iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59504

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

FIDO2 Passkey: The Passwordless Future

Ms. Sumi M[1], Sanmanul Faris A[2]
[1]*Assistant professor,* [2]*MCA Scholar, Department of MCA, Nehru College of Engineering and Research Centre, Pambady, India*

Abstract: ***FIDO2 passkeys represent a transformative step towards a passwordless future. This technology, developed by the FIDO Alliance, offers a user-friendly, secure, and privacy-preserving solution to the problem of password management. By leveraging public key cryptography and biometric or device-based authentication methods, FIDO2 passkeys eliminate the need for traditional, easy-to-forget, and often insecure passwords. The adoption of this technology could significantly enhance online security, reduce instances of identity theft, and streamline the user experience across various digital platforms***
Index Terms: Authentication ,Brute force attack, FIDO2 Passkey, Passwordless Authentication , Password , Phishing attack, Public key cryptography.

I. INTRODUCTION

Passwords continue to be the most used method of user authentication on the web. Regrettably, even with highly secured online services, phishing and credential stuffing assaults against passwords continue to do significant harm. The security issues with using passwords may only be partially resolved by encouraging the use of password managers and enforcing passwords through the use of risk-based authentication, two-factor authentication, and account security alerts [1]. According to a statistical report, 81% of hacking-related breaches are the result of weak or stolen passwords.

Malicious phishing emails have increased by 156% since Q4 2022, and 54% of consumers have noticed that phishing messages are getting more sophisticated [2].

Passwordless, single-factor authentication on the web is highlighted by the FIDO Alliance's FIDO2 suite of protocols, which builds on previous work to improve multi-factor authentication. a user's authenticator creates a distinct asymmetric cryptographic keypair linked to a certain website. This can be either software operating on an existing device or dedicated hardware, such a YubiKey. The website contains the public key, while the user's authenticator stores the private key. The user uses a biometric or PIN to authenticate locally to their authenticator, which utilizes the private key to authenticate to the remote website, in order to log in. Media attention concentrated on the idea that FIDO2 will "kill the password" at the moment the World Wide Web Consortium (W3C) approved FIDO2 as a web standard in 2019 [3].

Apple, Google, Microsoft, and other companies introduced passkeys, multi-device credentials that adhere to the FIDO2 standard, beginning in 2021. Though they include capabilities like syncing private keys across a user's devices (to prevent having to re-register on each device) or utilizing a single existing device (like a phone) as the authenticator across all devices, passkeys are really just a rebranding of the current FIDO2 technique. Passkeys were once again hailed by the mainstream media as the device that will "kill the password." FIDO2-based passwordless authentication is supported by the majority of popular operating systems and browsers today [3].

Scholars have examined the security and usability of FIDO2, concluding that it is both more secure and more user-friendly than passwords. Working groups led by the FIDO Alliance and W3C are tasked with encouraging the use of FIDO2. It is therefore unexpected that so few businesses have used passwordless authentication, either extensively or at all.

This article discusses the FIDO Alliance's open authentication protocol, which includes FIDO2 passkeys. These are cryptographic login credentials that are kept on the user's device and are intended to offer quick, safe, and password-free authentication. Since each passkey is exclusive to a particular service, security is improved because the compromising of one service does not impact others. Because FIDO2 passkeys employ public key cryptography and the user's device retains the private key at all times, they are immune to phishing attacks. This implies that an attacker cannot use login credentials to authenticate as a user, even if they are misled into entering them on a fraudulent website.

When it comes to usability, FIDO2 passkeys provide a practical way for users to log into websites and applications on many devices. Users can utilize their device's built-in security features, biometrics, or security keys to authenticate themselves instead of remembering and inputting passwords. Because they combine speed, convenience, and increased security, FIDO2 passkeys constitute a significant leap in online security.

II. BACKGROUND

A. Authentication

Verifying a user's, process', or device's identity is the process of authentication. Since computers have become more widely used in the previous several decades and we are living in a digital age, authentication has become more crucial to protecting networks, data, programs, and accounts. Authorization, on the other hand, establishes rights and permissions to access certain data and runs programs, confirming that an organization possesses the required authorizations. Authentication of users is required to guarantee that only authorized users may access particular files or accounts. Authentication serves as a means for users to get access to their accounts, download certain files, and alter programs they are authorized to use [4].

B. Traditional Method of Authentication

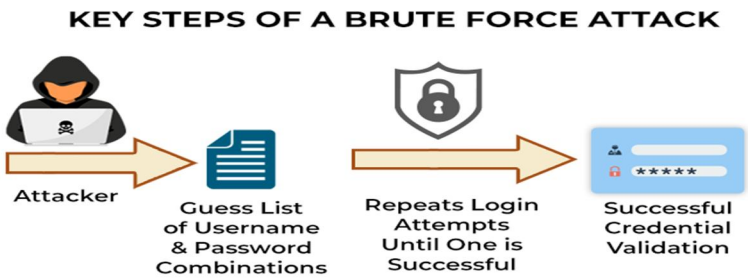
The most common and conventional method of authentication is passwords . When it comes to knowledge-based authentication, passwords are used, and the knowledge element is a secret that only the user is aware of. Put otherwise, a password is a personal secret consisting of a sequence of characters that are chosen at random and satisfy predetermined standards. There are advantages to password-based authentication as well as drawbacks. Because all that is needed to authenticate is memorizing the password, it is simple and easy to use on the one hand, but data indicate that users are worried about this authentication factor because of memorability issues Additionally, as more and more individuals use internet services, the number of passwords they have increases [4].

C. Threats of Passwordbased Authentication

Authentication systems are vulnerable to many known risks and vulnerabilities associated with passwords. This section will cover popular password-based authentication-related attacks and malware, including dictionary, phishing, and brute-force assaults, in addition to keylogger malware.

D. Brute-Force Attack

Since passwords are a commonly used authentication standard, there has been much study on password cracking as a means of obtaining sensitive and private data. A brute-force assault is one method of password cracking. In order to identify a combination that matches the password, the attacker attempts every conceivable combination of letters, numbers, and special characters in this assault. A weak password may be quickly and readily broken by employing a brute force assault[4].



E. Phishing Attacks

Phishing is a type of social engineering assault in which a hacker sends phony emails to victims in an attempt to trick them into divulging personal information or unintentionally infecting their machines with malware .These emails are skillfully crafted to mimic reputable companies and brands, giving victims the impression that they are authentic and motivating them to click on a link. Typically, a hacker seeks to take credit card numbers and other sensitive data, including personal identities. Phishing, as opposed to direct computer system attacks, focuses on the human component of the system [4] .

F. Keylogger

Malware that tracks and logs a user's keystrokes is called a keylogger. The hacker can record every keystroke once the virus has been placed on the victim's machine, possibly after clicking on a malicious link. Sensitive data including credit card numbers, passwords, and private communications may be included in this. Although keystroke tracking is still its main function, contemporary keyloggers also offer the ability to copy, paste, and cut data [4].

G. Passwordless Authentication

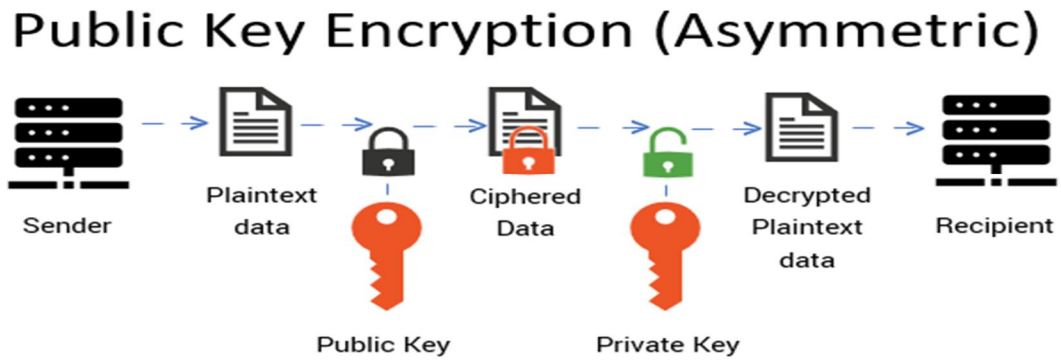
There is a trend toward a paradigm change from password-based authentication to passwordless authentication as technology advances. Passwordless authentication has several meanings. characterizes the process of authenticating a user without the need for a password or other knowledge-based secrets as password less authentication. As an illustration, consider email-based magic link authentication. OTP by email or SMS, biometric verification, authenticator apps, etc.

Password-based authentication is inferior than password-less authentication from a security standpoint. When using passwordless authentication, common password issues like reuse, sharing, and credential hacking are not as big of a concern. However, as there are several distinct passwordless authentication techniques, it is challenging to make generalizations regarding passwordless security since they vary depending on the technique. We will study the FIDO2 passkey in this paper. Fast Identity Online 2, or FIDO2, is an open set of standards created by the FIDO Alliance to improve the security of online authentication. With FIDO2, more secure and convenient techniques are intended to take the place of conventional passwords. Based on FIDO standards, passkeys take the role of passwords. Users accept the sign-in using the same biometric (such as their fingerprint or face) or PIN that they use to unlock their device when they log into an app or website. Users don't need to re-enroll in order to access their credentials on many devices thanks to the deployment ,

H. Public-key Cryptography

A pair of keys is used in public key cryptography, an asymmetric system, to encrypt data: a public key for encryption and a matching private key, also known as a secret key, for decryption. The user has the option to keep their private key private while making their public key public. The private key cannot be determined from the public key computationally. Information can only be encrypted and not decrypted by someone with access to a public key. The information cannot be decrypted by anybody other than the owner of the matching private key.

The main advantage of public key cryptography is that it makes safe message exchange possible even for those without any prior security arrangements. No private key is ever sent or exchanged, hence there is no longer a requirement for sender and recipient to exchange secret keys over a secure channel for any kind of communication. The technological innovation that makes robust cryptography accessible to the majority of adult users is public-key encryption [4].



III. LITERATURE SURVEY

In the realm of cybersecurity and authentication technologies, the emergence of FIDO2 represents a significant step towards a passwordless future. As I delve into the literature survey on the topic of "FIDO2: The Passwordless Future," it becomes evident that this innovative protocol holds great promise in revolutionizing how users securely access their digital accounts.

[1]G Eleftherios discussed in the paper "FIDO2 Overview, Use Cases, and Security Considerations" provides an in-depth explanation of the FIDO2 authentication mechanism. It discusses why this new mechanism is necessary, how it surpasses other authentication methods, and how it operates. The paper also presents several use cases and delves into the security considerations associated with FIDO2. The goal is to provide a comprehensive understanding of FIDO2, its advantages, and its potential security implications.

[3]Leona Lassak, Elleen Pan, Blase Ur, Maximilian Golla discussed in the Paper "WhyAren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication (Extended Version)" which explain about analysis and evaluation the potential of FIDO2 standard, which aims to diminish the dependence on passwords by advocating for passwordless authentication through public-key cryptography. It outlines obstacles hindering FIDO adoption, such as financial constraints, communication difficulties, and user experience issues. While CISOs and experts recognize the promise of FIDO, they point out sluggish adoption rates and unresolved challenges. Management perspectives on FIDO deployment vary, with concerns ranging from costs to communication barriers.

[4]The research "From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication" investigates the barriers to the widespread adoption of FIDO2, a passwordless authentication standard. Despite FIDO2 being more secure and user-friendly than traditional password-based methods, its adoption has been slow. The study identifies the lack of knowledge about passwordless authentication alternatives as the main obstacle. It also reveals that while all participants were willing to switch to passwordless authentication, they expressed concerns about the manual change in security settings and hoped for a more seamless transition.

[5]Dr.A.shaji George discussed in the paper "The Dawn of passkey: Evaluating Passwordless Future" , the author analyze and evaluate the potential of FIDO2 passkeys as a means of improving security and usability in authentication systems. The paper likely discusses the technical details of how passkeys work, their advantages over traditional passwords, and any potential drawbacks or limitations.

[6]Jonathan Luckett,discussed in the article "Phishing Resistant Systems: A Literature Review" published in the Journal of Computing Sciences in Colleges, provides an extensive review of systems designed to resist phishing attacks. The author discusses various solutions, including Microsoft enterprise solutions, the Web Authentication API, FIDO 2 standards, email authentication protocols, and browser-based detection systems. The paper also delves into the tactics used by threat actors to execute phishing schemes. Despite the existence of several promising phishing-resistant systems, the author concludes that no single product offers complete protection against phishing attacks.

[7]Sibi Chakkaravarthy Sethuraman, Aditya Mitra, Anisha Ghosh, Gautam Galada, Anitha Subramanian discussed in the Paper "MetaSecure: A Passwordless Authentication for the Metaverse" ,which explain the importance of security keys in authentication processes, highlighting their ability to generate RSA key pairs securely. It explains the workflow of FIDO authentication using security keys for user verification. The paper also delves into the concept of the Metaverse, emphasizing its role in virtual reality platforms for communication and digital asset protection. It introduces the Metasecure system as a novel multifactor authentication method for the Metaverse, incorporating physical security keys, device attestation, and facial recognition for enhanced security. The paper underscores the significance of biometric security, the challenges of presentation attack detection, and the need for robust authentication systems in the digital realm

[8] Martiño Rivera-Dourado, Marcos Gestal, Alejandro Pazos, and Jose Vázquez-Naya discussed in the research paper "A Novel Protocol Using Captive Portals for FIDO2 Network Authentication" introduces a new protocol named FIDO2CAP (FIDO2 Captive-portal Authentication Protocol). This protocol is designed for captive-portal network authentication using FIDO2 authenticators, such as security keys and passkeys.FIDO2 authentication is being applied in numerous web authentication services to replace passwords and their known vulnerabilities. However, this new authentication method has not yet been integrated with network authentication systems.To validate their proposal, the authors developed a prototype of FIDO2CAP authentication in a mock scenario. They performed a usability experiment with 15 real users.This work represents the first systematic approach for adapting network authentication to the new authentication paradigm relying on FIDO2 authentication.

[10] Liz Corbett discussed in the book "The 2023 Workforce Authentication Report: Embracing the Passwordless Future" which explain FIDO2 passkeys represent a promising step toward a passwordless future. Leveraging cryptographic credentials, these passkeys enhance security while simplifying user interactions. However, practical challenges—such as technical obstacles and regulatory requirements—persist. Major tech companies are committed to passwordless solutions, but a hybrid approach that combines passwordless methods with existing password-based systems may be more realistic. Researchers and practitioners should continue exploring this dynamic field to address challenges and unlock a more secure and user-friendly authentication landscape

[11]Kemal Bicakci and Yusuf Uzunay discussed in the "Is FIDO2 Passwordless Authentication a Hype or for Real?" The authors provides insights into the future of passwordless authentication using FIDO2 passkeys. While there is excitement around passwordless methods, the authors argue that completely eliminating passwords from the web remains challenging. They highlight technical obstacles, user behavior patterns, the need for account recovery options, regulatory requirements, and the necessity of a security culture. Despite these challenges, FIDO2 passkeys offer advantages such as enhanced security and resistance to attacks. The paper encourages a hybrid approach that combines passwordless methods with existing password-based systems. Overall, it contributes valuable perspectives for researchers and practitioners in the field of authentication mechanisms.

IV. METHODOLOGY

A. *Passkey Technology*

One emerging technology that seems promising is passkeys. Passkeys offer password-free authentication while prioritizing enhanced security, confidentiality, and ease of use. They do this by using public key cryptography and device-bound credentials. Passkeys eliminate the need to transmit and retain plaintext passwords by combining device cryptography, biometrics, and public key cryptography to provide greater threat protection. In locations where passwords commonly fail, the technique aims to greatly enhance security and user experience.However, passkeys are not a panacea. User inertia and well established password behaviors make it difficult to encourage adoption. Further advancements are also required in the domains of portability, accessibility, and passkey recovery. Any possible over-reliance on devices as a single point of failure needs to be mitigated. Further research is necessary to determine how effective passkeys are in the real world against malware and social engineering assaults.

B. *Passkey Technology vs Password technology*

The goal of the innovative passkey authentication technique is to eliminate the necessity for passwords [5][6]. The usage of public key cryptography distinguishes passkeys from shared secrets fundamentally. You may take use of enhanced security features and circumvent the inherent shortcomings of conventional password-based authentication by doing this. Users can create a secret string or passphrase that unlocks their account by utilizing passwords. The password must be provided to the server in plaintext each time you log in. The hashed password is saved for further verification by the system once it has been hashed. Still, weak passwords are still being used in server databases and during transmission. Every time you log in, the same duplicate of them is sent out, making them static.

As long as they have the password, attackers can gain unfettered access through phishing, leaks, or hacking. Passwords must also follow intricate rules and be reset frequently in order to lower risks, which is detrimental to their usage [6]. Conversely, passkeys don't even rely on mutually understood secret passwords. They make use of cryptographically generated keys linked to certain places and gadgets. When an account is created, the device generates a public and private key pair using the WebAuthn API. The device keeps the private key securely stored. After receiving the public key, the server links it to the user's account. After logging in again, the client uses the private key to sign a challenge nonce with the server and sends back the signed document.This signed answer contains the passkey. The server can verify the passkey's authenticity using the public key that has been saved. Crucially, though, the private key is always accessible on the user's device. There's no set password that you may steal or use on other websites. Phishing is pointless because there isn't a true password to steal [5][7].

Additionally, passkeys increase security by linking credentials to specific devices using on-device biometric verifications like fingerprint or face recognition. Users have to authenticate to the device before they may use the passkey. By doing this, you can increase security beyond what can be achieved with simple password entering [4]. Passkeys are also impervious to replay assaults. The passkey changes dynamically with each login as it is a signature of a randomly generated challenge nonce. It is not possible to replay static credentials between sessions. Cryptography makes sure that only the device with the corresponding private key could have created the legitimate login passkey [5]. By eliminating the requirement for plaintext password transmission and storage, passkeys get around most common password cracking techniques. Private keys are kept apart on user devices with hardware-backed security measures. It is not feasible to target a central password database. When passkeys are session specific, brute force is not helpful. In conclusion, security features provided by passkey technology are fundamentally better than those of password-based authentication. Passkeys solve a lot of the problems related to employing static password secrets in different circumstances. To improve end-user security without compromising usability, biometric binding, hardware-secured private keys, and cryptographically signed answers all function effectively. With their growing use, passkeys are well-positioned to usher in a new age of passwordless authentication.

C. Public key Cryptography in Passkey

Passkeys provide passwordless authentication through the use of public-key cryptography. This is not the same as conventional password authentication, which is reliant on shared secret keys. By using key pairings that comprise a public key and a private key, public-key cryptography improves security. The user provides their password text, which serves as a shared secret key, in order to enable password authentication. During each login session, the same static password is used for authentication. To authenticate each time, the system hashes the password and compares it to the hash that is saved. However, because the secret is constantly communicated and kept, this paradigm leaves passwords open to interception or leakage[6].

This problem is resolved by public-key cryptography, which uses asymmetric key pairs rather than shared secrets. The client device uses the WebAuthn API to create a distinct public/private key pair during passkey registration. While the public key is transferred and stored on the server, the private key is kept safe on the client device. Never let the private key escape the device. The server sends the client a challenge nonce for login. Next, using their private key, the client signs this nonce locally and returns the signature to the server. The passkey, a transient credential specific to that session, is this signature. By comparing the signature to the public key it has on file for that user account, the server verifies the passkey. Without disclosing the private key itself, this demonstrates that the passkey came from the same device that was carrying the corresponding private key. Hardware security mechanisms such as Trusted Platform Modules (TPM) and Secure Enclaves are leveraged by the private keys used in passkey creation. For security purposes, this separates them from other processes and operating systems. When not actively signing authentication challenges, private keys are encrypted. A second factor is provided by biometric verifications such as fingerprint or facial recognition, which need user prior to the private key being used for any kind of signature. The authorized user and the hardware are linked to the keys. A legitimate signature that verifies against the public key record can only be generated with the private key. The public keys themselves may be safely kept on servers or in databases and do not need to be kept a secret. There is never a clear storage or transmission of a shared password. Because the keys are asymmetric, passkeys are also immune to man-in-the-middle and phishing assaults. The public key cannot be used to generate or reconstruct the private key. Without the corresponding private key, intercepting the public key or signatures is inadequate for authentication[5][7].

By utilizing strong public key cryptography, which is already widely used in fields like TLS certificates and end-to-end encrypted transmission, passkeys improve security. Unlike typical password techniques, passkeys used to authentication allow passwordless login without ever disclosing or transferring the secret signature key. By using public/private key validation, each login challenge response is distinct and cryptographically provable.

D. Technical Implementation of Passkey

Passkeys readily connect into a variety of apps and websites by utilizing industry-standard cryptographic protocols and API specifications. These essential elements include the FIDO standards and the Web Authentication API (WebAuthn), which enable passwordless authentication. A browser-based interface for controlling public key credentials linked to passkeys is made possible by the WebAuthn component. The novel "create()" method safely stores the private key on the client's device and creates a distinct public/private key pair upon registration. After that, the matching public key is sent to the server. Users can utilize WebAuthn's "get()" method to verify signatures for authentication reasons. This function generates a secure passkey signature that is sent back to verify authenticity by using the user's private keys and personalized challenge nonce.

This simplified procedure removes from the developers' obligations any intricate cryptography processing or storage issues. Furthermore, FIDO protocols that are specifically created to improve web-based user validation procedures through additional standardization efforts are built upon these advancements. Specifically, servers themselves use their Relying Party feature as a crucial way to validate requests for both registration and authentication, which are made possible by specialized clients known as "FIDO Authenticators."

Basically, during the registration phase, this proprietary model makes use of extensive data parameters provided by the Receiving Parties to generate unique challenges, such as matching metadata arrays that are linked to the creation of appropriate Public/Private Key pairs. These challenges are made possible by advanced response objects, which accompany us in creating customized User IDs and Credentials that are neatly embedded inside said forms. Finally, Server Validation is able to check off the appropriate boxes for complete online enrollment.The second phase is creating extremely detailed instructions about three crucial elements that are included here, making our ground-breaking method much more alluring than before. 1. First thing on the list? Sign up! Now, everyone can just kick back and unwind, as we have you fully and utterly covered. No matter what occurs, it will always be evident! 2. The difficult part is about to begin. Authentication involves creating personalized requests for the appropriate nonces and then improving them even more to offer fully satisfactory verification services during the whole process. This includes perfectly matching Public Keys and Parameters and confirming the legitimacy of the user's identity overall. This process is not only incredibly convenient, but it also offers unmatched security levels! 3. In an effort to further enhance things, we've gone above and beyond with our amazing FIDO-certified solutions, which enable websites and applications to offer easier-than-ever integration possibilities without requiring additional work from you guys. This implies that you can always rely on WebAuthn API to be available for you, no matter when your business needs us most! WebAuth Api s is responsible for key element management and lower level cryptography. Passwordless and second factor authentication are the two main FIDO authentication techniques. In contrast, the former use passkeys as the only credential and does not require a backup password, while the latter requires both password and passkey verification for an additional layer of security. Prominent entities like Apple, Google, and Microsoft have initiated the integration of passkey functionality natively into their client-side hardware and operating systems. This will make it possible for passkeys to be used seamlessly across FIDO-compliant apps and websites. Furthermore, WebAuthn removes the need for any plugins or proprietary apps. When it comes to deployment, it could be essential to integrate with current account systems in order to provide registration procedures that adhere to FIDO protocols. Additionally, in order to validate replies from WebAuthn requests during login processes, Relying Party servers need to be set up properly. Identity providers can be crucial in accelerating the wider use of FIDO technology by providing pre-made solutions. Overall, the reliance on technical details regarding pass key adoption has decreased over time thanks to standardized protocols like WebAuthn and advancements within to provide essential specifications enabling universal functionality among browser-based platforms alongside native mobile applications. This suggests a future where passwords may be eliminated in favor of passkey services provided by platform-specific support[5][7][9][10][11].

E. Advantage of Passkey

By preventing the transmission of plaintext passwords and centralised repositories that reveal credentials to personnel and systems, passkeys enhance user privacy. Passkeys restrict visibility on personal devices by isolating private authentication factors. When using standard passwords, every time you log in, the same secrets are sent over the network and kept on business databases. Sensitive credentials are therefore made available to insiders via the backend storage and to any interceptors during transmission. Viewing passwords in databases is a common access permission for staff members and IT administrators. For commercial purposes, some companies could even demand access to employee passwords. Because of this, user privacy must be sacrificed in order to balance staff efficiency and security. By limiting their interactions with public keys to the server-side, passkeys reduce this risk.

Private keys are kept separate from business infrastructure on individual devices. The password is no longer in plaintext and cannot be leaked during the procedure. In order to access accounts without the corresponding private keys being in the user's hands, the public keys have no inherent value. Only information that was previously meant to be public is revealed by server breaches and network intercepts; secrets are kept hidden. The main concern for many threat models is having access to passwords. However, passkeys prevent the servers and network from ever being able to access those secrets. Stronger guarantees regarding user privacy throughout the authentication procedure are therefore given. Passkeys also improve privacy by completely eliminating centralized password databases. Passwords allow personal information to be compiled in company-controlled files, frequently with unrestricted There aren't many ways to refuse permission for password storage and collecting. However, users still own the authentication secrets stored on their devices when they utilize passkeys. Businesses never need access to their systems or accumulate personal passkeys. This protects confidentiality and avoids unauthorized personnel access to credentials. In the end, passkeys provide users authority over the elements required for account authentication. Businesses need to be able to rely on the authentication process's results without having to record or store the raw secrets. This moral change is consistent with growing privacy demands that reduce the amount of data collected. In conclusion, passkeys provide better privacy than conventional password approaches, which by communication and centralized storage invariably expose private information to servers, networks, and employees. On personal devices, passkeys preserve privacy by putting authentication factors at the hands of the user. Given that users and authorities are scrutinizing data processing, access restrictions, and permission more and more, this is a significant benefit.Passkeys offer notably greater security than passwords against phishing, data breaches, and other threats. By eliminating static passwords, passkeys are intended to get around a number of the attack vectors that make passwords fundamentally weak. First of all, passkeys completely exclude the possibility of phishing—the stealing of user credentials via bogus login websites. When employing passkeys, there isn't a true password to input or remember. Even if users are tricked into entering credentials on phishing websites, the only information that is disclosed is the public keys, which are worthless to attackers. Phishing obtains login credentials by impersonating someone in order to get passwords and account usernames. Passkeys essentially stop this at the source because only the user's device can generate a valid login signature using the private key. Since phishing sites don't have access to the secret key, gathering credentials is meaningless. This protection to phishing also confers resilience against human-operated social engineering attempts. Users cannot unintentionally reveal passkeys to fraudulent calls or emails asking credentials. If consumers do not own the private keys on their personal devices, there are no secrets to reveal. Passkeys also lessen the risk of password database invasions.

Business servers save conventional passwords in both unencrypted and reversibly encrypted formats. Attackers can get all the credentials needed to take over an account by breaking into these databases. When passkeys are used, there is no central password database. The secret keys are stored separately on user devices, while only the public keys are retained on business servers. In the event that matching private keys are not present, the security impact of a public key compromise is minimal. Passkeys also effectively resist attempts to crack passwords offline. Attackers can apply brute force cracking techniques to hashed passwords retrieved from password databases that have been compromised by utilizing GPU-powered tools. Account passwords can be retrieved via breaking.On the other hand, passkeys lack static credentials that may be found and used maliciously. Devices never lose their private keys; they are always kept secure. Passkey signatures are one-time, session-specific values. It is impossible for crackers to target reused passwords.

Furthermore, this advantage offers resilience against any internal attacks. Insider access to password databases may provide credentials to malicious actors. Accessing public passkey databases, however, does not provide authentication of any type. All things considered, because passkeys eliminate shared secrets, isolate keys on devices, and employ transitory session-based credentials, they are compliant with modern zero-trust frameworks. This decentralized approach is considerably less susceptible to a single point of failure than centrally stored static passwords. Passkeys prevent account takeovers through insider assaults, cracking, phishing, and database hacking. This raises the bar for organizations in terms of security dramatically.

F. Limitation of Passkey

Although passkeys circumvent several password flaws, their existing restrictions regarding features such as device mobility may impede their widespread implementation. Unlike passwords, which are easier to transmit between devices, passkeys rely on device-specific key pairs. For users used to the ease of passwords, this disparity causes friction. The ability to log in from any device that accepts a password is a fundamental benefit of passwords. All PCs, mobile devices, browsers, and applications share the same credentials. Accounts are easily accessible to users from Any location.however, the initial enrollment device—where the key pair is generated—is cryptographically tied to passkeys. The hardware of that device continues to hold the private key locally.

To use passkeys on new devices, each account must be re-registered and re-verified. Users who often transfer between platforms or devices may find this challenging. When re-enrolling passkeys, there is far more friction than when a password is tapped in. Users that use applications on different mobile devices find it difficult to maintain passkey synchronization.

Platforms like as Google and Apple are aiming for cross-device compatibility, synchronization, and secure passkey backup. However, these approaches are currently unpopular and add complexity. Fully realized transparent password-like portability is still a work in progress. Additionally, because passkeys are local, they cannot be accessed from shared or public devices, such as computers in libraries. On untrusted workstations, users have no mechanism to safely enter passkeys. Here, passwords are still more practical. In order to log in, passkey users also need to keep their initial enrolling device accessible. Account access can be permanently blocked by lost or broken devices, expired credentials on unused devices, or forgotten device passcodes. Users run the danger of being permanently locked out if backup plans aren't in place. The intrinsic device-centricity of passkeys now limits flexibility and creates additional hurdles in relation to the widespread ease of passwords, even though technical solutions to these problems are evolving. To get around this restriction, both users and providers will need to modify their authentication presumptions and practices. One of the biggest challenges for passkeys to provide password similar flexibility is still getting beyond portability constraints. Compared to device-agnostic passwords, users are unlikely to accept platform-restricted authentication. for passkey viability, seamless cross platform synchronization, backup and recovery are essential.

V. RESULT AND DISCUSSION

The Fast Identity Online (FIDO2) protocol is a significant advancement in the realm of digital security. It is a product of the combined efforts of the FIDO Alliance and the World Wide Web Consortium (W3C). The protocol leverages the physical devices of users to store credential information locally on secured hardware, which is then used to sign authentication challenges. This approach to authentication is a marked departure from traditional password-based systems, paving the way for a passwordless future. The FIDO2 protocol enables passwordless authentication by using passkeys as the primary factor for account authentication. This means that instead of relying on passwords, which can be easily forgotten or stolen, users can authenticate their accounts using physical devices such as security keys, smartphones, or biometric devices. This not only enhances the security of the authentication process but also improves the user experience by eliminating the need to remember complex passwords.

The move towards a passwordless future has been further bolstered by the support of tech giants like Apple, Google, and Microsoft. Their joint announcement to support passwordless authentication is a clear statement that FIDO2 is the preferred path towards a passwordless future. This support from major technology companies is likely to accelerate the adoption of FIDO2 and passwordless authentication.

FIDO2 passkeys offer several benefits. They remove the most common barriers to FIDO adoption by enabling users to enroll to FIDO once, sharing the credential between devices on the same platform, and being able to leverage registered FIDO devices on one platform to authenticate when logging in from another. This makes the authentication process more seamless and user-friendly. Despite its advantages, the transition to FIDO2 and a passwordless future has not been without challenges. One of the initial setbacks was the need to use weaker authentication mechanisms like passwords during the initial registration process. However, these challenges are being addressed as the technology evolves and matures.

In conclusion, FIDO2 passkeys present a comprehensive solution for a passwordless future. They offer a highly secure cryptographic login that is phishing resistant and easy to implement. However, the transition to a completely passwordless future will require overcoming certain challenges and widespread adoption of these technologies. The journey towards this future is well underway, and the continued development and adoption of FIDO2 passkeys will play a crucial role in shaping this future.

VI. FUTURE SCOPE

The future of passkeys for authentication is promising, with a shift towards passwordless methods. Passkeys are expected to play a significant role in this transition, offering an improved user experience by providing a consistent and familiar interface across all devices. Users can authenticate themselves using their face, fingerprint, or device PIN, similar to unlocking their devices. In terms of security, passkeys use FIDO Authentication, known for its resilience against phishing and remote attacks. Each passkey is unique for each service, reducing the risk of reuse. Furthermore, passkeys are always accessible to users, even if their devices are replaced. When synced, they are available across devices. The adoption of passkeys has been increasing. In 2023, the number of sites that could potentially log in using passkeys went from a handful to hundreds, encompassing billions of accounts. Other passwordless authentication methods, such as facial recognition and fingerprint scanning, are also becoming more common. These methods, along with passkeys, are expected to replace traditional passwords.

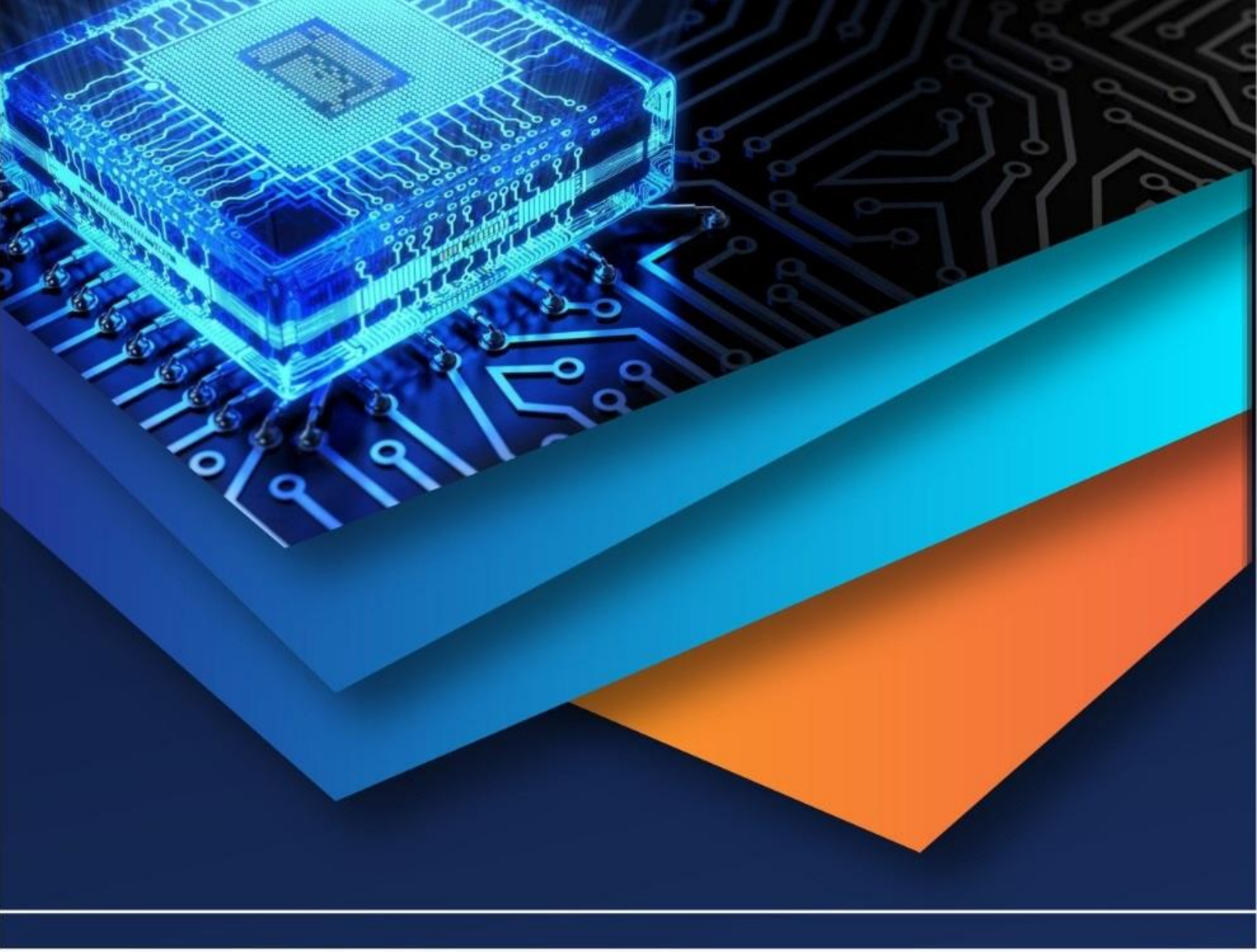
However, the transition to a completely passwordless world may still take some time. Despite the challenges, the future of passkeys for authentication looks bright, with potential for improved user experience, enhanced security, and wide-scale adoption.

VII. CONCLUSION

Passkey authentication represents a paradigm shift away from traditional password-based systems. It introduces a novel approach that combines robust security with user convenience. At the heart of passkey authentication lies a unique key pair. Users possess a private key, securely stored on their device, and a corresponding public key shared with websites. Think of this as a digital vault where your identity is safeguarded by these keys. When a user attempts to log in, the website sends a challenge—essentially a digital puzzle—to the user's device. The private key generates a unique signature, akin to a digital fingerprint, proving the user's identity without revealing the actual key. Even if the website is compromised, the login remains secure. At the heart of passkey authentication lies a unique key pair. Users possess a private key, securely stored on their device, and a corresponding public key shared with websites. Think of this as a digital vault where your identity is safeguarded by these keys. When a user attempts to log in, the website sends a challenge—essentially a digital puzzle—to the user's device. The private key generates a unique signature, akin to a digital fingerprint, proving the user's identity without revealing the actual key. Even if the website is compromised, the login remains secure. Passkeys are highly resistant to phishing attacks. Their use of public-key cryptography and website-specific binding ensures that even if attackers mimic a website, they cannot extract the private key. Unlike passwords stored on servers, passkeys don't require centralized storage. This minimizes the risk of data breaches. Complex cryptographic algorithms make passkeys robust against brute-force attacks. Passkeys eliminate the need to remember and type passwords. Biometric authentication (such as fingerprints or facial recognition) and device PINs provide seamless logins. Passkeys work seamlessly across multiple devices, allowing secure credential synchronization. Major tech companies (Apple, Google, Microsoft) and browser developers (Chrome, Safari, Firefox) endorse passkeys. While passkeys hold immense promise, their adoption is not yet universal. Websites and services must actively support this method for widespread use. In summary, passkey authentication represents a leap forward in online security. Its blend of strong encryption, ease of use, and cross-platform compatibility positions it as a potential replacement for traditional passwords. As technology evolves, passkeys may well become the new standard for authentication

REFERENCES

[1] G Eleftherios(2023) "FIDO2 Overview, Use Cases, and Security Considerations".IN researchgate.net
[2] "FIDO Alliance - Open Authentication Standards More Secure than Passwords." FIDO Alliance, n.d., (https://fidoalliance.org/).
[3] Leona Lassak, Elleen Pan, Blase Ur, Maximilian Golla() "WhyAren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication (Extended Version)" .Published in 33rd USENIX Security Symposium (USENIX Security 24)
[4] Ingunn Langtangen Furuberg and Marie Øseth "From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication" ,IN Norwegian University of Science and Technology
[5] Dr.A.shaji George (2024) "The Dawn of passkey: Evaluating Passwordless Future",IN Partners Universal Innovative Research Publication
[6] Jonathan Luckett,discussed (2023) "Phishing Resistant Systems: A Literature Review" In Consortium for Computing Sciences in Colleges Evansville, IN, United States
[7] Sibi Chakkaravarthy Sethuraman, Aditya Mitra, Anisha Ghosh, Gautam Galada, Anitha Subramanian(2023)" MetaSecure: A Passwordless Authentication for the Metaverse".In eprint arXiv:2301.01770
[8] Martiño Rivera-Dourado, Marcos Gestal, Alejandro Pazos, and Jose Vázquez-Naya ""A Novel Protocol Using Captive Portals for FIDO2 Network Authentication".IN International Federation for Information Processing.
[9] Passkey Developer Resources." *passkeys.dev*, n.d., (https://passkeys.dev/).
[10] Liz Corbett(2023) "The 2023 Workforce Authentication Report: Embracing the Passwordless Future" LastPass in collaboration with the FIDO Alliance
[11] Kemal Bicakci and Yusuf Uzunay(2022)"Is FIDO2 Passwordless Authentication a Hype or for Real?".IN IEEE 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY