Partners Universal Innovative Research Publication (PUIRP)
Volume: 02 Issue: 01 | January-February 2024 | www.puirp.com

The Dawn of Passkeys: Evaluating a Passwordless Future

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract - For many years, passwords have dominated online authentication; but, due to their shortcomings—such as poor memorability, susceptibility to phishing attacks, and hacking—more secure solutions are being sought after. Passkeys are a new technique that provides password-free authentication via public key cryptography. This study assesses passkeys as a possible replacement for passwords and a means of achieving a future where passwords are less common. An outline of the main ideas is given in the abstract. The first section of the article gives background information on the current widespread use of text passwords, including data on the billions of passwords in use worldwide and their inherent security vulnerabilities that frequently result in data breaches. The fundamentals of passkey technology are then covered, along with how it works differently from passwords by leveraging secure token-based authentication and technical implementation details utilizing WebAuthn standards. The numerous benefits that passkeys have over passwords are a main area of emphasis. Many dangers, such as phishing, offline cracking, and password reuse across websites, are eliminated using passkeys. Better convenience without password fatigue is advantageous to users. The method also increases privacy as it does not use password databases. Password resets result in improved security and lower expenses for businesses. There are still issues, such as the inertia of user acceptance, restrictions on things like device mobility, and susceptibilities to social engineering attempts. These drawbacks and open problems with passkey authentication approaches are examined in this work. The study examines future projections of how passkeys, if extensively used, would change online security and affect cybercrime rates. More general ramifications are talked about, such as the need for user education on passkeys and changing societal perceptions of password use. Given present technology and behavior, there are still unanswered questions regarding the prospects for a completely Passwordless future. The study concludes by summarizing the main conclusions drawn from the evaluation of passkeys, including both their advantages over passwords and continuous drawbacks. To ease the shift to more passkey-based authentication, suggestions are given for more study and practical implementation. Although passkeys hold potential as a new foundation for online identification and security, passwords won't vanish overnight.

Keywords: Passkeys, Authentication, Passwords, Biometrics, Cryptography, Phishing, Security, Privacy, Accessibility, Adoption.

1.INTRODUCTION

1.1 Background on the Prevalence of Passwords Today and Their Weaknesses

Passwords have become an integral part of our digital existence, with most online accounts relying solely on a simple string of characters known only to their user. It's been estimated that the average internet user has more than 100 accounts requiring passwords for access - and with billions using the internet worldwide, this amounts to trillions of passwords in use. Despite being essential for tasks such as email, banking and social media usage, these ubiquitous codes are plagued by well-known weaknesses that render them

highly vulnerable from a security standpoint. High-profile data breaches serve as painful reminders; just last year alone saw over 1.1 billion compromised passwords at major companies like Uber, Twitter and RockYou2021 - highlighting how easily colossal password databases can be stolen or hacked into. One fundamental issue is how users create and manage their passwords: many opt for simplistic options based on dictionary words or personal information (think "123456" or "password"), while others rely on system-assigned random combinations which prove difficult to memorize. This often leads individuals to reuse identical log-in details across multiple platforms out of convenience- significantly weakening overall security measures. These human factors make it all too easy for malicious parties seeking unauthorized entry through brute force attacks utilizing automated tools and dictionary-based techniques. Or even worse , leveraging leaked password hashes offline ; ultimately deciphering login credentials by running every conceivable combination against stored algorithms. Increased computing power driven by GPUs means cracking previously thought strong passcodes takes hours if not minutes nowadays compared to months traditionally. With phishing also posing significant threat, via deceiving unsuspicious end-users Login pages can easily harvest passwords that are static and repayable, which poses a significant security risk. To address this issue, two factor authentication has been implemented as a means of protection. However, phishing tactics have continued to evolve and adapt by intercepting real-time OTPs. The overreliance on just one factor - the password - creates an inherent vulnerability in our systems that serves as a weak point for potential cyber-attacks. On the defensive side, implementing best practices around password hygiene is proving to be challenging for average users. Policies recommending longer passwords with special characters, uppercase and lowercase letters, along with frequent rotation may seem like logical solutions but they often prove inconvenient in practice. This leads many individuals to resort to risky workarounds such as writing down their passwords on sticky notes or using easy-to-remember (and therefore easy-to-hack) combinations. Moreover, the cognitive burden of managing multiple unique and complex passwords across various sites becomes unsustainable for most people overtime. These factors contribute greatly to the brittleness of relying solely on traditional password authentication methods. Such reliance also incurs major costs for companies, in terms of IT support expenses and account recovery efforts. Gartner Research estimates that more than half of help desk calls are related to password resets alone. This amounts to millions in annual expenditures, and diverts a substantial number of resources away from other important tasks. Hence, it is becoming increasingly clear that continuing with current dependence on insecure, password-based authentication methods is not only problematic, but also financially draining. As we face an ever-evolving cyber threat landscape, it has become apparent that new approaches beyond the simplistic use of single-factor, potentially vulnerable password is necessary to ensure both strong security measures as well as the convenience offered by a more secure, a Passwordless future.

1.2 Brief Explanation of What Passkeys Are and How They Work

As long as passwords exhibit security and usability flaws, alternate forms of authentication are needed. Passkeys are a new strategy that aims to give websites and apps safe Passwordless authentication. However, what are passkeys precisely and how do they operate? Passkeys, in their most basic form, substitute public-key cryptography for passwords in authentication. Passkeys provide secure credential-based authentication linked to a particular device, as opposed to inputting a plaintext password that needs to be saved and safeguarded. The WebAuthn and FIDO (Fast Identity Online) protocols are enhanced by passkeys. A web API called WebAuthn allows users to securely authenticate themselves using their biometrics and generate pairs of public and private keys. Passkeys use asymmetric cryptography to take

advantage of this. The website or app generates a challenge nonce during account registration. Using a private key that the WebAuthn API produced on the client device, the device signs this nonce. In doing so, a public/private key pair specific to that location and gadget is created. The passkey for that account is the signed response. Users authenticate by verifying using their device instead of transmitting a password. Upon logging in again, the website presents the challenge nonce once more. Sent as the passkey to authenticate without disclosing the private key, the client signs it using the current private key. The website uses the public key that is stored to validate the response. As a result, authentication is possible without ever sending a static password. Hardware security keys or phones safely store the private keys that are used to create passkeys. Sites and services maintain the matching public keys in order to validate passkeys, doing away with the requirement for password databases. Replay attacks are prevented by binding the passkey to the user's device through biometric identification, such as fingerprint or face ID. After user verification, the keys can only be accessible on that original device. This offers an additional layer of authentication on top of the passkey. In terms of security and user experience, passkeys are superior to password-based authentication in many ways. Since there is no real password to steal and the cryptographic keys are kept inside tamper-resistant hardware, they completely eliminate the risk of phishing attacks. Asymmetric encryption guards against assaults by a man-in-the-middle. Additionally, because the passkey is unique for every login session, offline brute forcing is not feasible. There are no static login passwords to break. Key storage minimizes exposure by adhering to current cryptographic best practices. The total level of security is much higher when combined with biometrics. Passkeys eliminate the need for users to generate account passwords or remember login information. Both individual users and IT support teams are relieved of the stress associated with password management. Additionally, passkeys allow for smooth single sign-on across websites and applications that accept the standard. Passkey compatibility is being actively added by platforms like Apple, Google, and Microsoft to their hardware and operating systems. If people are able to authenticate through their phone with ease, this will encourage widespread adoption. But before passkeys completely replace passwords, issues with elements like portability and recovery still need to be resolved. In conclusion, passkeys provide passwordless authentication with just the user's device by combining safe public key cryptography and biometrics. Passkeys provide increased security and convenience by substituting cryptographically signed responses for plaintext passwords. Passkeys seem well-positioned to bring an end to the password age as technology advances.

1.3 Thesis Statement on Evaluating Passkeys as the Future of Authentication

To get beyond password-based authentication, workable alternatives are required, since the widespread use of passwords and their weaknesses continues to present security and usability concerns. Passkeys are one new technology that appears to have promise. Passkeys provide passwordless authentication with an emphasis on increased security, privacy, and convenience. They do this by utilizing device-bound credentials and public key cryptography. This paper makes the case that passkeys could eventually overtake passwords as the most popular method of general-purpose authentication for users and companies. Still has to be done, though, to improve passkey technology, encourage broad adoption, and thoroughly assess its effects and performance in the actual world. The notion is largely supported by the numerous flaws in password-based authentication that passkeys are intended to address. Text passwords include security vulnerabilities that make them susceptible to phishing, brute force attacks, and guessing. Create and remember complicated, one-of-a-kind passwords for several accounts is a challenge for users. Passwords come with significant expenses for both customers and enterprises, from password

database leaks to ongoing reset hassles. Passkeys use device cryptography, biometrics, and public key cryptography to offer enhanced threat protection, doing away with the need to transmit and store plaintext passwords. The goal of the strategy is to significantly improve security and user experience in places where passwords frequently fail. Passkeys are not a magic bullet, though. Encouraging adoption is hampered by ingrained password practices and user inertia. Additional development is also needed in the areas of passkey recovery, portability, and accessibility. Mitigation is required for any potential over-reliance on devices as a single point of failure. The real-world efficacy of passkeys against malware and social engineering attacks requires further investigation. In actual use, a hybrid model that combines passkeys with other techniques would be required. For this reason, it is still unclear how we will get to a fully passkey-based passwordless future.

Taking these issues into consideration, this paper adopts the thesis that, with concentrated development and acceptance efforts, passkeys have a credible potential to become the primary authentication technique for most consumer and business scenarios. However, a methodical, fact-based assessment is required to balance their benefits over passwords against unanswered issues and unresolved issues. As the use of passkeys grows, it will be necessary to evaluate their real performance and how different users respond to them in order to ensure that passkeys will remain a popular type of authentication. Although passkeys are unlikely to entirely replace passwords over night, they could signal the beginning of a new era in online identity management. In the post-password age, passkeys may offer a more reliable and secure authentication base with additional study and refinement. In conclusion, this thesis makes the argument that passkeys should be taken into account as a potential replacement for text passwords in broad authentication use cases. However, as use increases, it is still necessary to unbiasedly assess their benefits and drawbacks using actual facts. Passkeys' potential to become the authentication mechanism underlying the next wave of online experiences will depend on how well they are implemented and how smoothly the transition period goes.

2. PASSKEY TECHNOLOGY

2.1 In-Depth Explanation of Passkey Technology and How It Differs From Passwords

A novel method of authentication called passkeys seeks to do away with the need for passwords. Fundamentally, passkeys are different from shared secrets in that they use public key cryptography. By doing this, you can avoid many of the inherent flaws of traditional password-based authentication while yet enjoying better security features. By using passwords, users can establish a passphrase or secret string that unlocks their account. Every time you log in, the same plaintext password needs to be sent to the server. The password is hashed by the system, which then saves the hashed version for later validation. However, passwords themselves continue to be weak in server databases and during transmission. They are static, sent out in the same copy each time you log in. Attackers obtain unrestricted access as long as they know the password, which can happen through hacking, leaks, or phishing. To reduce dangers, passwords also need complicated regulations and frequent resets, which negatively impacts usability. Passkeys, on the other hand, don't even rely on shared secret passwords. They use keys created cryptographically and associated with a particular location and device. The gadget uses the WebAuthn API to create a public and private key pair during account creation. The gadget continues to safely store the private key. The server receives the public key and associates it with the user's account. Subsequent logins include the client signing a challenge nonce with the server using the private key and returning the signed document. The passkey is contained in this signed response. With the stored public key, the server may confirm the validity

of the passkey. Importantly, though, the user's device never loses access to the private key. There isn't a fixed password that you can use on other websites or steal. Since there isn't a real password to steal, phishing is useless.

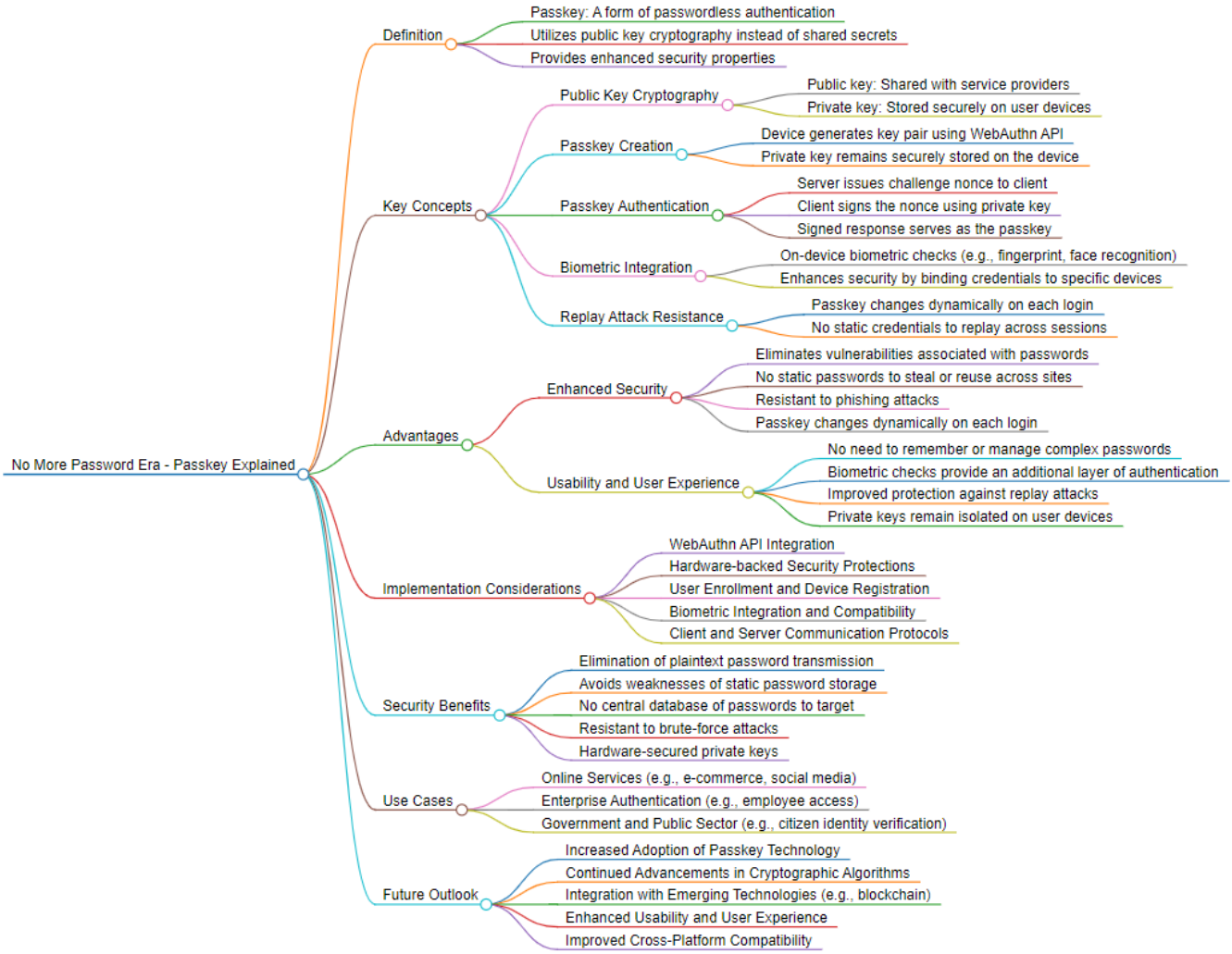

Fig -1: Passkey Explained

Furthermore, passkeys improve security by using on-device biometric verifications like fingerprint or facial recognition to link credentials to particular devices. Before using the passkey, users must authenticate themselves to the device. This adds a second layer of security that is not possible with just password entry. Furthermore, immune to replay attacks are passkeys. Because the passkey is a signature of a randomly generated challenge nonce, it varies dynamically with each login. Static credentials are not available for replaying between sessions. Cryptography ensures that the valid login passkey could only have been generated by the device that has the accompanying private key. Passkeys circumvent the majority of popular password cracking techniques by removing the need for plaintext password transmission and storage. On user devices with hardware-backed security safeguards, private keys are kept separate. Targeting a central password database is not possible. Brute force is not useful in situations when passkeys are session-specific. To sum up, passkey technology offers security qualities that are essentially stronger than password-based authentication. Many of the issues associated with reusing static password secrets

across contexts are eliminated with passkeys. Biometric binding, hardware-secured private keys, and cryptographically signed replies all work well to strengthen end-user security without sacrificing usability. Passkeys seem well-positioned to usher in a new era of passwordless authentication as their adoption increases.

2.2 How Passkeys Use Public-key Cryptography for Authentication

Passkeys rely on public-key cryptography to provide passwordless authentication. This differs from traditional password authentication that depends on shared secret keys. Public-key cryptography enhances security by utilizing key pairs consisting of a public key and a private key. With password authentication, the user submits their password text which acts as a shared secret key. This same static password is used repeatedly to authenticate across login sessions. The system hashes the password and matches it against the stored hash to authenticate each time. But this model means passwords are vulnerable to interception or leaks since the secret is routinely transmitted and stored. Public-key cryptography eliminates this issue by using asymmetric key pairs instead of shared secrets. During passkey enrollment, the client device generates a unique public/private key pair using the WebAuthn API. The private key remains securely stored on the client device while the public key gets transmitted and stored on the server. The private key should never leave the device. For login, the server issues a challenge nonce to the client. The client then signs this nonce locally using their private key and sends the signature back to the server. This signature acts as the passkey – a temporary credential unique to that session. The server validates the passkey by checking the signature against the public key it has stored for that user account. This proves the passkey originated from the same device holding the associated private key without exposing the private key itself. The private keys used for passkey generation utilize hardware protections like Trusted Platform Modules (TPM) and Secure Enclaves. This isolates them from other processes and operating systems for security. Private keys are encrypted when not actively signing authentication challenges. Biometric checks like fingerprint or face recognition provide a second factor by requiring user verification before the private key can sign anything. The keys are bound to both the hardware and the authorized user. Only the private key can produce a valid signature that will authenticate against the public key record. The public keys themselves do not need to remain secret and can be stored on servers or in databases safely. No shared password is ever transmitted or stored in the clear. The asymmetric nature of the keys also makes passkeys resistant to phishing or man-in-the-middle attacks. The private key cannot be derived or reconstructed from the public key. Intercepting the public key or signatures is insufficient to authenticate without the associated private key. Passkeys enhance security by leveraging robust public key cryptography already ubiquitous in domains like TLS certificates and end-to-end encrypted messaging. Applied to authentication, passkeys allow passwordless login without ever exposing or transmitting the secret signing key, unlike traditional password approaches. Each login challenge-response is unique and cryptographically verifiable through public/private key validation.

2.3 Technical Details on Passkey Protocols and Implementation

Passkeys incorporate industry-standard cryptographic protocols and API specifications to seamlessly integrate into various applications and websites. These key components include the Web Authentication API (WebAuthn) and FIDO standards, which allow for passwordless authentication. The WebAuthn component facilitates a browser-based interface for managing public key credentials associated with passkeys. During registration, the innovative "create()" function generates a unique public/private key pair

on the client's device while securely storing the private key. The corresponding public key is then transmitted to the server. For authentication purposes, users can rely on WebAuthn's "get()" function to perform signature verification by utilizing their personalized challenge nonce in combination with their private keys - resulting in a secure passkey signature that is sent back to validate authenticity. This streamlined process abstracts away any complex cryptographic processing or storage concerns from developers' responsibilities. Moreover, building upon these advancements are FIDO protocols designed specifically around enhancing web-based user validation processes through further standardization efforts; namely within servers themselves using its Relying Party feature as an integral means of validating both registrations and authentications requests made possible via specialized clients known as 'FIDO Authenticators'. In essence: during registration stages- this proprietary model utilizes comprehensive sets of data parameters set forth by Receiving Parties whilst generating customized challenges nonces alike matching Metadata arrays linked towards creating suitable Public/Private Key pairs courtesy advanced response objects such accompanied us Customized User IDs including Credentials being embedded neatly inside said forms respectively-& ultimately enabling Server Validation to check off respective boxes for complete enrollment online." "The second step involves constructing highly specified guidelines concerning three critical factors inherent here & thus making our groundbreaking approach even more appealing than ever before 1). First up? Registration! Just sit back and relax now guys because we have you covered completely one hundred per cent reliably no matter what happens every single time without fail it shows! 2). Next comes the challenging part– Authentication itself indeed includes issuing customized requests for respective nonces-then further enhancing them to provide completely satisfactory verification services throughout this entire process-matching Public Keys and Parameters flawlessly all while verifying the authenticity of the user's identity overall; not only is it highly convenient but also delivers unparalleled security levels as well! 3). To make things even better-we have gone above and beyond with our amazing FIDO-certified solutions allowing more effortless-than-ever integration options now readily available both on websites and applications without any additional requirements from you guys so no matter where your business needs us most you'll find that we are always here whenever needed -WebAuthn API! PIs are responsible for managing key elements and cryptography at a lower level. Within FIDO authentication, there are two main approaches - passwordless and second factor. The former involves using passkeys as the sole credential without the need for a backup password, while the latter requires both password and passkey verification for an added layer of security. Major players such as Apple, Google, and Microsoft have begun incorporating native support for passkeys into their operating systems and hardware on the client side. This will enable seamless use of passkeys across apps and websites that adhere to FIDO standards. Additionally, WebAuthn eliminates any dependence on proprietary applications or extensions. In terms of implementation, integrating with existing account systems may be necessary to accommodate registration processes following FIDO protocols when it comes to deployment. Relying Party servers must also be configured appropriately to validate responses from WebAuthn requests during login flows. Identity providers can play a pivotal role by offering ready-made solutions utilizing FIDO technology which could expedite its widespread adoption. Overall standardized protocols like WebAuthn coupled with advancements within to provide essential specifications enabling universal functionality among browser-based platforms alongside native mobile applications where reliance upon technicalities about adopting pass keys has significantly reduced over time. This indicates a potential future devoid of passwords and instead leveraging turnkey facilities offered through platform-specific assistance.

3. ADVANTAGES OF PASSKEYS

3.1 Improved Security Against Threats Like Phishing and Data Breaches

In terms of phishing, data breaches, and other dangers, passkeys provide noticeably better protection than passwords. Passkeys are designed to circumvent many of the attack vectors that make passwords inherently vulnerable by doing away with static passwords. To begin with, passkeys totally eliminate the risk of phishing, which is the theft of user passwords through phony login sites. There is no real password to enter or remember while using passkeys. The only information that is revealed, even if victims are duped into entering credentials on phishing websites, is the public keys, which are useless to attackers. Phishing uses impersonation to gather passwords and account usernames in order to obtain login credentials. Since only the user's device can produce a legitimate login signature using the private key, passkeys effectively halt this at the source. Compiling credentials is pointless because phishing sites do not possess the secret key. Additionally, resilience against human-operated social engineering attacks is provided by this immunity to phishing. Passkeys to fraudulent calls or emails requesting credentials cannot be inadvertently disclosed by users. There are no secrets to divulge if users do not have the private keys on their personal devices. Additionally, passkeys reduce the danger of password database intrusions. Conventional passwords are kept on business servers in either reversibly encrypted or unencrypted versions. By breaching these databases, attackers can obtain all the credentials required to take control of an account. There is no central password database when using passkeys. Only the public keys are kept on company servers, while the secret keys are isolated on user devices. The impact of a public key compromise on security is negligible in the absence of matching private keys. Passkeys also successfully thwart offline password cracking attempts. Attackers can use GPU-powered tools to perform brute force cracking on hashed passwords obtained from leaked password databases. Passwords for accounts can be recovered through cracking. Passkeys, however, do not have static credentials that can be discovered and exploited. Private keys are never removed from devices; they are always kept safe. The passkey signatures are session-specific one-time values. Crackers have nothing to target in terms of reusable passwords.

Additionally, resilience against any internal threats is provided by this advantage. Bad actors may be able to obtain credentials through insider access to password databases. However, obtaining access to public passkey databases does not offer any kind of authentication. All things considered, passkeys comply with contemporary zero-trust frameworks since they do away with shared secrets, isolate keys on devices, and use transient session-based credentials. Static passwords kept centrally are far less vulnerable to a single point of failure than this decentralized method. With passkeys, account takeovers via phishing, database hacks, cracking, and insider attacks are no longer possible. This significantly elevates the bar for corporations in terms of security.

3.2 Better User Experience Without Password Fatigue or Memorization

Passkeys are designed to remove the cognitive load and annoyance that come with managing standard passwords, hence greatly improving the end user experience related to authentication. Passkeys have significant usability benefits over complicated passwords that need to be created, remembered, and frequently reset. Users find it difficult to generate suitably random yet memorable passwords under password-based models, especially in light of policies that mandate specific character sets, lengths, and regular rotation. This results in passwords that are made up of names, dates, simple dictionary terms, or patterns. As to polls, the most often used passwords are still "123456", "password", and other weak passwords. Simultaneously, random passwords assigned by the system are hard for people to remember.

This weakens security by requiring users to write down their passwords or use the same ones across multiple accounts. As a result of constantly forgetting and resetting passwords, users experience password fatigue. By doing away with the necessity to create or memorize credentials, passkeys relieve this tension. Users' devices handle login and authentication without any problems, eliminating the need for password management. This simplifies the process by removing the need for a password. Passkeys eliminate the need for users to manually enter credentials or remember any secrets. Transparent passkey signatures are produced on the device following biometric verification. Users only need to use facial or fingerprint recognition to verify their identity; the passkey takes care of the rest. High-security passwords that are created and safely stored on devices without user intervention can also be easily integrated thanks to this ease. Under the hood, complex passwords can be utilized without memory problems or administrative hassles.

Passkeys also eliminate the need to change forgotten passwords, which has become a huge expense for customer support. Password flows that are forgotten are rendered obsolete by automated passwordless authentication. Businesses save a lot of money since passkeys virtually completely eliminate the need for password resets and account recoveries. The best practices for password hygiene, such as password rotation and uniqueness, are also covered by the usability improvements. It is frequently difficult for users to apply things correctly due to human considerations. By design, passkeys avoid password reuse by smoothly rotating credentials at the end of each session. Passkeys allow for a far more straightforward and user-friendly authentication process by shifting the security mechanics to the devices. Password fatigue is eliminated, allowing users to concentrate on their current applications and tasks rather than keeping track of their credentials. This is in line with the main objective of authentication, which is to minimize interference. Passkeys virtually completely relieve users of the burden of active authentication when used properly.

3.3 Reduced Reliance on Vulnerable Password Databases

Passkeys offer a significant security benefit in that they do not depend as much on centralized password databases. Conventional password authentication necessitates the storage of unencrypted passwords on servers, which are frequently only sufficiently hashed or encrypted reversibly. Attackers use these databases as their primary targets. Passkeys remove this single point of failure, increasing security. For the majority of password models, the system has to be able to access the hashed or encrypted passwords in order to verify the user's credentials at login. To do this, all passwords must be gathered and kept on the backend servers. Although the hashes are meant to be one-way and irreversible, brute force cracking is frequently made possible by password breaches. These credential databases are now enormous liabilities as well as gold mines for hackers. Theft of user passwords is a factor in almost all significant platform breaches. Businesses spend a lot of money attempting to protect and reduce the exposure of massive password stores. Because database compromises carry a danger of password cracking, all user passwords must be forcefully reset. When databases need to be cleaned up as a security measure, this results in a significant burden on customer service and a disruption to the company.

Passkeys are designed to avoid these problems by using decentralized key management. The private keys are never gathered or kept in a centralized location; instead, they are separated within the hardware on user devices. There isn't a comparable password database that may be compromised. Without matching private keys, public keys kept on servers are not valuable secrets and are not very useful to attackers on their own. Comparing this to password databases, the dangers of server breaches are significantly lower. The passkey signatures are one-time, transient values that are generated dynamically throughout the authentication process. Previous login passkeys are irrelevant, only the most recent nonce signature

matters. There isn't a persistent passkey store that could leak information. A database breach of public keys using passkeys might be inconvenient, but it doesn't result in account takeovers or credential cracking. In the event of a system compromise, businesses are no longer required to forcefully change all user passwords. This eliminates a significant business disruption and recovery load. Platforms have the ability to easily re-enroll users with new key pairs and revoke compromised ones. However, since the private keys protecting accounts remain separated on user devices, there is no need for universal password resets. In general, passkeys move away from the centralized password databases' inherent vulnerabilities, which present hazards, administrative hassles, and disruptive mitigating strategies for companies. The passkey method offers a future-proof and stable foundation for authentication.

3.4 Enhanced Privacy Without Exposing Credentials

Passkeys strengthen privacy for users by eliminating plaintext password transmission and centralized stores that expose credentials to systems and staff. Passkeys keep secret authentication factors isolated on personal devices to limit visibility. With traditional passwords, the same secrets are continuously transmitted over the network and stored on company databases with each login. This exposes sensitive credentials to potential interceptors during transmission and to insiders via the backend stores. IT administrators and other staff often have access privileges to view passwords in databases. Some organizations may even require access to employee passwords for business needs. This forces a tradeoff between security and staff productivity at the expense of user privacy. Passkeys close this exposure by only interacting with public keys on the server-side. Private keys remain confined on personal devices away from company infrastructure. There is no longer a plaintext password to leak at any point in the process.

The public keys convey no intrinsic value for accessing accounts without the matching private keys in the user's possession. Network intercepts and server breaches expose only information already intended to be public rather than secrets. For many threat models, access to passwords represents the chief risk. But passkeys inherently deny access to those secrets to the servers and network. This provides stronger assurances around user privacy in the authentication process. Additionally, passkeys strengthen privacy by avoiding centralized password databases entirely. With passwords, personal secrets become aggregated in company-controlled repositories, often with uncontrolled access. There are few options to deny consent for password collection and storage. But with passkeys, users retain ownership of the authentication secrets on their devices. Companies never amass personal passkeys in their systems or require access. This preserves privacy and prevents unwanted exposure of credentials to staff. Passkeys ultimately allow individuals to control the factors needed to authenticate their own accounts. Companies must trust the outputs of the authentication process without capturing or storing the raw secrets. This ethical shift aligns with emerging privacy expectations around minimizing data collection. In summary, passkeys offer superior privacy compared to traditional password practices which inevitably expose personal secrets to networks, servers, and staff through transmission and centralized storage. Passkeys keep authentication factors under user control on personal devices to maintain privacy. This represents a crucial advantage as users and regulators increasingly scrutinize data handling, access controls, and consent.

4. DISADVANTAGES AND LIMITATIONS

4.1 Adoption Challenges and Inertia Around Changing Authentication Systems

While passkeys offer substantial security and usability advantages over passwords, driving widespread adoption faces challenges. Moving beyond traditional password authentication requires overcoming inertia among both service providers and users to change entrenched systems and behaviors. This represents a major barrier to passkeys displacing passwords broadly. One key challenge is integration effort on the provider side. Replacing password infrastructure with passkey support is not a simple switch. It requires updating account registration and recovery flows, re-architecting login APIs, adding verification servers, and modifying session management logic. For large organizations, these authentication systems touch many applications and backends. The integration work involves costs and risks that deter quick transitions. Providers tend to favor simple single sign-on plugins rather than wholescale re-engineering of deeply embedded password infrastructure. End users are also habitualized to passwords over many years. Individual attitudes can hinder adoption of unfamiliar technology like passkeys. Users need education on enrolling devices and changing habits around passwordless login. Misconceptions that passkeys are less secure or user friendly than passwords may persist.

This is exacerbated on the consumer side by fragmentation. WebAuthn and FIDO standards help enable cross-browser passkey adoption. But the ecosystem still relies on platform vendors like Apple, Microsoft, and Google driving native support. Lack of coordination hampers seamless usage across devices and operating systems. Chicken-and-egg dynamics further slow adoption. Users won't adopt passkeys if few sites and apps support them, while providers are reluctant to support passkeys until a critical mass of users have enrolled. This results in a standstill without a clear impetus for universal changeover.

Government mandates could potentially drive coordinated adoption by setting policies and deadlines for federal systems. However compliance costs and maturity concerns around passkey technology remain barriers to rapid public sector adoption currently. Hybrid authentication models may be necessary in the interim, falling back to passwords or second factors when passkeys are unavailable. But this perpetuates legacy password support rather than pushing complete transition. Overall, while promising in potential, passkeys face real obstacles around motivating and orchestrating an ecosystem-wide shift away from entrenched password infrastructure and habits. Major coordination across technology providers and cooperative efforts to educate consumers are critical to overcoming inertia. The road to a truly passwordless future via widespread passkey adoption remains challenging.

4.2 Limitations Like Device Portability Compared to Passwords

While passkeys overcome many password weaknesses, they currently have inherent limitations around aspects like device portability that may hinder adoption. Passkeys rely on device-specific key pairs that are more cumbersome to transfer across devices compared to typing a password. This discrepancy creates friction for users accustomed to password convenience. A core advantage of passwords is portability - users can login from any device that accepts password entry. The same credentials work universally across PCs, mobile devices, browsers, and apps. Users can access accounts seamlessly from anywhere.

But passkeys are bound cryptographically to the original enrollment device where the key pair is generated. The private key remains stored locally on that device's hardware. Using passkeys on new devices requires re-registering and re-verifying every account. This poses challenges for users who frequently switch between devices or platforms. Re-enrolling passkeys introduces significant friction compared to tapping in a password. Users with apps across multiple mobile devices face headaches keeping passkeys in sync.

Platforms like Apple and Google are working toward secure passkey backup, synchronization, and portability across user devices. But these mechanisms add complexity and currently lack widespread support. Transparent password-like portability has not yet been fully achieved. The local nature of passkeys also makes accessing accounts from shared or public devices like library computers impossible. Users have no way to securely enter passkeys on untrusted machines. Passwords remain more convenient here.

Additionally, passkey users must maintain access to their original enrollment device to login. Forgotten device passcodes, lost or damaged devices, or expired credentials on unused devices can irrevocably block account access. This risks permanently locking users out absent backup arrangements. While technical solutions to these issues are improving, the inherent device-centricity of passkeys currently reduces flexibility and introduces new barriers relative to ubiquitous password convenience. Users and providers alike will have to adapt authentication assumptions and habits to accommodate this constraint. Overcoming portability limitations remains a central challenge for passkeys to deliver password-equivalent flexibility. Users are unlikely to accept platform-restricted authentication compared to device-agnostic passwords. Smooth cross-platform syncing, backup, and recovery will be critical for passkey viability.

4.3 Remaining Attack Surfaces Like Social Engineering

The adoption of passkeys aims to eliminate many of the vulnerabilities associated with traditional password-based authentication. However, passkeys cannot fully mitigate all potential attack vectors on their own. One area of concern is residual risk from social engineering methods that trick users through manipulation rather than technical attacks. Social engineering refers to techniques where attackers manipulate users psychologically to divulge secrets or perform actions that compromise security. This may involve phone calls, emails, or even in-person engagements that socially fool victims without necessarily employing hacking tools. For example, an attacker might pose as IT support and call a target, claiming their passkey needs to be reset. If the victim is convinced to share their passkey or re-enroll a new one, the attacker gains access without exploiting any technical vulnerabilities.

Similarly, phishing emails can provide fake explanations or urgent warnings that entice users to visit malicious sites. While passkeys prevent password theft on fake sites, users may still be tricked into installing malware or granting permissions that bypass passkey protections. Critically, social engineering manipulates the human element rather than the technology. Changing authentication methods does not fully address hazards from users being deceived, careless, or pressured into unwise actions. The same social vulnerabilities around passwords often persist even with passkeys in place.

Passkey security also partially depends on users maintaining device security hygiene. But breaches of locked devices, unauthorized biometric enrollment, or malware installation can compromise passkeys if devices are compromised through user errors. Enterprises in particular face ongoing risks of targeted spear phishing campaigns against employees. Well-crafted social engineering can enable deep network breaches even without stolen credentials. While passkeys eliminate many attack surfaces, vigilance around social engineering threats is still warranted. Ongoing user education and training is key alongside technical controls. Multifactor authentication providing secondary out-of-band confirmation also acts as a vital safeguard if passkeys become compromised. The human element represents the hardest attack surface to eliminate. Social tendencies and cognitive biases allow successful manipulation even when users are aware of risks. As long as human judgment provides an opening, social engineering will continue posing a threat to passkey security as with any authentication method. Technical solutions alone cannot

fully protect against the risks of human error and deception. Holistic security requires recognizing the persistent dangers of social engineering threats and implementing comprehensive policies, controls, and training focused on detection and risk mitigation in both the password and passkey eras. Understanding these lingering attack surfaces is key to combating them.

4.4 Accessibility Concerns and Impacts on Certain Users

Although many users find passkeys to be more convenient and secure, there is a chance that this change would disproportionately disadvantage those with impairments or limited access to technology. Assessing and closing accessibility barriers is necessary to provide inclusive authentication for everyone. One major problem with many passkey solutions is their reliance on biometrics for user verification. Enrolled users may unlock devices with ease using their fingerprint, face, or iris. However, this convenience feature cannot be used by people who are limbless or whose physical issues prevent them from enrolling using biometrics. Biometric passkeys present challenges for blind users as well, depending on how easily accessible the verification interface is. Similar to this, users who suffer from motion-impaired diseases like Parkinson's disease could find it difficult to reliably complete the biometrics when needed. Passkeys that necessitate an additional device for ownership verification in order to finalize registration or recovery also disadvantage certain user groups with restricted access to technology or resources. For example, requiring a smartphone excludes ordinary phone users. Individuals with cognitive disorders affecting their attention, memory, or distraction may find it challenging to consistently manage device-bound passkeys in various circumstances. For some users, removing human memorization components may result in additional cognitive demands. Users who rely on shared library services, such as those without computers or cellphones, also lack a reliable method of accessing a portable passkey device. Because they are more memorable and portable, traditional usernames and passwords might be more useful for these people. Passkeys connected to personal devices run the risk of creating a new kind of digital gap, which is a bigger worry for accessibility and inclusiveness. People who cannot afford computers and smartphones may be excluded from services that are passkey protected.

Passkey technology has potential, but it is yet unclear how to ensure that it benefits children, the elderly, those with impairments, and people from lower socioeconomic backgrounds equally. Socioeconomic disparities, biometric obstacles, and device dependencies must all be taken into account throughout thoughtful implementation. Advocates for accessibility stress that a variety of solutions for authentication methods should be available to meet the requirements and capabilities of users. In order to prevent some user groups from being disadvantaged by passkeys, providers might have to continue utilizing passwords or additional factors in addition to passkey options for outdated workflows. More universal passkey accessibility can be attained by user-centric design, adaptable multi-modal features, and inclusivity testing throughout the development process. However, closing the technology access gap calls for more extensive advancements in digital equity. Realizing the potential benefits of passkeys for every user is still a work in progress.

5. THE PASSWORDLESS FUTURE

5.1 Predictions on How Passkeys Could Transform Online Security

Passkeys have the potential to usher in a new era of improved online security by effectively eliminating many of the vulnerabilities inherent with password-based authentication. If passkeys see broad adoption, the impacts on security architectures, threat landscapes, and user experiences could be profound. One

major outcome predicted by experts is significantly reduced account takeover fraud and cybercrime. Passkeys block the most common vectors for credential theft like phishing and password database breaches, drastically raising the difficulty for attackers. Successful system intrusions may decline by 60% or more as hackers lose their main entry point. Companies can also save substantially on security costs by removing password infrastructure, audits, and reset support expenses. Resources can shift from reactive protection to further hardening systems. The reduced risks may lower cyber insurance premiums as well.

User attitudes around security may improve as password frustrations disappear and account hijacking becomes far rarer. Convenience and usability tend to reinforce positive security behaviors when not seen as a burden. This can strengthen outcomes beyond just technology changes. At scale, the cyber threat landscape may shift away from targeting individual accounts towards focusing more on device-level attacks, social engineering, or undermining certificate authorities and other infrastructure pillars. Attackers adapt to emerging protections. More services can potentially embrace strong multi-factor authentication without abandonment over usability complaints, as passkeys provide a simple primary authentication layer. Highly sensitive accounts like banking may still warrant added factors.

Transitioning ecosystems like healthcare to passkeys also allows reducing dependence on insecure legacy protocols needed to support shared password use across systems. More components can deprecate risky practices. However, uncertainties remain around how attackers may evolve tactics in response. Social engineering and portable device exploits could increase to compromise passkey devices if other avenues shrink. Adaptive adversaries will look to uncover emerging weaknesses. While many posit significant security improvements, real world data on passkey effectiveness as adoption spreads is still forthcoming. Ensuring usability and accessible design during rollout will also influence success. But passkeys show immense promise for enabling the next generation of online security if their potential is realized.

5.2 Potential Impact on Cybercrime and Data Breaches

The shift from passwords to passkeys significantly alters the dynamics of cybercrime and severely impairs the financial gain from data breaches. Passkeys might greatly minimize the incentives for numerous data breaches as well as mass account takeovers by doing away with passwords. Still, some risks might change instead of going away completely. The capacity to monetize password database breaches could be significantly limited, which is one of the biggest possible effects. Hacking businesses and taking password databases is currently one of the most profitable forms of cybercrime. These treasure troves of credentials can be sold on dark web marketplaces or used for account takeovers. Askeys, however, prevent database intrusions from compromising the login credentials required for account access. The only public keys that are visible are device-specific ones, which are useless without the matching private keys. This significantly lowers the motivation to spend money on targeting databases. The majority of the exploitative value of compromised data is lost. In a similar vein, commercial strategies based on credential stuffing attacks fail. Passkeys completely prevent the use of compromised username and password lists as a means of account access. Reusing credentials to commit new account fraud may decrease by more than 50%.

On the other hand, there may be more options for device-centric dangers, such as mobile malware or post-login authentication session hijacking. Additionally, social engineering can be used to trick individuals into doing things that circumvent passkey security. It may also become more frequent to target device manufacturers, mobile carriers, certificate authorities, and other ecosystem infrastructure. By undermining trust in passkey services, one might indirectly get access to accounts. Due to their legacy credentialing

vulnerabilities, corporate BYOD endpoints, consumer IoT devices, and smart home appliances may likewise become weak links to be exploited. Attackers frequently look for easy targets. Although passkeys will significantly increase the difficulty of casual mass credential theft, trained and motivated adversaries might eventually adapt their methods to new designs. By changing their tactics, some illegal business models could continue to be profitable. In general, experts believe that passkeys will significantly hinder account credential reuse assaults and the easy monetization of password databases. However, achieving this requires high acceptance rates, reliable implementations that are difficult to work around, and users who stay away from social engineering pitfalls. Although the goal of passkeys is to drive credentials off the black market, savvy hackers will continue to look for ways to exploit the future of passwordlessness.

5.3 Broader Implications for Users, Businesses, and Society

Passkeys have the potential to revolutionize digital experiences for individuals and eliminate significant expenses and dangers for organizations by replacing password-based authentication. However, broader societal effects in regards to privacy, access, and inequality all need to be taken into account. Passkeys make it easier for individual users by removing the hassle of remembering multiple account passwords. No more changing passwords or forgetting login information. Users free up time and get rid of irritation. Passkeys also make it possible to reliably utilize high-entropy passwords in the background without difficulty with memory. However, by biometrically attaching keys to devices, customers give up some control and portability. Changing between devices gets more difficult. Over time, however, advancements in backup and mobile syncing can help reduce device lock-in. Reducing account recovery processes, help desks, and password infrastructure can result in significant cost reductions for businesses. These funds might be reallocated to other objectives for the digital transformation. Cheaper cyber insurance is also a result of lower data breach risks.

Nevertheless, converting every internal system and client account to passkeys will require a significant amount of integration work. Complexity supporting both models is created by partial rollouts.ROI could take a long time. However, long-term productivity gains and security exceed costs. More general societal ramifications encompass matters such as privacy and inequality. Passkeys could exacerbate digital disparities by disadvantageously affecting groups lacking regular access to devices. Nevertheless, backup modes like SMS passkeys are useful. Eliminating password exchange with providers may improve user privacy. However, since businesses are also using other data sources to profile their clients, the problems associated with surveillance capitalism still exist. Passkeys don't completely address underlying issues with the business model. Governments must decide what regulations are acceptable for the passkey lifetime, backup, recovery, and access by law enforcement. Decisions made regarding policy have a broad effect on human rights and adoption. In conclusion, passkeys change authentication. They have advantages, but they also bring up difficult questions related to oversight, economics, and inclusivity. To optimize benefits from the passwordless future, a comprehensive examination that goes beyond the technological shift alone is necessary.

5.4 Discussions Around User Education and Shifting Cultural Norms

Transitioning from passwords to passkeys requires more than just technical implementation. Providers also need to focus on user education and shifting entrenched cultural attitudes tied to passwords. Smooth adoption depends on changing user mental models around credential management. One challenge is many users have preconceived negative perceptions of biometric systems due to past experiences or

privacy concerns. But modern passkeys keep biometric data localized on personal devices unlike central databases. Clarifying these technical safeguards and focusing on convenience benefits is key. Making enrollment intuitive is critical as users configure passkeys across devices and accounts. Guidance needs to communicate it as an upgrade over passwords rather than a disruption. Onboarding tutorials should frame biometrics as making passkeys seamlessly easy versus imposing unfamiliar technology.

Explaining the fundamental security benefits is also important for building user trust. Users need to understand passkeys mitigate common threats like phishing, data breaches, and password reuse that enable most account takeovers. Security education must extend beyond early adopters. But communication should emphasize enhanced ease of use just as much as improved security. Users are unlikely to embrace passkeys solely for abstract protection against unlikely threats. Real personal utility needs showcasing. Retraining users on updating existing recovery options will also be necessary. Reliance solely on passkey devices means alternate account recovery mechanisms take on greater importance if device access is lost. More broadly, providers need to help users unlearn years of accumulated password behaviors and assumptions. Cultural attitudes like sharing passwords or using simple passwords die hard. Rethinking access habits around passkeys will take time and repetition. Ultimately the goal is making passkeys invisible in use — where convenience, utility and security blend together. Users shouldn't have to think about passkeys in daily life any more than passwords. Frictionless experiences drive adoption. Succeeding with passkeys requires acknowledging the human factors at play, not just deploying technology. Well-planned user education and guidance focused on shifting entrenched mental models smooths the transition and unlocks full benefits.

6. CONCLUSION

6.1 Summary of Key Findings on Passkeys and Their Viability

Passkeys represent a promising new approach to authentication that aims to solve many of the security flaws inherent with passwords. Leveraging public key cryptography and device-bound credentials, passkeys offer a more secure and convenient user experience in many contexts. However, questions remain around overcoming adoption obstacles. A core benefit of passkeys is greatly enhanced resistance to data breaches, phishing, and common attacks that plague passwords. Private keys never leave devices, so there are no databases of shared secrets to steal, crack, or reuse across accounts. This massively raises the barrier for identity fraud through stolen credentials.

Additionally, passkeys improve usability by removing the need for password generation, memorization, and management. Users seamlessly authenticate through biometrics on personal devices they already own. This is faster and avoids the frustration of forgotten passwords. However, passkey convenience depends on secure roaming across devices. Users expect to access accounts from multiple devices and platforms. Platform vendors are making progress on cross-device syncing but need continued improvement for transparent portability. Widespread adoption also faces headwinds from entrenched password infrastructure and habits. Enterprises must upgrade systems and retrain users to switch authentication fully to passkeys. This represents significant cost and effort while passwords remain “good enough” for many.

Consumer perceptions that passkeys are less usable or secure compared to familiar passwords also hinder adoption absent better education. Passkeys involve some genuine tradeoffs around device dependencies that require user adaptation. While passkey limitations exist, their security and convenience benefits may steadily win converts if technology and design challenges continue improving. But universal adoption requires a concerted shift across industries and major platforms to reach critical mass. The

passwordless future remains aspirational pending further real-world validation. In conclusion, passkeys hold disruptive potential to fundamentally enhance online authentication if key obstacles around portability, backward compatibility, and user familiarity can be overcome. But a future where passwords fade into history will take time, investment, and continued innovation across security, usability, and inclusive accessibility for all users. Delivering on that promise remains a work in progress.

6.2 Recommendations for Future Research and Real-world Implementation

Although passkeys exhibit great promise as a passwordless authentication method, more investigation and careful use in the real world are necessary to fully realize their potential. Security analysis, usability research, standardization, and accessibility assessments ought to be primary areas of concentration. To ensure that passkey protocols and implementations are resilient against new attack vectors, extensive security testing is required. Hackers will look for inventive ways to get around or manipulate passkeys, which should be expected and prevented, as adoption grows. Red teaming continues to bolster defenses. Studies on consumer usability are also essential for informing intuitive design and user education strategies. User interactions need to be consistent across a range of demographics. Enrollment, recovery flows, and other touchpoints will be improved based on input from focus groups and field testing. To promote integration and interoperability, open standards centered around passkeys must be stabilized. Unified technical criteria are necessary for widespread adoption in order for a single passkey to function across systems and browsers. Creating best practices facilitates implementation consistency.

It will be crucial to comprehend the particular accessibility challenges that passkeys present, particularly with regard to dependence on biometrics. It should be a top priority to guarantee inclusive authentication alternatives for groups such as the visually impaired or users with limb differences. Important practical deployment knowledge is gained by piloting passkeys for sizable consumer and enterprise apps. Prior to a widespread rollout, there are possibilities to test setups with friendly users in low-risk scenarios. Feedback from small groups prepares the ground for a larger launch. As use grows, policymakers must also evaluate suitable rules on passkey lifecycle management, procedures for lawful access, and requirements for consumer education. Benefits are maximized when technology and policy are in line. In the end, passkeys are still an evolving technology that require further improvement in the areas of inclusive design for all use cases, clear user experiences, and security assurance. However, the road to achieving a password-free future will be paved with methodical study and controlled rollout.

6.3 Concluding Thoughts on the Outlook for a Passwordless Future

The transition from passwords to passkeys represents a monumental shift in authentication systems. Passwords persist out of entrenched legacy usage despite well-known flaws. Passkeys offer a viable path to finally displace passwords by addressing core security and usability weaknesses. However, major obstacles remain on the road to a truly passwordless future. Passkeys provide a compelling technology foundation through public key cryptography tightly bound to users' devices. This elegantly eliminates many of the vulnerabilities that make passwords inherently insecure yet pervasive. Passkeys also aim to deliver convenience and accessibility exceeding passwords. But technology capability alone is not sufficient. Moving beyond passwords requires overcoming decades of accumulated technical debt, engrained user habits, fragmented standards, and uneven platform support. The inertia of the status quo should not be underestimated.

Smoothly transitioning the entire online ecosystem will take time, coordination, and continued innovation. Usage divides between early adopters and laggards need bridging through education and seamless onboarding. Legacy compatibility and inclusive accessibility require ongoing focus. Consumer skepticism and enterprise reluctance to overhaul entrenched systems pose additional hurdles. Comprehensive adoption of passkeys may emerge gradually over years, not overnight. Hybrid authentication models will likely persist during the transition. Yet promising momentum continues building across industry and government. The technical underpinnings and user experience of passkeys keep maturing. Major platforms are steadily implementing support in OSes and browsers to reach critical mass. In time, generational shifts in attitudes and expectations around passwords may further catalyze change. Younger users embracing passkeys as the norm could displace antiquated password notions. Technology diffusion often benefits from demographics. While barriers persist, the passwordless future heralded by passkeys appears increasingly within reach. Passwords may never disappear entirely, but could realistically fade into minority legacy use. The next generation may know passkeys as the default, not passwords. That future outlook should motivate and guide current implementation efforts.

REFERENCES

[1] P. (2023, November 7). Support for passkeys in Windows - Windows Security. Support for Passkeys in Windows - Windows Security | Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/identity-protection/passkeys/

[2] Wash, R., & Rader, E. (2021, January 1). Prioritizing security over usability: Strategies for how people choose passwords. OUP Academic. https://doi.org/10.1093/cybsec/tyab012

[3] Shaji George, D. A. Securing the Future of Finance: How AI, Blockchain, and Machine Learning Safeguard Emerging Neobank Technology Against Evolving Cyber Threats | Partners Universal Innovative Research Publication. Securing the Future of Finance: How AI, Blockchain, and Machine Learning Safeguard Emerging Neobank Technology Against Evolving Cyber Threats | Partners Universal Innovative Research Publication. https://doi.org/10.5281/zenodo.10001735

[4] Hyder, M. A., & Razzak, J. (2020, November 24). Telemedicine in the United States: An Introduction for Students and Residents. PubMed Central (PMC). https://doi.org/10.2196/20839

[5] Goodin, D. (2023, May 8). Google passkeys are a no-brainer. You've turned them on, right? Ars Technica. https://arstechnica.com/information-technology/2023/05/passwordless-google-accounts-are-easier-and-more-secure-than-passwords-heres-why/

[6] Cormac Herley, Paul C van Oorschot, Frank Stajano, J. B. (n.d.). Passwords and the Evolution of Imperfect Authentication. Passwords and the Evolution of Imperfect Authentication | July 2015 | Communications of the ACM. https://cacm.acm.org/magazines/2015/7/188731-passwords-and-the-evolution-of-imperfect-authentication/fulltext

[7] Shaji George, D. A., & Hovan George, A. S. (2023, December 11). The Emergence of Cybersecurity Medicine: Protecting Implanted Devices from Cyber Threats | Partners Universal Innovative Research Publication. The Emergence of Cybersecurity Medicine: Protecting Implanted Devices From Cyber Threats | Partners Universal Innovative Research Publication. https://doi.org/10.5281/zenodo.10206563

[8] Login and authentication in 2023 explained - PassKeys, TOTP, FaceID. (n.d.). Login and Authentication in 2023 Explained - PassKeys, TOTP, FaceID. https://www.ory.sh/overview-login-password-passkey-webauthn-totp-sso-faceid/

[9] Passwordless Authentication: The Future of Login Security? - Computer Repairs. (2024, February 23). Computer Repairs. https://itfix.org.uk/passwordless-authentication-the-future-of-login-security/

[10] What is WebAuthn API? A definition from WhatIs.com. (2023, February 1). Security. https://www.techtarget.com/searchsecurity/definition/WebAuthn-API

[11] Using WebAuthn to Secure Your Digital Life. (n.d.). Auth0 - Blog. https://auth0.com/blog/using-webauthn-to-secure-your-digital-life/

[12] Passkey Authentication: Passwordless entry into online accounts. (2023, July 17). Passkey Authentication: Passwordless Entry Into Online Accounts. https://www.iplocation.net/passkey-authentication-passwordless-entry-into-online-accounts

[13] Trevino, A. (2023, October 17). Passkey vs Password: What's the Difference? Keeper Security Blog - Cybersecurity News & Product Updates. https://www.keepersecurity.com/blog/2023/10/17/passkey-vs-password-whats-the-difference/
[14] WebAuthn: what it is, and how it works | 1Password. (2022, October 14). 1Password Blog. https://blog.1password.com/what-is-webauthn/
[15] WebAuthn and Passkey 101. (2023, October 25). WebAuthn and Passkey 101. https://blog.logto.io/web-authn-and-passkey-101/
[16] Hedges, B. (2022, April 20). A Dive into the WebAuthn API in Joomla 4. Login to Joomla 4 Securely With Your FIDO2 Key - the Joomla Community Magazine. https://magazine.joomla.org/all-issues/april-2022/a-dive-into-the-webauthn-api-in-joomla-4
[17] Introduction to WebAuthn: What is it? How Does it Work? | Beyond Identity. (2022, August 29). Webauthn: What It Is and How It Works | Beyond Identity. https://www.beyondidentity.com/developers/blog/introduction-webauthn-what-it-how-does-it-work
[18] Guide to Web Authentication. (n.d.). Guide to Web Authentication. https://webauthn.guide
[19] Passkeys: The Bright Future Of Passwordless Authentication - Techviral. (2023, June 28). Techviral. https://techviral.tech/passkeys-passwordless-authentication/
[20] Team, B. K. (2024, January 2). Passkeys vs Security Keys: Which One Offers Better Protection? Passkeys Vs Security Keys: Which One Offers Better Protection? https://blog.bio-key.com/passkeys-vs-security-keys
[21] G. (2023, May 5). Making authentication faster than ever: passkeys vs. passwords. Google Online Security Blog. https://security.googleblog.com/2023/05/making-authentication-faster-than-ever.html
[22] Passkey Authentication: Google's Passwordless Breakthrough. (2023, June 6). Exabytes (Singapore) Official Blog. https://www.exabytes.sg/blog/passwordless-with-passkeys-authentication/
[23] Passkeys 101: the future of passwordless authentication [Q&A]. (2023, November 3). BetaNews. https://betanews.com/2023/11/03/passkeys-101-the-future-of-passwordless-authentication-qa/
[24] How Passkeys Work: The Tech Behind the Passwordless Future. (2023, December 17). AFP.one. https://afp.one/tech/how-passkeys-work-the-tech-behind-the-passwordless-future/
[25] Lawrence, A. (2023, December 1). Passkey vs. password: a new era of secure authentication. Stytch. https://stytch.com/blog/passkey-vs-password/
[26] Breza, T. (2023, November 14). The Possibilities of Passkeys: A Comprehensive Guide to Password-Less Authentication - Operum. Operum. https://operum.tech/blog/the-possibilities-of-passkeys/