through specialized software, the iris image is analyzed, extracting mathematical representations of the patterns. This analysis results in the creation of a unique iris code for each individual.

Advantages: Provides high accuracy as probability of two eye scans being identical is very low compared to other biometric techniques. Due to its distinctive and stable nature, eye recognition offers a high level of accuracy and dependability, minimizing the likelihood of mistaken identification. Non-contact and non-intrusive biometric technology. Quick verification capability and user-friendly interface make it ideal for time critical applications.

Disadvantages: The installation and maintenance costs of the software and hardware infrastructure can be high. Privacy concerns can arise as there is a potential risk that the stored eye data could be compromised, leading to identity theft or misuse. The quality of the captured iris image may be affected due to environmental conditions such as low lighting or extreme sunlight, leading to potential authentication errors.

2.10 Voice Authentication

Voice authentication is a technique enabled by deep learning which aims to identify, distinguish, and authenticate an individual's voice. It analyzes distinct voice features, such as frequency, pitch flow, and natural accent, to create a unique

biometric profile for each person. Instead of listening to a voice, these systems excel at evaluating and analyzing the shapes and sound characteristics produced by a speaker's mouth and throat to create a unique signature. This approach eliminates the risk of attempted voice disguises or imitations, as well as external factors like illness or time of day, which can affect a voice's audible qualities to a listener. In the process of speaker recognition, feature extraction is performed to obtain essential characteristics from the speech signal. These extracted features are then utilized to create speaker models for individual speakers. The generated models are stored in a voice database for subsequent use. Various modeling techniques are employed to create these speaker models, including Gaussian Mixture Models (GMM), Hidden Markov Models (HMM), pattern matching, frequency estimation, vector quantization, decision trees, and neural networks. During the enrollment phase, a speaker's voice is recorded, and unique features are extracted from the speech signal print. In the verification phase, a voice sample is compared to the previously stored voice print to determine whether they match. [6]

Advantages: Human vocal characteristics are unique and challenging to reproduce, making it a highly distinctive attribute. This significantly enhances security and fraud prevention capabilities. Users can authenticate themselves simply by speaking which provides a seamless and convenient user experience. Integrating voice authentication yields substantial cost reductions and time optimization for organizations. It eliminates the repetitive tasks associated with password resets, call center assistance for forgotten passwords, and the problematic practice of password sharing. Furthermore, voice authentication expedites the user authentication process, leading to enhanced operational efficiency.

Disadvantages: Noisy background can lead to potential false rejections or acceptances. Voice biometrics are known for their security, as they are challenging to duplicate. However, advancements in deep fake voice technology have emerged, capable of imitating a person's voice with remarkable accuracy [1]. The adoption of voice authentication across different platforms and devices is hindered by the absence of consistent protocols and widespread compatibility. Voice authentication collects and stores user’s biometric data, raising ethical and privacy concerns. Voice authentication accuracy can vary due change in voice due to factors such as colds, stress, and aging.

2.11 Certificate Based Authentication (CBA)

CBA utilizes digital certificates based on cryptography to identify users, devices, or machines before granting access to applications, networks, or other resources. Public keys are published but their corresponding private keys remain confidential. Data encrypted with a public key can only be decrypted using the corresponding private key. These certificates must be digitally signed by a Certificate Authority (CA) to ensure authenticity. During authentication, the client initiates a connection to the server, and the server responds by providing its public certificate. The client validates the server's certificate to ensure it is trusted. The client then signs a nonce using its private key and returns it to the server along with its public certificate. Using the client's certificate, the server verifies that the client signed the nonce and that the certificate is not expired or revoked. Upon successful verification of all the required attributes, the server maps the certificate attributes to a specific user within its system. This mapping facilitates the identification and authentication of the user. [14]

Advantages: Easier and user-friendly for authorized users to access privileged services and sites without requiring password. Reduces IT support costs and insecure password practices. Resistant to phishing and password attacks like brute force and rainbow table. Extensible to external users, as it's easy to roll certificates out to users outside the organization who may need access to the network. Highly responsive to actions such as issuance or revocation of certificates as they are centrally managed. Enhances access control measures by adhering to the principle of least privilege, ensuring that individuals have only the permissions necessary to perform their designated tasks [14]. Moves an enterprise toward a zero-trust architecture. No additional hardware is needed as certificates are stored locally on the machine or device.

Disadvantages: While creating a digital network infrastructure for certificate-based authentication is a non-recurring process, it comes at a significant cost. For startups and small businesses, it might not be a practical option. There are ongoing maintenance considerations for CBA, such as issuance, renewal, and revocation. These considerations include operational and licensing expenses for a Certificate Management System (CMS) responsible for safeguarding their private encryption keys. Typically operates through community-driven governance models for managing updates and modifications, which can lead to standardization and accountability challenges.

3. FUTURISTIC PASSWORDLESS AUTHENTICATION TECHNOLOGIES

3.1 Behavioral Biometric Authentication

Behavioral biometrics is a developing technology that authenticates users continuously by analyzing their behavioral patterns, such as typing and movement, rather than physical traits, possessions, or knowledge. Unlike traditional methods, which authenticate only upon access initiation, behavioral biometrics evaluates users' interactions in real time. Everyone's behavioral patterns are unique, including gait, vocal tone fluctuations, and typing cadence. These patterns are challenging for malicious actors to capture and replicate, making behavioral biometrics a secure authentication method. If a user's behavioral patterns deviate from their established profile, the system can promptly request additional authentication, block access, or lock the device.

Advantages: Enhances the recognition of trustworthy digital users and identifies potential fraud. Implements appropriate security measures for specific interactions or situations with higher risk.

Disadvantages: There is a strong correlation between behavior and cognitive functions. As a result, collecting behavioral observations can often raise privacy concerns. If the data collected is biased, it could lead to false positives or declined authentication.

3.2 Decentralized Authentication

In decentralized identity, users and entities can be identified and authenticated without the dependence on a single, central authority. In traditional centralized identity systems, user identities are stored and authenticated by a single authority, leading to silos of identity management. In contrast, decentralized identity gives users and organizations control over their identity management through a distributed approach. This approach leverages distributed ledger technology (DLT), such as blockchain, to store and manage identity information in a distributed manner, typically using a digital wallet. In

decentralized identity systems, public key infrastructure (PKI) cryptography is employed to safeguard and handle identity. Public Key Infrastructure (PKI) employs a pair of keys, a public key and a private key, to encrypt data. Blockchain transactions are immutable, ensuring they remain unalterable and are dispersed to all nodes in the distributed ledger, guaranteeing their integrity and resistance to tampering. A blockchain-based system introduces the concept of decentralized identifiers (DIDs) that represent a user's identity. Controlled by individuals, DIDs comprise a Uniform Resource Identifier (URI) scheme, method identifier, and DID method-specific identifier. This decentralized identity, backed by verifiable credentials and secured using cryptography on the blockchain, allows users to create and manage their identities independently. When needed, the identity stored on the blockchain can be conveniently shared with organizations and other users for verification purposes. The verification process involves locating the public key on the blockchain, where the decentralized identifier information is stored. [13]

Advantages: Decentralized identity enables developers to create applications that do not rely on vulnerable passwords to verify users. It enhances privacy by reducing and safeguarding personally identifiable information (PII). Additionally, it improves data security by providing an immutable and tamper-proof ledger for identifiers. Users gain greater individual control over their identity information and its usage. Decentralized identity allows organizations to conduct quick identity checks. Notably, it eliminates the central point of failure present in centralized identity systems. It also boosts identity portability and decreases the risk of certificate fraud, as centralized systems commonly rely on digital certificates for cryptography issued by certificate authorities that may be susceptible to misuse or alteration. [13]

Disadvantages: Decentralized identity presents several complexities for users and organizations compared to traditional centralized identity systems. Different decentralized identity platforms may encounter interoperability issues among themselves and with other technologies outside the Web3 ecosystem. Furthermore, the regulatory compliance landscape for decentralized identity in government and industry use cases remains uncertain. User adoption of decentralized identity is currently lower than centralized identity. Additionally, users hold the responsibility of safeguarding their private encryption keys. Typically operates through community-driven governance models for managing updates and modifications, which can lead to standardization and accountability challenges. [13]

3.3 Fast IDentity Online 2 (FIDO2)

In 2018, the FIDO Alliance released FIDO2, the most recent open standard for user authentication. FIDO2 aims to bolster people's trust in web services by enhancing the login process. It employs cryptographic algorithms to create corresponding secret and public passkeys. For user authentication, a key pair is used directly on the user's device. A passkey can be linked to a single device or synced across multiple devices using a cloud service. When a user registers with a FIDO2-supported service, the client device generates a key pair specific to that web application or website. The public key is encrypted and shared with the service, while the private key remains securely on the user's device. Every time the user attempts to log in, the service presents a unique challenge to the client, prompting the user to activate the passkey device. The passkey device signs the request with the private key and returns it, completing the authentication process [12]. This method ensures that the cryptographic process is protected from phishing attacks, thereby enhancing security. FIDO2 authenticators are devices that confirm the identity of a user requesting access to a device. There are two types of FIDO authenticators: roaming and platform. Roaming authenticators are portable hardware devices that connect to client devices through USB, NFC, or Bluetooth. These authenticators, also known as cross-platform authenticators, enable users to seamlessly authenticate on various computers at any time and from any location. Platform authenticators are embedded in client devices and require the user to sign in with their client device and authenticate through the same device. Examples of platform authenticators include Face ID, Apple Touch ID and Android Fingerprint. FIDO2 involves challenge-response mechanisms with browser participation, allowing the integration of the website's URL into the challenge. This approach makes relaying the response ineffective, effectively combating real-time phishing. U2F exemplifies this standard, where the response is computed using a hardware token [2].

Advantages: Safeguards against phishing, password theft, and replay attacks by utilizing unique cryptographic credentials instead of storing them on server. Eliminates the risk of sensitive information being exposed or stolen. Ensures secret codes and passwords are never revealed or shared, making it difficult for unauthorized parties to gain access to private data. Ensures privacy and security as the cryptographic data generated on devices remains unique across websites, and biometric data is never transmitted outside the device. Enhances access control to physical locations such as offices and residential buildings. A stolen key or passcode will not allow unauthorized parties to gain access to the premises. Provides interoperability across various platforms, devices, and web browsers, providing a convenient and consistent experience for users. Helps reduce costs by eliminating the expenses associated with credential-based attacks. [11]

Disadvantages: FIDO2 keys can be costly, especially when considering the total price for every token for multiple employees in a large organization. This cost is partially mitigated by the ability of a single token to store keys for multiple websites and apps. There are concerns related to efficiency and user experience. Increasing the number of authentication steps inherently increases the time and effort required for users to access services, which can be particularly problematic if users need to authenticate multiple times a day. [11]

4. PASSWORDLESS AUTHENTICATION TECHNOLOGIES COMPARISON

4.1 Security

Security is the core criteria for evaluating different passwordless authentication technologies, as it indicates their efficacy in safeguarding against common identity attacks such as phishing, brute force, man-in-the-middle, replay attacks, credential stuffing, SIM swapping, SIM card cloning and channel jacking.

Table 1. Security based comparison

Technology	Security	Key points
Password	Low	Vulnerable to phishing, brute force, credential stuffing, replay attacks.
Email	Medium	Vulnerable to phishing.

SMS	Medium	Vulnerable to phishing, SIM clone, SIM swap.
Magic Link	Medium	Vulnerable to phishing, man-in-the-middle attacks.
TOTP	Medium	Vulnerable to phishing and replay attacks.
HOTP	Medium	Vulnerable to phishing and replay attacks.
Push Notification	High	Resistant to push fatigue with number matching. Vulnerable to phishing.
Biometrics (Fingerprint, Face, Voice)	High	Resistant to phishing. Vulnerable to spoofing attacks.
Certificate Based Auth	High	Resistant to phishing and other common attacks.
FIDO2	High	Resistant to phishing and other common attacks.

4.2 Usability

Usability is an important criterion for evaluation, as it indicates the effectiveness and user satisfaction with the authentication process. Its primary objective is to alleviate the inconvenience and complexity encountered by users. Factors include frequency of authentication requests, number of steps involved, and quantity of information users must remember.

Table 2. Usability based comparison

Technology	Usability	Key points
Password	High	User-friendly. Easily accessible provided the user remembers the password or uses password manager.
Email	High	User-friendly. Easily accessible. Requires internet connection that can be unavailable.
SMS	Medium	Less User-friendly. Requires entering code from mobile which can be time intensive and prone to errors. Mobile devices can be lost, damaged, stolen and run out of battery. Cellular connection can be unavailable.
Magic Link	High	User-friendly. Easily accessible. Requires internet connection that can be unavailable.
TOTP	Medium	Less User-friendly. Requires entering code from mobile which can be time intensive and prone to errors. Mobile devices can be lost, damaged, stolen and run out of battery.
HOTP	Medium	Less User-friendly. Requires entering code from hardware which can be time intensive and prone to errors. Hardware can be lost, damaged and stolen.
Push Notification	High	User-friendly. Users need to tap allow or deny. Requires internet connection that can be unavailable. Requires mobile devices that can be lost, damaged, stolen and run out of battery.
Biometrics (Fingerprint, Face, Voice)	High	User-friendly, easily accessible and faster than OTP. Requires suitable environmental conditions and biometric sensors.
Certificate Based Auth	High	Good user experience. Requires smart card or USB tokens that can be lost, damaged, stolen and incompatible with devices.
FIDO2	High	Excellent User experience. Requires tapping token or Bluetooth NFC. Highly available

4.3 Cost

Cost is crucial when evaluating authentication methods as it affects the required initial investment and ongoing maintenance expenses. It includes hardware, software, and service costs.

Table 3. Cost based comparison

Technology	Cost	Key points
Password	Low	Storage cost. Operational cost like password reset.
Email	Low	Email service is mostly free. Low internet cost.
SMS	High	Low hardware and software cost. High messaging and service cost.
Magic Link	Low	Email service is free. Low internet cost.
TOTP	Medium	Mobile devices have low cost. Average software cost.
HOTP	High	High hardware token cost.
Push Notification	Low	Low hardware and software cost. Moderate service cost based on provider.
Biometrics (Fingerprint, Face, Voice)	Low	Most devices support fingerprint scanner, camera and microphone. Low Software cost.
Certificate Based Auth	Medium	One-time cost for setting infrastructure. Operational and maintenance cost.
FIDO2	Medium	High hardware cost. Low software and service cost.

5. CONCLUSION

The undeniable truth that passwords have become increasingly vulnerable to compromise in recent years has spurred a shift toward passwordless authentication as a means to eliminate these vulnerabilities. With the rapid technological advancement and evolving user expectations, adopting passwordless authentication technologies have become increasingly critical.

The future of authentication aims to strike a delicate balance between convenience and security, ensuring that users can have frictionless experience accessing their accounts and services without compromising their privacy or data. This comprehensive new study on passwordless authentication examines various state-of-the-art technologies and compares them based on security, usability, and cost. In comparison to password, passwordless authentication offers substantial benefits and is rapidly gaining traction in the Internet of Things (IoT) environment. Compared to the traditional method, authentication using FIDO keys, biometrics, push notifications, or one-time codes provides a quick, reliable, secure and user-friendly experience.

The adaptation of passwordless technology takes into account unique preferences and requirements on an organizational and user level. The best authentication technology for various features based on security, usability, and cost is selected as shown in the table below. The future of authentication will involve different approaches, and the transition from passwords to passwordless authentication is a significant one.

Table 4. Best authentication technology for different features

Security	Usability	Cost	Authentication Technology
High	High	Low	Biometrics (Fingerprint, Face, Voice), Push Notification
High	High	Medium	FIDO2, Certificate Based Authentication
Medium	High	Low	Email, Magic Link
Medium	Medium	Medium	TOTP
Medium	Medium	High	SMS, HOTP
Low	High	Low	Password

6. REFERENCES

[1] Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G.L., Roli, F.: Security evaluation of biometric authentication systems under real spoofing attacks. IET Biometrics 1(1), 11–24 (2012).

[2] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. 2021. Is Real-Time Phishing Eliminated With FIDO? Social Engineering Downgrade Attacks Against FIDO Protocols. In USENIX Security Symposium (SSYM '21). USENIX, Virtual Conference, 3811–3828.

[3] 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.

[4] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann. A Review on Authentication Methods. Australian Journal of Basic and Applied Sciences, 2013, 7 (5), pp.95-107.

[5] V. Parmar, H. A. Sanghvi, R. H. Patel and A. S. Pandya, A Comprehensive Study on Passwordless Authentication, 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), 2022, pp. 1266–1275, doi: 10.1109/ ICSCDS53736.2022.9760934.

[6] N. Singh, A. Agrawal, R. Khan, Voice biometric: A technology for voice based authentication, Advanced Science, Engineering and Medicine 10 (7-8) (2018) 754–759.

[7] Auth0 Passwordless Authentication with Magic Links, https://auth0.com/docs/authenticate/passwordless/authentication-methods/email-magic-link, Accessed on: Apr. 28, 2024, [Online].

[8] Okta Fingerprint Biometrics documentation: https://www.okta.com/identity-101/fingerprint-biometrics-definition-how-secure-it-is, Accessed on: Mar. 15, 2024, [Online].

[9] 1Kosmos Biometric Authentication documentation: https://www.1kosmos.com/biometric-authentication/fingerprint-authentication, Accessed on: Mar. 15, 2024, [Online].

[10] Wikipedia Passwordless Authentication, https://en.wikipedia.org/wiki/Passwordless_authentication, Accessed on: Feb 15, 2024, [Online].

[11] Securemetric FIDO Authentication documentation: https://www.securemetric.com/2019/05/17/pros-and-cons-of-fido-authentication, Accessed on: Feb. 22, 2024, [Online].

[12] Microsoft FIDO2 Authentication documentation: https://www.microsoft.com/en-us/security/business/security-101/what-is-fido2, Accessed on: Apr. 15, 2024, [Online].

[13] TechTarget Decentralized Identity documentation: https://www.techtarget.com/whatis/definition/decentralized-identity, Accessed on: May 1, 2024, [Online].

[14] Yubico Certificate Based Authentication documentation: https://www.yubico.com/resources/glossary/what-is-certificate-based-authentication, Accessed on: Mar. 15, 2024, [Online].